Voatz

11/22/21 13:58:57
WV Purchasing Division

State of West Virginia

CRFP-1600-SOS2200000001-1

Submission Date:
2021-11-22

BID RECEIVED LATE

BUYER

WITNESS

DISQUALIFIED

Welch, Toby L <toby.l.welch@wv.gov>

Responding to RFP E-Ballot Delivery Technology

3 messages

Donald DeFord <donald.deford@voatz.com> Thu, Nov 18, 2021 at 12:27 PM
To: TOBYLWELCH <TOBY.L.WELCH@wv.gov>

Toby,

Quick question on delivering our response to this RFP: I understand that using WVOASIS for submission has been prohibited for this RFP. As we are still completing our submission, we will be using the facsimile option. With supporting documentation, this is likely to be a long submission. Does your fax system physically print each page, or do you receive the fax as an electronic document? I just want to be sure that you can receive the entire response (paper and toner issues).

Also for a fax submission, should the separate pricing be sent as a separate fax, or should it simply be a separate section, perhaps with a separator page?

I appreciate your assistance,

Don DeFord

National Sales Manager

Phone: 503-269-7224

Email: donald.deford@voatz.com

Welch, Toby L <toby.l.welch@wv.gov> Thu, Nov 18, 2021 at 2:43 PM
To: Donald DeFord <donald.deford@voatz.com>

Thank you for your interest in this solicitation.

The fax will physically print each page, please keep in mind that all pages must be received by 1:30 p.m. on the day of the opening or your bid will be disqualified. The technical submission should be identified as "technical" with the RFP number and your cost submission should be submitted in a separate fax and identified as "cost" with the RFP number.

A better option may be overnight delivery to the address listed in the Instructions to Vendor Submitting Bids included with the solicitation.

Please let me know if you have any questions.

thanks so much

[Quoted text hidden]

--

--

Toby L. Welch, Buyer

West Virginia Purchasing Division

2019 Washington Street East

Capitol Complex Building 15

Charleston, WV 25305

304-558-8802 ext 57522

Toby.L.Welch@wv.gov

Confidentiality Notice: This e-mail communication and any attachments contain confidential, legally privileged, and/or non-public information and is for the sole use of the intended recipient(s). If you are not an intended recipient, and have received this communication, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution, saving, copying or other use of the communication, any attachments, or their contents is strictly prohibited. If you have received this communication in error, please: (1) notify the sender immediately by replying to this message and (2) immediately delete this communication, any attachments, and the reply to sender from your system without printing, forwarding, or saving any copies.

If you are the intended recipient, please secure the contents in accordance with all applicable state or federal requirements related to the privacy and confidentiality of information, including the HIPAA Privacy guidelines

---

Donald DeFord <donald.deford@voatz.com> Thu, Nov 18, 2021 at 3:16 PM
To: toby.l.welch@wv.gov

Thank you for the details. I think we'll find someone nearby who can hand deliver it Monday morning.

Thanks,
Don

Don DeFord
National Sales Manager
Phone: 503-269-7224
Email: donald.deford@voatz.com

Voatz

---- On Thu, 18 Nov 2021 11:43:28 -0800 **toby.l.welch@wv.gov** wrote ----
[Quoted text hidden]

Table of Contents

Cover Letter 1

Designated Contact & Certification and Signature Form 3

Addendum Acknowledgement Form 4

4.1 Project Goals and Mandatory Requirements 5

4.1.1 Goals and Objectives 5

4.1.2 Mandatory Project Requirements 11

4.1.3 Cyber Security Systems and Controls 31

4.2 Qualifications and Experience 33

4.2.1 Qualification and Experience Information 33

4.2.2 Mandatory Qualification/Experience Requirements 33

Attachment B: OWASP Application Level Security Verification Levels 1 – 3: Documentation 36

Attachment B: Supporting Documentation 60

Attachment C: OWASP Mobile Application Level Security Verification: Table 143

Attachment C: Supporting Documentation 148

Attachment D: Security Requirements for Databases: Table 167

Attachment D: Supporting Documentation 170

Attachment E: Select Controls from NIST SP 800-171: Table 184

Attachment E: Supporting Documentation 189

Attachment F: - POA&M Tracker 216

Attachment G - Pro V&V Report **Error! Bookmark not defined.**

Attachment H - Voatz, Inc. Accessibility Conformance Report 218

Attachment I - Full ProV&V Report 219

Attachment J - Resumes of Key Personnel 220

1. Cover Letter

Voatz Inc. ("Voatz") is pleased to provide this response to the State of West Virginia Request for Proposal SOS220000001 for E-Ballot Delivery for the 2022 primary and general elections.

Voatz, an award-winning online voting platform, provides election management solutions adapted to the needs of each election phase - Pre-Election, Election Day and Post-Election - including secure ballot marking and return on mobile devices and end-to-end auditing capabilities. The Company was founded to create the first online and mobile voting platform that enables eligible citizens to vote - regardless of their circumstances from virtually anywhere in the world. Voters use their smartphone to authenticate themselves, receive, mark, and submit their secret ballot using an immutable blockchain infrastructure. Election managers can easily consolidate remote and in-person results and take advantage of the system's unique audit features designed to facilitate independent auditing of the entire electoral process. The Voatz platform focuses on providing cutting-edge security alongside an easy-to-use mobile interface, to enable voters and election managers to engage in the electoral process in a convenient manner. Almost two million voters have used the Voatz platform in over 80 elections in national, state and local governments, unions, universities, nonprofits, major political parties, and around the world.

Voatz originated when the founders won the 'Hack to the Future' hackathon at the 2014 South by Southwest conference in Austin, Texas. The founders were intrigued by the possibilities of combining the latest security features in modern smartphones, with emerging techniques capable of real-time identity verification, with biometrics capable of assuring the registered voter is present, all with the irrefutability offered by blockchain and the concepts of a distributed ledger. Their winning prototype – a mobile application designed to assure the privacy of the voter, protect the integrity of the election, and reduce the chances of voter coercion – became the foundation for the current Voatz platform.

Following its first private election in 2016 (and more than 30 elections later), Voatz entered the public elections space in 2018, partnering with the state of West Virginia to record the first mobile vote in United States Federal Election history. In 2019, Voatz ran the first mobile vote in United States Municipal Election history with the City & County of Denver in Colorado. And in 2020, Voatz provided the first smartphone and blockchain based election system to be used for voting in a United States Presidential Election. The Voatz platform has been used in 30 counties across 5 United States states for public elections. In parallel to these public elections, Voatz has run political party conventions, elections, and committee votes in 5 different states working with both major political parties in the U.S.

Additionally, in 2020 Voatz was one of the election services providers selected to facilitate Venezuela's Consulta Popular, a referendum organized by the members of Venezuelan civil society, the Asamblea Nacional ("National Assembly") de Venezuela. Voatz was engaged by the organizers to create a digital participation platform for remote and in person citizen consultation. The voting platform was accessible through web browsers, mobile applications,

tablet applications as well as compatible with third party services (such as a Telegram bot voting application). During the referendum, over 1.7 million votes were processed via the Voatz platform.

Voatz has always emphasized security and testing, having worked with government agencies (such as the Department of Homeland Security which performed an infrastructure audit) and independent security partners (such as Consult Hyperion, LedgerOps and Synack) to conduct comprehensive security testing, penetration testing and provide feedback which Voatz incorporates into our platform. We also note that Voatz became the first RABDMR (Remote Accessible Ballot Delivery, Marking and Return) system to successfully complete comprehensive VSTL (Voting Systems Test Laboratory) testing with ProV&V in 2020, which determined that the Voatz system meets the applicable **subset** of requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 for Usability, Accessibility, Functionality, Security and Accuracy. To our knowledge, Voatz is the only online based solution to conduct such a comprehensive review within the United States by a federally accredited testing lab.

Many of the elections conducted by Voatz have included public, citizen-led post-election audits, where, for the first time in US election history, anyone can participate in the post-election audit process. Independent third parties such as The National Cybersecurity Center are currently responsible for managing the audit process, which involves a comparison between all ballot receipts, paper ballots, and the blockchain data to assure that the results are accurate, represent the will of the voters, and that the election holds integrity.

Voatz is the winner of several technical and civic innovation awards including the MassChallenge 2017 Gold Award Winner, Microsoft Civic Innovation Award 2017, Election Center's Democracy Award (Denver County) 2019, Innovative Entrepreneurship in Blockchain Award (Public Sector Services) 2019, and was a finalist at the GSMA Mobile World Congress 2020 Awards for Best Mobile Innovation for Accessibility and Inclusion. Voatz was recently recognized as an Honoree at the 2021 Webby Awards in the Apps and Software: Public Service & Activism Category and a Finalist and Honoree at the Fast Company World Changing Ideas Awards 2021 in three categories.

2. Designated Contact & Certification and Signature Form

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

Jesse Andrews / Director of Sales & Business Development

(Name, Title)

JESSE ANDREWS / DIRECTOR OF SALES & BUSINESS DEVELOPMENT

(Printed Name and Title)

50 MILK ST FL 16, BOSTON MA 02109

(Address)

727-515-3832

(Phone Number) / (Fax Number)

jesse@voatz.com

(email address)

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

Voatz, Inc.

(Company)

Nimit Sawhney / Co-Founder & CEO

(Authorized Signature) (Representative Name, Title)

NIMIT SAWHNEY / CO-FOUNDER & CEO

(Printed Name and Title of Authorized Representative)

22/November/2021

(Date)

617-669-6366

(Phone Number) (Fax Number)

3. Addendum Acknowledgement Form

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP 1600 SOS2200000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

- [x] Addendum No. 1
- [ ] Addendum No. 2
- [ ] Addendum No. 3
- [ ] Addendum No. 4
- [ ] Addendum No. 5
- [ ] Addendum No. 6
- [ ] Addendum No. 7
- [ ] Addendum No. 8
- [ ] Addendum No. 9
- [ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Voatz, Inc.
Company

Authorized Signature

22/November/2021
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

REQUEST FOR PROPOSAL

West Virginia Secretary of State
CRFP SOS2200000001
Election E-Ballot Delivery Technology

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Voatz, Inc.

(Company)

Nimit Sawhney / Co-Founder & CEO

(Representative Name, Title)

617-669-6366

(Contact Phone/Fax Number)

22/November/2021

(Date)

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: VOATZ, INC.

Authorized Signature: _____ (NIMIT SAWHNEY) Date: 22/NOVEMBER/2021

State of MASSACHUSETTS

County of NORFOLK, to-wit:

Taken, subscribed, and sworn to before me this 22 day of November, 2021.

My Commission expires April 1st, 2027.

AFFIX SEAL HERE

NOTARY PUBLIC _____

MARIA PAULA BAUTISTA CUELLAR
Notary Public
Commonwealth of Massachusetts
My Commission Expires April 1, 2027

4.1 Project Goals and Mandatory Requirements

4.1.1 Goals and Objectives

4.1.1.1

The Vendor provides an electronic ballot delivery and marking tool to all 55 West Virginia Counties in the State. The tool shall be ready for go-live use by no later than the statutory absentee ballot mailing deadline on March 26, 2022. All development, proofing, training, and other necessary actions shall be complete prior to that date.

Voatz complies with this requirement and the associated project timelines.

Voatz's award winning system permits seamless implementation and administration by authorized county or state election officials. In conjunction with the Clients' local resources, Voatz's team is composed of experienced project management staff, technical support staff and training resources to deliver the project as in all Voatz assisted election events.

The Voatz platform is complete and ready to meet the needs of West Virginia's voters. Our support center is fully operational and staffed and ready to support voters beginning on March 26, 2022.

4.1.1.2

The tool satisfies all West Virginia and federal requirements for electronic absentee voting, including but not limited to W. Va. Code § 3-3-1 ct seq., the Uniformed and Overseas Absentee Voting Act, the Military and Overseas Voter Empowerment Act, and the Americans with Disabilities Act.

Yes, Voatz complies with this requirement.

Voatz is the first remote ballot delivery system to undergo VSTL testing to applicable VVSG standards.

The following report summarizes their findings. Please see the full report in Attachment I for additional details.

Letter Report

PRO V&V

To: Linda Hutchinson – Voatz, Inc.

From: Wendy Owens - Pro V&V, Inc.

CC: Michael Walker - Pro V&V, Inc.

Date: July 16, 2020

Subject: Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System

---

Dear Ms. Hutchinson:

Pro V&V is providing this letter to report the results of the evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System to the applicable requirements in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 and the manufacturer-stated requirements set forth in the system documentation. The scope of the evaluation incorporated a sufficient spectrum of functional tests to verify that the RABDMR features and applications conform to the defined requirements.

The evaluation was conducted in two phases. Phase 1 consisted of a Usability and Accessibility Review. Phase 2 consisted of the following: 1) Verify that the RABDMR performs as documented in the provided system technical documentation, 2) Evaluate the RABDMR System as it relates to voter experience and transmission of the voter's selection to the jurisdiction, 3) Execute system use cases to evaluate system functionality, 4) Source Code Review, 5) Physical Configuration Audit (PCA), 6) Functional Configuration Audit (FCA), 7) System Integration Testing, including Accuracy Testing and Regression Testing, 8) Security Testing, and 9) Telecommunications Testing. All tests were performed to the VVSG 1.1 standards with the exception of the Accuracy Test, which was conducted on an abbreviated scale.

Based on the results obtained during the test campaign, Pro V&V determined the RABDMR, as presented for evaluation, meets the applicable requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1, with clarifications or exceptions noted in Section 4.0 of the final version of Pro V&V Test Report TR v. 01-02-VTZ-001-02.

Should you require additional information or would like to discuss this matter further, please contact me at 256-713-1111.

Sincerely,

Wendy Owens

Wendy Owens
VSTL Program Manager
wendy.owens@provandv.com

4.1.1.3

The tool's functionality allows convenient confirmation of voter eligibility, voter identity, and accessibility.

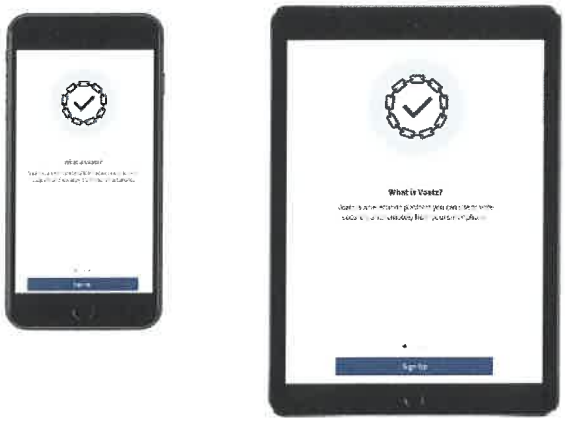
Yes, Voatz complies with this requirement.

The following guide describes the process of confirming voter eligibility and identity. Accessibility is an inherent feature of the mobile devices used by voters.

The Voatz Mobile App enables voting via compatible smartphones and tablets to increase accessibility and security in elections. Voters use their own Apple or Android smartphones to download a secure application that allows them to biometrically authenticate themselves before receiving any election material, automatically receive their ballot, mark and verify them electronically, and submit their secret ballot into the geographically distributed immutable blockchain infrastructure.

The Mobile Voting Experience

The Voatz Mobile Application can be accessed on both Apple & Android smartphones and tablets, as seen below. The steps below are illustrative of a potential voting workflow:



Download and access the app.

Downloading and accessing the Voatz application are the first steps in the voting process and the first phase of Identity Proofing. Here Voatz, in partnership with the jurisdiction, sends an email or letter inviting a registered voter to vote from their personal device. The correspondence contains instructions on how to configure their device to vote and a means of authenticating the voter.

The invitation contains instructions to download the Voatz application from the App Store (iOS) or Google Play Store (Android) and initiate an identity verification and proofing process. This process

ensures that, even though anyone can download the Voatz application, only duly registered voters can use the application to access their ballot.

Enrollment ensures that only designated registered voters can vote remotely.

Image: Account Creation

Sign-up procedure.

The solution includes a comprehensive identity verification and voter data management system that supports multiple forms of ID (as simple as webform self-affirmation scaling to standard government issued documents) and secondary verification sources.

The sign-up process is divided into two stages:

1. **Remote Identity Proofing:** In the first phase, the registered voter presents an approved government-issued photo ID (the "credential") to the jurisdiction. An authorized Credential Service Provider (CSP) verifies the validity of the government-issued credential. An authorized Identity Provider (IdP) performs a biometric test for "liveness." Identity validation is done by comparing the photo image of the remote person to the picture in the government issued credential. The secure communication between a relying party and third party CSPs and IdPs is done through the process called "federation" described below.

   Voatz uses the smartphone or tablet's digital camera to capture an approved credential (i.e. driver's license, passport or government issued photo ID). The Voatz application integrates a third party CSP to perform both credential verification and "liveness" detection. Credential verification is a sophisticated process in which the CSP automatically examines the security artifacts of the voter's credential against their database of known credentials. Confirmation of "liveness" is performed biometrically by taking a video "selfie" where the voter is asked to nod their head and blink their eyes. Voatz has two options to perform the comparison of the video selfie to the photograph of the voter's credential: manually by Voatz personnel during the small pilots of governmental elections and automatically during a relatively large election by requiring agreement between two competing

facial recognition services. When there is no agreement, an authorized human makes the decision which may include a video chat with the requesting person (e.g. via Skype). Biometric data is retained only as long as it takes to verify the identity of the registered voter in the real world.

Note: There may be a delay in comparing the video selfie to the voter's credentials; until then the Voatz application will indicate a "pending status." The voter cannot open their ballot until notification of a successful resolution of identity is received by the application.

Voatz bases its identity proofing mechanisms on the requirements of the Customer, and can support identity proofing mechanisms ranging from voting credentials distributed to voters via mail, to the government issued document verification process described above. While the latter process offers the greatest level of security, Voatz understands that each customer has unique needs, and offers a range of identity proofing options to meet those needs.

Identity proofing answers the question, "Is this person who they say they are and does that person exist in the real world?"

2. **Binding:** Binding is the final phase of identity proofing. Here the user biometrically binds the identity-proofed person to their personal smartphone or tablet. Binding prevents an identity-proofed person from voting on another device and prevents another person from voting on the device that went through the identity-proofing process. For security reasons, it is critical that this step be done in the same session as the identity proofing step.

   Binding is achieved when the Voatz application requests the user to re-authenticate themselves in the same way they did to gain access to their device – typically via fingerprint or face ID

   Binding prevents a remote voter from casting a ballot more than once and enables secure authentication.

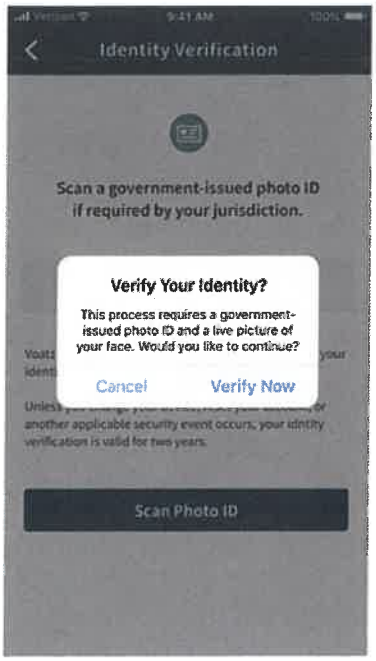


Image: Verify Identity

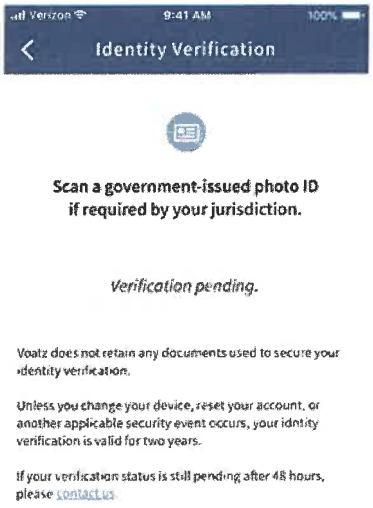


Image: Identity Verification Status.

Access to ballot and voter information.

Access to the ballot is granted through the following processes:

Authentication: Voter authentication occurs in every election; it is unlike identity proofing which is episodic. Authentication is central to the process of associating the device to the identity of a remote voter just prior to their act of voting – but not how they voted. Authentication is performed by verifying that the voter possesses at least one method, called a "valid authenticator," of ensuring that their identity can be confirmed at the time of voting. Devices with biometric capabilities can serve as a valid authenticator.

Voatz uses the smartphone or tablet as the "valid authenticator." In the Voatz application, authentication is requested twice in a voting session: once when the voter tries to open their blank ballot and again when the voter submits their voted ballot. Authentication – via fingerprint or face ID – provides a registered and identity-proofed voter with the authorization to access their blank ballot and the authorization to submit their voted ballot.

Voatz carefully follows the required protocols for certificate key exchange (using Elliptic Curve/Diffie-Hellman) and approved cryptographic encryption (using AES 256). These standards provide for secure communications between the application and the voter.

Authentication provides assurance that the person who voted today on their personal device is the same person who verified their identity previously on that device.

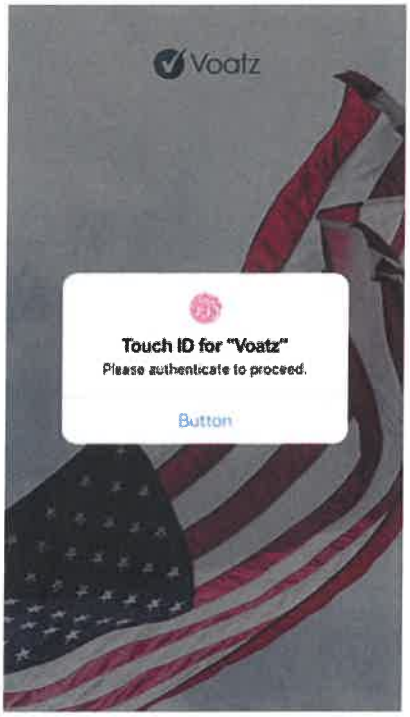


Image: Biometric Authentication.

Federation: Federation is a process that allows for the secure conveyance of authentication and voter attribute information across networked systems. In a federated system, the Credential Service Provider (CSP) and the Identity Provider(s) (IdP), provide identity services to the application developer, called the Relying Party (RP). Federation requires relatively complex multiparty protocols that have subtle security and privacy requirements and require careful consideration.

Voatz contracts with 3rd party providers who provide credential validation and "liveness" detection. Federation, as adopted by Voatz requires that these firms adhere to the NIST 800-63-3 or ISO/IEC 30107-3 (Biometric presentation attack detection) guidelines. Voatz carefully follows the required protocols for certificate key exchange using Elliptic Curve/Diffie-Hellman (see endnote v) and approved cryptographic encryption methods (using AES 256). These standards provide for secure communications between independent service providers, the relying party, the voter and the jurisdiction.

Federation speeds progress by enabling "best-of-breed" technologies to be securely integrated into a solution.

○ 4.1.2 Mandatory Project Requirements

4.1.2.1

The tool is capable of recognizing and reading each ballot style based on the "Ballot Design" files in the format provided by the Agency, a county, or a county's ballot programming vendor.

Voatz complies with this requirement.

Voatz coordinates with the primary election system vendor that produces the paper ballot designs. We have a set of automated utilities that read the Ballot Definition File ("BDF") from the paper ballot, PDF files (or XML files), and any available XY coordinate descriptions of the paper ballot design in order to produce the corresponding mobile/accessible ballot files for the Voatz system.

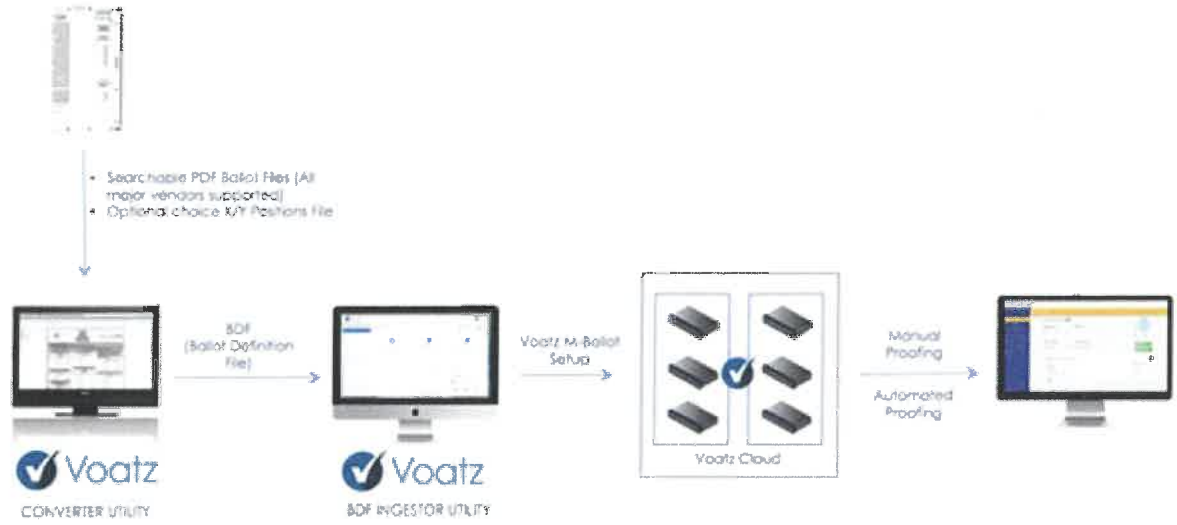


Image: Ballot Import Process

Voatz has a multi-pronged internal proofing process to ensure the accuracy of all electronic ballots.

In addition, Voatz also provides state election officials with a secure administrative portal to conduct proofing of electronic ballots.

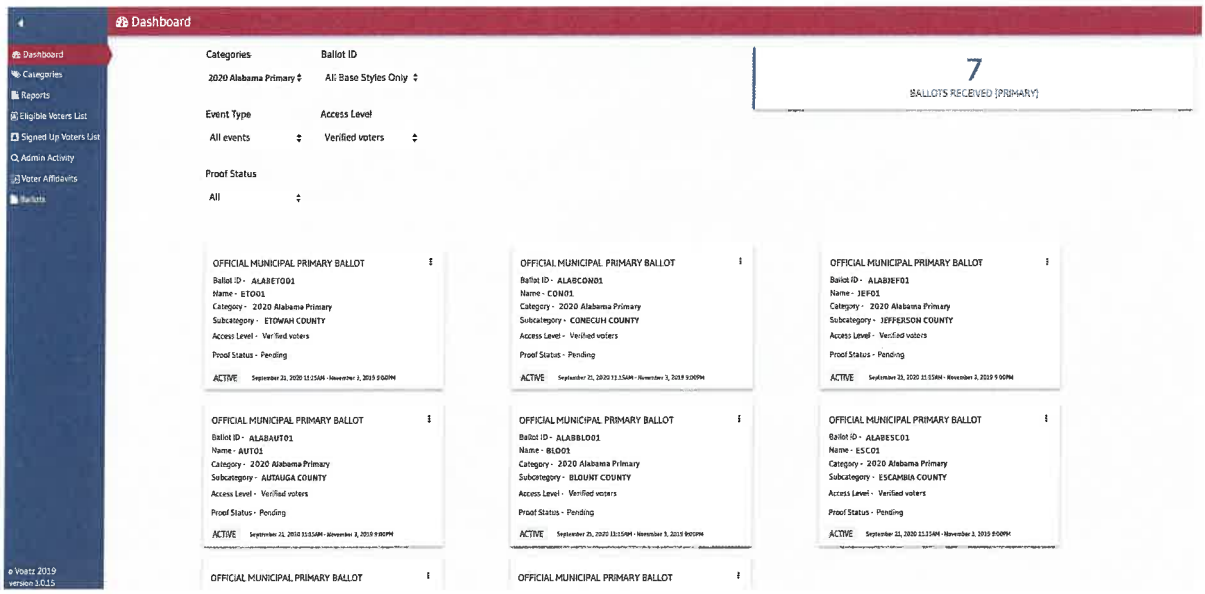


Image: Sample Screenshot of the Administrative Portal for Random Proofing

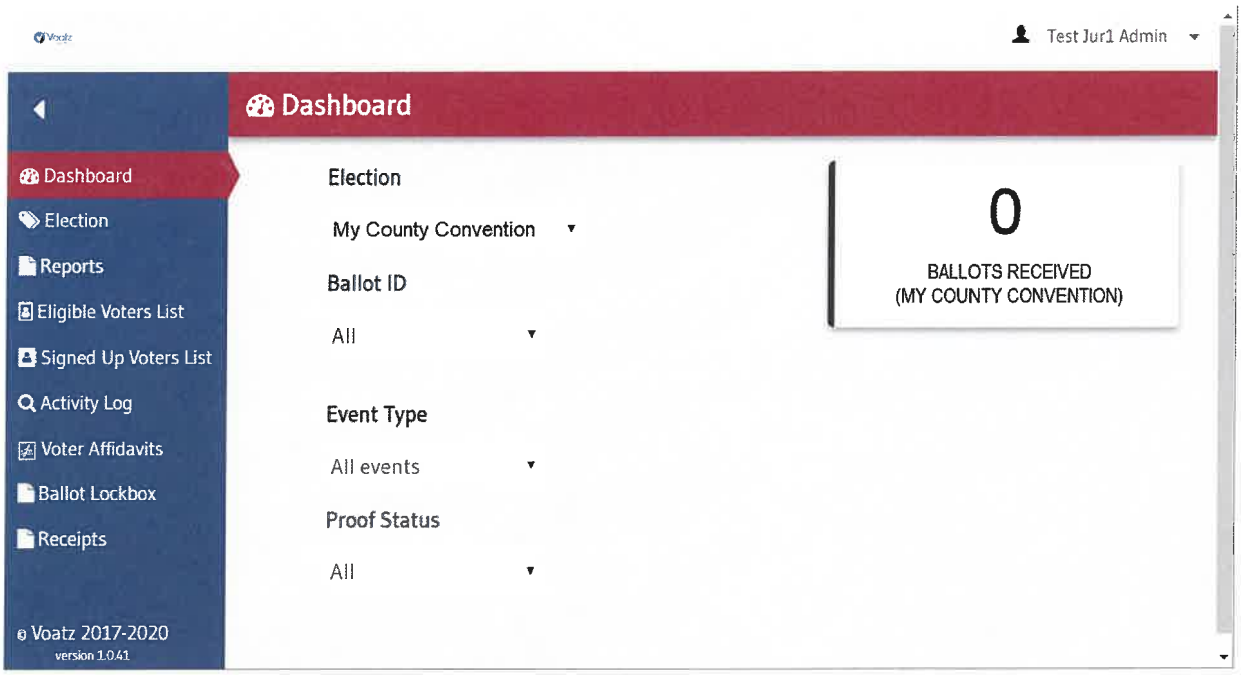
4.1.2.2

The tool includes a cloud server or equivalent backend which securely processes each electronic absentee ballot submission into a cast vote record (CVR) fomat, stores the records in a tamper-resistant manner, and enables all participating counties to access the CVRs as required by the election schedule and process for in-county tallying.

Yes, Voatz complies with this requirement.

The Voatz Admin Portal is a cloud-based web portal that election officials use to manage their Voatz online elections. Use the Admin Portal to:

1. Review and approve electronic ballots before the election
2. Manage voter lists for eligible and signed-up voters
3. Access submitted ballots, signed voter affidavits, and (if used) voter ballot receipts
4. Report on your election
5. Monitor Admin Portal system event logging



Access to the Admin Portal is role-based and two-factor authentication. Each Admin Portal user is assigned a *user role*. The user role determines what the user can see and do in the Admin Portal. A user's role aligns with their duties as an election official and reflects two things:

- Their election responsibilities
- Their precinct assignment(s), if any

For example, if you are a poll worker for Kanawha County, you will be assigned the role Organization User access to data from Kanawha County. Depending on your role, certain Admin Portal screens and activities may not be visible or enabled for you. Admin user roles and associated permissions are described in greater detail in the tables below:

Role	Typically Assigned To	Description
Organization User	Precinct poll worker	An Organization User is generally akin to a poll worker for a given precinct. Organization Users generally have read-only access to data, and may be limited to data for their precinct only. Organization Users do not have access to view voter affidavits, voter ballots, or ballot receipts.
Organization Admin - Affiliated	Precinct-level election administrator such as a town or county clerk	An Affiliated Organization Admin is an election administrator for one or more specific precincts. Affiliated Organization Admins can work with ballot styles, voter lists, voter affidavits, voter ballots, and ballot receipts, but are generally limited to data for their assigned precincts.
Organization Admin - Unaffiliated	Jurisdiction-level election administrator such as a supervisor of elections	An Unaffiliated Organization Admin has administrative access to functions and data for all precincts within the jurisdiction.

The following lists the permissions that accompany each Admin Portal user role.

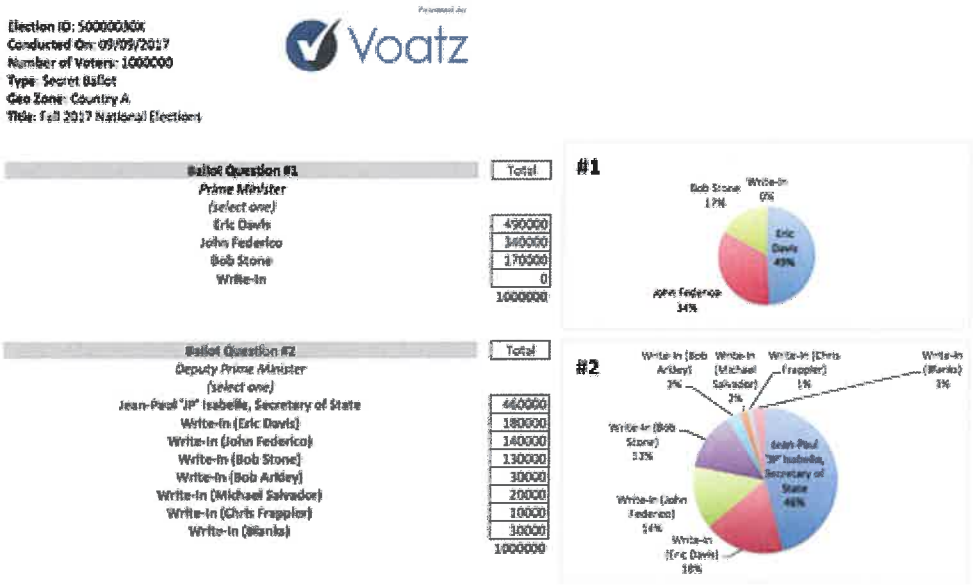
Screen	Description	Organization User	Organization Admin - Unaffiliated	Organization Admin - Affiliated
Dashboard	View	√	√	√
Ballot Styles	View	√	√	√ (assigned precinct(s) only)

	Approve/Reject		√	√ (assigned precinct(s) only)
Elections	Create		√	√
	Delete		√	√
Eligible Voters List	View		√	√
	Add Voter		√	√
	Export List		√	√
Signed-Up Voters List	View	√	√	√
	Delete Failed Verification		√	√
	Export List		√	√
Voter Affidavits	View, Approve, Reject		√	√
Voter Ballots	Designate co-openers		√	√
	Download individual ballots		√	√
	Bulk download ballots			√
	View	√	√	√

Ballot Receipts	Download		√	√
Reports	Run, View			
Activity Log	View, Export	√	√	√

Ballot Tabulation and Election Results

Voter ballot selections are written in aggregate to the Cast Vote Record, a secure, encrypted data file from which election results are tabulated. This feature supports a fully digital tallying and results preparation within the system or the seamless generation



.

Figure 32: Digital Results Tally

Each individual voter's selections can be rendered as a PDF of fully-marked, machine-tabulatable paper ballots. These PDF ballots are stored securely in a digital lockbox. For jurisdictions that tabulate results from paper ballots, these PDFs can be printed and scanned by the jurisdiction's external tabulation system. They are also available for post-election auditing.

Reporting

Prior-to, during, and following the election, election officials can use the Voatz Admin Portal to review summary use data for the election. The summary statistics include data such as:

- Eligible voters
- Signed up voters
- Ballots submitted
- Affidavits received
- Affidavits approved
- Votes by device
- Votes by jurisdiction

4.1.2.3

The tool includes a web-based or equivalent administration console for reporting and tracking voter participation.

Yes, Voatz complies with this requirement.

Voatz integrates with voter data in multiple ways:

- **Batch file transfer** of the most current voter database. This is handled typically via Secure File Transfer Protocols (SFTP or SCP). Voatz also supports frequent or on-demand re-syncing of the batch files to accommodate any changes to the voter data during the voting window.
- Web services API integration (typically via an **encrypted read-only API** into the state voter registration database allowing real-time syncing or a replica system with equivalent accuracy).

The import and management of voter data can be fully automated in the background or initiated manually by the election officials via the Administrative portal. All imported voter data is visible to the designed officials via the Administrative Interface.

The Voatz administrative portal allows authorized personnel to manage and approve absentee ballots for eligible voters.

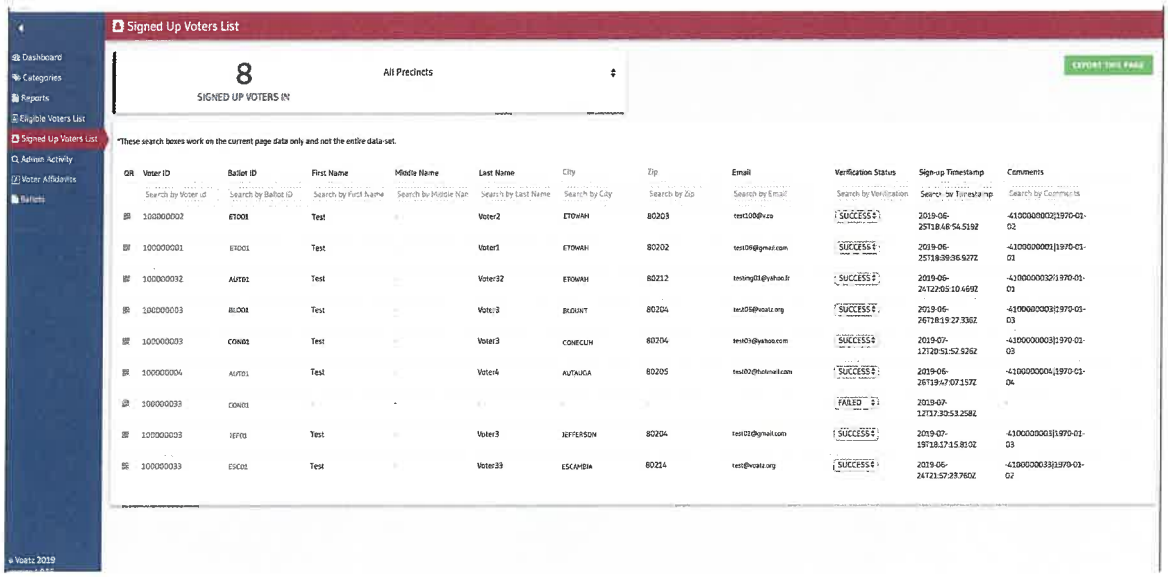


Image: Sample Screenshot of Voter Management, Approval

4.1.2.4

The tool permits a voter to mark a ballot independently and without assistance.

Yes, Voatz complies with this requirement.

Voatz designs and builds its product with usability and accessibility as priorities. The look, feel and continued evolution of the technology is informed by a design process that leverages in-depth user research, interviews, and prototyping with user personas ranging from 18-year-old to 80-year-old voters. Voatz prioritizes simplicity and ease in order to ensure a user-friendly application navigable by all.

Additionally, Voatz makes it a priority to ensure the application is accessibility-friendly so that persons with disabilities can plug and play their smartphone's native accessibility features (large fonts, voice assist) to navigate the application and successfully submit a vote.

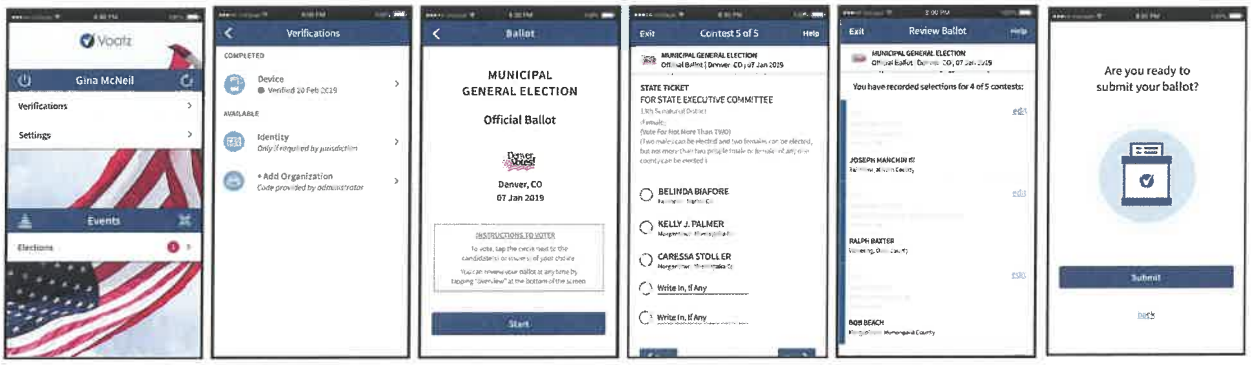


Image: Example Screens Viewed by Voters

4.1.2.5

The tool provides a voter the option to transmit a marked ballot, along with a return packet that includes the requisite forms and disclosures, to the county clerk electronically, or alternatively to print a voted ballot with the aforementioned return packet for return via other approved means to the county clerk.

Voatz complies with this requirement.

The voter has the option to print the marked ballot via the voter web portal. The voter is presented the option to print the ballot, either unmarked or after making and verifying their selections. This is available to any voters who either can not or do not want to submit electronically.

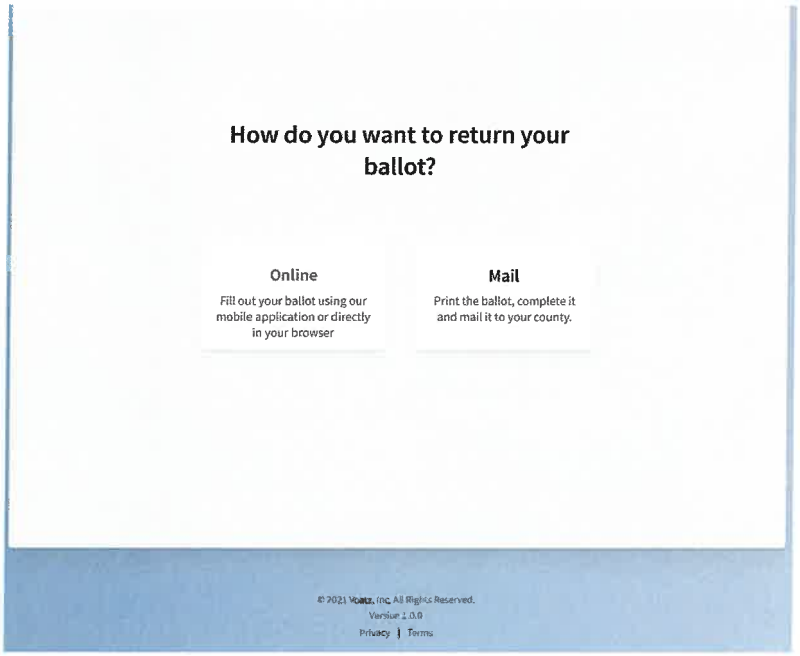


Image: Sample Wizard Showing Voters The Option To Print

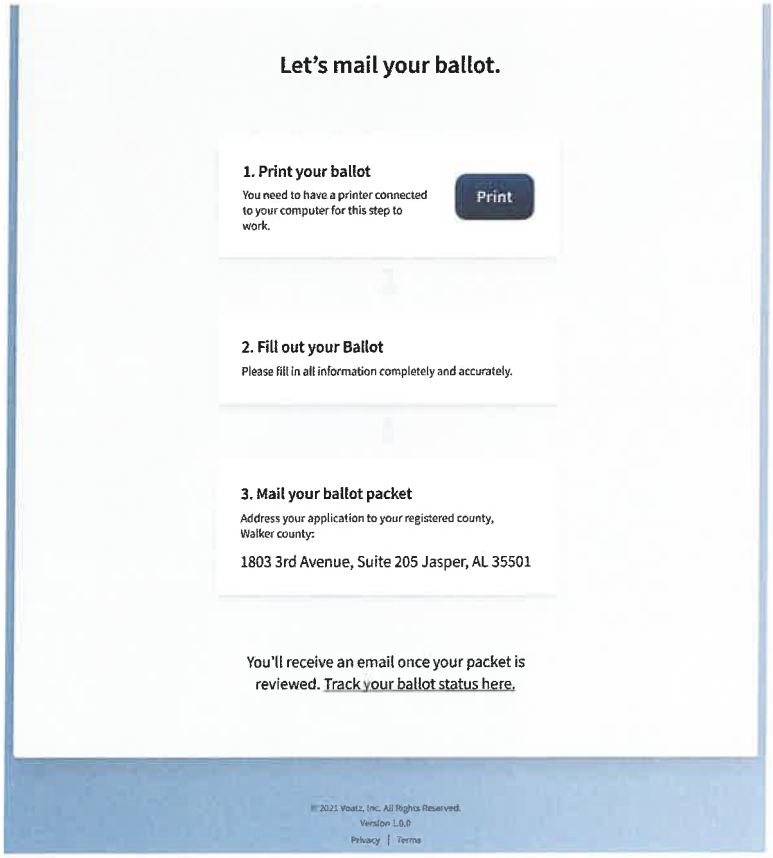


Image: Sample Wizard Showing the Print Options

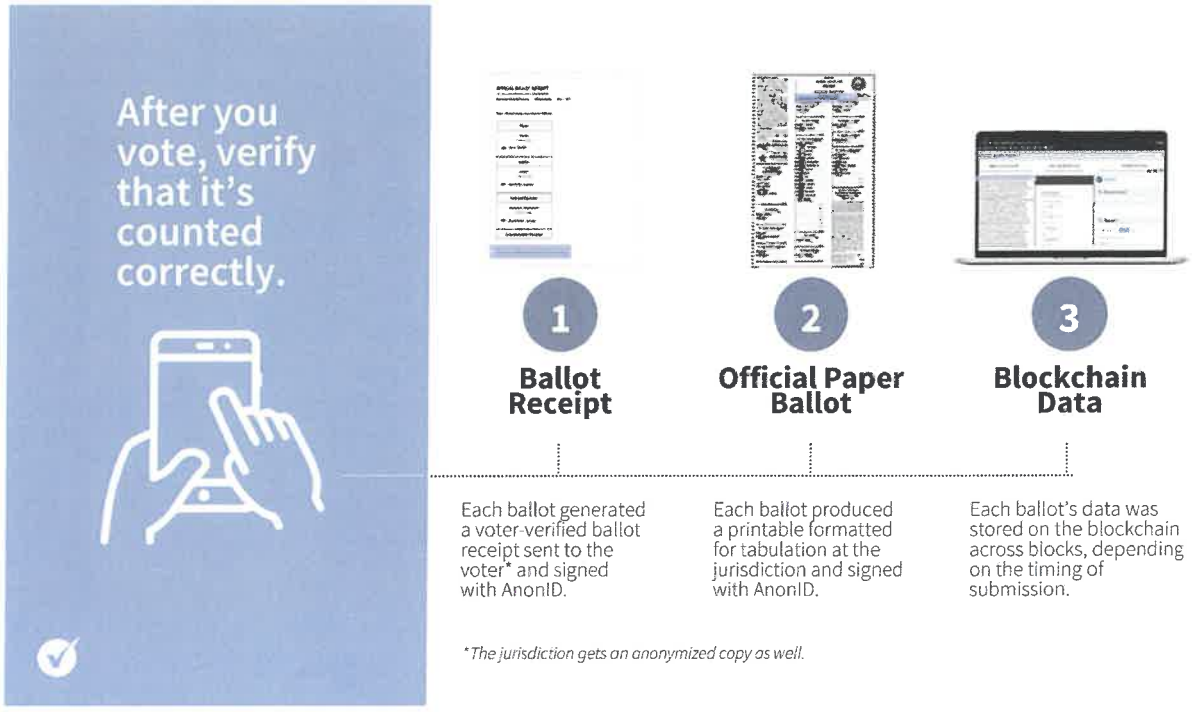
4.1.2.6

The tool includes a verification portal that permits a voter to review their marked, submitted ballot, in a secure and anonymous manner, and in a read-only format, affording the voter with the ability to confirm the ballot cast is the ballot received by the county.

Yes, Voatz complies with this requirement.

After voting, voters automatically receive a ballot receipt containing an anonymous ballot ID. Once a ballot is accepted by a county in the Admin Portal, the county also receives a copy of the ballot receipt with the anonymous ballot ID, separated from the voter's profile. The same anonymous ballot ID is recorded as part of the blockchain data. When accepted ballots are printed for tabulation, the printed ballots also contain this anonymous ballot ID. Only the voter knows their own anonymous ballot ID. It is not tied to the voter in any part of the platform once the ballot packet has been accepted by the county.

The Voatz Audit Portal allows for a full end-to-end audit of the election data by tracing the anonymous ballot ID across all channels. If a voter participates in a public audit of the election, they can look up their own anonymous ballot ID and compare their copy of their ballot receipt to the copy that the county received, as well as comparing it to the blockchain data to ensure that it was captured correctly in all instances.



4.1.2.7

The Vendor provides training and support to the Agency and counties during the duration of the contract.

Voatz complies with this requirement.

Voatz provides comprehensive training services (both in-person and online) covering the various aspects of the system including voting and the administrative functions. Voatz also provides mock community elections (prior to the actual election) wherein both citizens and officials can participate, provide feedback, etc.

Pursuant to state and local health guidelines concerning travel and COVID-19: In the event that in-person training is not permitted due to state or local health guidelines, virtual training will be provided in its place.

Voatz provides comprehensive documentation and user guides for the various activities pertaining to the system.

Voatz will provide comprehensive on-site support to the county elections personnel on the desired dates as needed. In the event that on-site support is not permitted due to state or local health guidelines, virtual support will be provided in its place.

This table lists key staff on the Voatz team designated to work on this project along with their project responsibilities. Curricula vitae for each are attached as an Attachment J to this document.

Contributor	Role / Specialty	Affiliation	Qualifications / Experience	Project Responsibilities

Ana Maria Quevedo	Project Manager	Voatz Employee	Project Leadership: 31 years Elections Space: 22 years BS: Engineering MS: Cybersecurity	Responsibilities include: Primary customer point of contact Develop/manage project plan and schedule Project communications Status updates and reporting
Jesse Andrews	Account Manager	Voatz Employee	Sales & Business Analyst: 10 years Elections Space: 5 years BS, MS: Finance	Responsibilities include: Contract owner Coordination with Client Legal and Financial Manage licensing
Don Deford	Customer Success Engineer	Voatz Employee	Sales: 22 years Elections Space: 12 years BA: Business	Customer Success Lead. Responsibilities include: Election Business/Process Analyst Assessments Training and support oversight Solution deployment coordinator
Nimit Sawhney	Developer/ Engineer	Voatz CEO / Founder	SW Engineer: 22 years Elections Space: 6 years MS: Computer Science	InfoSec Lead. Responsibilities include: Information security Platform and web services developer Reporting
Dolan Murvihill	Developer/ Engineer	Voatz Employee	SW Engineer: 6 years Elections Space: 3 years BS: Computer Science	Responsibilities include: • Develop browser web voting app developer • Web election administration app developer Platform back end and web services developer
Justin Witkowski	Developer/ Engineer	Voatz Employee	SW Engineer: 8 years Elections Space: 3 years BS: Information Technology andWeb Science	Responsibilities include: • Develop browser web voting app developer • Web election administration app developer Specialty in web forms and responsive design

Linda Hutchinson	Quality Assurance Engineer	Voatz Employee	Quality Assurance: 34 years Elections Space: 6 years BA: IMJR	Quality Assurance Lead. Responsibilities include: Author Test Execution Reports for system and system components Execute test plans Logic & Accuracy testing Specialty in accessibility

The following members from the Voatz team will serve as leads for the functional areas listed below.

Lead	Main Functional Area(s)	Email Address
Ana Maria Quevedo	Voatz Project Lead (scheduling, resourcing, project coordination)	anamaria.quevedo@voatz.com
Nimit Sawhney	Platform Security, IAM integration, Engineering	ns@voatz.com
Linda Hutchinson	Quality Assurance, Accessibility compliance	linda.hutchinson@voatz.com
Donald Deford	Customer Success (solution rollout, assessments, support, training)	donald.deford@voatz.com

Voatz provides comprehensive help desk services for voters and election administration personnel via phone, email, text chat and support web portals, and will maintain Help Desk statistics on help request volume, resolution, and response time, and provide reports to the Secretary of State upon request via our robust support reporting tools.

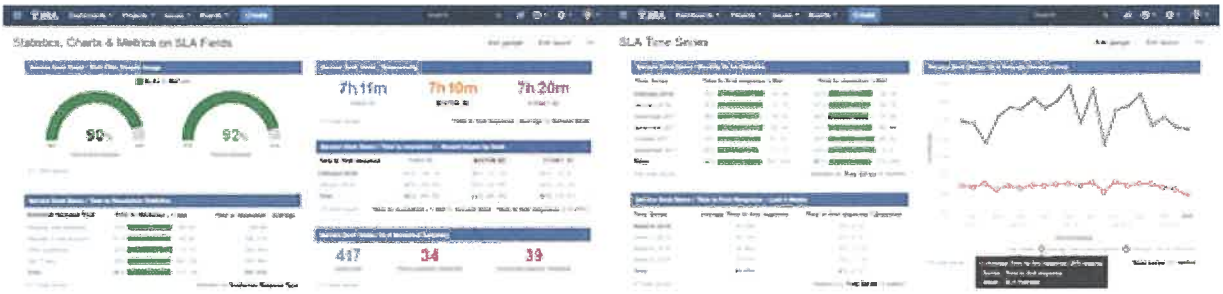


Image: Sample Screenshot of Help Desk Statistics Dashboard

4.1.2.8

Section 508 Compliance

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use Information and Communication Technology (ICT), it shall be accessible to people living with disabilities. Federal employees and members of the public who have disabilities must have access to, and use of, information and data that is comparable to people without disabilities.

Products, platforms and services delivered as part of this work statement that are ICT, or contain ICT, must conform to the Revised 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at h@s://www.access-board.gov/guidelines- andstandards/communications-and-it/about-the-ict-refresWfinal-rule/text-of-the- standardsand-guidelines

Yes, Voatz complies with this requirement.

The VoatzTM mobile elections platform provides robust support for all voters, including those with visual, cognitive, mobility, and dexterity disabilities. (Hearing is not required for voting unless using a screen reader.) Voters of all abilities can vote privately, independently and securely without the need for paper ballots or postal mail.

The Voatz Mobile App supports native smartphone accessibility features, including those listed here.

- VoiceOver and TalkBack screen readers
- Predictable navigation
- Configurable font size
- Speech-to-Text (for write-ins)
- Voice Command (iOS)
- Configurable session timeout
- Support for Bluetooth assistive devices

4.1.2.8.1

Provide list of item(s) that contains ICT. For each item, the following requirements apply:

Voter-facing software:

Voatz Mobile App (VMA)for iOS smartphones

Voatz Mobile App (VMA) for Android smartphones

Voatz Web App (VWA) for compatible browsers

4.1.2.8.1.1

All functional performance criteria apply when using an alternative design or technology that achieves substantially equivalent or greater accessibility and usability by individuals with disabilities, than would be provided by conformance to one or more of the requirements in Chapters 4-6 of the Revised 508 Standards, or when Chapters 4-6 do not address one or more functions of ICT.

Yes, Voatz complies with this requirement.

4.1.2.8.1.2

Software features and components: All WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application.

Yes, Voatz complies with this requirement.

4.1.2.8.1.3

Hardware features and components: All requirements apply.

Yes, Voatz complies with this requirement.

Voatz does not provide hardware. However, Voatz VMAs utilize the accessibility features native to iOS and Android smartphones.

4.1.2.8.1.4

Applicable support services and documentation: All requirements apply.

Yes, Voatz complies with this requirement.

4.1.2.8.2

Provide an Accessibility Conformance Report (ACR) for each commercially available ICT item offered through this contract. Create the ACR using the Voluntary Product Accessibility Template Version 2.1 or later, located at https://www.itic.org/policy/accessibility/vpat. Complete each ACR in accordance with the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the remarks/explanations column, or through additional narrative. All "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. Address each standard individually and with specificity, and clarify whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item.

Yes, Voatz complies with this requirement.

Reference the Voatz, Inc. Accessibility Conformance Report, attachment H.

4.1.2.8.3

Provide a description of the evaluation methods used to support Section 508 conformance claims. The Agency reserves the right, prior to making an award decision, to perform testing on some or all of the Vendor's proposed ICT items to validate Section 508 conformance claims made in the ACR.

Voatz incorporates accessibility and usability design throughout its development process, and incorporates a continuous practice of both real-world evaluation and design-to-standards in engineering.

- Voatz partnered with the National Center for Accessible Media for recommendations on usability and accessibility. Read more about the partnership here.
- Voatz software is evaluated in-house by professional testers with previous WCAG 2.1 and certified voting systems experience. Read the VPAT statement here.
- Voatz engaged Pro V&V, an independent EAC-approved voting system testing laboratory (VSTL) certified in assessing accessibility compliance with the U.S. Election Assistance Commission's Voluntary Voting System Guidelines (VVSG 1.1). View Pro V&V's Accessibility and Usability Test Report here.
- In addition to rigorous internal testing and remediation, Voatz continuously incorporates feedback from accessibility experts and voters with disabilities who have participated in elections using Voatz.

4.1.2.8.4

Describe your approach to incorporating universal design principles to ensure ICT products or services are designed to support disabled users.

Voatz incorporates accessibility and usability design throughout its development process:

- Voatz partnered with the National Center for Accessible Media for recommendations on usability and accessibility. Read more about the partnership here.
- Voatz software is evaluated in-house by professional testers with previous WCAG 2.1 and certified voting systems experience. Read the VPAT statement here.
- Voatz engaged Pro V&V, an independent EAC-approved voting system testing laboratory (VSTL) certified in assessing accessibility compliance with the U.S. Election Assistance Commission's Voluntary Voting System Guidelines (VVSG 1.1). View Pro V&V's Accessibility and Usability Test Report here.
- In addition to rigorous internal testing and remediation, Voatz continuously incorporates feedback from accessibility experts and voters with disabilities who have participated in elections using Voatz.

4.1.2.8.5

Describe plans for features that do not fully conform to the Section 508 Standards.

Neither accessibility nor security are concepts that are ever "done" 100%. Voatz is committed to continually improving both, and expects that both standards and user expectations will continue to drive those improvements. As a partner with many national and local accessibility user groups and standards bodies, Voatz intends to not only maintain compliance with applicable standards, but to lead the way in ensuring that voters with disabilities are able to vote privately and independently, regardless of standards or requirements. If features are identified that do not adequately meet the needs of voters with disabilities or current standards, Voatz is committed to identifying those issues, working with our customers to prioritize them by importance to their voters' needs, and tracking and reporting progress on the issues through our project management team.

4.1.2.8.6

Describe "typical" user scenarios and tasks, including individuals with disabilities, to ensure fair and accurate accessibility testing of the ICT product or service being offered.

Typical user tasks are described in the following process chart:

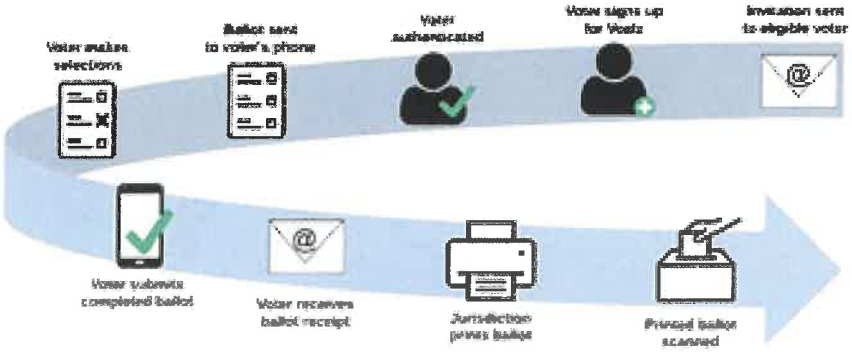


Figure 1-1. RABDMR Process Flow

Each step in this process is routinely tested by user groups with disabilities to identify weaknesses in the platform.

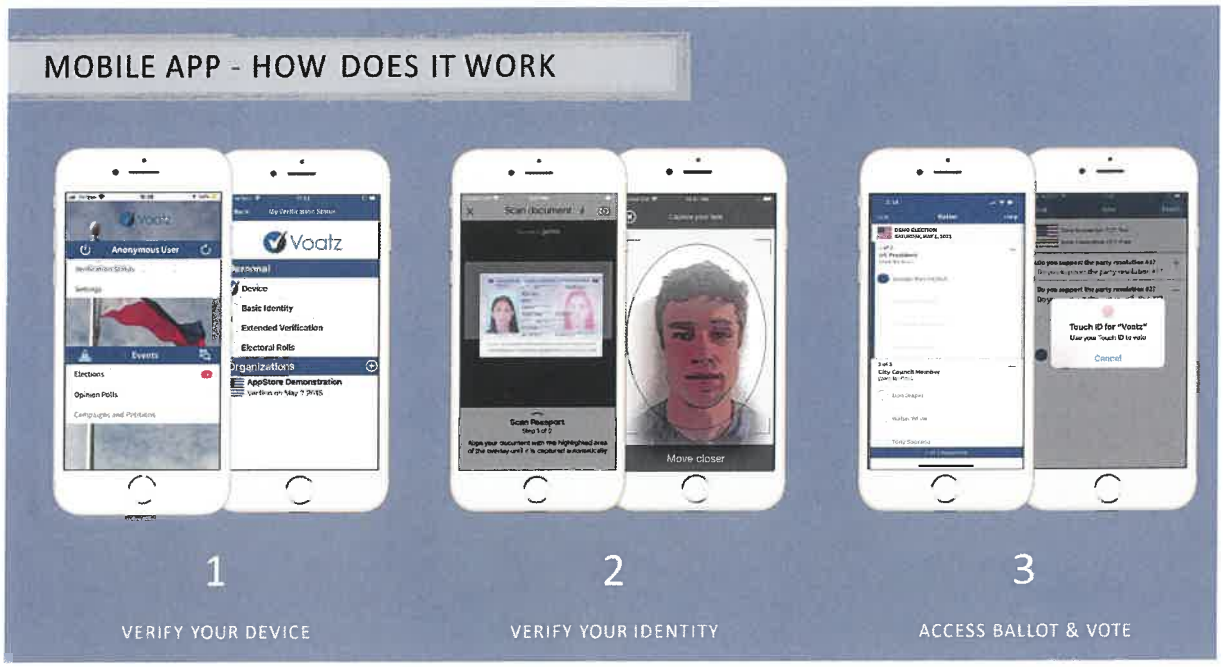
The Voatz system is composed of a mobile application (iOS, android), an administrative portal, blockchain vote storage, and a public bulletin for vote verification and auditing. *A traditional web based voter portal is also offered for voters who may not have a compatible device while encouraging most voters to use the most secure, accessible and convenient mobile option.*

A voter is able to download the mobile application and sign up with an active mobile number and email. Once signed up in the Voatz app, voters are required to authenticate themselves before gaining access to eligible elections. Authentication is a three-step process that uses the smartphone's camera and its biometric feature (i.e. fingerprint recognition or facial recognition): (1) the voter scans their state driver's license or passport, (2) takes a live facial snapshot (a video "selfie"), and (3) touches the fingerprint reader on the smartphone or activates the phone facial lock, which ties the voter's device to the voter. Once the voter is authenticated, the app matches the voter's "selfie" to the facial picture on their passport or driver's license and confirms the voter's eligibility to vote against the state's voter registration database.

Once the voter is verified, election jurisdictions initiate the voting process by sending a qualified voter a mobile ballot. Contained in the mobile ballot are "tokens" — think of them as potential votes — which are cryptographically tied to a candidate or ballot measure question. The number of tokens a given voter receives is the same as the number of ovals he or she would have received on a paper ballot handed out at the voter's precinct or sent through the mail.

A voter must then provide their biometric information to access the mobile application and again to submit any ballots. Voters will see eligible elections and ballots within the Voatz app during the corresponding voting period, and the voter will then make their desired selections and submit their ballot. These selections alter the tokens (like filling in a ballot oval). Overvotes are prevented, as each voter only receives a total number of tokens as they have potential votes. Once submitted, the votes for choices on the ballot are verified by multiple distributed servers called "verifiers", or validating nodes. Upon verification, the token is debited (i.e. subtracted) from the voter's ledger and credited (i.e. added) to the candidate's ledger. The blockchain on every verifier is automatically updated and the process repeats as additional voters submit their selections. Voters receive a digitally signed and encrypted pdf of their choices (optional, if desired by the jurisdiction) in which they may verify their submitted ballot.

The following images show the simple process that voters experience using the Voatz Mobile App.

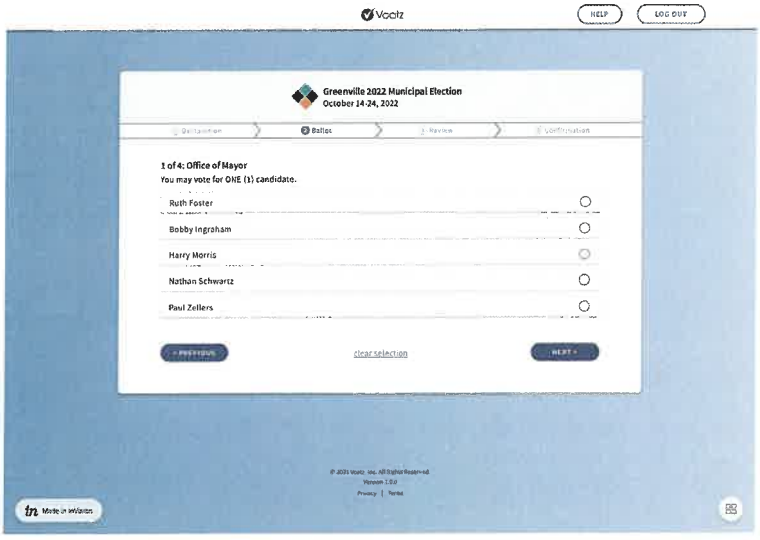


The following images show the simple process that voters experience using the Voatz Web App.

1. Authorized voters access the Voatz Web App via a URL provided to them for the election.
2. A Login screen prompts them to enter a mix of personal identification data as required by the jurisdiction, for example, name, date of birth, and Voter ID. This information is validated against voter data in the Voatz database.

3. Voters arrive at the first screen for their event. This can be a simple welcome screen that provides information about the election, or a declaration that the voter must agree with before proceeding with the ballot.

4. Voters are taken to the ballot. The image below displays a contest where voters can select multiple candidates. To make their choices, voters select the candidates they wish to vote for by clicking on their name or anywhere in their designated box on the screen. If desired, voters can select 'more information' to view additional information and resources for each candidate. The information found under the 'more information' tab can be customized by the jurisdiction and can include embedded media and links to external resources. If a voter has under-voted, they will receive a warning before the system allows them to move on to the next question. Overvoting is not allowed by the system.



5. After completing the ballot, voters are shown a review screen where they can see an overview of their selections. Voters can navigate back to any contest and change their selections by clicking the 'change' button located next to each contest.

6. Voters are prompted to confirm their intent to submit their ballot by clicking 'submit' when the popup appears as shown above. Until they click 'submit,' voters still have the option of navigating back to their ballot and changing their selections, by clicking 'back.' Additional submission requirements, such as an e-signatuare for affidavits (captured via touch screen or mouse), can be included in the submission process.

7. After submitting their ballot, voters are taken to a confirmation screen where they are provided with a confirmation number which they can print or email for their records. Or, optionally, an emailed vote receipt (with visual confirmation of a voter's individual oval choices) can be delivered to the voter upon submission (in addition to the confirmation code provided on screen, or in place of the confirmation code).

4.1.2.9

Prior to acceptance, the Agency reserves the right to perform testing on required ICT items to Validate the Vendor's Section 508 conformance claims. If the Agency determines that Section 508 conformance claims provided by the Vendor represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the Vendor to remediate the item to align with the Vendor's original Section 508 conformance claims prior to acceptance.

Yes, Voatz agrees to this requirement.

○ 4.1.3 Cyber Security Systems and Controls

The tables in Attachments B-E contain lists the requirements for Sections 4.1.3.1.1-4, along with an indication of Yes/No/Partial to note whether or not we meet the given requirement. Those items that are not applicable are indicated with a "Yes" in the table, but have an "N/A" designation in the subsequent description in the attachment, with relevant comments.

4.1.3.1

Cybersecurity systems and controls are essential to distinguish, counteract, or decrease security risks. These measures are required to manage threats targeting computer systems and networks. These

measures must be adaptive and robust. To determine whether your cyber security systems and controls meet our desired standards:

4.1.3.1.1

Please complete Attachment B — OWASP Application Level Security Verification Levels I —3. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F — POA&M Tracker.

Yes, Voatz complies with **239 of 239** requirements in Attachment B: OWASP Application Level Security Verification Levels 1 - 3. One of these is a partial fulfillment of the requirement; a certain option within that requirement may be disallowed for security reasons. Five of these requirements are in active development (to facilitate some feature enhancements) and we expect to have the associated features completed and tested by the end of January 2022.

See Attachment B for the documentation for each requirement, along with comments.

4.1.3.1.2

Please complete Attachment C — OWASP Mobile Application Level Security Verification if applicable. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F — POA&M Tracker. If not applicable, please put N/A by all requirements.

Yes, Voatz complies with **69 of 69** requirements in Attachment C: OWASP Mobile Application Level Security Verification.

See Attachment C for the documentation for each requirement, along with comments.

4.1.3.1.3

Please complete Attachment D — Security Requirements for Databases. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F — POA&M Tracker.

Yes, Voatz complies with **43 of 43** requirements in Attachment D: Security Requirements for Databases.

See Attachment D for the documentation for each requirement, along with comments.

4.1.3.1.4

Please complete Attachment E — Select Controls Lom NIST SP 800-171. For all listed requirements please provide 2 pieces of supporting documentation. For any requirements that are lacking supporting documentation, please add to Attachment F — POA&M Tracker.

Yes, Voatz complies with **80 of 80** requirements in Attachment E: Select Controls from NIST SP 800-171.

See Attachment E for the documentation for each requirement, along with comments.

4.2 Qualifications and Experience

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar in size, scope and complexity to those requested in this RFP. Information and documentation should include, but are not limited to, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects including the value and period of performance of past projects, and any other information that Vendor deems relevant to the items identified as desirable or mandatory below.

4.2.1 Qualification and Experience Information

Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

4.2.1.1

Vendor's tool has been reviewed by at least one (l) independent, nationally recognized organization supporting the Disability Community for its user acceptance and Section 508 conformity for voters living with disabilities. Copies of any reports or public statements by the organization(s) should be provided to the Agency for Confidential review.

Yes, Voatz complies with this requirement.

Reference the 'Voatz Mobile App Accessibility Conformance Report,' Attachment H for further detail.

4.2.2 Mandatory Qualification/Experience Requirements

The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.2.2.1

Implemented tool in at least two (2) previous federal elections. A list of all previous federal elections, including the jurisdiction, shall be provided to the Agency.

Yes, Voatz complies with this requirement.

Company Name/Project Owner: Utah County, Utah

Contract Description/Work Performed by Bidder: Voatz provided remote online voting services for UOCAVA voters and voters with disabilities and their caretakers in Utah County, Utah during the 2020 United States General Election. The Client relationship extends to early 2019 and includes five total elections.

Contact Person Name: Josh Daniels

Contact Person Title: County Clerk

Contact Person Employer: Utah County, Utah

Contact Person Phone Number: (801) 234-0676

Contact Person Email: joshd@utahcounty.gov

Company Name/Project Owner: Jackson County, Oregon

Contract Description/Work Performed by Bidder: Voatz provided remote online voting services for deployed military and overseas voters in Jackson County, Oregon during the 2020 United States General Election. The Client relationship extends to early 2019 and includes four total elections. Voatz provided the following services: Project Management; Product Customization; Staff Training; Digital Ballot Design & Proofing; Voter Data List Integration; Help Desk Support to the Client and to Voters Online Voting (remote) Designated Accessible Voting; Tablets for in- home or curbside voters; Production of Paper Ballot Audit Trail; Post Election Reports and Audit

Contact Person Name: Christine Walker

Contact Person Title: County Clerk

Contact Person Employer: Jackson County, Oregon

Contact Person Phone Number: (541) 774-6125

Contact Person Email: walkercd@jacksoncounty.org

Company Name/Project Owner: State of West Virginia

Contract Description/Work Performed by Bidder: Voatz provided remote online voting services for deployed military and overseas voters from the state of West Virginia during the 2018 United States Primary Elections and Midterm Election. Voatz provided the following services: Project Management, Product Customization, Communications and Media Preparation, Staff Training, Digital Ballot Design & Proofing, Voter Data List Integration, Help Desk Support to the Client and to Voters, Online Voting (remote), Production of Paper Ballot Audit Trail, Post Election Reports and Independent Audit, Cybersecurity Review and Assessment.

Contact Person Name: Donald Kearsey

Contact Person Title: State Election Director, Deputy General Counsel

Contact Person Employer: State of West Virginia

Contact Phone Number: (866) 767-8683

Contact Person Email: dkersey@wvsos.gov

4.2.2.2

Vendor's applicable network and systems or tool have been assessed for security vulnerabilities by at least two (2) independent, federally recognized, certified, of industry specific equivalent technology or cybersecurity auditors. Copies of all assessments or equivalent reports shall be provided to the Agency.

Yes, Voatz complies with this requirement.

Please review Attachments I and J for additional information.

4. Attachment B: OWASP Application Level Security Verification Levels 1 – 3: Documentation

Attachment B: OWASP Application Level Security Verification Levels 1 - 3	Yes/No /Partial
	238
Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 1	
Password Security Requirements	
Verify that user set passwords are at least 8 characters in length (after multiple spaces are combined).	Yes
Verify that passwords 64 characters are longer are permitted but may be no longer than 128 characters.	Yes
Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space.	Yes
Verify that any printable Unicode character, including language neutral characters such as spaces and Emojis are permitted in passwords.	Yes
Verify users can change their password.	Yes
Verify that password change functionality requires the user's current and new password.	Yes
Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which mach the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password.	Yes
Verify that a password strength meter is provided to help users set a stronger password.	Yes

Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters.	Yes
Verify that there are no periodic credential rotation or password history requirements.	Yes
Verify that "paste" functionality, browser password helpers, and external password managers are permitted.	Partial
Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as a built in functionality.	Yes
General Authenticator Requirements	
Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.	Yes
Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.	Yes
Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.	Yes
Authenticator Lifecycle Requirements	
Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.	Yes
Credential Recovery Requirements	

Verify that a system generated initial activation or recovery secret is not sent in clear text to the user.	Yes
Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.	Yes
Verify password credential recovery does not reveal the current password in any way.	Yes
Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").	Yes
Verify that if an authentication factor is changed or replaced, that the user is notified of this event.	Yes
Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as TOTP or other soft token, mobile push, or another offline recovery mechanism.	Yes
Out of Band Verifier Requirements	
Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.	Yes
Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.	Yes
Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.	Yes
Verify that the out of band authenticator and verifier communicates over a secure independent channel.	Yes
Single or Multi-factor One Time Verifier Requirements	
Verify that time-based OTPs have a defined lifetime before expiring	Yes
Fundamental Session Management Requirements	
Verify the application never reveals session tokens in URL parameters	Yes
Session Binding Requirements	
Verify the application generates a new session token on user authentication.	Yes

Verify that session tokens possess at least 64 bits of entropy.	Yes
Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.	Yes
Session Logout and Timeout Requirements	
Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.	Yes
Cookie Based Session Management	
Verify that cookie-based session tokens have the 'Secure' attribute set.	Yes
Verify that cookie-based session tokens have the 'HttpOnly' attribute set.	Yes
Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks.	Yes
Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.	Yes
Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible.	Yes
General Access Control Design	
Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.	Yes
Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	Yes
Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.	Yes
Verify that the principle of deny by default exists whereby new users/roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.	Yes

Verify that access controls fail securely including when an exception occurs.	Yes
Operation Level Access Control	
Verify that the sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.	Yes
Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.	Yes
Other Access Control Considerations	
Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.	Yes
Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of files or directory metadata such as Thumbs.db, .DS_Store, .git or .svn folders.	Yes
Input Validation Requirements	
Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).	Yes
Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.	Yes
Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (whitelisting).	Yes
Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).	Yes
Verify that URL redirects and forwards only allow whitelisted destinations, or show a warning when redirecting to potentially untrusted content.	Yes

Sanitization and Sandboxing Requirements	
Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.	Yes
Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.	Yes
Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.	Yes
Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.	Yes
Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.	Yes
Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, use whitelisting of protocols, domains, paths and ports.	Yes
Verify that the application sanitizes, disables, or sandboxes user-supplied SVG scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.	Yes
Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.	Yes
Output Encoding and Injection Prevention Requirements	
Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL Parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ã-ã“ or O'Hara).	Yes
Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.	Yes
Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.	Yes

Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.	Yes
Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.	Yes
Verify that the application projects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, CSP bypasses, DOM XSS, and JavaScript expression evaluation.	Yes
Verify that the application protects against LDAP Injection vulnerabilities, or that specific security controls to prevent LDAP Injection have been implemented.	Yes
Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.	Yes
Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.	Yes
Verify that the application protects against XPath injection or XML injection attacks.	Yes
Deserialization Prevention Requirements	
Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering	Yes
Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks.	Yes
Verify that desterilization of untrusted data is avoided or protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).	Yes
Verify that when parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.	Yes
Algorithms	
Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.	Yes

Log Content Requirements	
Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.	Yes
Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy.	Yes
Error Handling	
Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.	Yes
Client-side Data Protection	
Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.	Yes
Verify that data stored in client side storage (such as HTML5 local storage, session storage, IndexedDB, regular cookies or Flash cookies) does not contain sensitive data or PII.	Yes
Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.	Yes
Sensitive Private Data	
Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.	Yes
Verify that users have a method to remove or export their data on demand.	Yes
Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.	Yes
Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.	Yes
Deployed Application Integrity Controls	
Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.	Yes

Verify that the application employs integrity protections, such as code signing or sub-resource integrity. The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.	Yes
Verify that the application has protection from sub-domain takeovers if the application relies upon DNS entries or DNS sub-domains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.	Yes
Business Logic Security Requirements	
Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.	Yes
Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.	Yes
Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.	Yes
Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.	Yes
Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modeling or similar methodologies.	Yes
File Upload Requirements	
Verify that the application will not accept large files that could fill up storage or cause a denial of service.	Yes
File Execution Requirements	
Verify that user-submitted filename metadata is not used directly with system or framework file and URL API to protect against path traversal.	Yes
Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).	Yes

Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files (RFI), which may also lead to SSRF.	Yes
Verify that the application protects against reflective file download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.	Yes
Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.	Yes
File Storage Requirements	
Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.	Yes
Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.	Yes
File Download Requirements	
Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.	Yes
Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.	Yes
SSRF Protection Requirements	
Verify that the web or application server is configured with a whitelist of resources or systems to which the server can send requests or load data/files from.	Yes
Generic Web Service Security Verification Requirements	
Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.	Yes
Verify that access to administration and management functions is limited to authorized administrators.	Yes

Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.	Yes
RESTful Web Service Verification Requirements	
Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.	Yes
Verify that JSON schema validation is in place and verified before accepting input.	Yes
Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: triple or double submit cookie pattern (see references), CSRF nonces, or ORIGIN request header checks.	Yes
SOAP Web Service Verification Requirements	
Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.	Yes
Dependency	
Verify that all components are up to date, preferably using a dependency checker during build or compile time.	Yes
Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.	Yes
Verify that if application assets, such as JavaScript libraries, CSS stylesheets or web fonts, are hosted externally on a content delivery network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.	Yes
Unintended Security Disclosure Requirements	
Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.	Yes
Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.	Yes

Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.	Yes
HTTP Security Headers Requirements	
Verify that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8, ISO 8859-1).	Yes
Verify that all API responses contain Content-Disposition: attachment; filename="api.json" (or other appropriate filename for the content type).	Yes
Verify that a content security policy (CSPv2) is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.	Yes
Verify that all responses contain X-Content-Type-Options: nosniff.	Yes
Verify that HTTP Strict Transport Security headers are included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.	Yes
Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".	Yes
Verify that the content of a web application cannot be embedded in a third party site by default and that embedding of the exact resources is only allowed where necessary by using a suitable Content Security Policy: frame-ancestors and X-Frame-Options response headers.	Yes
Validate HTTP Request Header Requirements	
Verify that the application server only accepts that HTTP methods in use by the application/API, including pre-flight OPTIONS and logs/alerts on any requests that are not valid for the application context.	Yes
Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.	Yes
Verify that the Cross Origin Resource Sharing (CORS) Access-Control-Allow-Origin header uses a strict white-list of trusted domains to match against and does not support the "null" origin.	Yes
Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 2	

Secure Software Development Lifecycle	
Verify the use of a secure software development lifecycle that addresses security in all stages of development.	Yes
Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.	Yes
Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.	Yes
Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.	Yes
Authentication Architectural Requirements	
Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges needed.	Yes
Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect abuse or breaches.	Yes
Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.	Yes
Access Control Architectural Requirements	
Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.	Yes
Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.	Yes
Verify that attribute or feature-based access control is used whereby the code checks the user's authorization for a feature/data item rather than just their role. Permissions should still be allocated using roles.	Yes
Input and Output Architectural Requirements	

Verify that input and output requirements clearly define how to handle and process data based on type, content, and applicable laws, regulations, and other policy compliance.	Yes
Verify that serialization is not used when communicating with untrusted clients. If this is not possible, ensure that adequate integrity controls (and possibly encryption if sensitive data is sent) are enforced to prevent deserialization attacks including object injection.	Yes
Cryptographic Architectural Requirements	
Verify that there is an explicit policy for management of cryptographic keys and that a cryptographic key lifecycle follows a key management standard such as NIST SP 800-57.	Yes
Verify that consumers of cryptographic services protect key material and other secrets by using key vaults or API based alternatives.	Yes
Verify that all keys and passwords are replaceable and are part of a well-defined process to re-encrypt sensitive data.	Yes
Verify that the architecture treats client-side secrets - such as symmetric keys, passwords, or API tokens - as insecure and never uses them to protect or access sensitive data.	Yes
Errors, Logging and Auditing Architectural Requirements	
Verify that a common logging format and approach is used across the system.	Yes
Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation.	Yes
Data Protection and Privacy Architectural Requirements	
Verify that all sensitive data is identified and classified into protection levels.	Yes
Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.	Yes
Communications Architecture Requirements	
Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.	Yes

Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.	Yes
Malicious Software Architectural Requirements	
Verify that a source code control system is in use, with procedures to ensure that check-ins are accompanied by issues or change tickets. The source code control system should have access control and identifiable users to allow traceability of any changes.	Yes
Secure File Upload Architectural Requirements	
Verify that user-uploaded files are stored outside of the web root.	Yes
Verify that user-uploaded files - if required to be displayed or downloaded from the application - are served by either octet stream downloads, or from an unrelated domain, such as a cloud file storage bucket. Implement a suitable content security policy to reduce the risk from XSS vectors or other attacks from the uploaded file.	Yes
Configuration Architectural Requirements	
Verify the segregation of components of differing trust levels through well-defined security controls, firewall rules, API gateways, reverse proxies, cloud-based security groups, or similar mechanisms.	Yes
Verify that the build pipeline warns of out-of-date or insecure components and takes appropriate actions.	Yes
Verify that the build pipeline contains a build step to automatically build and verify the secure deployment of the application, particularly if the application infrastructure is software defined, such as cloud environment build scripts.	Yes
Verify that application deployments adequately sandbox, containerize and/or isolate at the network level to delay and deter attackers from attacking other applications, especially when they are performing sensitive or dangerous actions such as deserialization.	Yes
Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.	Yes
Credential Storage Requirements	

Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.	Yes
Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.	Yes
Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations.	Yes
Credential Recovery Requirements	
Verify that if OTP or multi-factor authentication factors are lost, that evidence of identity proofing is performed at the same level as during enrollment.	Yes
Look-up Secret Verifier Requirements	
Verify that lookup secrets can be used only once.	Yes
Verify that lookup secrets have sufficient randomness (112 bits of entropy), or if less than 112 bits of entropy, salted with a unique and random 32-bit salt and hashed with an approved one-way hash.	Yes
Verify that lookup secrets are resistant to offline attacks, such as predictable values.	Yes
Out of Band Verifier Requirements	
Verify that the out of band verifier retains only a hashed version of the authentication code.	Yes
Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).	Yes
Single or Multi-factor One Time Verifier Requirements	
Verify that symmetric keys used to verify submitted OTPs are highly protected, such as by using a hardware security module or secure operating system based key storage.	Yes
Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.	Yes

Verify that time-based OTP can be used only once within the validity period.	Yes
Verify that if a time-based multi factor OTP token is re-used during the validity period, it is logged and rejected with secure notifications being sent to the holder of the device.	Yes
Cryptographic Software and Devices Verifier Requirements	
Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a TPM or HSM, or an OS service that can use this secure storage.	Yes
Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.	Yes
Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.	Yes
Service Authentication Requirements	
Verify that if passwords are required for service authentication, the service account used is not a default credential (e.g. root/root or admin/admin are default in some services during installation)	Yes
Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.	Yes
Session Binding Requirements	
Verify that session tokens are generated using approved cryptographic algorithms	Yes
Session Logout and Timeout Requirements	
Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.	Yes
Verify that users are able to view and (having re-entered login credentials) log out of any or all currently active sessions and devices.	Yes
Token Based Session Management	

Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.	Yes
Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.	Yes
Other Access Control Considerations	
Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems and/or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.	Yes
Data Classification	
Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.	Yes
Algorithms	
Verify that industry proven or government approved cryptographic algorithms, modes, and libraries are used, instead of custom coded cryptography.	Yes
Verify that encryption initialization vector, cipher configuration, and block modes are configured securely using the latest advice.	Yes
Verify that random number, encryption or hashing algorithms, key lengths, rounds, ciphers or modes, can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks.	Yes
Verify that known insecure block modes (i.e. ECB, etc.), padding modes (i.e. PKCS#1 v1.5, etc.), ciphers with small block sizes (i.e. Triple-DES, Blowfish, etc.), and weak hashing algorithms (i.e. MD5, SHA1, etc.) are not used unless required for backwards compatibility.	Yes
Verify that nonces, initialization vectors, and other single use numbers must not be used more than once with a given encryption key. The method of generation must be appropriate for the algorithm being used.	Yes
Random Values	
Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically	Yes

secure random number generator when these random values are intended to be not guessable by an attacker.	
Verify that random GUIDs are created using the GUID v4 algorithm, and a cryptographically-secure pseudo-random number generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.	Yes
Secret Management	
Verify that a secrets management solution such as a key vault is used to securely create, store, control access to and destroy secrets.	Yes
Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations.	Yes
Log Content Requirements	
Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.	Yes
Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.	Yes
Log Processing Requirements	
Verify that all authentication decisions are logged, without storing sensitive session identifiers or passwords. This should include requests with relevant metadata needed for security investigations.	Yes
Verify that all access control decisions can be logged and all failed decisions are logged. This should include requests with relevant metadata needed for security investigations.	Yes
Log Protection Requirements	
Verify that the application appropriately encodes user-supplied data to prevent log injection.	Yes
Verify that all events are protected from injection when viewed in log viewing software.	Yes
Verify that security logs are protected from unauthorized access and modification.	Yes

Verify that time sources are synchronized to the correct time and time zone. Strongly consider logging only in UTC if systems are global to assist with post-incident forensic analysis.	Yes
Error Handling	
Verify that a "last resort" error handler is defined which will catch all unhandled exceptions.	Yes
General Data Protection	
Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.	Yes
Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.	Yes
Verify the application minimizes the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.	Yes
Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.	Yes
Sensitive Private Data	
Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.	Yes
Verify that sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.	Yes
Verify that sensitive or private information that is required to be encrypted, is encrypted using approved algorithms that provide both confidentiality and integrity.	Yes
Verify that sensitive personal information is subject to data retention classification, such that old or out of date data is deleted automatically, on a schedule, or as the situation requires.	Yes
Client Communications Security Requirements	
Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.	Yes

Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.	Yes
Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.	Yes
Server Communications Security Requirements	
Verify that connections to and from the server use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.	Yes
Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.	Yes
Verify that all encrypted connections to external systems that involve sensitive information or functions are authenticated.	Yes
Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.	Yes
Malicious Code Search	
Verify that the application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.	Yes
Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.	Yes
Business Logic Security Requirements	
Verify the application has configurable alerting when automated attacks or unusual activity is detected.	Yes
File Integrity Requirements	

Verify that the files obtained from untrusted sources are validated to be of expected type based on the file's content.	Yes
File Execution Requirements	
Verify that the application does not include and execute functionality from untrusted sources, such as unverified content distribution networks, JavaScript libraries, node npm libraries, or server-side DLLs.	Yes
RESTful Web Service Verification Requirements	
Verify that the message headers and payload are trustworthy and not modified in transit. Requiring strong encryption for transport (TLS only) may be sufficient in many cases as it provides both confidentiality and integrity protection. Per-message digital signatures can provide additional assurance on top of the transport protections for high-security applications but bring with them additional complexity and risks to weigh against the benefits.	Yes
SOAP Web Service Verification Requirements	
Verify that the message payload is signed using WS-Security to ensure reliable transport between client and service.	Yes
GraphQL and other Web Service Data Layer Security Requirements	
Verify that query allow list or a combination of depth limiting and amount limiting should be used to prevent GraphQL or data layer expression denial of service (DoS) as a result of expensive, nested queries. For more advanced scenarios, query cost analysis should be used.	Yes
Build	
Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.	Yes
Verify that compiler flags are configured to enable all available buffer overflow protections and warnings, including stack randomization, data execution prevention, and to break the build if an unsafe pointer, memory, format string, integer, or string operations are found.	Yes
Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.	Yes

Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.	Yes
Dependency	
Verify that third party components come from pre-defined, trusted and continually maintained repositories.	Yes
Verify that the attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behavior into the application.	Yes
Validate HTTP Request Header Requirements	
Verify that HTTP headers added by a trusted proxy or SSO devices, such as bearer token, are authenticated by the application.	Yes
Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 3	
General Authenticator Requirements	
Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.	Yes
Verify that where a credential service provider (CSP) and the application verifying authentication are separated, mutually authenticated TLS is in place between the two endpoints.	Yes
Session Logout and Timeout Requirements	
If authenticators permit users to remain logged in, verify that re-authentication occurs periodically with 2FA both when actively used after 12 hours or after an idle period of 15 minutes	Yes
Algorithms	
Verify that encrypted data is authenticated via signatures, authenticated cipher modes, or HMAC to ensure that ciphertext is not altered by an unauthorized party	Yes
General Data Protection	

Verify that regular backups of important data are performed and that test restoration of data is performed.	Yes
Verify that backups are stored securely to prevent data from being stolen or corrupted.	Yes
Malicious Code Search	
Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.	Yes
Verify that the application source code and third party libraries does not contain time bombs by searching for date and time related functions.	Yes
Verify that the application source code and third party libraries does not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.	Yes
Verify that the application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.	Yes

a. Attachment B: Supporting Documentation

Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 1

Password Security Requirements

Verify that user set passwords are at least 8 characters in length (after multiple spaces are combined).

1. Onboarding and Identity Verification with Voatz: See video at time 0:46.
   https://vimeo.com/533255584/1baa3910a6

2. Blockchain Technology Pilot Using Mobile Voting, City of Chandler, AZ: See time 0:46.
   https://www.chandleraz.gov/government/elections-and-voting/blockchain-mobile-voting

   Comments: Voatz mobile apps mandate a minimum of 8 characters (iOS devices require an 8-digit PIN and Android devices require a 12-digit PIN). Web apps require a complex 10 char or more password

Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters.

1. Ticket VMA-1895: [iOS] Transition from numeric PIN to complex password
   In order to improve both the security and usability of the Voatz App, we are currently transitioning away from a PIN based access to complex password based approach and the support for 64-128 character length passwords is in active development as per the updated NIST guidelines from October 2020.

   Notable aspects of the NIST recommendations:

   - Minimum password length of 8 characters.
   - Accept at least 64 characters.
   - Limit passwords to 128 characters.

2. Ticket VMA-1896: [Android] Transition from numeric PIN to complex password
   In order to improve both the security and usability of the Voatz App, we are currently transitioning away from a PIN based access to complex password based approach and the support for 64-128 character length passwords is in active development as per the updated NIST guidelines from October 2020.

   Notable aspects of the NIST recommendations:

   - Minimum password length of 8 characters.
   - Accept at least 64 characters.
   - Limit passwords to 128 characters.

   Comments: Internal work tickets Ticket VMA-1895: [iOS] and VMA-1896: [Android] are being used to track this change that is scheduled to be ready for rollout by the end of January 2022.

Verify that password truncation is not performed. However, consecutive multiple spaces may be replaced by a single space.

1. The Voatz mobile applications don't perform password truncation in compliance with updated NIST guidance below from October 2020.

   Notable aspects of the NIST recommendations:

   NIST 800-63B, Section 5.1.1.2: Memorized Secret Verifiers:
   Truncation of the secret SHALL NOT be performed.

2. The Voatz web applications don't perform password truncation in compliance with updated NIST guidance below from October 2020.

   Notable aspects of the NIST recommendations:

   NIST 800-63B, Section 5.1.1.2: Memorized Secret Verifiers:
   Truncation of the secret SHALL NOT be performed.

   Comments:

Verify that any printable Unicode character, including language neutral characters such as spaces and emojis are permitted in passwords.

1. Ticket VMA-1895: [iOS] Transition from numeric PIN to complex password
   In order to improve both the security and usability of the Voatz Apps, we are currently transitioning away from a PIN based access to complex password based approach and the support for such characters is in active development as per the updated NIST guidelines from October 2020.

   Notable aspects of the NIST recommendations:

   - No restrictions on character combinations (for e.g. requiring uppercase, lowercase, number and special character)
   - No restrictions on any printable Unicode character, including emojis.

2. Ticket VMA-1896: [Android] Transition from numeric PIN to alphanumeric password
   In order to improve both the security and usability of the Voatz Appw, we are currently transitioning away from a PIN based access to complex password based approach and the support for such characters is in active development as per the updated NIST guidelines from October 2020.

   Notable aspects of the NIST recommendations:

   - No restrictions on character combinations (for e.g. requiring uppercase, lowercase, number and special character)
   - No restrictions on any printable Unicode character, including emojis.

Comments: Currently, only numerical PINs are supported in the mobile apps for accessibility reasons. Internal work tickets Ticket VMA-1895: [iOS] and VMA-1896: [Android] are being used to track this change that is scheduled to be ready for rollout by the end of January 2022.

Verify users can change their password.

1. Internal work ticket VMA-2002: [iOS] supports this change.

2. Internal work ticket VMA-2014: [Android] supports this change

   Comments: To prevent misuse, the Voatz platform currently requires the user to go through a comprehensive re-verification and account reset workflow to change the password. As part of Internal work tickets Ticket VMA-1895: [iOS] and VMA-1896: [Android], this feature is being enhanced and is scheduled to be ready for rollout by the end of January 2022.

Verify that password change functionality requires the user's current and new password.

1. Ticket VMA-1895: [iOS] Transition from numeric PIN to complex password

2. Ticket VMA-1896: [Android] Transition from numeric PIN to complex password

   Comments: To prevent misuse, the Voatz platform currently requires the user to go through a comprehensive re-verification and account reset workflow to change the password. As part of Internal work tickets Ticket VMA-1895: [iOS] and VMA-1896: [Android], this feature is being enhanced and is scheduled to be ready for rollout by the end of January 2022.

Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's password policy) or using an external API. If using an API a zero knowledge proof or other mechanism should be used to ensure that the plain text password is not sent or used in verifying the breach status of the password. If the password is breached, the application must require the user to set a new non-breached password.

1. Ticket VMA-1895: [iOS] Transition from numeric PIN to complex password
   In order to improve both the security and usability of the Voatz App, we are transitioning away from a PIN based access to complex password based. As part of this work, integration with the Enzoic API is being implemented to check against a known set of breached passwords.
   https://www.enzoic.com/docs-passwords-api/

   Notable aspects of the NIST recommendations:

   - Restrict passwords appearing in a blacklist dictionary.

2. Ticket VMA-1896: [Android] Transition from numeric PIN to complex password
   In order to improve both the security and usability of the Voatz App, we are transitioning away from a PIN based access to complex password based. As part of this work, integration with the Enzoic API is being implemented to check against a known set of breached passwords.
   https://www.enzoic.com/docs-passwords-api/

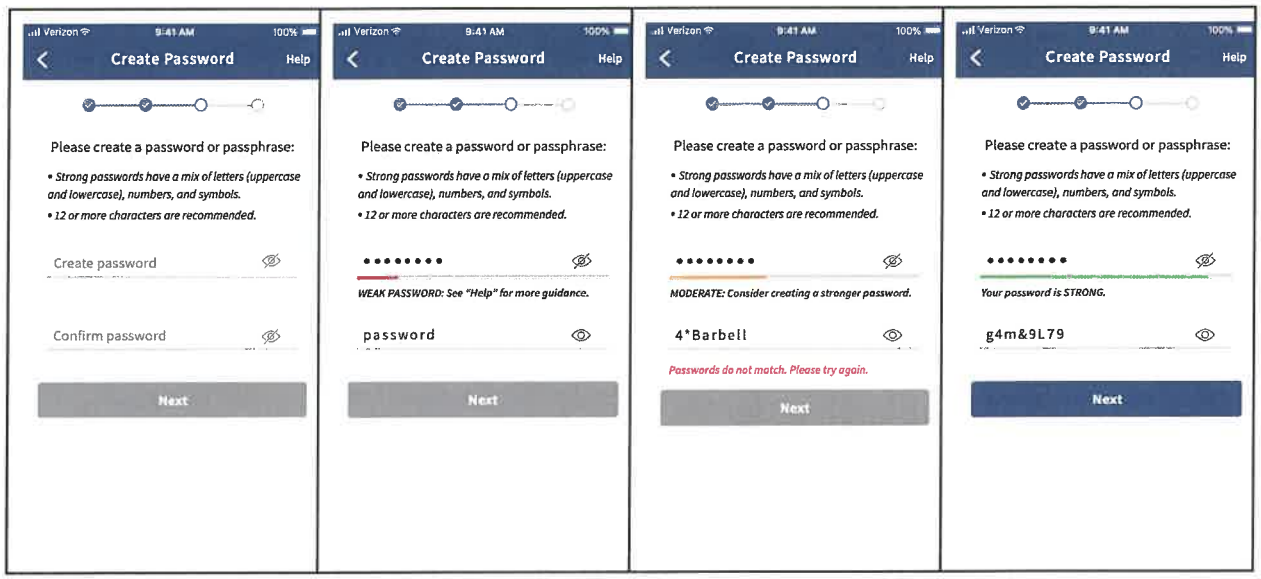
Notable aspects of the NIST recommendations:

- Restrict passwords appearing in a blacklist dictionary.

Comments: This feature is in active development and will be included in VMA in time for the spring primaries. Passwords will be checked to make sure that they do not appear in a blacklist dictionary.

Verify that a password strength meter is provided to help users set a stronger password.

1. Please see sample screens below from work tickets VMA-1895 and VMA-1896.



2. Ticket VMA-1895 and VMA-1896 for iOS and Android: Transition from numeric PIN to complex password.
   - Provide a strength indicator to users.

Comments: This feature enhancement is in active development and will be available for rollout by the end of January 2022. Four security levels will be shown: Gray for no password, Red for insecure passwords (less than 48 bits of entropy), Yellow for passwords of moderate (48 to 64 bits) entropy, and Green for high (more than 64 bits) entropy.

Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters.

1. Ticket VMA-1895 for iOS: Transition from numeric PIN to complex password.

NIST updated its recommendations in October 2020. Notable aspects of the NIST recommendations:

- No restrictions on character combinations (for e.g. requiring uppercase, lowercase, number and special character).

2. Ticket VMA-1896 for Android: Transition from numeric PIN to complex password.

NIST updated its recommendations in October 2020. Notable aspects of the NIST recommendations:

- No restrictions on character combinations (for e.g. requiring uppercase, lowercase, number and special character).

Comments: This feature is in active development and will be available for rollout by the end of January 2022

Verify that there are no periodic credential rotation or password history requirements.

1. This is fully supported on all customer facing mobile platforms in accordance with the updated guidance from NIST in October 2020. Notable aspects of the NIST recommendations:

   NIST 800-63B, Section 5.1.1.2: Memorized Secret Verifiers:
   Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).

2. This is fully supported on all customer facing web platforms in accordance with the updated guidance from NIST in October 2020. Notable aspects of the NIST recommendations:

   Notable aspects of the NIST recommendations:
   NIST 800-63B, Section 5.1.1.2: Memorized Secret Verifiers:
   Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).

   Comments: This feature is currently implemented.

Verify that "paste" functionality, browser password helpers, and external password managers are permitted.

1. Ticket VMA-1895 for iOS: Transition from numeric PIN to alphanumeric password.
   NIST updated its recommendations in October 2020. Notable aspects of the NIST recommendations:
   Allow integration/paste with password managers.
   - Test with: LastPass, 1Password, Dashlane, Keeper.

2. Ticket VMA-1896 for Android: Transition from numeric PIN to alphanumeric password.

NIST updated its recommendations in October 2020. Notable aspects of the NIST recommendations:

Allow integration/paste with password managers.

- Test with: LastPass, 1Password, Dashlane, Keeper.

Comments: This feature is in active development and will be included for production rollout in time for the spring primaries, though we may not allow paste functionality for security reasons.

Verify that the user can choose to either temporarily view the entire masked password, or temporarily view the last typed character of the password on platforms that do not have this as a built-in functionality.

1. Onboarding and Identity Verification with Voatz: See time 0:53.
   https://vimeo.com/533255584/1baa3910a6

2. Blockchain Technology Pilot Using Mobile Voting, City of Chandler, AZ: See time 0:53.
   https://www.chandleraz.gov/government/elections-and-voting/blockchain-mobile-voting

   Comments: Please see the above videos for reference.

General Authenticator Requirements

Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

1. From a voter authentication module:

```
val throttleInterval = if(attempt == 0){
  30 + Cryptography.issueRandomInt(1, 10)
}else{
  val min = (attempt)*10
  val max = (attempt+1)*10
  latestInterval + Cryptography.issueRandomInt(min, max)
```

2. Tickets VMA-1895 and VMA-1896: [iOS] and [Android] Transition from numeric PIN to alphanumeric password
   In order to improve both the security and usability of the Voatz App, we are transitioning away from a PIN based access to password based.

NIST updated its recommendations in October 2020. Notable aspects of the NIST recommendations:

- Restrict passwords appearing in a blacklist dictionary.

Comments: VMA is throttled at each failed login attempt, initially at least 30 seconds, with successive login attempts being throttled by at least 40 seconds, 60 seconds, 90 seconds, and so on. There can be no more than 12 failed attempts per hour.

Verify that the use of weak authenticators (such as SMS and email) is limited to secondary verification and transaction approval and not as a replacement for more secure authentication methods. Verify that stronger methods are offered before weak methods, users are aware of the risks, or that proper measures are in place to limit the risks of account compromise.

1. Onboarding and Identity Verification with Voatz
   https://vimeo.com/533255584/1baa3910a6

2. Blockchain Technology Pilot Using Mobile Voting, City of Chandler, AZ: See time 0:53.
   https://www.chandleraz.gov/government/elections-and-voting/blockchain-mobile-voting

   Comments: Biometric verification is included as a standard feature on the Voatz platform and is offered as the first choice before the users are permitted to change to a weaker method. Additionally, identity verification and liveness checks along with digital signature verification are used as well.

Verify that secure notifications are sent to users after updates to authentication details, such as credential resets, email or address changes, logging in from unknown or risky locations. The use of push notifications - rather than SMS or email - is preferred, but in the absence of push notifications, SMS or email is acceptable as long as no sensitive information is disclosed in the notification.

1. From the onboarding module:
   def notifyIfEmailOrMobileDifferentFromSignup(mobileNumber, emailAddress,…)
   val preRegEmail = customerPreregSnap.emailAddress.trim
   val reqEmail = emailAddress.trim
   val emailMatch = preRegEmail.equalsIgnoreCase(reqEmail)

   RegistrationSettingsAsync.getRegistrationSettings() map{registrationSettings =>
   if(!emailMatch){
   MessagingAsync.sendReregisterWithDiffEmailOrMobileNotification(preRegEmail, reqEmail, ...

2. From the onboarding module:
   val preRegMobile = customerPreregSnap.mobileNumber
   val mob ileMatch = preRegMobile.equalsIgnoreCase(mobileNumber)
   RegistrationSettingsAsync.*getRegistrationSettings*() map{registrationSettings =>
   if(!mobileMatch){
   MessagingAsync.*sendReregisterWithDiffEmailOrMobileNotification*(preRegEmail, mobileNumber,...

   Comments: The user is notified of any updates to authentication details via well defined notifications.

Authenticator Lifecycle Requirements

Verify system generated initial passwords or activation codes SHOULD be securely randomly generated, SHOULD be at least 6 characters long, and MAY contain letters and numbers, and expire after a short period of time. These initial secrets must not be permitted to become the long term password.

1. In a voter onboarding module:

   val totp = Totp(Cryptography.issueRandomKey(256).getBytes, 6, SHA256, 30).generate()

2. Onboarding and Identity Verification, see example at 0:33:
   https://vimeo.com/533255584/1baa3910a6

   Comments: Two 6-digit activation codes are sent: one is a push notification sent to the mobile device and another to the supplied email address. Neither code is long enough to be the long-term password.

Credential Recovery Requirements

Verify that a system generated initial activation or recovery secret is not sent in clear text to the user.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - storage on disk, particularly secrets and user passwords.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-STORAGE-7: **Pass**, June 19, 2020.

   Comments: The initial activation is sent via push notification, which is transmitted over https.

Verify password hints or knowledge-based authentication (so-called "secret questions") are not present.

1. Onboarding and Identity Verification with Voatz.
   https://vimeo.com/533255584/1baa3910a6

2. Blockchain Technology Pilot Using Mobile Voting, City of Chandler, AZ.
   https://www.chandleraz.gov/government/elections-and-voting/blockchain-mobile-voting

   Comments: The examples above show that no such hints are present in the app.

Verify password credential recovery does not reveal the current password in any way.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-7: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-7: **Pass**, June 19, 2020.

   Comments:

Verify shared or default accounts are not present (e.g. "root", "admin", or "sa").

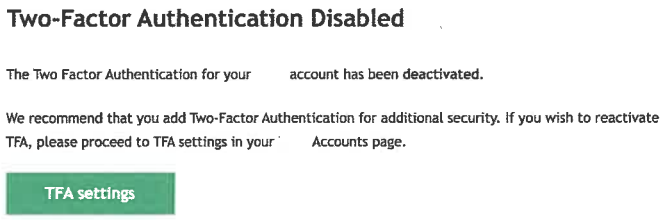
1. Policy A.9: Access Control Policy, Section 3.0: Business Requirements:
   Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz aims for a layered approach to manage access to corporate and elections assets which includes:
   Not permitting the use of shared account credentials.

   Comments: Account creation involves verifying phone number and email address, linking the device to a specific user.

Verify that if an authentication factor is changed or replaced, that the user is notified of this event.

1. One notification is sent to the user using a primary factor (e.g. email or mobile number) along with information for remediation in case of malicious activity detection.



2. A secondary notification is delivered using an alternate channel (e.g. push notification or backup email/mobile number).

   Comments:

Verify forgotten password, and other recovery paths use a secure recovery mechanism, such as TOTP or other soft token, mobile push, or another offline recovery mechanism.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-5: **Pass**, June 19, 2020.

   Comments: Secure push notifications are used to recover an account.

Out of Band Verifier Requirements

Verify that clear text out of band (NIST "restricted") authenticators, such as SMS or PSTN, are not offered by default, and stronger alternatives such as push notifications are offered first.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-5: **Pass**, June 19, 2020.

   Comments: Push notifications are offered as a first preference by default.

Verify that the out of band verifier expires out of band authentication requests, codes, or tokens after 10 minutes.

1. From the voter onboarding module:
   ```
   def checkOtpTimestamp(otpTimestamp: String, nowTimestamp: String, onBoardingLimits:
   OnboardingLimitsSnapshot): Boolean = {
     val now = OffsetDateTime.parse(nowTimestamp)
     val otpts = OffsetDateTime.parse(otpTimestamp)
     val differenceInSeconds = ChronoUnit.SECONDS.between(otpts, now)
     differenceInSeconds <= onBoardingLimits.timeout
   ```

2. Voter onboarding limits are defined as:
   ```
   (timeout: Int, consecutiveRequestInterval: Int, consecutiveRequests: Int,
   consecutiveRequestFromSameIpInterval: Int,
     consecutiveRequestsFromSameIp: Int)
   ```
   where timeout is configured as 600 (10 minutes * 60 seconds)

   Comments: The timeout for out of band auth requests, codes or tokens can be set as desired by the jurisdiction.

Verify that the out of band verifier authentication requests, codes, or tokens are only usable once, and only for the original authentication request.

1. From a voter onboarding module:

   ```
   else if(otpAlreadyVerified){
    log.error(s"otp $otp already verified for mobile $mobileNumber")
    val err = "An error occurred. Please request new codes."
   ```

2. ```
   else if(!sideChannelSnapOpt.isDefined || !sideChannelSnapOpt.get.otpTimestamp.isDefined) {
                log.error(s"No verified side channel otp record found for preRegisterId $preRegId")
   ```

   Comments: The server checks if the one-time push notification had been already used or if it came from a different mobile phone. In either case, the verification request is rejected.

Verify that the out of band authenticator and verifier communicates over a secure independent channel.

1. Push notifications are used as one of the secure independent communication channel

2. In app auth codes or code delivery via sms/voice calls are used as additional independent channels
   ```

Comments: Voatz integrates seamlessly with third party services such as the Duo App, Google Authenticator, Authy App, Microsoft Authenticator, etc.

Single or Multi-factor One Time Verifier Requirements

Verify that time-based OTPs have a defined lifetime before expiring.

1. From a voter onboarding module:

```
if(checkOtpTimestamp(snapshot.timestamp, timestamp, onBoardingLimits)){
  ...
}
else{
  val error = "Otp timeout was exceeded"
```

2. From an API routing module:

```
setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true, secure =
config.HttpConfig.UseHttps, expires =
```

Comments: Time-based OTPs have a well defined timeout setting to eliminate any possibility of expired OTPs from being used.

Fundamental Session Management Requirements

Verify the application never reveals session tokens in URL parameters.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
    - All web applications via the most secure version of SSL/TLS.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - App/client communication with back end infrastructure.

   Comments: Session tokens are transmitted in HTTP headers, but not the URL.

Session Binding Requirements

Verify the application generates a new session token on user authentication.

1. From a voter authentication module:

```
def createSession(customerId: Int): HttpApiSession = {
  val userHash = Cryptography.hash64(customerId.toString())
  val sessionCookie = Cryptography.hash64(Cryptography.issueRandomKey(64) + userHash)
  val csrfToken = Cryptography.issueRandomKey(64)
```

2. From an API routing module:

```
respondWithHeader(RawHeader(CsrfToken, session.csrfToken)) {
  setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true, secure =
config.HttpConfig.UseHttps,
  expires =
```

   Comments: A new session token is generated with each API call to a Voatz server.

Verify that session tokens possess at least 64 bits of entropy.

1. From an authentication module:

```
csrfToken = Cryptography.issueRandomKey(64)
```

2. Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management,
   Key generation must be seeded from an industry standard random number generator.

   Comments: Session tokens are derived from a cryptographically secure random number generator and have 256 bits of entropy.

Verify the application only stores session tokens in the browser using secure methods such as appropriately secured cookies (see section 3.4) or HTML 5 session storage.

1. From an API router module:

```
validate(sessionCookie, csrfToken)
```

2. HttpApiSession(sessionCookie: String, csrfToken: String, customerId: Int, lastUse: Long)

   Comments: Further, on a mobile device, the session token is stored in restricted device storage.

Session Logout and Timeout Requirements

Verify that logout and expiration invalidate the session token, such that the back button or a downstream relying party does not resume an authenticated session, including across relying parties.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-AUTH-4: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-AUTH-4: **Pass**, June 19, 2020.

   Comments: Upon logging out, the session is deleted in the database, so it cannot be resumed.

Cookie Based Session Management

Verify that cookie-based session tokens have the 'Secure' attribute set.

1. From a voter authentication module:

   setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true, secure = true

2. From an API configuration module:

   val UseHttps = httpConfig.getBoolean("use-https")

   Comments: All communications with Voatz servers are over https, so session tokens have the Secure attribute set.

Verify that cookie-based session tokens have the 'HttpOnly' attribute set.

1. From a voter authentication module:

   setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true,

2. CSRF token from an organization authentication module:

   HttpCookie(CsrfToken, payload.csrfToken, httpOnly = true, secure = true

   Comments:

Verify that cookie-based session tokens utilize the 'SameSite' attribute to limit exposure to cross-site request forgery attacks.

1. CSRF tokens are used to prevent such attacks. From a voter authentication module:

   respondWithHeader(RawHeader(CsrfToken, session.csrfToken))

2. General cookies sent to any client using the API router include a CSRF token. From an API session authentication module:

   session = HttpApiSession(sessionCookie, csrfToken, customerId, System.currentTimeMillis)

   Comments:

Verify that cookie-based session tokens use "__Host-" prefix (see references) to provide session cookie confidentiality.

1. From the API routing module
   setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true, secure = true,expires = Some(DateTime.now.+(validInterval)), domain = domainVal, path = pathVal)) {

2. From another API routing module:

   setCookie(HttpCookie(SessionCookie, payload.sessionCookie, httpOnly = true, secure = config.HttpConfig.UseHttps,
   expires = Some(DateTime.now.+(cookieExpiration)), domain = domainVal, path = pathVal),

   Comments: The routing module sets the domain and path along with the Secure prefix set to true which offers the security offered by the Host prefix. Like the Host prefix, cookies with the Secure prefix can only be set from a secure connection.

Verify that if the application is published under a domain name with other applications that set or use session cookies that might override or disclose the session cookies, set the path attribute in cookie-based session tokens using the most precise path possible.

1. From a voter API router module:

   setCookie(HttpCookie(SessionCookie, session.sessionCookie, httpOnly = true, secure = true,
   expires = Some(DateTime.now.+(validInterval)), domain = domainVal, path = Some(pathVal)))

2. From an API routing module:

   def allRoutes: Route = encodeResponse {
   path(

   Comments: The API router controls the path precision by defining the paths that are allowed for an HTTP request to make.

General Access Control Design

Verify that the application enforces access control rules on a trusted service layer, especially if client-side access control is present and could be bypassed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-AUTH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-AUTH-1: **Pass**, June 19, 2020.

   Comments: Any operation which requires API calls to a Voatz server requires certain authentication and authorization, which are tightly controlled.

Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.

1. Policy A.9: Access Control Policy, Section 1.0 Purpose
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

2. Policy A.12: Operational Security Policy, Section 9.0 Technical Vulnerability Management
   Voatz limits lateral movement through the network by implementing least privilege and segregating the network into corporate and elections, and further into development, test, and production environments with limited and monitored access across.

   Comments: User data, which in this case is voter data and election-specific data, can only be manipulated by those with appropriate authorization. Most importantly, however, the most crucial data, marked ballots and affidavits, cannot be modified.

Verify that the principle of least privilege exists - users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization. This implies protection against spoofing and elevation of privilege.

1. From Policy A.9: Access Control Policy, Section 3.0: This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

   - Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
   - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
   - Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
   - Need to Use – users will only be able to access physical and logical facilities required for their role.

2. Policy AC9: Server Security, Section 4.2 General Configuration and Backup Guidelines:
   Always use the least privilege to perform a function. Do not use root/admin accounts when a non-privileged account is sufficient.

   Comments:

Verify that the principle of deny by default exists whereby new users/roles start with minimal or no permissions and users/roles do not receive access to new features until access is explicitly assigned.

1. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

   - Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
   - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;

2. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.
   - Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
   - Need to Use – users will only be able to access physical and logical facilities required for their role.

   Comments:

Verify that access controls fail securely including when an exception occurs.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-6: **Pass**, June 19, 2020.

   Comments:

Operation Level Access Control

Verify that the sensitive data and APIs are protected against Insecure Direct Object Reference (IDOR) attacks targeting creation, reading, updating and deletion of records, such as creating or updating someone else's record, viewing everyone's records, or deleting all records.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application Encryption shall be implemented in:
   - During sensitive data transmission over public networks

2. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS.

Comments: All data in flight is encrypted via AES GCM with non repeating nonce. Additionally, each API is secured by authorization checks of the form:

```
val snapByDevIdOptFut = UserModule.getByDeviceId(apiRequest.deviceId, sessionCookieOpt)
snapByDevIdOptFut onComplete {
 case Success(snapByDevIdOpt) => {
  if (!snapByDevIdOpt.isDefined) {
   val err = "user not found"
  }else {
 val userIdFromDevId = snapByDevIdOpt.get
 SessionAuthenticatorAsync.validateSessionAgainstUser(sessionCookieOpt, userIdFromDevId)
onComplete{
  case Success(sessionValid) => {
   if(!sessionValid){
    theSender ! ForbiddenError("Session cookie provided does not authorize you to perform this
action")
   }else{
    if (userIdFromDevId != request.userId) {
     theSender ! ForbiddenError("Supplied deviceId does not belong to requested user")
    } else {
```

where the user attached to the device sending the request is validated against the user holding the current session, which in turn is matched against the user making the request, thus eliminating the possibility of IDOR attacks.

Verify that the application or framework enforces a strong anti-CSRF mechanism to protect authenticated functionality, and effective anti-automation or anti-CSRF protects unauthenticated functionality.

1. CSRF tokens are used to prevent such unauthenticated functionality. From a voter authentication module:

   respondWithHeader(RawHeader(CsrfToken, session.csrfToken))

2. General cookies sent to any client using the API router include a CSRF token. From an API session authentication module:

   session = HttpApiSession(sessionCookie, csrfToken, customerId, System.currentTimeMillis)

   Comments: CSRF tokens disallow all unauthenticated functionality.

Other Access Control Considerations

Verify administrative interfaces use appropriate multi-factor authentication to prevent unauthorized use.

1. Policy AC.5: Password Policy, Section 5.1: General:
   Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.

2. Policy A.9: Access Control Policy, Section 6.4 - Use of Privileged Utility Programs:
   - Where possible and appropriate privileged utility programs must incorporate multi-factor authentication (MFA).

   Comments: The election administration portal ensures that 2FA via 3rd party 2FA apps such as DUO is enforced on every authentication attempt.

Verify that directory browsing is disabled unless deliberately desired. Additionally, applications should not allow discovery or disclosure of files or directory metadata such as Thumbs.db, .DS_Store, .git or .svn folders.

1. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

   - Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
   - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;

2. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.
   - Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
   - Need to Use – users will only be able to access physical and logical facilities required for their role.

   Comments: Directory browsing is not allowed and applications do not allow unauthorized users to view files and directory metadata.

Input Validation Requirements

Verify that the application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, or environment variables).

1. N/A

2. N/A

   Comments: N/A: Voatz applications and servers never concatenate unvalidated user input into urls, eliminating the possibility of injecting query string delimiters to perform a malicious task via an HPP attack. No API endpoints make use of unvalidated query string parameters.

Verify that frameworks protect against mass parameter assignment attacks, or that the application has countermeasures to protect against unsafe parameter assignment, such as marking fields private or similar.

1. N/A

2. N/A

   Comments: N/A: Voatz applications and servers use explicit parameter assignment with strong type checking, eliminating the possibility of any mass parameter assignment attacks.

Verify that all input (HTML form fields, REST requests, URL parameters, HTTP headers, cookies, batch files, RSS feeds, etc) is validated using positive validation (whitelisting).

1. From an API routing module:

   ```
   def allRoutes: Route = encodeResponse {  // formerly compressResponse()
    path(
   ```

2. From an API routing module:

   ```
   private def heartbeat() = post {
   ```

   Comments: The API router has explicit validation of requests as above, only accepting post requests and only to white-listed APIs.

Verify that structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as checking that suburb and zip/postcode match).

1. Server code is written in Scala, which is a strongly typed language.

2. All data is checked for allowed characters, length, etc. as appropriate. Data from addresses taken from official ID is checked against USPS data for validity.

   Comments:

Verify that URL redirects and forwards only allow whitelisted destinations, or show a warning when redirecting to potentially untrusted content.

1. From an API routing module:

   def allRoutes: Route = encodeResponse { // formerly compressResponse()
   path(

2. From an API routing module:

   handleNotFound {
   log.error(s"The requested resource could not be found")

   Comments: The API router has explicit validation of requests as above, only accepting post requests and only to whitelisted APIs; Any request to a non whitelisted resource is denied.

Sanitization and Sandboxing Requirements

Verify that all untrusted HTML input from WYSIWYG editors or similar is properly sanitized with an HTML sanitizer library or framework feature.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that unstructured data is sanitized to enforce safety measures such as allowed characters and length.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application sanitizes user input before passing to mail systems to protect against SMTP or IMAP injection.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application avoids the use of eval() or other dynamic code execution features. Where there is no alternative, any user input being included must be sanitized or sandboxed before being executed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application protects against template injection attacks by ensuring that any user input being included is sanitized or sandboxed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application protects against SSRF attacks, by validating or sanitizing untrusted data or HTTP file metadata, such as filenames and URL input fields, use whitelisting of protocols, domains, paths and ports.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application sanitizes, disables, or sandboxes user-supplied SVG scriptable content, especially as they relate to XSS resulting from inline scripts, and foreignObject.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application sanitizes, disables, or sandboxes user-supplied scriptable or expression template language content, such as Markdown, CSS or XSL stylesheets, BBCode, or similar.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Output Encoding and Injection Prevention Requirements

Verify that output encoding is relevant for the interpreter and context required. For example, use encoders specifically for HTML values, HTML attributes, JavaScript, URL Parameters, HTTP headers, SMTP, and others as the context requires, especially from untrusted inputs (e.g. names with Unicode or apostrophes, such as ãã“ or O'Hara).

1. From API routing module:
   import org.owasp.encoder.Encode
   ctx.complete(HttpResponse(StatusCodes.OK, Encode.forHtml(e.getMessage()), getAllHeaders))

2. From API routing module:
   import org.owasp.encoder.Encode
   ctx.complete(*HttpResponse*(StatusCodes.*InternalServerError*, Encode.*forHtml*(e.getMessage()), getAllHeaders))
   complete(*HttpResponse*(*BadRequest*, Encode.*forHtml*(message), getAllHeaders))

   Comments: Voatz servers use relevant output encoders from OWASP.

Verify that output encoding preserves the user's chosen character set and locale, such that any Unicode character point is valid and safely handled.

1. From the validations module
   ```
   def convertStringFromHexToUTF8(str: String) = {
    val matcher = Pattern.compile("\\\\x[a-z0-9]{2}\\\\x[a-z0-9]{2}").matcher(str)
    val sb = new StringBuilder
    try {
      while (matcher.find) {
        sb.append(matcher.group(0))
      }
    }catch{
      case e: Exception => log.error(s"error matching $str with pattern for unicode hex strings: " +
   e.getMessage)
    }
    val s = sb.toString
    str.replace(s, new String(getHexBytes(s), StandardCharsets.UTF_8))
   }
   ```

   import org.apache.commons.codec.binary.Hex

```
def getHexBytes(s: String) = {
 try {
  Hex.decodeHex(s.replace("\\x", ""))
 }catch{
  case e: Exception => log.error(s"error converting $s from hex to byte array" +
e.getMessage);Array[Byte]()
 }
}
```

2. From the validations module
   import org.apache.commons.lang3.StringUtils
   StringUtils.*stripAccents*(lastNameFromUser).replace("`", "")
   .replace("'", "").replace("'", "").replace(".", "")

   Comments: Voatz applications and servers preserve the user's chosen character set and locale by using standard Apache Commons libraries.

Verify that context-aware, preferably automated - or at worst, manual - output escaping protects against reflected, stored, and DOM based XSS.

1. From user verification api response
   < Content-Type: application/json; charset=UTF-8
   < Content-Length: 3888
   < X-Content-Type-Options: nosniff
   < X-XSS-Protection: 1; mode=block

2. From user login api response
   < Csrf-Token: nvhSh0hGnM+ufTna+4zoc0u+yeTmQ3zxX0LfWgnTpbk=
   < Content-Type: text/plain; charset=UTF-8
   < Content-Length: 2
   < Set-Cookie: WS=MZdQe4iMq/6HJJjkDvbBgjo655tM1JNBBWBQYj8XkeI=; Expires..

   Comments: Voatz applications and servers filter/sanitize input on arrival, properly encode data on output to prevent it from being interpreted as active content, and use appropriate response headers such as Content-Type to ensure that responses are interpreted as intended.

Verify that data selection or database queries (e.g. SQL, HQL, ORM, NoSQL) use parameterized queries, ORMs, entity frameworks, or are otherwise protected from database injection attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz applications and servers never create parameterized queries with unvalidated user input, thus eliminating the possibility of any database injection attacks.

Verify that where parameterized or safer mechanisms are not present, context-specific output encoding is used to protect against injection attacks, such as the use of SQL escaping to protect against SQL injection.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

Comments:

Verify that the application projects against JavaScript or JSON injection attacks, including for eval attacks, remote JavaScript includes, CSP bypasses, DOM XSS, and JavaScript expression evaluation.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

Comments:

Verify that the application protects against LDAP Injection vulnerabilities, or that specific security controls to prevent LDAP Injection have been implemented.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

Comments:

Verify that the application protects against OS command injection and that operating system calls use parameterized OS queries or use contextual command line output encoding.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

Comments:

Verify that the application protects against Local File Inclusion (LFI) or Remote File Inclusion (RFI) attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that the application protects against XPath injection or XML injection attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Deserialization Prevention Requirements

Verify that serialized objects use integrity checks or are encrypted to prevent hostile object creation or data tampering.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-8: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-8: **Pass**, June 19, 2020.

   Comments: Sensitive serialized objects are encrypted and all serialized objects are subject to rigorous exception and rejection handling.

Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that desterilization of untrusted data is avoided or protected in both custom code and third-party libraries (such as JSON, XML and YAML parsers).

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that when parsing JSON in browsers or JavaScript-based backends, JSON.parse is used to parse the JSON document. Do not use eval() to parse JSON.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Algorithms

Verify that all cryptographic modules fail securely, and errors are handled in a way that does not enable Padding Oracle attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-6: **Pass**, June 19, 2020.

   Comments: All modules are subject to rigorous exception and rejection handling.

Log Content Requirements

Verify that the application does not log credentials or payment details. Session tokens should only be stored in logs in an irreversible, hashed form.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-3: **Pass**, June 19, 2020.

   Comments:

Verify that the application does not log other sensitive data as defined under local privacy laws or relevant security policy.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-3: **Pass**, June 19, 2020.

   Comments:

Error Handling

Verify that a generic message is shown when an unexpected or security sensitive error occurs, potentially with a unique ID which support personnel can use to investigate.

1. Example from a voter onboarding module on the server:
   ```
   if(threatDetected){
     val threatName = threatNameOpt.get
     val err = s"Voatz has detected an unexpected issue with your device. Please quit the app and try again, or contact Voatz."
     log.error(s"Threat $threatName detected on device $deviceIdFromReq")
   ```

2. Policy AC.9: Server Security Policy, Section 4.3 Monitoring
   All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

   - Logs are accessible only to appropriate applications and trusted users.

   Comments: Generic error messages are shown to the user in order to stymie attempts by an attacker to deduce internal app and server logic.

Client-side Data Protection

Verify the application sets sufficient anti-caching headers so that sensitive data is not cached in modern browsers.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments:

Verify that data stored in client side storage (such as HTML5 local storage, session storage, IndexedDB, regular cookies or Flash cookies) does not contain sensitive data or PII.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments:

Verify that authenticated data is cleared from client storage, such as the browser DOM, after the client or session is terminated.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments:

Sensitive Private Data

Verify that sensitive data is sent to the server in the HTTP message body or headers, and that query string parameters from any HTTP verb do not contain sensitive data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-6: **Pass**, June 19, 2020.

   Comments:

Verify that users have a method to remove or export their data on demand.

1. From the user management module:
   ApiCleanupUserRequest(emailAddress: String, org: Option[Boolean], basic: Option[Boolean])

2. From the user management module:
   if(request.basic.getOrElse(false) && request.org.getOrElse(false)){
   Signups.*deleteAllForCustomer*(customerId)
   OrgVerificationProfile.*deleteAllForCustomer*(customerId)
   DatastoreKeyMap.*deleteAllForCustomer*(customerId)
   ControlNumber.*deleteAllForCustomer*(customerId)
   deleteAllBasicIdoRecords(customerId)
   ...
   else if(request.basic.getOrElse(false)){
   deleteAllBasicIdoRecords(customerId)
   deleteAllBasicIdvRecords(customerId)

   Comments: Voatz provides users with well defined options to remove their data on demand. However, access to such API/resources is strictly controlled to eliminate the possibility of misuse.

Verify that users are provided clear language regarding collection and use of supplied personal information and that users have provided opt-in consent for the use of that data before it is used in any way.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-12: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-12: **Pass**, June 19, 2020.

   Comments: This information is provided to the users in EULA and the app permissions from the Google Play Store and the Apple App Store

Verify that all sensitive data created and processed by the application has been identified, and ensure that a policy is in place on how to deal with sensitive data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments: All sensitive data is encrypted. Once sensitive data is no longer needed, it is deleted.

Deployed Application Integrity Controls

Verify that if the application has a client or server auto-update feature, updates should be obtained over secure channels and digitally signed. The update code must validate the digital signature of the update before installing or executing the update.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CRYPTO-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CRYPTO-3: **Pass**, June 19, 2020.

   Comments:

Verify that the application employs integrity protections, such as code signing or sub-resource integrity.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-1: **Pass**, June 19, 2020.

   Comments:

The application must not load or execute code from untrusted sources, such as loading includes, modules, plugins, code, or libraries from untrusted sources or the Internet.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments:

Verify that the application has protection from sub-domain takeovers if the application relies upon DNS entries or DNS sub-domains, such as expired domain names, out of date DNS pointers or CNAMEs, expired projects at public source code repos, or transient cloud APIs, serverless functions, or storage buckets (autogen-bucket-id.cloud.example.com) or similar. Protections can include ensuring that DNS names used by applications are regularly checked for expiry or change.

1. Voatz has domain/sub-domain protection measures enabled at each of its registrars that include periodic rotation of DNSSEC keys

2. Voatz has set up weekly alerts at its DNS registrars that provide summary updates on any upcoming expiries or attempts to tamper with its DNS entries.

   Comments:

Business Logic Security Requirements

Verify the application will only process business logic flows for the same user in sequential step order and without skipping steps.

1. Walker, Michael and Owens, Wendy. Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Marking (RABM) System, Pro V&V (May 28, 2020).

2. Walker, Michael and Owens, Wendy. Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System, Pro V&V (July 17, 2020).

   Comments:

Verify the application will only process business logic flows with all steps being processed in realistic human time, i.e. transactions are not submitted too quickly.

1. From the transaction validations module:

```
private def resolvePreconditions: Future[(Boolean, String)] = {
 resolveUser map{ userValidation =>
  if(!userValidation.valid){
   Future{Future{(false, userValidation.reason)}}
  }else{
   resolveEvent map{ eventValidation =>
    if(!eventValidation.valid){
     Future{(false, eventValidation.reason)}
    }else{
     resolveControlNumber map{ controlNumberValidation =>
      if(!controlNumberValidation.valid){
```

```
            (false, controlNumberValidation.reason)
          }else{
            (true, "")
          }
        }
      }
    }
  } flatMap(x => x) flatMap(y => y)
}
```

2. From the transaction validations module
   private def resolveCustomer: Future[ValidReasonPair] = {
   UserModule.*getByUserId*(...
   ...
   private def resolveEvent: Future[ValidReasonPair] = {
   EventModule.getByEventId(....
   ...
   private def resolveControlNumber: Future[ValidReasonPair] = {
   ControlNumberModule.*controlNumberValidAsFut*(userId, eventId
   ...

   Comments: Critical transactions are split into multiple steps as part of a state machine where subsequent steps check/validate successful completion of preceding steps and any failure detected results in rollback. This ensures that no transaction is submitted too eagerly.

Verify the application has appropriate limits for specific business actions or transactions which are correctly enforced on a per user basis.

1. Walker, Michael and Owens, Wendy. Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Marking (RABM) System, Pro V&V (May 28, 2020).

2. Walker, Michael and Owens, Wendy. Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System, Pro V&V (July 17, 2020).

   Comments: Strict controls in the app code and server restrict such transactions. Most importantly, users are restricted to a single cast ballot per election.

Verify the application has sufficient anti-automation controls to detect and protect against data exfiltration, excessive business logic requests, excessive file uploads or denial of service attacks.

1. Andreae, Philip; Braseth, Hilary; and Sawhney, Nimit. State-of-the-Art Security Performs First-Rate Threat Mitigation in Convention Elections, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/DR-V-Security-Whitepaper.pdf

2. Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf

Comments: Denial of Service attacks are prevented using multiple layers of defense, including DDoS attack mitigation provided through Cloudflare.

Verify the application has business logic limits or validation to protect against likely business risks or threats, identified using threat modeling or similar methodologies.

1. Andreae, Philip; Braseth, Hilary; and Sawhney, Nimit. State-of-the-Art Security Performs First-Rate Threat Mitigation in Convention Elections, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/DR-V-Security-Whitepaper.pdf

2. Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf

   Comments:

File Upload Requirements

Verify that the application will not accept large files that could fill up storage or cause a denial of service.

1. let router = RestApiRouter.submitDocumentImage(parameters: parameters)
   restApiManager.makeHTTPRequest(router: router) { response in
   let currentStatus = UploadStatus(image: nil, url: url, position: side, type: .imageToServer)

2. let router = RestApiRouter.submitUserImage(parameters: parameters)
   restApiManager.makeHTTPRequest(router: router) { response in
   let currentStatus = UploadStatus(image: nil, url: url, position: .faceDetection, type: .imageToServer)

   Comments: Voatz Mobile Apps only send HTTPS urls of user/document images uploaded to secure cloud storage with well defined IAM roles and bucket policies and never upload any files to the application/web tier directly, so there is no possibility of a denial of service.

File Execution Requirements

Verify that user-submitted filename metadata is not used directly with system or framework file and URL API to protect against path traversal.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz mobile apps never upload files directly to Voatz servers. Live document images/selfies are captured via the device camera and uploaded with strict file naming conventions to secure file storage with well defined IAM roles and bucket policies where micro services process the files further thus eliminating the possibility of path traversal attacks.

Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure, creation, updating or removal of local files (LFI).

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz mobile apps never upload files directly to Voatz servers. Live document images/selfies are captured via the device camera and uploaded with strict file naming conventions to secure file storage with well defined IAM roles and bucket policies where micro services process the files further thus eliminating the possibility of disclosure, creation, updating or removal of local files.

Verify that user-submitted filename metadata is validated or ignored to prevent the disclosure or execution of remote files (RFI), which may also lead to SSRF.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz mobile apps never upload files directly to Voatz servers. Live document images/selfies are captured via the device camera and uploaded with strict file naming conventions to secure file storage with well defined IAM roles and bucket policies where micro services process the files further thus eliminating the possibility of disclosure or execution of remote files.

Verify that the application protects against reflective file download (RFD) by validating or ignoring user-submitted filenames in a JSON, JSONP, or URL parameter, the response Content-Type header should be set to text/plain, and the Content-Disposition header should have a fixed filename.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz mobile apps never upload files directly to Voatz servers. Live document images/selfies are captured via the device camera and uploaded with strict file naming conventions to secure file storage with well defined IAM roles and bucket policies where micro services process the files further thus eliminating the possibility of RFD attacks

Verify that untrusted file metadata is not used directly with system API or libraries, to protect against OS command injection.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

Comments: No file metadata is ever used directly with system APIs. All files uploads employ secure cloud storage with well defined IAM roles and bucket policies eliminating any possibility of OS command injection.

File Storage Requirements

Verify that files obtained from untrusted sources are stored outside the web root, with limited permissions, preferably with strong validation.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

Comments: Files are never uploaded to the web server or application server directly. All file uploads employ secure cloud storage with well defined IAM roles and bucket policies.

Verify that files obtained from untrusted sources are scanned by antivirus scanners to prevent upload of known malicious content.

1. Andreae, Philip; Braseth, Hilary; and Sawhney, Nimit. State-of-the-Art Security Performs First-Rate Threat Mitigation in Convention Elections, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/DR-V-Security-Whitepaper.pdf

2. Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf

Comments: All file uploads employ secure cloud storage where files are processed via dedicated micro services that sanitize/scan uploads via Sophos followed by analyzing them for type, size and other metadata.

File Download Requirements

Verify that the web tier is configured to serve only files with specific file extensions to prevent unintentional information and source code leakage. For example, backup files (e.g. .bak), temporary working files (e.g. .swp), compressed files (.zip, .tar.gz, etc) and other extensions commonly used by editors should be blocked unless required.

1. From web config:
   <Files ~ "\.(bak|swp|zip|gz|cgi|shtml|phtml|php3?)$">
   Require all denied
   </Files>

2. The web server config explicitly denies file extensions to prevent unintentional information leakage.

   Comments:

Verify that direct requests to uploaded files will never be executed as HTML/JavaScript content.

1. N/A

2. N/A

   Comments: N/A: End users are never allowed to upload any files directly to Voatz servers. Files are uploaded internally via well defined micro services that communicate with secure cloud storage using private/restricted APIs employing strict access control and AES GCM encryption with non repeating nonce. Any files uploaded via mobile apps to secure cloud storage such as live document images/selfies for identity verification are secured via specific IAM roles and bucket policies.

SSRF Protection Requirements

Verify that the web or application server is configured with a whitelist of resources or systems to which the server can send requests or load data/files from.

1. Policy A.13: Network Security Policy, Section 4.0:
   All the traffic to and from a particular list of IPs and Domains (Blacklisted) should be denied at the Firewall Level.

2. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines:
   Operating System configuration should be in accordance with approved Voatz, Inc. IT guidelines. Services and applications that will not be used must be disabled where practical.

   Comments: Voatz web servers only communicate with whitelisted APIs on the application servers. Files are never uploaded to the web server or application server directly. All file uploads employ secure cloud storage with well defined IAM roles and bucket policies.

Generic Web Service Security Verification Requirements

Verify that all application components use the same encodings and parsers to avoid parsing attacks that exploit different URI or file parsing behavior that could be used in SSRF and RFI attacks.

1. From an API routing module (used by all application components):

   ```
   // Defines all of the routing supported.
   def allRoutes: Route = encodeResponse {
   ```

2. From an API routing module for receipts (used by all application components):

   ```
   routes = handleExceptions(exceptionHandler) {
    withRequestTimeoutResponse(request => timeoutResponse) {
   ```

   Comments:

Verify that access to administration and management functions is limited to authorized administrators.

1. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows least privilege when granting access to information and application system functionality.

   Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

2. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

   Comments: These restrictions apply to election administrators and Voatz system administrators alike.

Verify API URLs do not expose sensitive information, such as the API key, session tokens etc.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-7: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-7: **Pass**, June 19, 2020.

   Comments: Voatz API urls are obfuscated with random UUIDs that are rotated periodically eliminating the possibility of exposing sensitive information.

RESTful Web Service Verification Requirements

Verify that enabled RESTful HTTP methods are a valid choice for the user or action, such as preventing normal users using DELETE or PUT on protected API or resources.

1. From an API routing module:

   ```
   private def heartbeat() = post {
    requireAuthorization(Customer.View) {
   ```

2. From an API routing module:

   ```
   private def updateOrganizationUser() = put {
    requireAuthorization(OrganizationUser.Edit) {
     entity(as[OrganizationUserSnapshot]) { apiRequest =>
   ```

   Comments: Each API request is either a DELETE, GET, POST, or PUT request. Each request requires appropriate authentication. For example, put and delete requests require authentication that identifies the request as originating from an organization user, i.e., an election administrator. Every other request requires similar authentication, depending on the nature of the API request.

Verify that JSON schema validation is in place and verified before accepting input.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz APIs perform strict json validation for parameter types and mandatory/optional attributes. Such checks are automatically enforced by the routing layer and any requests that fail such
   checks are prevented from reaching the application layer.

Verify that RESTful web services that utilize cookies are protected from Cross-Site Request Forgery via the use of at least one or more of the following: triple or double submit cookie pattern (see references), CSRF nonces, or ORIGIN request header checks.

1. From an API routing module:

   ```
   protected val CsrfToken = "Csrf-Token"
   protected val SessionCookie = "WS"
   ```

2. From an API routing module:

   ```
   authenticateOrRejectWithChallenge[HttpApiSession](None =>
   SessionAuthenticatorAsync.validate(sessionCookie, csrfToken)
   ```

   Comments: CSRF tokens/nonces are used and origin request headers are checked in a CORS router inside the API router.

SOAP Web Service Verification Requirements

Verify that XSD schema validation takes place to ensure a properly formed XML document, followed by validation of each input field before any processing of that data takes place.

1. N/A

2. N/A

Comments: N/A: No SOAP based web services are used internally in any Voatz applications. No external SOAP based web services are invoked by any Voatz applications.

Dependency

Verify that all components are up to date, preferably using a dependency checker during build or compile time.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-6: **Pass**, June 19, 2020.

   Comments: Voatz uses OWASP's dependency check scanner that catalogs all open source components used in Voatz applications. Dependency check is integrated into SBT, Gradle and Jenkins CI server to automate dependency checks on each build.

Verify that all unneeded features, documentation, samples, configurations are removed, such as sample applications, platform documentation, and default or example users.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-1: **Pass**, June 19, 2020.

   Comments:

Verify that if application assets, such as JavaScript libraries, CSS stylesheets or web fonts, are hosted externally on a content delivery network (CDN) or external provider, Subresource Integrity (SRI) is used to validate the integrity of the asset.

1. Voatz admin portal js resources are bundled by webpack at build time and subresource integrity is added to these files by adding the -subresource-integrity option to the build script as follows:

   "ng build --subresource-integrity"

2. Once the flag is added, angular-cli automatically generates a hash for the application resources and adds to the index.html when running npm run build:

```
<script
 type="text/javascript"
 src="runtime.js"
 integrity="sha.."
 crossorigin="...">
</script
```

   Comments:

Unintended Security Disclosure Requirements

Verify that web or application server and framework error messages are configured to deliver user actionable, customized responses to eliminate any unintended security disclosures.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-4: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-4: **Pass**, June 19, 2020.

   Comments: Well defined error codes are used to ensure that the error is actionable, eliminating any unintended security disclosures. From the validations module:
   val *errorCodes*: Map[String, String] = *Map*("DAERR01" -> "Org. verification failed. Please contact your elections administrator",
   "DAERR02" -> "Attendance record already exists",
   "DCERR01" -> "A user account with the information provided already exists. Please login.")

Verify that web or application server and application framework debug modes are disabled in production to eliminate debug features, developer consoles, and unintended security disclosures.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-4: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-4: **Pass**, June 19, 2020.

   Comments: The logback config is set to ERROR in production to eliminate unintended security disclosures

Verify that the HTTP headers or any part of the HTTP response do not expose detailed version information of system components.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-6: **Pass**, June 19, 2020.

   Comments: No http responses contain such information.

HTTP Security Headers Requirements

Verify that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8, ISO 8859-1).

1. From verification API HTTP response:
   < Access-Control-Max-Age: 1728000

< Content-Type: application/json; charset=UTF-8
< Content-Length: 3888
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block

2. In an API router:

   HttpEntity(ContentTypes.`text/plain(UTF-8)`

   Comments: Each HTTP response contains the "Content-Type" header. Accepted types include UTF-8.

Verify that all API responses contain Content-Disposition: attachment; filename="api.json" (or other appropriate filename for the content type).

1. Response from user routing module
   respondWithHeader(`Access-Control-Expose-Headers`(*Seq*("Content-Disposition"))) {
   respondWithHeader(`Content-Disposition`("attachment", *Map*(("filename", payload.fileName))))
   {
   respondWithMediaType(MediaTypes.*`application/pdf`*) {

2. API response from a user routing module:
   respondWithMediaType(MediaTypes.*`application/pdf`*) {

   Comments: The Content-Disposition header is set, along with the Media Type on REST API responses.

Verify that a content security policy (CSPv2) is in place that helps mitigate impact for XSS attacks like HTML, DOM, JSON, and JavaScript injection vulnerabilities.

1. From verification API HTTP response
   < Access-Control-Max-Age: 1728000
   < Content-Type: application/json; charset=UTF-8
   < Content-Length: 3888
   < X-Content-Type-Options: nosniff
   < X-XSS-Protection: 1; mode=block

2. ISO Policy A.14.2.5 - Secure System Engineering Principles:
   Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

   Comments: The X-XSS-Protection response header stops the response payload from loading when a reflected cross-site scripting (XSS) attack is detected.

Verify that all responses contain X-Content-Type-Options: nosniff.

1. From verification API HTTP response
   < Access-Control-Max-Age: 1728000

< Content-Type: application/json; charset=UTF-8
< Content-Length: 3888
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block

2. All REST API responses contain X-Content-Type-Options: nosniff.

   Comments:

Verify that HTTP Strict Transport Security headers are included on all responses and for all subdomains, such as Strict-Transport-Security: max-age=15724800; includeSubdomains.

1. From verification API HTTP response
   < Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

2. All REST API responses contain Strict-Transport-Security: max-age=..; includeSubdomains.

   Comments:

Verify that a suitable "Referrer-Policy" header is included, such as "no-referrer" or "same-origin".

1. The following referrer policy is strictly enforced:
   For same-origin send the full Referrer, for cross-origin send only the origin, unless it's an HTTPS to HTTP request, in which case send nothing.

2. Voatz APIs enforce the strict-origin-when-cross-origin referrer policy in any pre-fight as well as subsequent real requests.

   Comments:

Verify that the content of a web application cannot be embedded in a third party site by default and that embedding of the exact resources is only allowed where necessary by using a suitable Content Security Policy: frame-ancestors and X-Frame-Options response headers.

1. Voatz admin portal employs the following tag to prevent the access from a website independently from the request.

   <meta http-equiv="X-Frame-Options" content="deny">

   This prevents the page from being displayed in a frame, regardless of the site that tries to do it. In additions CORS checks are used as well.

2. Voatz's voter-facing web applications employ the above checks along with additional domain whitelisting.

   Comments:

Validate HTTP Request Header Requirements

Verify that the application server only accepts HTTP methods in use by the application/API, including pre-flight OPTIONS and logs/alerts on any requests that are not valid for the application context.

1. From an API router module, which whitelists those methods and requests that are accepted.

   var *allHeaders* = *`Access-Control-Allow-Methods`*(HttpMethods.*OPTIONS,HttpMethods.POST*
   ...

2. From an API router module, which logs an error when a request cannot be completed.

   handleNotFound {
   log.error(s"The requested resource could not be found")
   complete(HttpResponse(NotFound, getAllHeaders, "The requested resource could not be found"))

   Comments: All REST APIs enforce the Access-Control-Allow-Methods header.

Verify that the supplied Origin header is not used for authentication or access control decisions, as the Origin header can easily be changed by an attacker.

1. From an API router:

   validate(sessionCookie, csrfToken)

2. HttpApiSession(sessionCookie: String, csrfToken: String, customerId: Int, lastUse: Long)

Comments: Authentication and access control are based on session cookies and CSRF tokens.

Verify that the Cross Origin Resource Sharing (CORS) Access-Control-Allow-Origin header uses a strict white-list of trusted domains to match against and does not support the "null" origin.

1. From a CORS router module:

   CORSSupport {
   private val allowOriginHeader = `Access-Control-Allow-Origin`.white_list

2. From an API routing module:

   if(originOpt.isDefined){
   if(originOpt.get.matches(" ... ")){

   Comments: Trusted domains are whitelisted.

Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 2

Secure Software Development Lifecycle

Verify the use of a secure software development lifecycle that addresses security in all stages of development.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-10: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-10: **Pass**, June 19, 2020.

   Comments:

Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-1: **Pass**, June 19, 2020.

   Comments:

Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-5: **Pass**, June 19, 2020.

   Comments:

Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.

1. Policy A.14: Software Development Security Policy, Section 3.2 Development Methodology:

   To ensure that code is developed in a secure manner and that the security controls are implemented throughout every stage, Voatz, Inc. development methodology includes:
   - Testing of the application's security features.

2. Policy A.14: Software Development Security Policy, Section 3.2 Development Methodology:

   To ensure that code is developed in a secure manner and that the security controls are implemented throughout every stage, Voatz, Inc. development methodology includes:

   - Ensuring secure coding standards are followed.

Comments: As part of Voatz' ISO 27001 certification process, such policies were established.

Authentication Architectural Requirements

Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges needed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-AUTH-10: **Pass**, June 19, 2020.

2. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines:
   - Always use the least privilege to perform a function.
   - Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

   Comments:

Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect abuse or breaches.

1. Policy A.13: Network Security Policy, 5.9 Encrypt sensitive network traffic:
   - Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

2. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines:
   - Access to services should be logged and protected through access-control methods.

3. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   - All security-related events on critical or sensitive systems must be logged and audit trails saved.

   Comments: Voatz mobile apps employ a biometric (touch/face) element to authenticate with the app and strong identity verification is necessary in order to perform the most important task on the app: submitting a marked ballot. Similarly, admin portal users must enroll in 2FA. All security related events on the server such as authentication attempts are logged via well defined audit transitions which log the source, type and timestamp of the transaction.

Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.

1. From an API router module:

   ```
   authenticateOrRejectWithChallenge[HttpApiSession](None =>
   SessionAuthenticatorAsync.validate(sessionCookie, csrfToken))
   ```

2. From an API router module:

   authorize(performAuthorization(authorizationKey, session))

   Comments: The same authentication pathway is implemented consistently across all REST APIs. Any password based authentication involves slow hashing primitives such as B-crypt and no weak hashing primitives are employed. Any encryption is performed using AES GCM with a unique nonce per request and no insecure padding/block modes are employed.

Access Control Architectural Requirements

Verify enforcement of the principle of least privilege in functions, data files, URLs, controllers, services, and other resources. This implies protection against spoofing and elevation of privilege.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows least privilege when granting access to information and application system functionality.

   Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

   Comments: The principle of least privilege applies to users as well as Voatz team members. Access to certain resources is only granted on a need-to-know basis.

Verify the application uses a single and well-vetted access control mechanism for accessing protected data and resources. All requests must pass through this single mechanism to avoid copy and paste or insecure alternative paths.

1. App users access functionality through an API router, which enforces access control:

   ```
   requireAuthentication(User.View) {
    entity(as[ApiRequest]) { apiRequest =>
     optionalCookie("WS"){sessionCookie =>
       val request = ApiRequest(apiRequest, sessionCookie)
   ```

   where requireAuthentication is defined as:

   ```
   def requireAuthentication(directive: HttpApiSession => RequestContext => Unit):
   RequestContext => Unit = optionalHeaderValueByName(CsrfToken) {
    csrfToken =>
     optionalCookie(SessionCookie) { sessionCookie =>
       authenticate(SessionAuthenticatorAsync.validate(sessionCookie, csrfToken)) .
   ```

   Additionally, every API is secured by authorization checks of the form:

```
val snapByDevIdOptFut = UserModule.getByDeviceId(apiRequest.deviceId, sessionCookieOpt)
snapByDevIdOptFut onComplete {
 case Success(snapByDevIdOpt) => {
  if (!snapByDevIdOpt.isDefined) {
   val err = "user not found"
  }else {
 val userIdFromDevId = snapByDevIdOpt.get
 SessionAuthenticatorAsync.validateSessionAgainstUser(sessionCookieOpt, userIdFromDevId)
onComplete{
  case Success(sessionValid) => {
   if(!sessionValid){
    theSender ! ForbiddenError("Session cookie provided does not authorize you to perform this
action")
   }else{
    if (userIdFromDevId != request.userId) {
     theSender ! ForbiddenError("Supplied deviceId does not belong to requested user")
    } else {
```

where the user attached to the device sending the request is validated against the user holding the current session, which in turn is matched against the user making the request.

2. Voatz team members access protected data and resources via a VPN.

   Policy AC.7: Virtual Private Network Policy, Section 1.0: Purpose:
   The purpose of this policy is to provide guidelines for Remote Access via Virtual Private Network (VPN) connections to the Voatz, Inc. corporate network.

   Comments:

Verify that attribute or feature-based access control is used whereby the code checks the user's authorization for a feature/data item rather than just their role. Permissions should still be allocated using roles.

1. From election admin user module:

```
val orgAdminUserFut = SessionAuthenticatorAsync.getUserIfOrgAdmin(sessionCookie,
request.organizationId)
orgAdminUserFut onComplete {
 case Success((true, _, userId)) => {
  val validFut = OrganizationValidationsModule.isGetBallotsRequestValid(request, userId)
  validFut onComplete {
   case Success(validReasonPair) => {
    if(validReasonPair.valid){
     val resultFut = OrganizationModule.getBallots(...
```

where the initial call to getUserIfOrgAdmin checks whether the user has the appropriate role to access the requested resource and the subsequent call to isGetBallotsRequestValid which is defined as:

```
def isGetBallotsRequestValid(request: ApiGetBallotsRequest, userId: Int)(implicit db: Database):
Future[ValidReasonPair] = async{
 val orgId = request.organizationId
 val canUserGetBallots = await(OrganizationUserMod.canUserGetBallots(userId, orgId))
 if(!canUserGetBallots){
   ValidReasonPair(false, "Forbidden: user does not have permission to perform this action")
```

This checks whether the user with the Admin role has the more fine grained permission to access the specifically requested feature/resource.

2. Users are granted access using a matrix of roles (for e.g. Org. Admin, Org. User, etc.) and fined grained feature based access.
   For instance, the user below can enroll for fetching the cast vote record but cannot access voter affidavits.

   "org" : ..73, "user" : ...814, "enrollcvr" : true, "getaffidavits" : false, "getballots" : true, "getballotstatus" : true, "getcvr" : true

   But the user below can do both.

   "org" : ..73, "user" : ...813, "enrollcvr" : true, "getaffidavits" : true, "getballots" : true, "getballotstatus" : true, "getcvr" : true

   Comments:

Input and Output Architectural Requirements

Verify that input and output requirements clearly define how to handle and process data based on type, content, and applicable laws, regulations, and other policy compliance.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. 2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that serialization is not used when communicating with untrusted clients. If this is not possible, ensure that adequate integrity controls (and possibly encryption if sensitive data is sent) are enforced to prevent deserialization attacks including object injection.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-8: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-8: **Pass**, June 19, 2020.

Comments: Voatz APIs employ AES GCM encryption with non repeating nonce to prevent any deserialization attacks. Additionally, Voatz apps employ certificate pinning, state of the art code virtualization/obfuscation techniques and can only be used on non-rooted/non-jailbroken devices.

Cryptographic Architectural Requirements

Verify that there is an explicit policy for management of cryptographic keys and that a cryptographic key lifecycle follows a key management standard such as NIST SP 800-57.

1. Policy A.10: Cryptography, Section 3.6: Key Management:
   - **Generation:**
     - Cryptographic keys must be generated and stored in a secure manner that prevents loss, interception, theft, or compromise.
     - Key generation must be seeded from an industry standard random number generator.

2. Policy A.10: Cryptography, Section 3.6: Key Management:
   - **Key Removal:**
     - Key removal shall occur after an archival phase and after adequate analysis to ensure that loss of that key will not correspond to loss of data or other keys.

   Comments:

Verify that consumers of cryptographic services protect key material and other secrets by using key vaults or API based alternatives.

1. Policy A.6.2.1: Mobile Device Management Policy, Section 3.1 Technology and Security Requirements
   If the user is storing passwords in the device, an encrypted password store must be used.

2. Policy A.10: Cryptography, Section 3.1 Encryption Method and Application:
   All private keys for encryption must be password protected and not stored in the clear on systems.

   Comments:

Verify that all keys and passwords are replaceable and are part of a well-defined process to re-encrypt sensitive data.

1. Policy AC.10: Database Credentials Policy, Section 4.4 Access to Database Usernames and Passwords:
   - Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

2. Policy AC.5: Password Policy, Section 5.3: Password Protection Standards:

    - If an account or password is suspected to have been compromised, report the incident to Voatz, Inc. IT and change all passwords immediately.
    - Password cracking or guessing may be performed on a periodic or random basis by Voatz, Inc. IT Ops or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

    Comments:

Verify that the architecture treats client-side secrets - such as symmetric keys, passwords, or API tokens - as insecure and never uses them to protect or access sensitive data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

    Comments:

Errors, Logging and Auditing Architectural Requirements

Verify that a common logging format and approach is used across the system.

1. From an application module:

    ```
    import org.slf4j.{Logger, LoggerFactory}
    private implicit val log: Logger = LoggerFactory.getLogger("...")
    ```

2. From an API routing module:

    ```
    import org.slf4j.LoggerFactory
    private val log = LoggerFactory.getLogger("...")
    ```

    Comments: Standard and consistent system loggers are used across the platform.

Verify that logs are securely transmitted to a preferably remote system for analysis, detection, alerting, and escalation.

1. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

2. Policy A.11: Physical and Environmental Security Policy, Section 4.2 Physical Access Control:
   Maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.

    Comments:

Data Protection and Privacy Architectural Requirements

Verify that all sensitive data is identified and classified into protection levels.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-4: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-4: **Pass**, June 19, 2020.

Comments:

Verify that all protection levels have an associated set of protection requirements, such as encryption requirements, integrity requirements, retention, privacy and other confidentiality requirements, and that these are applied in the architecture.

1. Policy A.10: Acceptable Encryption Policy, Section 3.3: Data Protection:
    - Data at rest:
        - All Voatz, Inc. and customer data deemed a secret shall be stored in an encrypted manner.
    - Data in motion:
        - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.
        - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted.
2. Policy A.18: Information Security/Sensitivity, Section 3.2 Data Protection Standards
Each classification of data has different requirements for protection throughout the lifecycle of use.

Comments:

Communications Architecture Requirements

Verify the application encrypts communications between components, particularly when these components are in different containers, systems, sites, or cloud providers.

1. Policy A.10: Acceptable Encryption Policy, Section 3.3: Data Protection:
    - Data in motion:
        - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.

2. Policy A.10: Acceptable Encryption Policy, Section 3.3: Data Protection:
    - Data in motion:
        - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted.

Comments: Communication between systems is encrypted via TLS v. 1.2 and in cases where it is appropriate, encrypted at the application layer as well.

Verify that application components verify the authenticity of each side in a communication link to prevent person-in-the-middle attacks. For example, application components should validate TLS certificates and chains.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-2: **Pass**, June 19, 2020.

   Comments: TLS certificates are checked.

Malicious Software Architectural Requirements

Verify that a source code control system is in use, with procedures to ensure that check-ins are accompanied by issues or change tickets. The source code control system should have access control and identifiable users to allow traceability of any changes.

1. Policy A.9: Access Control Policy, Section 3.0: Business Requirements:
   Cloud-based collaboration systems (e.g. Jira, Dropbox, Confluence, Slack)

2. Policy A.14: Software Development Security Policy, Section 3.3 Code and Configuration Reviews:
   During implementation and maintenance, all source code and system configurations must be reviewed and approved before deployment by a team member who did not participate in implementing the change. Exceptions must be documented in Jira and approved by Voatz CEO or CTO.

   Comments: A version control system is in place for all application and server code. All changes are connected to tickets on a collective board and comments or code branches reflect the appropriate ticket or version. All changes and code branches are tracked.

Secure File Upload Architectural Requirements

Verify that user-uploaded files are stored outside of the web root.

1. Policy AC.9: Server Security Policy, Section 4.2: General Configuration and Backup Guidelines
   Always use the least privilege to perform a function. Do not use root/admin accounts when a non-privileged account is sufficient.

2. Policy A.9: Access Control Policy, Section 6.1 Information Access Restriction
   Voatz follows least privilege when granting access to information and application system functionality.

   Comments: End users are never allowed to upload any files directly to Voatz servers. Files are uploaded internally via well defined micro services that communicate with secure cloud storage

using private/restricted APIs employing strict access control and AES GCM encryption with non repeating nonce.

Verify that user-uploaded files - if required to be displayed or downloaded from the application - are served by either octet stream downloads, or from an unrelated domain, such as a cloud file storage bucket. Implement a suitable content security policy to reduce the risk from XSS vectors or other attacks from the uploaded file.

1. N/A

2. N/A

   Comments: N/A: User uploaded files (e.g., identity document images, selfies, etc.) are never displayed or downloaded via the application and are never uploaded directly to Voatz servers. These images are placed in secure cloud storage controlled via well defined IAM (Identity and Access Management) roles and bucket policies, processed via well defined private micro services using AES GCM encryption with non repeating nonce, and deleted from secure cloud storage after being processed for document/identity verification.

Configuration Architectural Requirements

Verify the segregation of components of differing trust levels through well-defined security controls, firewall rules, API gateways, reverse proxies, cloud-based security groups, or similar mechanisms.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-5: **Pass**, June 19, 2020.

   Comments:

Verify that the build pipeline warns of out-of-date or insecure components and takes appropriate actions.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-6: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-6: **Pass**, June 19, 2020.

   Comments: Voatz integrates Snyk with Atlassian to achieve DevSecOps within existing CI/CD development workflows. This enables software component analysis to track and analyze open source component dependencies, enforce security and compliance policies, and fix potential vulnerabilities at source.

Verify that the build pipeline contains a build step to automatically build and verify the secure deployment of the application, particularly if the application infrastructure is software defined, such as cloud environment build scripts.

1. Voatz integrates Snyk with Atlassian to achieve DevSecOps within existing CI/CD development workflows. This enables software component analysis to track and analyze open source component dependencies, enforce security and compliance policies, and fix potential vulnerabilities at source.

2. This also provides much needed context such as severity and exploit maturity for vulnerabilities, enables creation of fix pull requests to upgrade the direct dependencies or patch vulnerabilities, and prioritize fixes via priority scores while integrating with Jira issue tracking.

   Comments:

Verify that application deployments adequately sandbox, containerize and/or isolate at the network level to delay and deter attackers from attacking other applications, especially when they are performing sensitive or dangerous actions such as deserialization.

1. Voatz employs SELinux security policy functions as a whitelist for user and application behavior by isolating applications into specific SELinux domains that are tailored to the application's permitted behaviors. Access to files, local interprocess communications (IPC) mechanisms, the network, and various other system resources are restricted on a per-domain basis.

2. By ensuring that every service that listens on a network is run in a confined SELinux domain, an attacker's access to resources, ability to pivot, read, and write, and the possible damage they can do is limited.

   Comments:

Verify the application does not use unsupported, insecure, or deprecated client-side technologies such as NSAPI plugins, Flash, Shockwave, ActiveX, Silverlight, NACL, or client-side Java applets.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: Voatz applications and servers only use secure third-party services via well defined application dependencies or SDKs. No insecure or deprecated client side plugins such as Flash, ActiveX, Silverlight or Java applets are used anywhere in the Voatz architecture.

Credential Storage Requirements

Verify that passwords are stored in a form that is resistant to offline attacks. Passwords SHALL be salted and hashed using an approved one-way key derivation or password hashing function. Key derivation and password hashing functions take a password, a salt, and a cost factor as inputs when generating a password hash.

1. From Policy A.10: Cryptography, Section 3.5:
   - Where applicable, user passwords shall be stored in a secure manner by using HMAC with hash.
   - All user passwords should be salted on a per secret basis.
     - The salt should be random.
     - The salt size should be the same length as the output of the hashing function.
     - The salt should not be considered a secret.

2. From a cryptographic module:
```
def hashPassword(password: String): PasswordHash = {
  val salt = generateSalt
  PasswordHash(password.bcrypt(salt))
}
```

Comments:

Verify that the salt is at least 32 bits in length and be chosen arbitrarily to minimize salt value collisions among stored hashes. For each credential, a unique salt value and the resulting hash SHALL be stored.

1. From Policy A.10: Cryptography, Section 3.5:
   - The salt should be random.
2. From a cryptographic module:

   ```
   private static final int BCRYPT_SALT_LEN = 16;
   ```

   Comments: The salt is 128 bits (16 bytes) in length.

Verify that if PBKDF2 is used, the iteration count SHOULD be as large as verification server performance will allow, typically at least 100,000 iterations.

1. From a cryptographic module:

   ```
   PasswordHash(password.bcrypt(salt))
   ```

2. From a cryptographic module:
   ```
   password.isBcrypted(passwordHash.hash)
   ```

   Comments: PBKDF2 is not used as the password hash; bcrypt is used instead.

Credential Recovery Requirements

Verify that if OTP or multi-factor authentication factors are lost, that evidence of identity proofing is performed at the same level as during enrollment.

1. From an API router module:

   authenticateOrRejectWithChallenge[HttpApiSession](None =>
   SessionAuthenticatorAsync.validate(sessionCookie, csrfToken))

2. From an API router module:

   authorize(performAuthorization(authorizationKey, session))

   Comments: When login credentials are lost, the account is reactivated using the same process as during activation, using the same authentication and authorization checks as above.

Look-up Secret Verifier Requirements

Verify that lookup secrets can be used only once.

Comments: N/A: No lookup secrets are used.

Verify that lookup secrets have sufficient randomness (112 bits of entropy), or if less than 112 bits of entropy, salted with a unique and random 32-bit salt and hashed with an approved one-way hash.

Comments: N/A: No lookup secrets are used.

Verify that lookup secrets are resistant to offline attacks, such as predictable values.

Comments: N/A: No lookup secrets are used.

Out of Band Verifier Requirements

Verify that the out of band verifier retains only a hashed version of the authentication code.

1. In a database module:

   val pinSet = set("pin", Cryptography.hashPassword(requestCustomerSnap.pin).hash)

2. In a voter authentication module:

   val customerPinHashOpt = await(getPin(customerId))

   Comments:

Verify that the initial authentication code is generated by a secure random number generator, containing at least 20 bits of entropy (typically a six digital random number is sufficient).

1. From Policy A.10: Cryptography, Section 3.6:

- Key generation must be seeded from an industry standard random number generator.

2. From a voter authentication module:

```
val totp = Totp(Cryptography.issueRandomKey(256).getBytes, 6, SHA256,
30).generate()
```

3. From a cryptographic module:

```
import java.security.SecureRandom;
```

Single or Multi-factor One Time Verifier Requirements

Verify that symmetric keys used to verify submitted OTPs are highly protected, such as by using a hardware security module or secure operating system based key storage.

1. From Policy A.10: Cryptography, Section 3.6: Key Management:
   - Cryptographic keys must be generated and stored in a secure manner that prevents loss, interception, theft, or compromise.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments:

Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.

1. From Policy A.10: Cryptography, Section 3.6: Key Management:
   - Key generation must be seeded from an industry standard random number generator.
2. From a voter authentication module:

```
val totp = Totp(Cryptography.issueRandomKey(256).getBytes, 6, SHA256,
30).generate()
```

Verify that time-based OTP can be used only once within the validity period.

1. In a voter authentication module:

```
else if(otpAlreadyVerified){
  log.error(s"otp $otp already verified for mobile $mobileNumber")
```

2. From a voter authentication module:

```
if(checkOtpTimestamp(snapshot.timestamp, timestamp, onBoardingLimits)){
  ...
}
else{
  val error = "Otp timeout was exceeded"
```

   Comments:

Verify that if a time-based multi factor OTP token is re-used during the validity period, it is logged and rejected with secure notifications being sent to the holder of the device.

1. In an API routing module:

   log.error(s"EncryptVerifyOtp request failed: $err")

2. In an API routing module:

   HttpResponse(StatusCodes.InternalServerError, entity = "otp verification request failed")

   Comments:

Cryptographic Software and Devices Verifier Requirements

Verify that cryptographic keys used in verification are stored securely and protected against disclosure, such as using a TPM or HSM, or an OS service that can use this secure storage.

1. Policy A.10: Acceptable Encryption Policy, Section 3.6 Key Management:
   Cryptographic keys must be generated and stored in a secure manner that prevents loss, interception, theft, or compromise.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-STORAGE-1: **Pass**, June 19, 2020.

   Comments: All cryptographic keys on a mobile app are generated and stored in a TPM if such is available. Otherwise, these keys are generated and stored in sandboxed storage only accessible by the app.

Verify that the challenge nonce is at least 64 bits in length, and statistically unique or unique over the lifetime of the cryptographic device.

1. From a cryptographic module:

   val GCM_NONCE_LENGTH = 12

2. From a cryptographic module:

   val nonce = (firstIV zip toUnsignedByteArray(sequenceNumber, 12))

   Comments: All nonces are at least 96 bits in length so it is statistically unlikely that a nonce will repeat.

Verify that approved cryptographic algorithms are used in the generation, seeding, and verification.

1. From Policy A.10: Cryptography, Section 3.6:
   Key generation must be seeded from an industry standard random number generator.

2. From the cryptographic module:

```
import java.security.SecureRandom;
val ranGen = new SecureRandom()
val key = new Array[Byte](size)
ranGen.nextBytes(key)
```

Comments:

Service Authentication Requirements

Verify that if passwords are required for service authentication, the service account used is not a default credential (e.g. root/root or admin/admin are default in some services during installation)

1. Policy A.9: **Access Control Policy, Section** 4.4 Management of Secret Authentication Information of Users
    - Where Voatz IT Ops issues initial passwords, these are sent out of band and users are asked to change their passwords and any default passwords.

2. Policy A.13: Network Security Policy, Section 5.2 Privilege Access Control:
    - Privileged access to prevent configuration changes should be restricted to authorized personnel only.
    - Passwords shall follow strong password mechanisms outlined under the Password Guidelines.
    - Access control shall be used to provide separate authentication, authorization, and accounting services for network-based access.
    - A Privileged Access Management solution can control credentials accessing the device and commands that can be executed when a session is initiated, providing a complete audit of both commands and sessions.

Comments:

Verify that passwords are stored with sufficient protection to prevent offline recovery attacks, including local system access.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
    - storage on disk, particularly secrets and user passwords.

2. Policy A.10: Acceptable Encryption Policy, Section 3.5: User Passwords
    - Where applicable, user passwords shall be stored in a secure manner by using HMAC with hash.

Comments: Passwords are stored in secure device storage.

Session Binding Requirements

Verify that session tokens are generated using approved cryptographic algorithms

1. From Policy A.10: Cryptography, Section 3.1: All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. From Policy A.10: Cryptography, Section 3.2: The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by Voatz, Inc. IT Ops.

   Comments: Session tokens are derived from a cryptographically secure random number generator and have 256 bits of entropy.

Session Logout and Timeout Requirements

Verify that the application gives the option to terminate all other active sessions after a successful password change (including change via password reset/recovery), and that this is effective across the application, federated login (if present), and any relying parties.

1. From the user management module, the following routine is called as part of the password reset/recovery flow:
   deleteAllPreviousSessions(userId)
   which is responsible for deleting any active sessions for the user in cache.

2. All active sessions are terminated on successful password change and the user is forced to authenticate again with the new credentials before being able to access any features in the app.

   Comments:

Verify that users are able to view and (having re-entered login credentials) log out of any or all currently active sessions and devices.

1. From an API routing module:

   private def encryptedLogoutUser() = post {

2. Onboarding and Identity Verification with Voatz:
   https://vimeo.com/533255584/1baa3910a6

   Comments:

Token Based Session Management

Verify the application uses session tokens rather than static API secrets and keys, except with legacy implementations.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-AUTH-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-AUTH-3: **Pass**, June 19, 2020.

   Comments: Voatz applications and servers employ CSRF tokens and session tokens generated via cryptographically secure random generators. No static API secrets or keys are used in the Voatz architecture.

Verify that stateless session tokens use digital signatures, encryption, and other countermeasures to protect against tampering, enveloping, replay, null cipher, and key substitution attacks.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-AUTH-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-AUTH-3: **Pass**, June 19, 2020.

   Comments:

Other Access Control Considerations

Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems and/or segregation of duties for high value applications to enforce anti-fraud controls as per the risk of application and past fraud.

1. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows least privilege when granting access to information and application system functionality. Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know basis depending on the segregation of duties.

2. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

   Comments: These restrictions apply to election administrators and Voatz system administrators alike.

Data Classification

Verify that regulated private data is stored encrypted while at rest, such as Personally Identifiable Information (PII), sensitive personal information, or data assessed likely to be subject to EU's GDPR.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   Encryption shall be implemented in:
   - storage on disk, particularly secrets and user passwords.

2. Policy A.10: Acceptable Encryption Policy, Section 3.3 Data Protection:
   - Data at rest:

All Voatz, Inc. and customer data deemed a secret shall be stored in an encrypted manner.

Comments: All sensitive private data on disk is encrypted at rest using FIPS 140-2 approved cryptographic modules.

Algorithms

Verify that industry proven or government approved cryptographic algorithms, modes, and libraries are used, instead of custom coded cryptography.

1. From Policy A.10: Cryptography, Section 3.1: All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. From Policy A.10: Cryptography, Section 3.2: The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by Voatz, Inc. IT Ops.

   Comments: Bulk encryption is done via AES in GCM. ECC and ECDSA are used for public key encryption and digital signatures; NSA and NIST-approved curves are used for both in all apps. SHA-256 and bcrypt are the secure hash algorithms used.

Verify that encryption initialization vector, cipher configuration, and block modes are configured securely using the latest advice.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CRYPTO-3: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CRYPTO-3: **Pass**, June 19, 2020.

   Comments:

Verify that random number, encryption or hashing algorithms, key lengths, rounds, ciphers or modes, can be reconfigured, upgraded, or swapped at any time, to protect against cryptographic breaks.

1. The code is sufficiently modularized in order to allow for ciphers, hash functions, keys, and other parameters to be changed as necessary. In particular, we are cognizant of the anticipated need to adopt post-quantum cryptographic algorithms and are awaiting standards to be published from NIST before proceeding with such implementations.

2. From a cryptographic module (Examples to show modularity):
   def getX509EncPublicKey(encodedPublicKey: String, keyAlgorithm: String)

   def generatePublicKeys(numOfKeys: Option[Int], keySizeOpt: Option[Int])(implicit cryptoAlgorithm: CryptoAlgorithm)

   Comments:

Verify that known insecure block modes (i.e. ECB, etc.), padding modes (i.e. PKCS#1 v1.5, etc.), ciphers with small block sizes (i.e. Triple-DES, Blowfish, etc.), and weak hashing algorithms (i.e. MD5, SHA1, etc.) are not used unless required for backwards compatibility.

1. From Policy A.10: Cryptography, Section 3.1:
   All Voatz, Inc. encryption shall be done using approved cryptographic modules. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Voatz, Inc.'s key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows. All private keys for encryption must be password protected and not stored in the clear on systems.

2. From a cryptographic module:
   val cipher = Cipher.getInstance("AES/GCM/NoPadding", "SunJCE")

Verify that nonces, initialization vectors, and other single use numbers must not be used more than once with a given encryption key. The method of generation must be appropriate for the algorithm being used.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CRYPTO-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CRYPTO-5: **Pass**, June 19, 2020.

   Comments: Every new request is encrypted with a new random nonce obtained via:

```
def getNewNonce() = {
 val GCM_NONCE_LENGTH = 12
 val random = SecureRandom.getInstanceStrong()
 val nonce = new Array[Byte](GCM_NONCE_LENGTH)
 random.nextBytes(nonce)
 nonce
}
```

   Similarly, every response is encrypted with a new random nonce obtained via the above method

Random Values

Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved cryptographically secure random number generator when these random values are intended to be not guessable by an attacker.

1. From Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management
   Key generation must be seeded from an industry standard random number generator.

2. From a cryptographic module, taken from java.util.Random.
   val random = SecureRandom.getInstanceStrong()

   Comments: All random values are generated using a cryptographically secure random number generator from entropy gathered by the operating system. In particular, random numbers on the server are generated using the SecureRandom class in the java.security library.

Verify that random GUIDs are created using the GUID v4 algorithm, and a cryptographically-secure pseudo-random number generator (CSPRNG). GUIDs created using other pseudo-random number generators may be predictable.

1. From Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management
   Key generation must be seeded from an industry standard random number generator.

2. From a cryptographic module, taken from java.util.Random.
   val random = SecureRandom.getInstanceStrong()

   Comments: All GUIDs (i.e., UUIDs) are generated using the aforementioned random number generator.

Secret Management

Verify that a secrets management solution such as a key vault is used to securely create, store, control access to and destroy secrets.

1. Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management:
   Key management should be planned which will include secure key generation, use, storage, distribution, recovery, and removal.

2. Policy AC.5: Password Policy, Section 2.0: Purpose:
   The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

   Comments:

Verify that key material is not exposed to the application but instead uses an isolated security module like a vault for cryptographic operations.

1. Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management:
   Key management should be planned which will include secure key generation, use, storage, distribution, recovery, and removal.

2. Policy AC.5: Password Policy, Section 2.0: Purpose:
   The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

   Comments:

Log Content Requirements

Verify that the application logs security relevant events including successful and failed authentication events, access control failures, deserialization failures and input validation failures.

1. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines: Operating System configuration should be in accordance with approved Voatz, Inc. IT guidelines. Services and applications that will not be used must be disabled where practical.
    - Access to services should be logged and protected through access-control methods.

2. Example of a logged error in an API router:

   val logError = s"Authentication failed for customer $customerId with error: $reason"
   log.error(logError)

   Comments: The server logs all security related events via well defined audit transactions that record the source, type and timestamp of the transaction.

Verify that each log event includes necessary information that would allow for a detailed investigation of the timeline when an event happens.

5. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.
6. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

   Comments: Server logs include timestamps and all relevant information necessary to trace intrusion attempts. These logs have enabled Voatz to identify and mitigate threats in real time.

Log Processing Requirements

Verify that all authentication decisions are logged, without storing sensitive session identifiers or passwords. This should include requests with relevant metadata needed for security investigations.

1. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.
2. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

   Comments: All authentication requests are logged using well defined audit transactions that log the source, type and timestamp along with relevant non-sensitive metadata such as IP address, device id, etc.

Verify that all access control decisions can be logged and all failed decisions are logged. This should include requests with relevant metadata needed for security investigations.

1. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring

Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

2. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

   Comments: All access control decisions (including failures) are logged using well defined audit transactions along with relevant metadata such as IP address, device id, host, etc.

Log Protection Requirements

Verify that the application appropriately encodes user-supplied data to prevent log injection.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments:

Verify that all events are protected from injection when viewed in log viewing software.

1. N/A

2. N/A

   Comments: N/A: Log viewing is enabled via local micro services that access log files in read only mode, thus eliminating the possibility of any injection attacks. Additionally, logs are always archived with checksums.

Verify that security logs are protected from unauthorized access and modification.

1. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

   - Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
   - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;

2. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

- Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
- Need to Use – users will only be able to access physical and logical facilities required for their role.

Comments: Security logs are protected from unauthorized access by denying any external application access to the log files. Any log aggregation for viewing/inspection is done via local micro services with strict access control and no public interfaces.

Verify that time sources are synchronized to the correct time and time zone. Strongly consider logging only in UTC if systems are global to assist with post-incident forensic analysis.

1. From the user onboarding module:
```
def checkOtpTimestamp(otpTimestamp: String, nowTimestamp: String, onBoardingLimits:
OnboardingLimitsSnapshot): Boolean = {
 val otpts = OffsetDateTime.parse(otpTimestamp)
 val now = OffsetDateTime.parse(nowTimestamp)
 val differenceInSeconds = ChronoUnit.SECONDS.between(otpts, now)
 differenceInSeconds <= onBoardingLimits.timeout
}
```

2. From the voter file management module:
```
val recordToCreateWithTs = recordToCreate.:+(KeyValuePair("insertTimestamp",
OffsetDateTime.now.toString))
```

   Comments: All timestamps are logged with an offset from UTC/Greenwich in the ISO-8601 calendar system

Error Handling

Verify that a "last resort" error handler is defined which will catch all unhandled exceptions.

1. From an API routing module:

```
implicit def exceptionHandler: ExceptionHandler =
                ExceptionHandler {
                case e => { ctx =>
                        //log.error(e, "Unhandled api exception")
                        log.error("Unhandled api exception", e)
```

2. From an API routing module:

```
implicit val myRejectionHandler: RejectionHandler = RejectionHandler.newBuilder()
...
.handleNotFound {
        log.error(s"The requested resource could not be found")
        complete(HttpResponse(NotFound, getAllHeaders, "The requested resource could
not be found"))
```

General Data Protection

Verify the application protects sensitive data from being cached in server components such as load balancers and application caches.

1. Policy A.10: Acceptable Encryption Policy, Section 3.3: Data Protection:
   Data at rest:
   - All Voatz, Inc. and customer data deemed a secret shall be stored in an encrypted manner.
2. Policy A.10: Acceptable Encryption Policy, Section 3.3: Data Protection:
   Data in motion:
   - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.
   - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted.

Comments: No sensitive data such as PII or user credentials is cached in application caches or load balancers. As a rule of thumb, all information cached in application caches is short lived, relates to the current/active user session, and is purged automatically in accordance with well defined TTL (time to live) settings. Additionally, such caches are not accessible via any public interface/API and protected with cryptographically secure random secrets known only to the process accessing the cache.

Verify that all cached or temporary copies of sensitive data stored on the server are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data.

1. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.
   - Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
   - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
2. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.
   - Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
   - Need to Use – users will only be able to access physical and logical facilities required for their role.

Comments: All cached information on Voatz servers is protected via well defined TTL (time to live) settings and such cached information is automatically purged after the TTL settings expire.

Additionally, there is no public access to the caching layer via any API and it is protected by cryptographically secure random secrets known only to the process accessing the cache.

Verify the application minimizes the number of parameters in a request, such as hidden fields, Ajax variables, cookies and header values.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-1: **Pass**, June 19, 2020.

   Comments: Only those parameters that are necessary are collected.

Verify the application can detect and alert on abnormal numbers of requests, such as by IP, user, total per hour or day, or whatever makes sense for the application.

1. Policy A.12: Operations Security Policy, Section 7.0: Logging and Monitoring:
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

2. Policy A.16 Information Security Incident Management, Section 1.0: Overview:
   It is critical to the organization that incidents that threaten the security or privacy of critical information are properly identified, contained, investigated, and remedied.

   Comments: The following code from the user onboarding module tracks requests by IP, mobile, email, deviceId within a certain configurable interval to detect abnormal number of requests from a source and block access, if necessary

```
def maxRequestsExceededByIp(ipAddress: String, onBoardingLimits:
OnboardingLimitsSnapshot)(implicit db: Database, ec: ExecutionContext): Future[Boolean] = {
   val nowMillis = OffsetDateTime.now.toInstant.toEpochMilli
   val key = s"userpreregisterread$ipAddress"
   Cache.getListOfStringFromCache(key) map{ recordIpFromCacheOpt =>
    if(recordIpFromCacheOpt.isDefined){
      val exceeded =
recordIpFromCacheOpt.get.map(OffsetDateTime.parse(_).toInstant.toEpochMilli).filter { x =>
nowMillis-x < onBoardingLimits.consecutiveRequestInterval}.size >=
onBoardingLimits.consecutiveRequests
      if(exceeded){
       log.error(s"max. consecutive requests from same ip $ipAddress exceeded")
      }
      exceeded
    }else{
      false
    }
   }
 }
```

```
def maxRequestsExceededByMobile(mobileNumber: String, onBoardingLimits:
OnboardingLimitsSnapshot)(implicit db: Database, ec: ExecutionContext): Future[Boolean] = {
  val nowMillis = OffsetDateTime.now.toInstant.toEpochMilli
  val key = s"userpreregisterread$mobileNumber"
  Cache.getListOfStringFromCache(key) map{ recordMobileFromCacheOpt =>
   if(recordMobileFromCacheOpt.isDefined){
    recordMobileFromCacheOpt.get.map(OffsetDateTime.parse(_).toInstant.toEpochMilli).filter
{ x => nowMillis-x < onBoardingLimits.consecutiveRequestInterval}.size >=
onBoardingLimits.consecutiveRequests
   }else{
    false
   }
  }
 }
```

Sensitive Private Data

Verify accessing sensitive data is audited (without logging the sensitive data itself), if the data is collected under relevant data protection directives or where logging of access is required.

1. Policy A.9: Access Control Policy, Section 4.1 User Registration and De-registration
   Voatz IT Ops is responsible for registering and de-registering users. They shall establish and maintain an agreed process for the registration and de-registration of users. The process shall ensure that:
   - The request to register or de-register a user has come from someone with appropriate authority and shall be auditable.
   - A record of the request and the action taken is kept for audit purposes.

2. Policy A.9: Access Control Policy, Section 4.2 User Access Provisioning
   Voatz IT Ops is responsible for assigning and revoking access rights for all user types to all systems and services. They shall establish and maintain agreed upon processes for managing the user access rights. These shall ensure that:
   - A record of the request and the action taken is kept for audit purposes.

   Comments:

Verify that sensitive information contained in memory is overwritten as soon as it is no longer required to mitigate memory dumping attacks, using zeroes or random data.

1. From the iOS app API encryption module which creates a wrapper around the Swift Data type to wipe out bytes on deallocation so secrets cannot be brought back to live by reverse engineering
   public class ClearableData {
   var value: Data

```
    deinit {
      value.deinitialize()
    }
....
func replaceSubrange(_ subrange: Range<Data.Index>, with data: [UInt8]) {
      value.replaceSubrange(subrange, with: data)
    }
```

This is used to replace sensitive data with random, meaningless data

```
var mask = ClearableData()
        for counter in 0 ..< interval {
          tseed.replaceSubrange((tseed.count - 4) ..< tseed.count, with: pack(counter))
          mask.append(CC.digest(tseed, alg: digest))
        }
        mask.count = maskLength
        return mask
```

2. From the Android app API encryption module which defines an extension to de-initialize byte arrays:

```
fun ByteArray?.deInitialize() {
 if (this != null && this.isNotEmpty()) {
   val size = this.size
   for (i in 0 until size) {
    this[i] = 0
   }
 }
}
```

This is used to replace sensitive data that is no longer processed by the app.

```
val decryptedBytes: ByteArray?
   try {
     decryptedBytes = cipher.doFinal(data)
     val decryptedBytesToString = String(decryptedBytes)
     decryptedBytes.deInitialize()
```

Comments: Voatz iOS and Android applications implement approaches to zeroing out/randomizing sensitive data in memory as soon as it is no longer required to mitigate memory dumping attacks.

Verify that sensitive or private information that is required to be encrypted, is encrypted using approved algorithms that provide both confidentiality and integrity.

1. From Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application
   - All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. From Policy A.10: Acceptable Encryption Policy, 3.2 Proprietary Encryption Algorithms

- The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by Voatz, Inc. IT Ops.

Comments: Voatz applications and servers employ AES GCM with non repeating nonce to encrypt all sensitive information in flight. Additionally, all sensitive information on disk is encrypted at rest.

Verify that sensitive personal information is subject to data retention classification, such that old or out of date data is deleted automatically, on a schedule, or as the situation requires.

1. Policy AM.1: Equipment Disposal, Section 4.1 Technology Equipment Disposal:
   Selection of data destruction methods should be based on the sensitivity of the data being destroyed. Methods may include those procured in-house use and the use of off-site secure data destruction services provided by vetted third parties as necessary.
   - Erasing/overwriting
     - Erasing by overwriting is an acceptable method of scrubbing data that is not sensitive or requires safeguarding. Multiple passes should be performed with random overwrite patterns – not just all zeros or another single character. A minimum of three (3) overwrites is required; additional overwriting is recommended depending upon the sensitivity of the data to be erased.

2. Policy A.18: Information Security/Sensitivity, Section 3.2 Data Protection Standards
   Data Retention
   - Data shall be retained for as long as is necessary to provide the service to the client. After the retention period is over or upon specific request by the client, data shall be destroyed in accordance with Destruction and Disposal defined in this policy.

   Destruction and Disposal

   - IT Ops maintains and shall enforce a detailed list of approved destruction methods appropriate for each type of information stored, whether in physical storage media or in database records or backup files. When systems containing data are decommissioned, they must follow the following destruction policy:
   - Paper documents containing Level 1, Level 2 information shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by a security screened personnel. (CIC provides)
   - Level 1 and Level 2 information on electronic files and data on Reusable Electronic Storage Devices should be reliably erased or physically destroyed using DOD Standard for Secure Data Sanitation (DOD 5220.22M). Functional electronic media that can be overwritten using a secure erase tool then may be recycled or disposed of. Non-functional electronic media (damaged disk drives) must be physically destroyed.

   Comments:

Client Communications Security Requirements

Verify that secured TLS is used for all client connectivity, and does not fall back to insecure or unencrypted protocols.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   - All web applications via the most secure version of SSL/TLS.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-1: **Pass**, June 19, 2020.

   Comments: All http traffic is secured using TLS v. 1.2 or newer

Verify using online or up to date TLS testing tools that only strong algorithms, ciphers, and protocols are enabled, with the strongest algorithms and ciphers set as preferred.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   - All web applications via the most secure version of SSL/TLS.
2. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: All Voatz, Inc. encryption shall be done using approved cryptographic modules. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Voatz, Inc.'s key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

   Comments:

Verify that old versions of SSL and TLS protocols, algorithms, ciphers, and configuration are disabled, such as SSLv2, SSLv3, or TLS 1.0 and TLS 1.1. The latest version of TLS should be the preferred cipher suite.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   - All web applications via the most secure version of SSL/TLS.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-1: **Pass**, June 19, 2020.

   Comments: TLS v. 1.2 (or newer) is used with an approved and standard cipher suite.

Server Communications Security Requirements

Verify that connections to and from the server use trusted TLS certificates. Where internally generated or self-signed certificates are used, the server must be configured to only trust specific internal CAs and specific self-signed certificates. All others should be rejected.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-1: **Pass**, June 19, 2020.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-2: **Pass**, June 19, 2020.
3. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-3: **Pass**, June 19, 2020.

Comments: All http traffic is secured using TLS v. 1.2 or newer.

Verify that encrypted communications such as TLS is used for all inbound and outbound connections, including for management ports, monitoring, authentication, API, or web service calls, database, cloud, serverless, mainframe, external, and partner connections. The server must not fall back to insecure or unencrypted protocols.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   - All web applications via the most secure version of SSL/TLS.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-NETWORK-1: **Pass**, June 19, 2020.

   Comments: All http traffic is secured using TLS v. 1.2 or newer.

Verify that all encrypted connections to external systems that involve sensitive information or functions are authenticated.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-AUTH-1: **Pass**, June 19, 2020.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-AUTH-1: **Pass**, June 19, 2020.

   Comments:

Verify that proper certification revocation, such as Online Certificate Status Protocol (OCSP) Stapling, is enabled and configured.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-NETWORK-2: **Pass**, June 19, 2020.
2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-NETWORK-2: **Pass**, June 19, 2020.

   Comments:

Malicious Code Search

Verify that the application source code and third party libraries do not contain unauthorized phone home or data collection capabilities. Where such functionality exists, obtain the user's permission for it to operate before collecting any data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-STORAGE-12: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-STORAGE-12: **Pass**, June 19, 2020.

   Comments: The user gives permission for Voatz servers and apps to store only as much information as is needed to verify identity, receive a ballot, and submit a ballot. All unnecessary user information is deleted when it is no longer needed.

Verify that the application does not ask for unnecessary or excessive permissions to privacy related features or sensors, such as contacts, cameras, microphones, or location.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-1: **Pass**, June 19, 2020.

   Comments: Voatz mobile Apps only request for permissions that are absolutely necessary to conduct secure operations on the device. Voatz mobile apps never request permissions for contact list, mics and never track user location in the background. Voatz mobile apps request camera permission to enable the user to take a picture of their identity document to prove eligibility for an election.

Business Logic Security Requirements

Verify the application has configurable alerting when automated attacks or unusual activity is detected.

1. Policy A.12: Operations Security Policy, Section 5.0 Protection from Malware
   A defense in depth approach shall be taken to protect Voatz from malware including, as a minimum:
   - Firewalls: these shall be installed at all points where internal networks are connected to the internet. Further requirements on firewall configuration and maintenance are contained in the Communications Security Policy.
   - Anti-virus: this shall be installed on all key devices including firewalls, proxy servers, all servers and all end-user devices.
   - Threat monitoring: information about emerging threats shall be obtained from appropriate sources and necessary action taken, e.g. ensuring that users are alerted proactively of potential attacks.

2. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

   Comments:

File Integrity Requirements

Verify that the files obtained from untrusted sources are validated to be of expected type based on the file's content.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-PLATFORM-2: **Pass**, June 19, 2020.

   Comments: Voatz applications and servers never accept files from untrusted sources. Additionally, files are never uploaded directly to the servers and are instead processed via secure cloud storage configured with relevant IAM roles/permissions.

File Execution Requirements

Verify that the application does not include and execute functionality from untrusted sources, such as unverified content distribution networks, JavaScript libraries, node npm libraries, or server-side DLLs.

1. N/A

2. N/A

   Comments: N/A: Voatz applications and servers rely on a well defined set of external libraries from trusted/verified sources and these libraries have been demonstrated/proven to function consistently across numerous open source projects. Voatz applications and servers never use unverified CDNs. Additionally, Voatz servers run on Linux and do not employ any server side DLLs.

RESTful Web Service Verification Requirements

Verify that the message headers and payload are trustworthy and not modified in transit. Requiring strong encryption for transport (TLS only) may be sufficient in many cases as it provides both confidentiality and integrity protection. Per-message digital signatures can provide additional assurance on top of the transport protections for high-security applications but bring with them additional complexity and risks to weigh against the benefits.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - App/client communication with back end infrastructure.

   Comments: All http traffic is secured using TLS v. 1.2 or newer.

SOAP Web Service Verification Requirements

Verify that the message payload is signed using WS-Security to ensure reliable transport between client and service.

1. N/A

2. N/A

   Comments: N/A: No SOAP based web services are used.

GraphQL and other Web Service Data Layer Security Requirements

Verify that query allow list or a combination of depth limiting and amount limiting should be used to prevent GraphQL or data layer expression denial of service (DoS) as a result of expensive, nested queries. For more advanced scenarios, query cost analysis should be used.

1. N/A

2. N/A

   Comments: N/A: No GraphQL is used in Voatz applications. All APIs that depend on queries run on data sources enforce strict pagination to control/limit the amount of data queried from the underlying data source.

Build

Verify that the application build and deployment processes are performed in a secure and repeatable way, such as CI / CD automation, automated configuration management, and automated deployment scripts.

1. Voatz employs Atlassian Bitbucket pipelines enabling efficient storage and management of build configurations allowing management of the entire development workflow from code to deployment.

2. Additionally, Voatz integrates Snyk into Bitbucket pipelines to achieve DevSecOps within existing CI/CD development workflows. This enables software component analysis to track and analyze open source component dependencies, enforce security and compliance policies, and fix potential vulnerabilities at source.

   Comments:

Verify that compiler flags are configured to enable all available buffer overflow protections and warnings, including stack randomization, data execution prevention, and to break the build if an unsafe pointer, memory, format string, integer, or string operations are found.

1. For Swift/iOS in XCode, -fobjc-arc for automatic ref counting, -PIE for position independent execution to ensure address space layout randomization, and -fstack-protector-all for stack smashing protection is enabled by default. For Objective C code, these are enabled explicitly.

2. For Kotlin/Android, concurrent mark and sweep GC is used by default, -Werror=format-security is used for format string vulnerability protections, mmap_min_addr is used to mitigate null

pointer dereference privilege escalation, ASLR to randomize key locations in memory, dmesg_restrict and kptr_restrict to avoid leaking kernel addresses.

Comments:

Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.

1. Voatz integrates Snyk into Bitbucket pipelines to achieve DevSecOps within existing CI/CD development workflows. This enables software component analysis to track and analyze component dependencies, enforce security and compliance policies, and fix potential vulnerabilities at source.

2. Vulnerability fixes are prioritized via priority scores and Jira tickets.This enables hardening of the server configuration regularly based on thorough analysis of component dependencies. Additionally, CVSS scores for all server components and dependencies are tracked to ensure compliance with security policies.

   Comments:

Verify that the application, configuration, and all dependencies can be re-deployed using automated deployment scripts, built from a documented and tested runbook in a reasonable time, or restored from backups in a timely fashion.

1. Voatz employs Atlassian Bitbucket pipelines to automate build, testing, and deployment of code.

2. This process is based on well defined pipeline configuration files.

   Comments:

Dependency

Verify that third party components come from pre-defined, trusted and continually maintained repositories.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: A comprehensive list of the various third party components and their corresponding repositories used is available upon request. They are not listed here. Notable components and repositories include Amazon S3 for secure cloud storage, Redis for application cache, and Mongo/MySQL for a secure database.

Verify that the attack surface is reduced by sandboxing or encapsulating third party libraries to expose only the required behavior into the application.

1. Third party libraries are always encapsulated to introduce only the required behavior into the application. For example, the AWS SDK for Java exposes all AWS services but by pulling only the selected module for AWS storage and IAM, Voatz apps and servers ensure that any issues related to other unrelated AWS services such ec2, sts, dynamodb, etc. do not impact the application.

2. Such selective encapsulation is applied on all third party libraries used by mobile and web apps as well as servers.

   Comments:

Validate HTTP Request Header Requirements

Verify that HTTP headers added by a trusted proxy or SSO devices, such as bearer token, are authenticated by the application.

1. Voatz applications and servers do not employ HTTP header based authentication schemes such as bearer tokens. Any CSRF tokens or session cookies issued via cryptographically secure random generators and added to HTTP request/response headers are strictly validated at the routing layer.

2. The following code snippet demonstrates how such token/cookie headers are validated before granting access to any APIs

```
def validate(sessionCookieOpt: Option[HttpCookie], csrfTokenOpt: Option[String])(implicit ec:
ExecutionContext): Future[Authentication[HttpApiSession]] = (sessionCookieOpt,
csrfTokenOpt) match {
 case (Some(cookie), Some(token)) => {
  getSession(cookie.content) map{sessionOpt =>
   sessionOpt match{
    case Some(HttpApiSession(sessionCookie, csrfToken, userId, lastUse)) => {
     if (csrfToken != csrfTokenOpt.get) {
      Left(AuthenticationFailedRejection(CredentialsRejected, List()))
```

   Comments:

Select Controls from Open Web Application Security Project - Application Security Verification Standard 4.0.2 Level 3

General Authenticator Requirements

Verify impersonation resistance against phishing, such as the use of multi-factor authentication, cryptographic devices with intent (such as connected keys with a push to authenticate), or at higher AAL levels, client-side certificates.

1. Andreae, Philip; Braseth, Hilary; and Sawhney, Nimit. State-of-the-Art Security Performs First-Rate Threat Mitigation in Convention Elections, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/DR-V-Security-Whitepaper.pdf

2. Voatz Mobile Voting Platform An Overview: Security, Identity, Auditability, Voatz (2020). https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf

   Comments: The most effective means to thwart phishing attempts for VMA is to use biometric identification. VMA authenticates a voter by requiring an official photo identification, along with a live video of the voter's face; the two images must match. MFA authentication occurs on the administrative end with two administrators needing their authenticator device in order to access the cast ballot record.

Verify that where a credential service provider (CSP) and the application verifying authentication are separated, mutually authenticated TLS is in place between the two endpoints.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application: Encryption shall be implemented in:
   - App/client communication with back end infrastructure.

   Comments: TLS v. 1.2 or newer is used to securely transmit information.

Session Logout and Timeout Requirements

If authenticators permit users to remain logged in, verify that re-authentication occurs periodically with 2FA both when actively used after 12 hours or after an idle period of 15 minutes

1. From the session management module, user sessions are created with a TTL of 15 minutes, after which re-authentication is triggered:

```
def createMobileSession(sessionCookie: String, session: HttpApiSession) = {
 cache.set(s"mobilesession$sessionCookie", session, Some(Duration(900,
TimeUnit.SECONDS)))
}
..
```

2. Voatz iOS and Android apps employ an in-app idle timer which automatically logs out after x minutes of inactivity. The following code from the Android app. shows a warning dialog box and logs out when the timer expires:

```
private fun warningTimer(
 context: Context,
 isScreenOn: Boolean,
 dialog: MaterialDialog?
) {
 warningTimer =
  object : CountDownTimer(remainingIdleTime.toLong(), 100) {
```

```
override fun onTick(millisUntilFinished: Long) {
 if (isScreenOn) {
  if (TimeUnit.MILLISECONDS.toSeconds(millisUntilFinished).toInt() == 16) {
   (dialog)?.contentView?.announceForAccessibility(
    String.format(context.getString(R.string.logout_timeout_message), "15")
   )
  }
  (dialog)?.setContent(
   String.format(
    context.getString(R.string.logout_timeout_message),
    TimeUnit.MILLISECONDS.toSeconds(
     millisUntilFinished
```

Comments: Voatz iOS and Android employ in-app idle timers that call log out and redirect the user to login/authenticate when the idle timer expires.

Algorithms

Verify that encrypted data is authenticated via signatures, authenticated cipher modes, or HMAC to ensure that ciphertext is not altered by an unauthorized party

1. From a cryptographic module:
   def verifySignature(publicKey: PublicKey, signedData: String, signature: String, signatureAlgorithm: String)

2. From a cryptographic module:
   def aes256GCMDecryptUsingKey(encryptedBytes: Array[Byte], key: Array[Byte], nonce: Array[Byte], tag: Array[Byte])

   Comments: Galois Counter Mode (GCM) is used as the message authenticator for AES to ensure data integrity. ECDSA with an NSA and NIST-approved elliptic curve is used for digital signatures.

General Data Protection

Verify that regular backups of important data are performed and that test restoration of data is performed.

1. Backup and Restoration Policy, Section 3.0: Policy:
   - All user-level and system-level information maintained by Voatz, Inc. shall be backed up periodically. The backup media (if it exists) and backup copies shall be stored with sufficient protection and proper environmental conditions.
2. Backup and Restoration Policy, Section 3.1 Review and Testing
   Voatz will carry out annual Testing to verify the effectiveness of the plan, train the DR team on what to do in actual disaster scenarios and highlight areas where the plan needs to be improved. Backup restores are also tested annually to ensure the integrity of the backups in case of a disaster.

Comments:

Verify that backups are stored securely to prevent data from being stolen or corrupted.

1. Backup and Restoration Policy, Section 3.0: Policy:
   - Physical access controls implemented at offsite backup storage locations (if applicable) must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored.
2. Backup and Restoration Policy, Section 3.0: Policy:
   - All backup data must be stored encrypted using strong encryption mechanisms.

Comments:

Malicious Code Search

Verify that the application source code and third party libraries do not contain back doors, such as hard-coded or additional undocumented accounts or keys, code obfuscation, undocumented binary blobs, rootkits, or anti-debugging, insecure debugging features, or otherwise out of date, insecure, or hidden functionality that could be used maliciously if discovered.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: All code is reviewed internally and web, app, and server code is audited regularly by trusted third-party security experts to identify any such unwanted functionality.

Verify that the application source code and third party libraries does not contain time bombs by searching for date and time related functions.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: All code is reviewed internally and web, app, and server code is audited regularly by trusted third-party security experts to identify any such unwanted functionality.

Verify that the application source code and third party libraries do not contain malicious code, such as salami attacks, logic bypasses, or logic bombs.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: All code is reviewed internally and web, app, and server code is audited regularly by trusted third-party security experts to identify any such unwanted functionality.

Verify that the application source code and third party libraries do not contain Easter eggs or any other potentially unwanted functionality.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-CODE-5: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-CODE-5: **Pass**, June 19, 2020.

   Comments: All code is reviewed internally and web, app, and server code is audited regularly by trusted third-party security experts to identify any such unwanted functionality.

7. Attachment C: OWASP Mobile Application Level Security Verification: Table

Attachment C: OWASP Mobile Application Level Security Verification	Yes/No /Partial
Open Web Application Security Project - Mobile Application Security Verification Standard 1.2 Level 1	
Architecture, design, and threat modeling	
All app components are identified and known to be needed	Yes
Security controls are never enforced only on the client side, but on the respective remote endpoints.	Yes
A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	Yes
Data considered sensitive in the context of the mobile app is clearly identified.	Yes
The app should comply with privacy laws and regulations.	Yes
Data Storage and Privacy	
System credential storage facilities need to be used to store sensitive data, such as PII, user credentials, or cryptographic keys.	Yes
No sensitive data should be stored outside of the app container or system credential storage facilities.	Yes
No sensitive data is written to application logs.	Yes
No sensitive data is shared with third parties unless it is a necessary part of the architecture.	Yes
The keyboard cache is disabled on text inputs that process sensitive data.	Yes
No sensitive data is exposed via IPC mechanisms.	Yes
No sensitive data, such as passwords or pins, is exposed through the user interface.	Yes
Cryptography	
The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	Yes
The app uses proven implementations of cryptographic primitives.	Yes
The app uses cryptographic primitives that are appropriate for the particular use case with parameters that adhere to industry best practices.	Yes
The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes	Yes

The app doesn't re-use the same cryptographic key for multiple purposes.	Yes
All random values are generated using a sufficiently secure random number generator.	Yes
Authentication and Session Management	
If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is performed at the remote endpoint.	Yes
If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.	Yes
If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.	Yes
The remote endpoint terminates the existing session when the user logs out.	Yes
A password policy exists and is enforced at the remote endpoint.	Yes
The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.	Yes
Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.	Yes
Network Communication	
Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	Yes
The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	Yes
The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	Yes
Platform Interaction	
The app only requests the minimum set of permissions necessary.	Yes
All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.	Yes
The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.	Yes
The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.	Yes
JavaScript is disabled in WebViews unless explicitly required.	Yes
WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.	Yes

If native methods of the app are exposed to a WebView, verify that the WebView only renders JavaScript contained within the app package.	Yes
Object deserialization, if any, is implemented using safe serialization APIs.	Yes
Code Quality and Build Setting	
The app is signed and provisioned with a valid certificate, of which the private key is properly protected.	Yes
The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).	Yes
Debugging symbols have been removed from native binaries.	Yes
Debugging code and developer assistance code (e.g. test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.	Yes
All third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.	Yes
The app catches and handles possible exceptions.	Yes
Error handling logic in security controls denies access by default.	Yes
In unmanaged code, memory is allocated, freed and used securely.	Yes
Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.	Yes
Select Controls from Open Web Application Security Project - Mobile Application Security Verification Standard 1.2 Level 2	
Architecture, design, and threat modeling	
All app components are defined in terms of the business functions and/or security functions they provide.	Yes
A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.	Yes
All security controls have a centralized implementation.	Yes
There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.	Yes
A mechanism for enforcing updates of the mobile app exists.	Yes
Security is addressed within all parts of the software development lifecycle.	Yes
A responsible disclosure policy is in place and effectively applied.	Yes
Data Storage and Privacy	
No sensitive data is included in backups generated by the mobile operating system.	Yes
The app removes sensitive data from views when moved to the background.	Yes

The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.	Yes
The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.	Yes
No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote endpoint when needed and only be kept in memory.	Yes
Authentication and Session Management	
A second factor of authentication exists at the remote endpoint and the 2FA requirement is consistently enforced.	Yes
Network Communication	
The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.	Yes
The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.	Yes
The app only depends on up-to-date connectivity and security libraries.	Yes
Platform Interaction	
The app protects itself against screen overlay attacks. (Android only)	Yes
A WebView's cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed.	Yes
Verify that the app prevents usage of custom third-party keyboards whenever sensitive data is entered (iOS only).	Yes
Select Controls from Open Web Application Security Project - Mobile Application Security Verification Standard 1.2	
Impede Dynamic Analysis and Tampering	
The app detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.	Yes
The app prevents debugging and/or detects, and responds to, a debugger being attached. All available debugging protocols must be covered.	Yes
Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.	Yes
Impede Comprehension	
All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.	Yes
Impede Eavesdropping	

As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.	Yes

a. Attachment C: Supporting Documentation

Open Web Application Security Project - Mobile Application Security Verification Standard 1.2 Level 1

Note: Both the Android and iOS versions of the Voatz Mobile App were developed with these very security properties in mind, along with numerous other security considerations from OWASP. A "Pass" indication for the Android and iOS apps indicate that the "requirement is applicable to the mobile app and implemented according to best practices."

Architecture, design, and threat modeling

All app components are identified and known to be needed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Security controls are never enforced only on the client side, but on the respective remote endpoints.

1. From a voter onboarding module on the server:
   ```
   if(threatDetected){
                   val threatName = threatNameOpt.get
     val err = s"Voatz has detected an unexpected issue with your device. Please quit the
     app and try again, or contact Voatz."
                   log.error(s"Threat $threatName detected on device $deviceIdFromReq")
   ```

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS, MSTG-ARCH-3: **Pass**, June 19, 2020.

   Comments:

A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Data considered sensitive in the context of the mobile app is clearly identified.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-4: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-4: **Pass**, June 19, 2020.

   Comments:

The app should comply with privacy laws and regulations.

1. Walker, Michael and Owens, Wendy. Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System, Pro V&V (July 17, 2020).

   Req. 3.2.a.1.C: The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot. (Pass)

2. Req. 3.2.7: HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting age population). Thus, election officials must ensure that the voting system they deploy is capable of handling the languages meeting the legal threshold within their districts. (Pass)

   Comments:

Data Storage and Privacy

System credential storage facilities need to be used to store sensitive data, such as PII, user credentials, or cryptographic keys.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Such sensitive data is stored in a TPM or dedicated app storage.

No sensitive data should be stored outside of the app container or system credential storage facilities.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

No sensitive data is written to application logs.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

No sensitive data is shared with third parties unless it is a necessary part of the architecture.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Sensitive data that is shared with a third party include information sent to an identity verification service.

The keyboard cache is disabled on text inputs that process sensitive data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

No sensitive data is exposed via IPC mechanisms.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

No sensitive data, such as passwords or pins, is exposed through the user interface.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments:

Cryptography

The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Symmetric cipher keys (i.e., AES) are ephemeral and created with the server in a secure ECDH based key agreement protocol that utilized NIST approved Elliptic curves.

The app uses proven implementations of cryptographic primitives.

1. From Policy A.10: Cryptography, Section 3.1: All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. From Policy A.10: Cryptography, Section 3.2: The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by Voatz, Inc. IT Ops.

   Comments:

The app uses cryptographic primitives that are appropriate for the particular use case with parameters that adhere to industry best practices.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.

1. From Policy A.10: Cryptography, Section 3.1: All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS: **Pass**, June 19, 2020.

   Comments:

The app doesn't re-use the same cryptographic key for multiple purposes.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

All random values are generated using a sufficiently secure random number generator.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: All random numbers are generated using a cryptographically secure random number generator using device-collected entropy.

Authentication and Session Management

If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is performed at the remote endpoint.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS: **Pass**, June 19, 2020.

2. Authentication on the server in an API routing module.

   case *EncryptedAuthenticateCustomer*(request, ipAddress, hostName) => {

   Comments: A user-defined PIN accesses the app, but rigorous identity verification must be performed in order to perform the most vital app functions.

If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the user's credentials.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS: **Pass**, June 19, 2020.

2. Issuance of random session identification in an API router module.

   val request = EncryptedIssueControlNumber(apiRequest, sessionCookie, ip

   Comments:

If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The remote endpoint terminates the existing session when the user logs out.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: All sessions are created with a TTL (time to live) setting and such sessions are automatically cleared when the TTL expires, even if the remote logout endpoint is not explicitly called.

A password policy exists and is enforced at the remote endpoint.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: After an unsuccessful login attempt, the user is throttled and cannot successfully login for at least 31 seconds. Throttle intervals increase at least 10 seconds for each additional unsuccessful login attempt. Less than 12 unsuccessful login attempts are allowed per hour.

Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: All sessions are created with a TTL (time to live) setting and such sessions are automatically cleared when the TTL setting expires. Additionally, Voatz iOS and Android apps implement in-app inactivity/idle timers that explicitly call logout on the remote endpoint when the idle timer expires.

Network Communication

Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application:
   - All web applications via the most secure version of SSL/TLS.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS: **Pass**, June 19, 2020.

   Comments:

The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Currently, TLS v. 1.2 is used.

The app verifies the X.509 certificate of the remote endpoint when the secure channel is established.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Voatz iOS and Android apps use certificate pinning to verify the validity of remote endpoints. Additionally, both apps employ state of the art root/jailbreak detection, obfuscation and
   code virtualization techniques to ensure that all communication with remote endpoints is secure.

Only certificates signed by a trusted CA are accepted.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Platform Interaction

The app only requests the minimum set of permissions necessary.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments:

All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

JavaScript is disabled in WebViews unless explicitly required.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

WebViews are configured to allow only the minimum set of protocol handlers required (ideally, only https is supported). Potentially dangerous handlers, such as file, tel and app-id, are disabled.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

If native methods of the app are exposed to a WebView, verify that the WebView only renders JavaScript contained within the app package.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Object deserialization, if any, is implemented using safe serialization APIs.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Code Quality and Build Setting

The app is signed and provisioned with a valid certificate, of which the private key is properly protected.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: The certificate is provided by Google Play Store and the Apple App Store for the Android and iOS versions of VMA, respectively.

The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Debugging symbols have been removed from native binaries.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Debugging code and developer assistance code (e.g. test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

All third party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app catches and handles possible exceptions.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Error handling logic in security controls denies access by default.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

In unmanaged code, memory is allocated, freed and used securely.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Select Controls from Open Web Application Security Project - Mobile Application Security Verification Standard 1.2 Level 2

Architecture, design, and threat modeling

All app components are defined in terms of the business functions and/or security functions they provide.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

All security controls have a centralized implementation.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.

1. Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management:
   - Key management should be planned which will include secure key generation, use, storage, distribution, recovery, and removal.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android and iOS: **Pass**, June 19, 2020.

   Comments:

A mechanism for enforcing updates of the mobile app exists.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Security is addressed within all parts of the software development lifecycle.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

A responsible disclosure policy is in place and effectively applied.

1. Policy A.16: Incident Response Policy

2. Policy A.18: Voatz, Inc. Information Security/Sensitivity, Section 3.2: Data Protection Standards: Incident Reporting
   - Any unauthorized disclosure or loss of Level 1 or Level 2 information must be reported to Voatz IT Ops.

   Comments:

Data Storage and Privacy

No sensitive data is included in backups generated by the mobile operating system.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: On Android, backups are explicitly disabled by setting android:allowBackup="false" in the app. manifest. On iOS, all sensitive data is encrypted and no sensitive data is stored outside of the device's secure enclave to prevent any accidental leakage of information in plaintext via iCloud backups.

The app removes sensitive data from views when moved to the background.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments: Voatz iOS and Android apps call logout explicitly and redirect the user to the login view
as soon as the app. is moved to the background, thus invalidating the current user session.

The app does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments: Voatz iOS and Android apps explicitly zero out sensitive data from memory as soon as
feasible, as seen from the code snippets below:
The iOS app. creates a wrapper around the Swift Data type to wipe out bytes on deallocation so secrets cannot be brought back to live by reverse engineering.

```
public class ClearableData {
   var value: Data

   deinit {
      value.deinitialize()
   }
....
func replaceSubrange(_ subrange: Range<Data.Index>, with data: [UInt8]) {
      value.replaceSubrange(subrange, with: data)
   }
```

This is used to replace sensitive data with random, meaningless data

```
var mask = ClearableData()
        for counter in 0 ..< interval {
           tseed.replaceSubrange((tseed.count - 4) ..< tseed.count, with: pack(counter))
           mask.append(CC.digest(tseed, alg: digest))
        }
        mask.count = maskLength
        return mask
```

From the Android app API encryption module which defines an extension to de-initialize byte arrays:

```
fun ByteArray?.deInitialize() {
 if (this != null && this.isNotEmpty()) {
   val size = this.size
   for (i in 0 until size) {
    this[i] = 0
```

```
    }
  }
}
```

```
This is used to replace sensitive data that is no longer processed by the app.
val decryptedBytes: ByteArray?
  try {
    decryptedBytes = cipher.doFinal(data)
    val decryptedBytesToString = String(decryptedBytes)
    decryptedBytes.deInitialize()
```

The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote endpoint when needed and only be kept in memory.

1. Policy AC.4: Mobile Device Encryption, Section 4.2 Cell phones and Tablets
   Any sensitive Voatz, Inc. data stored on a cell phone or tablet must be saved to an encrypted file system using Voatz, Inc.-approved(in the future) software.

2. Some sensitive data is stored on the iPhone Keychain. The accessibility is set to "kSecAttrAccessibleWhenUnlockedThisDeviceOnly", so they are only available when the device is unlocked, and will never move to a new device. Thus, after restoring from a backup of a different device, these items will not be present.

   Comments:

Authentication and Session Management

A second factor of authentication exists at the remote endpoint and the 2FA requirement is consistently enforced.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Network Communication

The app either uses its own certificate store, or pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app doesn't rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and account recovery.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

The app only depends on up-to-date connectivity and security libraries.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments:

Platform Interaction

The app protects itself against screen overlay attacks. (Android only)

1. The Toast Overlay attack on Android targets versions prior to Android 8. The Voatz Mobile App for Android does not run on these older Android versions, so this attack does not apply in that case.

2. For versions 9 and above, the "Draw on Top" permission must be explicitly granted by the user in Settings in order to perform a screen overlay attack. The Voatz Mobile App for Android never requests for such a permission. Specifically, VMA for Android does not ask for the android.permission.SYSTEM_ALERT_WINDOW permission needed to draw on top.

In general, it is considered best practice to disable this permission and only enable it, if absolutely necessary, for trusted apps.

Comments:

A WebView's cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed.

1. iOS: Not applicable. WKWebView in select components of VMA for iOS: Terms and Conditions, Resources URL, and WebUrl on candidates when desired by the client.

2. Android: Not applicable. WKWebView in select components of VMA for Android: Terms and Conditions, Resources URL, and WebUrl on candidates when desired by the client.

   Comments: WebViews are only used for informational purposes to display official election authority/agency approved web resources (HTTPS only) where the user can find additional information about the election. Core application functionality does not rely on WebViews.

Verify that the app prevents usage of custom third-party keyboards whenever sensitive data is entered (iOS only).

1. Ticket VMA-1203: [iOS] Prevent Custom Keyboards from being used in the app.

2. From a user interface module:

```
func application(_ application: UIApplication, shouldAllowExtensionPointIdentifier
extensionPointIdentifier: UIApplication.ExtensionPointIdentifier) -> Bool {
        return extensionPointIdentifier != .keyboard
        }
```

   Comments:

Select Controls from Open Web Application Security Project - Mobile Application Security Verification Standard 1.2

Impede Dynamic Analysis and Tampering

The app detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

   Comments: Voatz iOS and Android apps employ state of the art quantum secure root/jailbreak detection techniques. If the device is rooted or jailbroken, then the user will be unable to authenticate

with the app., initiate identity verification or receive a ballot.

The app prevents debugging and/or detects, and responds to, a debugger being attached. All available debugging protocols must be covered.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments: Voatz iOS and Android apps employ state of the art debugger detection, code obfuscation
and virtualization techniques. Additionally, on Android, all devices must successfully complete Google license verification and safety net checks which explicitly disable debugging.

Obfuscation is applied to programmatic defenses, which in turn impede de-obfuscation via dynamic analysis.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments: Voatz Android and iOS apps employ state of the art code obfuscation and virtualization techniques which severely impede dynamic analysis.

Impede Comprehension

All executable files and libraries belonging to the app are either encrypted on the file level and/or important code and data segments inside the executables are encrypted or packed. Trivial static analysis does not reveal important code or data.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android: **N/A**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS: **Pass**, June 19, 2020.

Comments: All application files are encrypted using file level obfuscation to prevent static analysis.
Additionally, specific code and data segments deemed critical for the secure functioning of the app.
are secured via another round of encryption.

Impede Eavesdropping

As a defense in depth, next to having solid hardening of the communicating parties, application level payload encryption can be applied to further impede eavesdropping.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
    - App/client source code to secure voter data and selections (Android and iOS)

2. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
    - App/client communication with back end infrastructure. (Android and iOS)

Comments: All application data payloads are encrypted in flight using AES GCM with non repeating
nonce where ephemeral key exchange is facilitated by ECDH based key agreement protocols employing NIST approved Elliptic curves.

8. Attachment D: Security Requirements for Databases: Table

Attachment D: Security Requirements for Databases	Yes/No
	43
The DMBS must limit the number of concurrent sessions to an organization-defined number per user for all accounts and/or account types.	Yes
The DBMS must protect against a user falsely repudiating having performed organization-defined actions.	Yes
The DBMS must be able to generate audit records when privileges/permissions are retrieved.	Yes
The DBMS must be able to generate audit records when unsuccessful attempts to retrieve privileges/permissions occur.	Yes
The DBMS must initiate session auditing upon startup.	Yes
The DBMS must produce audit records containing sufficient information to establish what type of events occurred.	Yes
The DBMS must produce audit records containing time stamps to establish when the events occurred.	Yes
The DBMS must produce audit records containing sufficient information to establish where the events occurred.	Yes
The DBMS must produce audit records containing sufficient information to establish the sources (origins) of the events.	Yes
The DBMS must produce audit records containing sufficient information to establish the outcome (success or failure) of the events.	Yes
The DBMS must produce audit records containing sufficient information to establish the identity of any user/subject or process associated with the event.	Yes
The DBMS must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject.	Yes
The DBMS must by default shut down upon audit failure, to include the unavailability of space for more audit log records; or must be configurable to shut down upon audit failure.	Yes
The DBMS must be configurable to overwrite audit log records, oldest first (First-In-First-Out - FIFO), in the event of unavailability of space for more audit log records.	Yes
The DBMS must use system clocks to generate time stamps for use in audit records and application data.	Yes
The audit information produced by the DBMS must be protected from unauthorized	Yes

read access.	
The audit information produced by the DBMS must be protected from unauthorized modification.	Yes
The audit information produced by the DBMS must be protected from unauthorized deletion.	Yes
The DBMS must protect its audit features from unauthorized access.	Yes
The DBMS must protect its audit configuration from unauthorized modification.	Yes
The DBMS must protect its audit features from unauthorized removal.	Yes
The DBMS must limit privileges to change software modules, to include stored procedures, functions and triggers, and links to software external to the DBMS.	Yes
The DBMS software installation account must be restricted to authorized users.	Yes
Database software, including DBMS configuration files, must be stored in dedicated directories, or DASD pools, separate from the host OS and other applications.	Yes
Database objects (including but not limited to tables, indexes, storage, stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be owned by database/DBMS principals authorized for ownership.	Yes
The role(s)/group(s) used to modify database structure (including but not necessarily limited to tables, indexes, storage, etc.) and logic modules (stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be restricted to authorized users.	Yes
Default demonstration and sample databases, database objects, and applications must be removed.	Yes
Unused database components, DBMS software, and database objects must be removed.	Yes
Unused database components that are integrated in the DBMS and cannot be uninstalled must be disabled.	Yes
Access to external executables must be disabled or restricted.	Yes
The DBMS must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	Yes
If passwords are used for authentication, the DBMS must store only hashed, salted representations of passwords.	Yes
If passwords are used for authentication, the DBMS must transmit only encrypted representations of passwords.	Yes
The DBMS must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Yes

The DBMS must use NIST FIPS 140-2 validated cryptographic modules for cryptographic operations.	Yes
The DBMS must separate user functionality (including user interface services) from database management functionality.	Yes
The DBMS must invalidate session identifiers upon user logout or other session termination.	Yes
The DBMS must recognize only system-generated session identifiers.	Yes
The DBMS must maintain the authenticity of communications sessions by guarding against man-in-the-middle attacks that guess at Session ID values.	Yes
The DBMS must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	Yes
In the event of a system failure, the DBMS must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	Yes
The DBMS must protect the confidentiality and integrity of all information at rest.	Yes
The DBMS must isolate security functions from non-security functions.	Yes

a. Attachment D: Supporting Documentation

The DBMS must limit the number of concurrent sessions to an organization-defined number per user for all accounts and/or account types.

1. N/A

2. N/A

   Comments: N/A: Voatz application logic limits a single user to one active session at any given time i.e. it is not possible to have multiple concurrent sessions and any attempt to establish a new session invalidates the previous session.

The DBMS must protect against a user falsely repudiating having performed organization-defined actions.

1. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

2. Policy A.13: Network Security Policy, Section 5.2 Privilege Access Control:
   - Privileged access to prevent configuration changes should be restricted to authorized personnel only.
   - Access control shall be used to provide separate authentication, authorization, and accounting services for network-based access.
   - A Privileged Access Management solution can control credentials accessing the device and commands that can be executed when a session is initiated, providing a complete audit of both commands and sessions.

   Comments:

The DBMS must be able to generate audit records when privileges/permissions are retrieved.

1. An example of an audit log entry generated when a user access level is retrieved to list signups in a certain election:
   "txnId" : NumberLong(948126), "txnType" : "accesslevel", "txnStatus" : "SUCCESS", "auditSourceId" : "800000040", "timestamp" : "2021-11-05T14:50:01.045450Z", "ipAddress" : "172.58.21.118", "action" : "GETSIGNUPS", "userId" : 900000199, "channel": "VAP"

2. An example of an audit log entry generated when a user access level is retrieved to list affidavits in a certain election:
   "txnId" : NumberLong(948393), "txnType" : "accesslevel", "txnStatus" : "SUCCESS", "auditSourceId" : "800000053", "timestamp" : "2021-11-07T23:31:58.654373Z", "ipAddress" : "68.110.100.196", "action" : "GETAFFIDAVITS", "userId" : 900000810, "channel": "VAP"

Comments: An audit log entry is written to the database whenever an access level is retrieved to determine whether the user has the necessary privileges to execute a certain action for e.g. get list of signups, get list of affidavits, etc.

The DBMS must be able to generate audit records when unsuccessful attempts to retrieve privileges/permissions occur.

1. An example of an audit log entry generated when an attempt to perform an action that the user does not have permissions for is detected:
"txnId" : NumberLong(943250), "txnType" : "accesslevel", "txnStatus" : "FAILURE", "auditSourceId" : "800000043", "timestamp" : "2020-10-15T13:17:09.036230Z", "ipAddress" : "94.59.239.90", "action" : "GETSIGNUPS", "userId" : 900000190, "channel" : "VAP"

2. An audit log entry is generated whenever an unsuccessful attempt to retrieve permissions is detected.

   Comments:

The DBMS must initiate session auditing upon startup.

1. Voatz servers employ event sourcing to automatically initiate auditing on startup where log entries corresponding to each event type are logged.

2. Along with the event source, Voatz servers initiate event channel, event timestamp, and other metadata relevant for the specific transaction upon startup.

   Comments:

The DBMS must produce audit records containing sufficient information to establish what type of events occurred.

1. An example of an audit log entry indicating auth (login/logout) requests from a certain Voatz Mobile App user:
"txnId" : NumberLong(813767), **"txnType" : "login"**, "txnStatus" : "SUCCESS", "userId" : 1730153853, "channel" : "VMA", "timestamp" : "2021-11-19T19:51:04.596Z", "ipAddress" : "198.241.2.100", "deviceId" : "ios-EE2B7626-EB6D..""

   "txnId" : NumberLong(813766), **"txnType" : "logout"**, "txnStatus" : "SUCCESS", "userId" : 1699377507, "channel" : "VMA", "timestamp" : "2021-11-19T19:29:50.347Z", "ipAddress" : "71.223.122.232", "deviceId" : "ios-C1581EB3-89B3-..""

2. An example of an audit log entry indicating creation of a ballot (event) for a certain election:
"txnId" : NumberLong(951029), **"txnType" : "event"**, "txnStatus" : "SUCCESS", "auditSourceId" : "500014250", "timestamp" : "2021-11-08T06:37:01.117621Z", "ipAddress" : "73.219.188.197", "action" : "CREATE", "userId" : 900000001, "channel" : "VAP"

   Comments: Audit log entries use the transaction type attribute (txnType) to clearly indicate the type of audit event being logged

The DBMS must produce audit records containing time stamps to establish when the events occurred.

1. An example of an audit log entry generated when a new Voatz Mobile App user is created:
   txnId" : NumberLong(948186), "txnType" : "customer", "txnStatus" : "SUCCESS", "auditSourceId" : "1689187950", **"timestamp" : "2021-11-06T01:13:24.267Z"**, "ipAddress" : "172.58.21.118", "action" : "CREATE", "channel": "VMA"

2. An example of an audit log entry generated when a user attempts to login to the Voatz Admin Portal:
   "txnId" : NumberLong(947431), "txnType" : "orguser", "txnStatus" : "SUCCESS", "auditSourceId" : "800000042", **"timestamp" : "2021-11-04T01:17:15.667266Z"**, "ipAddress" : "135.84.57.144", "action" : "LOGIN", "userId" : 900000171, "channel": "VAP"

   Comments: All audit log entries contain a timestamp with an offset from UTC/Greenwich in the ISO-8601 calendar system

The DBMS must produce audit records containing sufficient information to establish where the events occurred.

1. An example of an audit log entry generated on an attempt to verify a user for an election via Voatz Mobile App. (VMA):
   "txnId" : NumberLong(954201), "txnType" : "orgidv", "txnStatus" : "Success", "authData" : [{ "key" : "oidvSource", "value" : "datastore" }, { "key" : "oidvReferenceId", "value" : "oidv_100080_800000073_1636333827" }, { "key" : "Text", "value" : "14802485495" }], "userId" : 1645667116, **"channel" : "VMA"**, "timestamp" : "2021-11-19T20:39:08.178284Z", "ipAddress" : "135.84.57.36", "deviceId" : "ios-6D83B064-E97B..."

2. An example of an audit log entry generated when a user attempts to login to Voatz Admin Portal (VAP)
   "txnId" : NumberLong(947431), "txnType" : "orguser", "txnStatus" : "SUCCESS", "auditSourceId" : "800000023", "timestamp" : "2021-11-04T01:17:15.667266Z", "ipAddress" : "135.84.57.144", "action" : "LOGIN", "userId" : 900000451, **"channel": "VAP"**

   Comments: All audit log entries contain a channel attribute that clearly indicates where the log event occured.

The DBMS must produce audit records containing sufficient information to establish the sources (origins) of the events.

1. An example of audit log entry generated when a new Voatz Mobile App user is created:
   txnId" : NumberLong(948186), **"txnType" : "customer"**, "txnStatus" : "SUCCESS", **"auditSourceId" : "1689187950"**, "timestamp" : "2021-11-06T01:13:24.267Z", "ipAddress" : "172.58.21.118", "action" : "CREATE", **"channel": "VMA"**

2. An example of an audit log entry generated

"txnId" : NumberLong(947431), **"txnType" : "orguser"**, "txnStatus" : "SUCCESS", **"auditSourceId" : "800000042"**, "timestamp" : "2021-11-04T01:17:15.667266Z", "ipAddress" : "135.84.57.144", "action" : "LOGIN", "userId" : 900000171, **"channel": "VAP"**

Comments: All audit log entries contain an audit source id (auditSourceId) attribute which together with the transaction type and channel uniquely identifies the origin of the audit log event

The DBMS must produce audit records containing sufficient information to establish the outcome (success or failure) of the events.

1. An example of an audit log entry generated on an attempt to verify a user's identity via the Voatz Mobile App:
"txnId" : NumberLong(954210), "txnType" : "basicidoidv", **"txnStatus" : "PENDING"**, **"authData"** : [{ "key" : "idvReferenceId", "value" : "Auto" }, { "key" : "idvSource", "value" : "Blockscore" }, { "key" : "voatzIdvStatus", "value" : "SUCCESS" }, { "key" : "extAPIIdvStatus", "value" : "valid" }, { "key" : "voatzIdvTimestamp", "value" : "2021-11-19T22:25:43.512Z" }, { "key" : "extAPIIdvTimestamp", "value" : "2021-11-19T22:25:43.512Z" }, { "key" : "voatzIdvFailureReason", "value" : "" }, { "key" : "extAPIIdvFailureReason", "value" : "" }, { "key" : "idoReferenceId", "value" : "5cede519-9472-462b-a9e2-f2e7adca96e4" }, { "key" : "idoSource", "value" : "NETVERIFY" }, { "key" : "voatzIdoStatus", "value" : "PENDING" }, { "key" : "extAPIIdoStatus", "value" : "" }, { "key" : "voatzIdoTimestamp", "value" : "2021-11-19T22:25:43.880Z" }

2. All audit log entries contain a transaction status attribute which, together with the authData attribute (only relevant for certain transaction types), clearly establishes the outcome of the event generating the audit log entry.

   Comments:

The DBMS must produce audit records containing sufficient information to establish the identity of any user/subject or process associated with the event.

1. An audit log entry generated when a Voatz mobile app user attempts to login
"txnId" : NumberLong(954213), "txnType" : "login", "txnStatus" : "SUCCESS", **"userId" : 1697138693**, "channel" : "VMA", "timestamp" : "2021-11-19T22:40:10.460Z", "ipAddress" : "24.23.61.46", "deviceId":"ios-6D83B064-E9.."

2. An audit log entry generated when a Voatz mobile app user attempts to logout:
"txnId" : NumberLong(813766), "txnType" : "logout", "txnStatus" : "SUCCESS", **"userId" : 1699377507**, "channel" : "VMA", "timestamp" : "2021-11-19T19:29:50.347Z", "ipAddress" : "71.223.122.232", "deviceId" : "ios-C1581EB3-89B3-..."

   Comments: Audit log entries contain a user id (userId) attribute that uniquely identifies the subject associated with the log entry event.

The DBMS must include additional, more detailed, organization-defined information in the audit records for audit events identified by type, location, or subject.

1. An example of an audit log entry generated on an attempt to verify a user for an election via Voatz Mobile App. (VMA):
"txnId" : NumberLong(954201), "txnType" : "orgidv", "txnStatus" : "Success", **"authData" : [{ "key" : "oidvSource", "value" : "datastore" }, { "key" : "oidvReferenceId", "value" : "oidv_100080_800000073_1636333827" }, { "key" : "Text", "value" : "14802485495" }],** "userId" : 1645667116, "channel" : "VMA", "timestamp" : "2021-11-19T20:39:08.178284Z", "ipAddress" : "135.84.57.36", "deviceId" : "ios-6D83B064-E97B..."

2. Audit log entries contain an organization specific authorization data (authData) attribute which allows an organization to define/configure its own audit attributes. In the example above, the
datastore reference **oidv_100080_800000073_1636333827** defines a mandatory field **Text** which must be supplied by/associated with the verifying entity as part of their verification workflow. Additionally, attributes such as location, etc. can be easily configured to be logged as part of audit log
entries.

   Comments:

The DBMS must by default shut down upon audit failure, to include the unavailability of space for more audit log records; or must be configurable to shut down upon audit failure.

1. N/A

2. N/A

   Comments: N/A: Voatz databases cannot be shutdown due to the global nature of the application. Log entries are periodically archived and such archives are encrypted via cryptographically secure random secrets. Due to the nature of the archival process on dedicated backup environments, unavailability of disk space in production environments is never an issue.

The DBMS must be configurable to overwrite audit log records, oldest first (First-In-First-Out - FIFO), in the event of unavailability of space for more audit log records.

1. N/A

2. N/A

   Comments: N/A: Voatz audit log entries are never overwritten/updated. These log entries are generated via append only event sourcing which eliminates any possibility of mutable updates. Log entries are periodically archived and such archives are encrypted via cryptographically secure random secrets. Due to the nature of the archival process on dedicated backup environments, unavailability of disk space in production environments is never an issue.

The DBMS must use system clocks to generate timestamps for use in audit records and application data.

1. From a database module, which is an example of a timestamp being put on a record:

   val createTsSet = set("createTs", OffsetDateTime.now.toString())

2. The OffsetDateTime module used, from the aforementioned database module:

   import java.time.OffsetDateTime

   Comments: All audit log entries contain a timestamp with an offset from UTC/Greenwich in the ISO-8601 calendar system

The audit information produced by the DBMS must be protected from unauthorized read access.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality.

   Additionally, access to information/data deemed sensitive or confidential is limited, based on a need to know.

   Comments: Audit log entries are not available via any public APIs and are only available in read only mode via local micro services with strict access control.

The audit information produced by the DBMS must be protected from unauthorized modification.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality.

   Additionally, access to information/data deemed sensitive or confidential is limited, based on a need to know.

   Comments: Audit log entries cannot be created/updated/deleted via any public APIs and are only available in read only mode via local micro services with strict access control.

The audit information produced by the DBMS must be protected from unauthorized deletion.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality.

Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

Comments: Audit log entries cannot be created/updated/deleted via any public APIs and are only available in read only mode via local micro services with strict access control.

The DBMS must protect its audit features from unauthorized access.

1. Policy AC10: Database Credentials Policy, Section 4.1: General
   Database credentials must not be stored in a location that can be accessed by unauthorized parties.

2. Policy AC10: Database Credentials Policy, Section 4.2: Storage of Database Credentials
   Database credentials shall be stored only in an encrypted manner.

   Comments: Audit logging features are strictly controlled by Voatz server modules for transactions that are deemed relevant for auditing purposes. Audit log features cannot be created/updated/deleted via any public APIs.

The DBMS must protect its audit configuration from unauthorized modification.

1. Policy AC10: Database Credentials Policy, Section 4.1: General
   Database credentials must not be stored in a location that can be accessed by unauthorized parties.

2. 2. Policy AC10: Database Credentials Policy, Section 4.2: Storage of Database Credentials
   Database credentials shall be stored only in an encrypted manner.

   Comments: Audit logging configuration is strictly controlled by Voatz server modules. Audit log configuration cannot be created/updated/deleted via any public APIs.

The DBMS must protect its audit features from unauthorized removal.

1. Policy AC10: Database Credentials Policy, Section 4.1: General
   Database credentials must not be stored in a location that can be accessed by unauthorized parties.

2. Policy AC10: Database Credentials Policy, Section 4.2: Storage of Database Credentials
   Database credentials shall be stored only in an encrypted manner.

   Comments: Audit logging features are strictly controlled by Voatz server modules for transactions that are deemed relevant for auditing purposes. Audit log features cannot be created/updated/deleted via any public APIs.

The DBMS must limit privileges to change software modules, to include stored procedures, functions and triggers, and links to software external to the DBMS.

1. Policy A.9: Access Control Policy, Section 4.2 User Access Provisioning:
   Access to critical corporate and election systems shall be managed and controlled by the Voatz IT Ops Super User(s).

2. Policy A.9: Access Control Policy, Section 6.1 Information Access Restriction
   Read-only access is granted to users based on their roles, while functions that allow users to

create, modify, or delete information is restricted to designated super users/admins. (E.g., Only admins can create or delete code repositories, while developers are restricted to adding new code, and editing existing code. Only a super admin or designated alternate with super admin access can push code to the live/production environment.

Comments: Any software modules required for the DBMS to function can only be installed/updated by a super user. There is no public access to such features and private access is limited/controlled strictly by role.

The DBMS software installation account must be restricted to authorized users.

1. Policy A.9: Access Control Policy, Section 4.2 User Access Provisioning:
   Access to critical corporate and election systems shall be managed and controlled by the Voatz IT Ops Super User(s).

2. Policy A.9: Access Control Policy, Section 6.1 Information Access Restriction
   Only a super admin or designated alternate with super admin access can push code to the live/production environment.

   Comments: Any software modules required for the DBMS to function can only be installed/updated by a super user. There is no public access to such features and private access is limited/controlled strictly by role.

Database software, including DBMS configuration files, must be stored in dedicated directories, or DASD pools, separate from the host OS and other applications.

1. Policy A.9: Access Control Policy, Section 6.5 - Access Control to Program Source Code
   - Source code shall be managed using on-premise repositories that segregate the code into the major parts of the service - Frontend (mobile apps, web application), Backend (server, database, blockchain).

2. Policy OM.2: Information Security Management System (ISMS) Policy, Section 4.0: General ISMS Policy Statements:
   The Voatz Mobile Platform hosts political and non-political elections and is committed to protecting its data and that of its customers. To achieve this, the company has implemented security and privacy protections throughout its corporate and elections infrastructure.
   Voatz ISMS covers the following components of the Voatz Mobile Elections Platform:

   - Corporate Infrastructure which includes the employees involved with and systems used create, deploy, maintain and store the source code and proprietary information pertaining to Voatz mobile apps, web based portals, and other Voatz products
   - Elections Infrastructure which consists of software applications that support elections operations including, client applications (ios, android apps), core server, web servers, database, and blockchain.

Comments: Voatz servers employ separate partitions for host OS and DBMS related files. As seen from the snapshot below, all DBMS related features are installed under /var, separate from the OS kernel under /boot and all other OS files and applications under / .

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda2	30G	23G	7.0G	77%	/
/dev/sda1	497M	106M	391M	22%	/boot
/dev/sdb1	252G	4G	248G	2%	/var

Database objects (including but not limited to tables, indexes, storage, stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be owned by database/DBMS principals authorized for ownership.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality.

   Comments: Voatz application logic uses roles and granular feature based access levels to limit access to the DBMS. User roles are clearly distinguished from Admin roles and any APIs consumed by user roles never provide ownership to DBMS objects.

The role(s)/group(s) used to modify database structure (including but not necessarily limited to tables, indexes, storage, etc.) and logic modules (stored procedures, functions, triggers, links to software external to the DBMS, etc.) must be restricted to authorized users.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality.

   Comments: Voatz application logic uses roles and granular feature based access levels to limit access to the DBMS. User roles are clearly distinguished from Admin roles and any APIs consumed by user roles cannot access any features that modify the DBMS structure.

Default demonstration and sample databases, database objects, and applications must be removed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-1: **Pass**, June 19, 2020.

   Comments: No demo/sample databases/objects are used in any Voatz environment.

Unused database components, DBMS software, and database objects must be removed.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-1: **Pass**, June 19, 2020.

Comments:

Unused database components that are integrated in the DBMS and cannot be uninstalled must be disabled.

1. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – Android, MSTG-ARCH-1: **Pass**, June 19, 2020.

2. OWASP Mobile Application Security Checklist Evaluation, Security Requirements – iOS, MSTG-ARCH-1: **Pass**, June 19, 2020.

Comments:

Access to external executables must be disabled or restricted.

1. Policy AC.10: Database Credentials Policy, Section 1.0: Purpose

   Systems running on Voatz, Inc.'s managed networks often require the use of internal databases. In order to access any internal databases, a system must authenticate to the database by presenting acceptable credentials. Database usernames and passwords (i.e., database credentials) must be securely stored and retrieved.

2. Policy AC.10: Database Credentials Policy, Section 4.1 General:
   In order to maintain the security of Voatz, Inc.'s internal databases, access by software programs must be granted only when authenticated. The credentials used for this authentication must not reside in the program's source code in clear text. Database credentials must not be stored in a location that can be accessed by unauthorized parties.

Comments:

The DBMS must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

1. Policy AC.10: Database Credentials Policy, Section 1.0: Purpose

   Systems running on Voatz, Inc.'s managed networks often require the use of internal databases. In order to access any internal databases, a system must authenticate to the database by presenting acceptable credentials. Database usernames and passwords (i.e., database credentials) must be securely stored and retrieved.

2. Policy AC.10: Database Credentials Policy, Section 4.1 General:

In order to maintain the security of Voatz, Inc.'s internal databases, access by software programs must be granted only when authenticated. The credentials used for this authentication must not reside in the program's source code in clear text. Database credentials must not be stored in a location that can be accessed by unauthorized parties.

Comments: Each organization created in Voatz databases controls its own set of organization users where a new organization user must be created with an existing organizationId and can only access resources available to that organization. Voatz application logic uses roles and granular feature based access levels to ensure that an organization user will never be able to access any resources outside of their organization.

If passwords are used for authentication, the DBMS must store only hashed, salted representations of passwords.

1. Policy A.10: Acceptable Encryption Policy, Section 3.5: User Passwords
   - Where applicable, user passwords shall be stored in a secure manner by using HMAC with hash.
   - All user passwords should be salted on a per secret basis.

2. Policy AC10: Database Credentials Policy, Section 4.2: Storage of Database Credentials
   Passwords or passphrases used to access a database must adhere to the Password Policy.

   Comments: All user credentials are hashed using slow hashing primitives such as B-Crypt.

If passwords are used for authentication, the DBMS must transmit only encrypted representations of passwords.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application
   All private keys for encryption must be password protected and not stored in the clear on systems.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application
   Encryption shall be implemented in:
   - During sensitive data transmission over public networks

   Comments: Any data transmitted by Voatz applications is encrypted via AES GCM with non repeating nonce. Specifically, any credentials used for authenticating against databases are never transmitted in cleartext.

The DBMS must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

1. Policy A.9: Access Control Policy, Section 6.2 - Secure Log-on Procedures
   Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

2. Policy A.10: Cryptography: Section 3.1: Encryption Method and Application:
   Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS,

- Device/file encryption i.e. partial disk encryption and full disk encryption,
- During data transmission between and among infrastructure components,
- During sensitive data transmission over public networks,
- storage on disk, particularly secrets and user passwords.

Comments:

The DBMS must use NIST FIPS 140-2 validated cryptographic modules for cryptographic operations.

1. From Policy A.10: Cryptography, Section 3.6: Key Management:
    - Key generation must be seeded from an industry standard random number generator.

2. From Policy A.10: Cryptography, Section 3.1: All Voatz, Inc. encryption shall be done using approved cryptographic modules.

    Comments: Sample of NIST FIPS validated modules used for encryption at rest:
    SHOW GLOBAL VARIABLES LIKE 'have_openssl';
    have_openssl YES
    SHOW GLOBAL VARIABLES LIKE 'version_ssl_library';
    version_ssl_library OpenSSL 1.x.y-fips ...

The DBMS must separate user functionality (including user interface services) from database management functionality.

1. From Policy A.9: Access Control Policy, Section 3.0: This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.
    - Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
    - Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
    - Need to Use – users will only be able to access physical and logical facilities required for their role.

2. Policy AC9: Server Security, Section 4.2 General Configuration and Backup Guidelines:
    Always use the least privilege to perform a function. Do not use root/admin accounts when a non-privileged account is sufficient.

    Comments: Organization users can only access DBMS through well defined APIs subject to roles and granular feature based access levels. These APIs do not offer any database management functionality.

The DBMS must invalidate session identifiers upon user logout or other session termination.

1. All logout requests explicitly delete the user's session :
   case *EncryptedLogoutCustomer*(request, sessionCookieOpt, ipAddress) =>{
   ...
    case *Some*(sessionCookie) => {
     SessionAuthenticator.*deleteSession*(sessionCookie.content) match {

2. Additionally, all sessions are created with a TTL (time to live) setting such that the session is automatically cleared on TTL expiry, even if logout is not explicitly called:

   def createMobileSession(sessionCookie: String, session: HttpApiSession) = {
    Cache.set(s"mobilesession$sessionCookie", session, *Some*(*Duration*(900,
   TimeUnit.*SECONDS*)))
   }

   Comments: Session identifiers are generated using cryptographically secure random generators and are invalidated on logout. Additionally, sessions are created with a TTL (time to live) setting and are automatically cleared on TTL expiry.

The DBMS must recognize only system-generated session identifiers.

1. Session identifiers are generated via well defined auth APIs that create such identifiers using cryptographically secure random generators before persisting them.

2. It is not possible to create session identifiers outside of these APIs or directly in the DBMS.

   Comments:

The DBMS must maintain the authenticity of communications sessions by guarding against man-in-the-middle attacks that guess at Session ID values.

1. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS.
2. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
   - During sensitive data transmission over public networks.

   Comments: All communication to the servers and DBMS uses TLS v. 1.2. Additionally, all data in flight is encrypted with AES in Galois Counter Mode with non repeating nonce.

The DBMS must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.

1. Voatz servers are architected with a clear separation of concerns.

2. This architecture ensures that the DBMS state is never compromised in the event of system failure.

   Comments:

In the event of a system failure, the DBMS must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.

1. Voatz servers employ event sourcing based on Akka persistence using databases separate from the core transactional databases.

2. This event sourcing makes it possible to restore to a previous stable state in the event of failure.

   Comments:

The DBMS must protect the confidentiality and integrity of all information at rest.

1. Policy A.10: Acceptable Encryption Policy, Section 3.3 Data Protection
   - Data at rest:
     - All Voatz, Inc. and customer data deemed a secret shall be stored in an encrypted manner.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1: Encryption Method and Application: Encryption shall be implemented in:
   - storage on disk, particularly secrets and user passwords.

   Comments: All data at rest is protected using FIPS 140-2 cryptographic modules. Additionally, all archives and backups are also secured using such cryptographic modules in dedicated backup environments, separate from production environments.

The DBMS must isolate security functions from non-security functions.

1. Voatz servers are architected with a clear separation of concerns and employ separate databases for security functionality, such as access levels, authentication, and auditing.

2. For reasons of security, the aforementioned activities are never mixed with the core transactional databases.

   Comments:

9. Attachment E: Select Controls from NIST SP 800-171: Table

Attachment E: Select Controls from NIST SP 800-171	Yes/No
Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Yes
Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Yes
Monitor and control remote access sessions.	Yes
Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Yes
Allow wireless access prior to allowing such connections.	Yes
Protect wireless access using authentication and encryption.	Yes
Control connection of mobile devices.	Yes
Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	Yes
Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Yes
Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Yes
Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Yes
Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	Yes
Establish and enforce security configuration settings for information technology products employed in organizational systems.	Yes
Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Yes
Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Yes
Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Yes

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	Yes
Identify system users, processes acting on behalf of users, and devices.	Yes
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Yes
Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	Yes
Store and transmit only cryptographically-protected passwords.	Yes
Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Yes
Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Yes
Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Yes
Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Yes
Control the use of removable media on system components.	Yes
Ensure that organizational systems containing sensitive data are protected during and after personnel actions such as terminations and transfers.	Yes
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	Yes
Protect and monitor the physical facility and support infrastructure for organizational systems.	Yes
Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Yes
Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	Yes
Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Yes
Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	Yes

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Yes
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Yes
Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Yes
Protect the authenticity of communications sessions.	Yes
Identify, report, and correct information and information system flaws in a timely manner.	Yes
Provide protection from malicious code at appropriate locations within organizational information systems.	Yes
Monitor system security alerts and advisories and take action in response.	Yes
Update malicious code protection mechanisms when new releases are available.	Yes
Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Yes
Employ the principle of least privilege, including for specific security functions and privileged accounts.	Yes
Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	Yes
Perform maintenance on organizational systems.	Yes
Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Yes
Prohibit the use of portable storage devices when such devices have no identifiable owner.	Yes
Screen individuals prior to authorizing access to organizational systems containing sensitive data.	Yes
Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of sensitive data.	Yes
Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Yes
Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission unless otherwise protected by alternative physical safeguards.	Yes

Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive information.	Yes
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	Yes
Identify unauthorized use of organizational systems.	Yes
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Yes
Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Yes
Limit unsuccessful login attempts.	Yes
Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Yes
Terminate (automatically) a user session after a defined condition.	Yes
Route remote access via managed access control points.	Yes
Verify and control/limit connections to and use of external information systems.	Yes
Limit use of portable storage devices on external systems.	Yes
Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Yes
Review and update logged events.	Yes
Alert in the event of an audit logging process failure.	Yes
Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Yes
Limit management of audit logging functionality to a subset of privileged users.	Yes
Analyze the security impact of changes prior to implementation.	Yes
Control and monitor user-installed software.	Yes
Enforce a minimum password complexity and change of characters when new passwords are created.	Yes
Allow temporary password use for system logons with an immediate change to a permanent password.	Yes
Obscure feedback of authentication information.	Yes
Test the organizational incident response capability.	Yes
Supervise the maintenance activities of maintenance personnel without required access authorization.	Yes
Protect the confidentiality of backup sensitive information at storage locations.	Yes
Escort visitors and monitor visitor activity.	Yes
Remediate vulnerabilities in accordance with risk assessments.	Yes

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Yes
Establish and manage cryptographic keys for cryptography employed in organizational systems.	Yes
Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	Yes

a. Attachment E: Supporting Documentation

Attachment E: Supporting Documentation

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

1. Policy A.9: Access Control, Section 3.0:
   Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

2. ISO Control A.6.2.1: Mobile Device Management Policy, Section 3.1: Technology and Security Requirements:
   When remote, devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection.

   Comments:

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

1. Policy A.9: Access Control, Section 3.0:
   Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

2. Policy AC.9: Server Security Policy, Section 4.1 Ownership and Responsibilities:
   All servers deployed at Voatz, Inc. must be the responsibility of corporate IT Ops.

   Comments:

Monitor and control remote access sessions.

1. Policy AC.6: Remote Access Policy, Section 4.2: Requirements:
   Secure remote access must be strictly controlled. Access must be approved by Voatz, Inc. IT Ops.

2. Policy A.12: Operations Security Policy, Section 8.0: Control of Operational Software
   Voatz monitors systems to detect unauthorized access and modification.

   Comments:

Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

1. Policy A.13: Network Security Policy, Section 5.9 Encrypt sensitive network traffic:
   Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

2. Policy AC.7: Virtual Private Network (VPN) Policy, Section 3.0: Policy:

The VPN should be controlled by a strong authentication method. Initial configuration will be done by Voatz, Inc. IT OPs and users will be responsible for selecting a strong password after initial login.

Comments:

Allow wireless access prior to allowing such connections.

1. Policy A.8: IT Asset Management Policy, Section 5.1: Asset Types
   The following asset types are subject to tagging and tracking:
   - Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), wireless access points, and storage)

2. Policy IC.7: Wireless Communication Policy, Section 4.4 Access to Wireless Networks
   Access shall be granted according to the user's role. Voatz, Inc. is responsible for maintaining the confidentiality, integrity, and availability of its resources and must manage the roles accordingly. Access to the Voatz, Inc. corporate network through any device not on site must use remote access authentication through the Voatz VPN.

   Comments:

Protect wireless access using authentication and encryption.

1. Policy A.13: Network Security Policy, Section 5.9 Encrypt sensitive network traffic:
   Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

2. Policy IC.7: Wireless Communication Policy, Section 4.1: General Requirements:
   All wireless infrastructure devices that reside at Voatz, Inc. sites and connect to Voatz, Inc. networks, or provide access to information classified as Voatz, Inc. Confidential (requiring notification or otherwise) must:
   - Use Voatz, Inc. approved authentication protocols and infrastructure.
   - Use Voatz, Inc. approved encryption protocols.

   Comments:

Control connection of mobile devices.

1. Policy A.6.2.1: Mobile Device Management Policy, Section 3.1: Technology and Security Requirements
   Only devices managed by IT or authorized by IT will be allowed to connect directly to the internal corporate network.

2. Policy A.6.2.1: Mobile Device Management Policy, Section 3.1: Technology and Security Requirements
   When remote, devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection.

Comments:

Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

1. From Voatz Security Awareness Training:
   It's important to have security policies and processes in place in order to comply with our customers', partners', and election industry security and privacy requirements.

   Additionally, security audits conducted by external entities often request documentation covering all areas of our mobile elections platform, so it's important for all employees and contractors to review these policies at least annually.

2. Example from Security Training Videos:
   - **Training Videos**
     ISO 27001 --https://www.youtube.com/watch?v=io6w3Yw4q9w

   Comments: Such training has been implemented in accordance with ISO 27001 certification.

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

1. Policy A.7: Personnel Security Policy, Section 4.4: Personnel Onboarding
   The organization must upon personnel start:
   - Provide onboarding guidance via handbook, intranet, etc.
   - Obtain a signed NDA and prior inventions agreement.
   - Obtain signed employment agreement with security and privacy expectations.

2. Policy AC.7: Virtual Private Network (VPN) Policy:
   Organization members understand when and how to use virtual private networks.

   Comments:

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

1. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   All security-related events on critical or sensitive systems must be logged and audit trails saved.

2. Policy A.11: Physical and Environmental Security Policy, Section 4.2 Physical Access Control:
   Maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.

   Comments:

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

1. Policy AC.9: Server Security Policy, Section 4.3 Monitoring:
   Security-related events will be reported to Voatz, Inc. IT Ops, who will review logs and escalate incidents as necessary.

2. Policy A.16 Information Security Incident Management
   Voatz, Inc.'s response to situations that threaten the security or privacy of confidential information shall ensure events and activities associated with those events are properly identified, contained, investigated, and remedied.

   Comments:

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

1. Policy AC.9: Server Security Policy: Section 4.1: Ownership and Responsibilities:
   Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Voatz, Inc. IT Ops.

2. Policy A.8: Asset Management Policy: Section 1.0: Overview:
   Asset management is the process of receiving, tagging, documenting, and disposing of equipment. It is important to maintain up to date inventory and asset controls to ensure that equipment locations and dispositions are understood. Lost or stolen equipment can contain sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

   Comments:

Establish and enforce security configuration settings for information technology products employed in organizational systems.

1. Policy AC.9: Server Security Policy, Section 2.0: Scope:
   Based on the type of servers, such as Cloud Managed Systems, Cloud Managed Instances or Physical Servers, the policy for handling patching, configuration, backups, and monitoring shall vary. Configuration and Backup of remote and on-premises servers managed by Voatz, Inc.

2. Policy A.10: Acceptable Encryption Policy, Section 3.1 Encryption Method and Application

   Encryption shall be implemented in:

   - Device/file encryption i.e. partial disk encryption and full disk encryption.

   Comments:

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

1. Policy A.11: Physical and Environmental Security Policy, Section 4.2: Physical Access Control: The organization will control entry/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).

2. Policy AC9: Server Security Policy, Section 4.1: Ownership and Responsibilities:
Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run a server) is the responsibility of Voatz, Inc. in the case of on-premise physical servers being used.

   Comments:

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

1. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines: Operating System configuration should be in accordance with approved Voatz, Inc. IT guidelines. Services and applications that will not be used must be disabled where practical.

2. Policy AC.9: Server Security Policy:
The organization manages, configures and protects organization servers and hosts based on industry best practices.

   Comments:

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

1. ISO Control A.6.2.1: Mobile Device Management Policy, Section 3.2: User Requirements:
   - Users may only load corporate data that is essential to their role onto their mobile device(s).

2. ISO Control A.6.2.1: Mobile Device Management Policy, Section 3.2: User Requirements:
   - Applications must only be installed from official platform-owner approved sources. Installation of applications from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT.

   Comments:

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

1. Policy A.13: Network Security Policy, Section 4.0:
All the traffic to and from a particular list of IPs and Domains (Blacklisted) should be denied at the Firewall Level.

2. Policy AC.9: Server Security Policy, Section 4.2 General Configuration and Backup Guidelines: Operating System configuration should be in accordance with approved Voatz, Inc. IT guidelines. Services and applications that will not be used must be disabled where practical.

Comments:

Identify system users, processes acting on behalf of users, and devices.

1. A.9 Access Control Policy: Section 1.0 Purpose
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

2. A.8 Asset Management Policy: Section 2.0 Purpose
   This policy provides procedures and protocols supporting effective organizational asset management specifically focused on electronic devices.

   Comments:

Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

1. Policy A.6.2.1: Mobile Device Management Policy, Section 3.1: Technology and Security Requirements:
   Only devices managed by IT or authorized by IT will be allowed to connect directly to the internal corporate network.

2. Policy A.9: Access Control Policy, Section 3.0 Business Requirements
   Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

   Comments:

Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.

1. Policy AC.5: Password Policy, Section 5.1: General:
   Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.

2. Policy A.9: Access Control Policy, Section 6.4 - Use of Privileged Utility Programs:
   - Where possible and appropriate privileged utility programs must incorporate multi-factor authentication (MFA).

   Comments:

Store and transmit only cryptographically-protected passwords.

1. Policy A.10: Cryptography: Section 3.3:
   - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.
   - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted.

2. Policy A.10: Cryptography: Section 3.5:
   - Where applicable, user passwords shall be stored in a secure manner by using HMAC with hash.

   Comments:

Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

1. Policy A.16 Information Security Incident Management Policy: Section 1.0: Overview

   The purpose of this policy is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information.

2. Documentation for ISO Control A.16.1.4: Assessment of and Decision on Information Security Events

   Comments: The purpose of the Voatz Information Security Incident Management Policy is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information. Supporting documentation includes guidance for assessing security events and making decisions about when to declare an incident, Incident Response Checklist, and Reporting/Notification Contact information.

Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

1. Policy A.16 Information Security Incident Management Policy: Section 1.0: Overview

   The purpose of this policy is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information.

2. Documentation for ISO control A.16.1.4 Assessment of and Decision on Information Security Events

   Comments: The purpose of the Voatz Information Security Incident Management Policy is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information. Supporting documentation includes guidance for assessing security events and making decisions about when to declare an incident, Incident Response Checklist, and Reporting/Notification Contact information.

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

1. Policy AC9: Server Security Policy, Section 4.1: Ownership and Responsibilities:

Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run a server) is the responsibility of Voatz, Inc. in the case of on-premise physical servers being used.

2. Policy A.9: Access Control Policy, Section 3.0: Business Requirements:

   Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

   Comments:

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

1. Policy AC5: Password Policy, Section 5.1: General:
   Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.

2. Policy A.9: Access Control Policy, Section 6.4: Use of Privileged Utility Programs:
   Where possible and appropriate privileged utility programs must incorporate multi-factor authentication (MFA).

   Comments:

Control the use of removable media on system components.

1. Policy IC6: Removable Media Policy, Section 5.0: Policy:
   - Voatz, Inc. staff may only use Voatz, Inc. IT Ops approved removable media in their work computers.

2. Policy IC6: Removable Media Policy, Section 5.0: Policy:
   - Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Voatz, Inc. Acceptable Encryption Policy.

   Comments:

Ensure that organizational systems containing sensitive data are protected during and after personnel actions such as terminations and transfers.

1. Policy A.7: Personnel Security Policy, Section 4.5 Personnel Termination:
   The organization must upon personnel termination:
   - Terminate information asset access.
   - Conduct exit interviews.
   - Retrieve all security-related organizational information system-related property.
   - Retain access to organizational information and information assets formerly controlled by terminated personnel.

2. Policy A.7: Personnel Security Policy, Section 4.6 Personnel Transfer:
   The organization must review logical and physical access to information assets and facilities when personnel are re-assigned or transferred to other positions within the organization.

   Comments:

Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

1. Policy A.11: Physical and Environmental Security Policy, Section 4.1 Physical Access Authorization:
   Develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
2. Policy AC9: Server Security, Section 4.2: General Configuration and Backup Guidelines:
   Servers should be physically located in an access-controlled environment.

   Comments:

Protect and monitor the physical facility and support infrastructure for organizational systems.

1. Policy A.11: Physical and Environmental Security Policy, Section 4.2 Physical Access Control:
   Employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
2. Policy A.11: Physical and Environmental Security Policy, Section 4.4 Monitoring Physical Access:
   Review physical access logs at a defined frequency and upon occurrence of security incidents.

   Comments: Physical security is provided by CIC.

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

1. Laptops, desktops, and servers are protected with Sophos Endpoint, which scans for malware.
2. Policy A.6.2.1: Mobile Device Management Policy, Section 3.1: Technology and Security Requirements:
   Devices must have endpoint protection/anti-malware installed. Where possible this is supplied by Voatz IT Ops.

   Comments: Laptops, desktops, and servers are protected with Sophos Endpoint, which scans for malware.

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

1. Voatz Risk Assessment and Risk Treatment Methodology: Section 1.0 Overview
   An effective risk management process is an important component of a successful information security program. Risk management is the process of identifying risk, assessing risk and taking

steps to reduce risk to an acceptable level. This guideline provides a foundation for the effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within Voatz, Inc.

2. Policy OM.2: Voatz Information Security Management System (ISMS) Policy: Section 2.0 Purpose
   The purpose of this document is to outline the approach Voatz will take to ensure the security of the processes, technology, data/information, and people involved in the development, operation, administration, maintenance and delivery of the Voatz mobile platform.

   Comments: Voatz, Inc. utilizes the Tugboat Logic Virtual CISO Platform Platform to manage its ISMS. Voatz strives to take a methodical approach to identify risks associated with each of its infrastructure components, evaluate the potential for threats/threat actors to exploit flaws or vulnerabilities in these components, and take the necessary action to protect individual privacy as well as the confidentiality, integrity, and availability of Voatz, Inc. resources and data.

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

1. Policy OM.2: Voatz Information Security Management System (ISMS) Policy: Section 2.0 Purpose
   The purpose of this document is to outline the approach Voatz will take to ensure the security of the processes, technology, data/information, and people involved in the development, operation, administration, maintenance and delivery of the Voatz mobile platform.

2. Voatz Risk Assessment and Risk Treatment Methodology: Section 1.0 Overview
   An effective risk management process is an important component of a successful information security program. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. This guideline provides a foundation for the effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within Voatz, Inc.

   Comments: Voatz, Inc. utilizes the "Tugboat Logic Virtual CISO Platform Platform" to manage InfoSec policies, provide security awareness training, implement and document security controls, and track compliance with customers, 3rd party vendors, independent auditors, and regulatory agencies.

Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

1. A.13 Communications Security Policy: Section 1.0: Purpose
   The purpose of this policy is to ensure the availability and reliability of network devices to ensure safe and secure connections to the information assets owned by Voatz, Inc.

2. A.12 Operations Security Policy

   Comments: The purpose of the Voatz Communications and Network security policy is to ensure the availability and reliability of network devices to ensure safe and secure connections to the information assets owned by Voatz, Inc.. The purpose of Operations policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security

requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy. This includes the stipulation that Voatz, Inc. will operate in a manner that meets its Information Security Objectives. As listed in the Information Security Policy, these objectives include:

- Operating a voting platform that meets the confidentiality, integrity and availability requirements of jurisdictions around the world.
- Continuously improving the Voatz service by keeping technology up to date, employing additional security controls where these make sense to maintain a strong security posture.
- Proactively managing risks.

Voatz, Inc. processes are designed to meet information security requirements of its corporate and elections operations.

The following environments are involved with Voatz Operations:

- Corporate Environment (on-premise employee laptops and on-premise servers including Jira, Confluence, etc.and some test servers in AWS and Azure)
- Mobile/Elections Environment (including the app, cloud hosted core servers, databases, blockchain)

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

1. A.14 System Acquisition, Development and Maintenance: Section 1.0 Purpose
   This policy ensures that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

2. ISO Control A.14.2.1 Secure Development Policy
   Voatz Secure Development Policy provides for secure methodologies during the design and implementation of Voatz, Inc. products and services. It incorporates best practices in software and operations design and implementation processes with security and vulnerability reviews throughout their lifecycle so that implementation ensures that Voatz, Inc. products are only used as intended and are not vulnerable to attack or abuse.

   Comments: Voatz policy ensures that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

1. A.12 Operations Security Policy: Section 3.0: Business Requirements:
   The following environments are involved with Voatz Operations:

- Corporate Environment (on-premise employee laptops and on-premise servers including JIRA, Confluence, etc.and some test servers in AWS and Azure)
- Mobile/Elections Environment (including the app, cloud hosted core servers, databases, blockchain)

2. ISO Control A.12.1.4 Separation of Development, Testing and Operational Environments

   Comments: The purpose of Voatz Operations Security policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

1. From an API routing module:

   // Defines all of the routing supported.
   def allRoutes: Route = encodeResponse {
…
   }

2. Policy A.13: Network Security Policy, Section 4.0:
   - All traffic and protocols should be expressly denied except for those necessary for business purposes.
   - All the traffic to and from a particular list of IPs and Domains (Blacklisted) should be denied at the Firewall Level.

   Comments:

Protect the authenticity of communications sessions.

1. Policy A.13: Network Security Policy, Section 5.9: Encrypt sensitive network traffic: Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

2. Policy A.13: Network Security Policy, Section 5.2: Privilege Access Control: Access control shall be used to provide separate authentication, authorization, and accounting services for network-based access.

   Comments:

Identify, report, and correct information and information system flaws in a timely manner.

1. Policy A.12 Operations Security Policy, Section 1.0: Purpose

The purpose of this policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

2. ISO Control A.12.1.2 Change Management
   Voatz Change Control and Configuration Process process in which change requestors create tickets, request approval by stakeholders, and implement changes to ensure changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.

   Comments: The purpose of the Voatz Operation Security policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

Provide protection from malicious code at appropriate locations within organizational information systems.

1. Policy A.12 Operation Security Policy, Section 1.0: Purpose
   The purpose of this policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

2. Policy A.12.2.1 - Controls Against Malware

   Comments: Purpose of Voatz Operation Security policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy. A defense in depth approach shall be taken to protect Voatz from malware including, as a minimum:

   - **Firewalls**: these shall be installed at all points where internal networks are connected to the internet. Further requirements on firewall configuration and maintenance are contained in the Communications Security Policy.
   - **Anti-virus**: this shall be installed on all key devices including firewalls, proxy servers, all servers and all end-user devices
   - **Threat monitoring**: information about emerging threats shall be obtained from appropriate sources and necessary action taken, e.g. ensuring that users are alerted proactively of potential attacks.
   - **Security Awareness Training**: as phishing it is a major delivery mechanism for malware, Voatz conducts regular security awareness training.

Monitor system security alerts and advisories and take action in response.

1. Policy A.12: Operations Security Policy, Section 7.0: Logging and Monitoring:

Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

2. Policy A.16 Information Security Incident Management, Section 1.0: Overview:
   It is critical to the organization that incidents that threaten the security or privacy of critical information are properly identified, contained, investigated, and remedied.

   Comments:

Update malicious code protection mechanisms when new releases are available.

1. Policy A.12 Operations Security Policy, Section 1.0 Purpose
   The purpose of this policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

2. Policy A.12.2.1 Controls against malware:
   Employee laptops have enterprise anti-malware/endpoint protection installed and servers are running a capability that detects changes as indicators of the presence of malware.

   Comments: The purpose of Voatz Operations Security policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

1. A.13 Communications Security: Section 1.0: Purpose
   The purpose of this policy is to ensure the availability and reliability of network devices to ensure safe and secure connections to the information assets owned by Voatz, Inc.

2. ISO Control A.13.1.2 - Security of Network Services
   This policy is to ensure the availability and reliability of network devices to ensure safe and secure connections to the information assets owned by Voatz, Inc. The policy applies to all network devices, (includes switches, firewalls, and wireless access points) that are owned and managed by Voatz, Inc.

   Comments:

Employ the principle of least privilege, including for specific security functions and privileged accounts.

1. Policy A.9: Access Control Policy, Section 3.0:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

- Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
- Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
- Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
- Need to Use – users will only be able to access physical and logical facilities required for their role.

2. Policy AC9: Server Security, Section 4.2 General Configuration and Backup Guidelines:
   Always use the least privilege to perform a function. Do not use root/admin accounts when a non-privileged account is sufficient.

   Comments:

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

1. A.9 Access Control Policy, Section 1.0: Purpose:
   This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

2. A.12 Operations Security Policy
   The purpose of Voatz Operations Security policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy. Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure.

   Comments: Voatz Access Control Policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege. Under the policy Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

Perform maintenance on organizational systems.

1. Policy AC.9: Server Security Policy, Section 4.1: Ownership and Responsibilities:
   Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run a server) is the responsibility of Voatz, Inc. in the case of on-premise physical servers being used.

2. Policy A.13: Network Security Policy, Section 4.0:

- Every network device deployed in the Voatz, Inc. network shall be appropriately configured and meet security requirements for their individual purposes (internal, public facing).

Comments:

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

1. Policy A.12 Operations Security Policy, Section 5.0: Protection from Malware:
   A defense in depth approach shall be taken to protect Voatz from malware.

2. Policy IC.6: Removable Media Policy, Section 1.0: Overview:
   Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. It is important to utilize removable media carefully.

   Comments: The purpose of Voatz Operations Security policy policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

Prohibit the use of portable storage devices when such devices have no identifiable owner.

1. Policy A.12 Operations Security Policy
   The purpose of Voatz Operations Security policy policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

2. Policy IC.6: Removable Media Policy, Section 1.0: Overview:
   Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. It is important to utilize removable media carefully.

   Comments:

Screen individuals prior to authorizing access to organizational systems containing sensitive data.

1. Policy A.7: Personnel Security Policy, Section 4.3: Personnel Screening
   The organization must screen individuals prior to access to sensitive information. In addition, the organization must rescreen individuals every seven years.

2. A.9 Access Control Policy

   The purpose of Voatz access control is to ensure access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege. In addition to the specific requirements, a number of general

principles will be used when designing access controls for Voatz' systems and services. These are:

- Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
- Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
- Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
- Need to Use – users will only be able to access physical and logical facilities required for their role

Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of sensitive data.

1. Policy A.7: Personnel Security Policy, Section 4.2: Position Categorization
   Conduct performance evaluations and review and revise position risk designations on an annual basis.

2. Voatz Risk Assessment; ISO Clause 8.2-Information Security Risk Assessment

   Comments:

Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

1. Policy A.12 Operations Security, A.14 System Acquisition, Development and Maintenance

2. Policy A.12.6.1 - Management of Technical Vulnerabilities

   Comments: Purpose of the policy is to ensure that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

Implement cryptographic mechanisms to prevent unauthorized disclosure of sensitive information during transmission unless otherwise protected by alternative physical safeguards.

1. Policy A.10: Cryptography: Section 3.3:
   - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.
   - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted.

2. Policy A.13, Section 5.9 Encrypt sensitive network traffic

Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

Comments:

Employ FIPS-validated cryptography when used to protect the confidentiality of sensitive information.

1. Policy A.10: Cryptography: Section 3.1: Encryption Method and Application:
   All Voatz, Inc. encryption shall be done using approved cryptographic modules.

2. Policy A.10: Cryptography: Section 3.1: Encryption Method and Application:
   Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Voatz, Inc.'s key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

   Comments:

Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

1. Policy A.12: Operations Security Policy, Section 9.0 Technical Vulnerability Management
   Voatz conducts regular vulnerability scans for all internal and external assets to identify known vulnerabilities.

2. Policy A.12: Operations Security Policy, Section 10.0 Information Systems Audit
   For hosts in production, scans and other audit activities must be scheduled to run during times that minimize disruption to live events.

   Comments:

Identify unauthorized use of organizational systems.

1. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

2. Policy A.12: Operations Security Policy, Section 8.0: Control of Operational Software:
   Voatz monitors systems to detect unauthorized access and modification.

   Comments:

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

1. Policy A.9: Access Control Policy, Section 3.0: Business Requirements:
   Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

2. Policy A.9: Access Control Policy, Section 6.1 Information Access Restriction:

All Voatz, Inc. systems must enforce approved authorizations for access to the system in accordance with applicable policy and users requiring access must receive approval directly from the system/application owner.
Voatz follows least privilege when granting access to information and application system functionality.

Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

Read-only access is granted to users based on their roles, while functions that allow users to create, modify, or delete information is restricted to designated super users/admins. (E.g., Only admins can create or delete code repositories, while developers are restricted to adding new code, and editing existing code. Only a super admin or designated alternate with super admin access can push code to the live/production environment.

Comments:

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

1. Policy A.9: Access Control Policy, Section 6.4: Use of Privileged Utility Programs:
   - Utility programs must have secure authentication mechanisms that use identification, authentication and authorization and accounting/audit procedures.

2. Policy A.11: Physical and Environmental Security Policy, Section 4.2 Physical Access Control: The organization will control entry/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).
   - Maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.

   Comments:

Limit unsuccessful login attempts.

1. From a database authentication module:

```
def checkLast3LoginAttempts(userId: Int)(implicit db: MongoDatabase): Future[Boolean] =
async{
        //log.debug("checking last 2 login attempts - including this attempt, 3 failed in a
row")
 val (last3AttemptsFailed, lastAttemptTs) = await(last3LoginAttemptsFailed(userId))
 if(last3AttemptsFailed){
        val (latestInterval, attempt) =
await(ThrottledLoginAsync.getLatestThrottleIntervalAndCount(userId))
  ThrottledLoginAsync.create(userId, lastAttemptTs, latestInterval, attempt)
  false
 }else{
  true
 }
```

```
}
```

2. From an authentication module:

```
val throttleInterval = if(attempt == 0){
  30 + Cryptography.issueRandomInt(1, 10)
}else{
  val min = (attempt)*10
  val max = (attempt+1)*10
  latestInterval + Cryptography.issueRandomInt(min, max)
```

Comments:

Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

1. From Android:

```
disposable = RxBus.instance.listen(RxEvent.InAppEventAdd::class.java)
      .subscribe {
        InAppIdleTimer.getInstance()
          .showWarningDialogBox(this)
....
```

where showWarningDialogBox shows an inactivity logout warning to the user:

```
fun showWarningDialogBox(context: Context) {
    val dialog = MaterialDialog.Builder(context)
      .title(context.resources.getString(R.string.timeout_title))
      .content(String.format(context.resources.getString(R.string.logout_timeout_message), "30"))
```

2. iOS has equivalent logic to Android.

Comments:

Terminate (automatically) a user session after a defined condition.

1. From Android:

```
if (User.isLoggedIn) {
  if (isScreenOn && (dialog)!!.isShowing) {
    dialog.contentView?.announceForAccessibility(
      context.getString(R.string.timeout_message)
    )
    User.logoutButtonClicked(context, apiService, compositeDisposable)
    dialog.dismiss()
```

2. iOS has equivalent logic to Android.

Comments:

Route remote access via managed access control points.

1. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction
   Voatz aims for a layered approach to manage access to corporate and elections assets which includes:
   - Disabling all ports or services on critical assets not needed.
2. Policy AC.6: Remote Access Policy, Section 4.2: Requirements:
   - Voatz, Inc. employees and contractors with remote access privileges must ensure that their Voatz, Inc.-owned or personal computer or workstation, which is remotely connected to Voatz, Inc.'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Comments:

Verify and control/limit connections to and use of external information systems.

1. Policy A.9: Access Control Policy, Section 3.0: Business Requirements:
   The access control measures implemented shall be appropriate to the business requirements. These requirements may depend on factors such as:
   - Contractual obligations to external third parties;
2. For VMA, this is not applicable; VMA does not connect to or use external information systems. The app. may provide the user with a link to the election authority's official website where the user can find additional information, but such links will always be over HTTPS.

Comments:

Limit use of portable storage devices on external systems.

1. Policy IC6: Removable Media Policy, Section 5.0: Policy:
   - Voatz, Inc. staff may only use Voatz, Inc. IT Ops approved removable media in their work computers.
2. Policy IC6: Removable Media Policy, Section 5.0: Policy:
   - Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Voatz, Inc. Acceptable Encryption Policy.

Comments:

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

1. Policy A.6.2.1: Mobile Device Management Policy, Section 3.2 User Requirements:
   If a user suspects that company data has been sent from a personal email account, either in the body text or as an attachment, they must notify Voatz, Inc. IT Ops immediately.

2. Policy A.8: IT Asset Management Policy, Section 7.0 Responsibilities
   Voatz IT Ops is responsible for implementing this policy. This team will be responsible for:

   - Reporting any incorrect disposal or misuse of an IT asset.

   Comments:

Review and update logged events.

1. Policy AC.9: Server Security, Section 4.3: Monitoring:
   Security-related events will be reported to Voatz, Inc. IT Ops, who will review logs and escalate incidents as necessary. Corrective measures will be prescribed as needed.

2. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

   Comments:

Alert in the event of an audit logging process failure.

1. Policy A.12: Operations Security Policy, Section 7.0 Logging and Monitoring
   Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity.

2. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz monitors systems to detect unauthorized access and modification.

   Comments:

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows the principle of least privilege when granting access to information and application system functionality. Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know. Read-only access is granted to users based on their roles, while functions that allow users to create, modify, or delete information is restricted to designated super

users/admins.

Comments:

Limit management of audit logging functionality to a subset of privileged users.

1. Policy A.12: Operations Security Policy, 8.0 Control of Operational Software:
   Voatz also follows the principle of least privilege to limit the access to critical systems and limit the ability to make changes.

2. Policy A.9: Access Control Policy, Section 6.1: Information Access Restriction:
   Voatz follows least privilege when granting access to information and application system functionality.

   Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

   Read-only access is granted to users based on their roles, while functions that allow users to create, modify, or delete information is restricted to designated super users/admins.

   Comments:

Analyze the security impact of changes prior to implementation.

1. A.14 System Acquisition, Development and Maintenance, Section 1.0 Purpose
   This policy ensures that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

2. ISO control A.14.2.2 - System Change Control Procedures

   Comments: Voatz policy ensures that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

Control and monitor user-installed software.

1. Policy A.6.2.1: Mobile Device Management Policy, Section 3.2: User Requirements:
   Applications must only be installed from official platform-owner approved sources. Installation of applications from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT.

2. Policy IC.8: Workstation Security Policy, Section 4.2 Operational Safeguards:
   The following operational safeguards shall be implemented:

   - Ensuring that latest OS and software updates are installed.
   - Never installing unauthorized software on workstations.

Comments:

Enforce a minimum password complexity and change of characters when new passwords are created.

1. From AC 5: Password Policy, Section 5.2.1: General Password Construction Guidelines
   All users should be aware of how to select strong passwords.
   Administrative passwords should be 15 (semi-random) characters long.

2. From AC 5: Password Policy, Section 5.2.2: Passphrases
   Passphrases can be used as an alternative to passwords.

   Comments:

Allow temporary password use for system logons with an immediate change to a permanent password.

1. Policy A.9: Access Control Policy, Section 4.4 Management of Secret Authentication Information of Users:
   Users select their own passwords. Where Voatz IT Ops issues initial passwords, these are sent out of band and users are asked to change their passwords and any default passwords.

2. Policy AC.5: Password Policy, Section 5.2.3. Use of Passwords and Passphrases for Remote Access Users:
   Access to the Voatz, Inc. network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

   Comments:

Obscure feedback of authentication information.

1. Policy A.9: Access Control Policy, Section 6.2 - Secure Log-on Procedures
   Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

2. Policy A.10: Cryptography: Section 3.1: Encryption Method and Application:
   Encryption shall be implemented in:
   - All web applications via the most secure version of SSL/TLS,
   - Device/file encryption i.e. partial disk encryption and full disk encryption,
   - During data transmission between and among infrastructure components,
   - During sensitive data transmission over public networks,
   - storage on disk, particularly secrets and user passwords.

   Comments:

Test the organizational incident response capability.

1. A.16 Information Security Incident Management Policy

2. A.17 Information Security Aspects of Business Continuity Management

Comments: Voatz Information Security and Incident Management Policy's purpose is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information

The purpose of Voatz Business Continuity policy is to ensure Information security continuity is embedded in the organization's business operations and provides guidance on how to ensure continuous secure operations during any adverse event affecting Voatz, Inc. assets.

Supervise the maintenance activities of maintenance personnel without required access authorization.

1. Policy A.11: Physical and Environmental Security Policy, Section 4.2 Physical Access Control:
   - Establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.
2. Policy AC.1: Visitor and Contractor Premises Access Policy, Section 4.4 Visitor Badges
   Visitor Badges issued must be worn at all times. Visitors requiring access to locked areas should arrange times with their sponsor and Voatz IT Ops.

   Comments:

Protect the confidentiality of backup sensitive information at storage locations.

1. Policy A.8: IT Asset Management Policy, Section 5.2 Asset Value,
   Assets, which store data, regardless of cost, shall be tracked as part of a computing device or as a part of network attached storage. These assets include:
   - Network Attached Storage (NAS), Storage Area Network (SAN) or other computer data storage.
   - Temporary storage drives.
   - Tape or optical media with data stored on them including system backup data.
2. Policy A.8: IT Asset Management Policy, Section 7.0: Responsibilities:
   Voatz IT Ops is responsible for implementing this policy. This team will be responsible for:

   Coordinating IT asset audit activities and updating and maintaining the accuracy of the asset inventory
   - Checking IT equipment is returned in the same configuration as expected;
   - Administrating the control and security of IT equipment held in stock for issuing and awaiting reissue or disposal;
   - Ensuring that all IT equipment is returned to Voatz upon replacement or when the holder leaves the organization
   - Ensuring that any IT asset that is retired is disposed of according to the Equipment Disposal policy
   - Giving appropriate advice to users on the correct handling of IT assets; and

- Reporting any incorrect disposal or misuse of an IT asset.

Comments:

Escort visitors and monitor visitor activity.

1. Policy AC.1: Visitor and Contractor Premises Access Policy, Section 4.3: Visitor Logs
   Visitors will be asked to sign-in at visitor control. Voatz sponsors will also ensure visitors sign-in once they arrive at the Voatz office. Voatz will also keep a log of visitors.

2. Policy AC.1: Visitor and Contractor Premises Access Policy, Section 4.4 Visitor Badges
   Visitor Badges issued must be worn at all times. Visitors requiring access to locked areas should arrange times with their sponsor and Voatz IT Ops.

   Comments:

Remediate vulnerabilities in accordance with risk assessments.

1. Policy A.16 Information Security Incident Management, Section 3.1: Voatz Election Infrastructure Policy:
   Voatz leadership will direct remediation and recovery efforts and reach out to external incident response and investigation resources as necessary.

2. Policy A.16 Information Security Incident Management, Section 3.2: Voatz Corporate Network Policy:
   Risk mitigation: Identify and recommend strategies to mitigate the risk of harm arising from this incident.

   Comments:

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

1. Policy AC.6: Remote Access Policy, Section 4.2 Requirements:
   - All remote access connections must include a "time-out" system. In accordance with Voatz, Inc.'s security policies, remote access sessions for all SSH sessions will time out after 30 minutes of inactivity and will terminate after unlimited hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks.

2. Policy A.13: Network Security Policy, Section 4.0 Policy
   - Network devices owned and managed by Voatz, Inc. must be configured securely and designed to secure network traffic between trusted and untrusted network zones.

   Comments:

Establish and manage cryptographic keys for cryptography employed in organizational systems.

1. Policy A.10: Acceptable Encryption Policy, Section 3.6: Key Management:

- Key management should be planned which will include secure key generation, use, storage, distribution, recovery, and removal.

2. Policy AC.5: Password Policy, Section 5.1 General
   - Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.
   - All production system-level passwords must be part of the Voatz, Inc. IT Ops administered global password management database.

Comments:

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

1. Risk Assessment and Risk Treatment Methodology, Section 8.0 Monitor and Review:
   The risk management process should be an iterative process and should be the subject of a structured monitoring and review process.
2. Policy A.12: Operations Security Policy, Section 1.0 Purpose
   The purpose of this policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

   Comments:

10. Attachment F: - POA&M Tracker

System Name: Voatz, Inc.

POA&M ID	Type	Governing Control	Weakness Description
VMA-1895 / VMA-2002	MA	OWASP	Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters. Verify that any printable Unicode character, including language neutral characters such as spaces and emojis are permitted in passwords. Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's

VMA-1896 / VMA-2014	MA	OWASP	Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters. Verify that any printable Unicode character, including language neutral characters such as spaces and emojis are permitted in passwords. Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. Verify that passwords submitted during account registration, login, and password change are checked against a set of breached passwords either locally (such as the top 1,000 or 10,000 most common passwords which match the system's

VSP-1100	WA / Admin Portal OWASP	Verify that "paste" functionality, browser password helpers, and external password managers are permitted. "Verify that passwords 64 characters or longer are permitted but may be no longer than 128 characters. Verify that any printable Unicode character, including language neutral characters such as spaces and emojis are permitted in passwords. Verify that there are no password composition rules limiting the type of characters permitted. There should be no requirement for upper or lower case or numbers or special characters. Verify that passwords submitted during account registration, login, and

Source Identifying Weakness	Original Detection Date
Self assessment	1-Jun-21

Self assessment 1-Jun-21

Self assessment 1-Jun-21

Scheduled Completion Date	POC	Resources Required	Vendor Dependency
31-Jan-22	Linda Hutchinson	1 iOS developer	None

31-Jan-22	Linda Hutchinson	1	Android developer	None

31-Jan-22	Linda Hutchinson	1 web app developer	None

Last Vendor Check-in Date	Vendor Dependent Product Name
n/a	n/a

n/a

n/a

n/a

n/a

Planned Milestones	Milestone Changes	Status Date	Original Risk Rating
Development sprints 37,38,39	n/a	11/22/2021	

Development sprints 37,38,39	n/a	11/22/2021

Development sprints 37,38,39	n/a	11/22/2021

Adjusted Risk Rating	Mitigating Factors	Comments
	Biometric authentication is used currently on all our mobile apps and passwords are only used in case of a backup so the risk here is significantly mitigated	

Biometric authentication is used currently on all our mobile apps and passwords are only used in case of a backup so the risk here is significantly mitigated

MFA is used (using Yubikeys or Duo App) so risk of compromise is minimized here.

11. Attachment H - Voatz, Inc. Accessibility Conformance Report

Voatz™ Mobile App Accessibility Conformance Statement

Voatz Remote Accessible Ballot Marking System
Voatz, Inc.

This Voluntary Product Accessibility Template® (VPAT®) disclosure assesses Voatz' compliance with regulatory and industry accessibility guidelines. Voatz Inc.'s native smartphone apps comply to the accessibility standards below:

- World Wide Web Consortium's *Web Content Accessibility Guidelines v2.1* level AA (WCAG 2.1/AA)
- U.S. Election Assistance Commission's *Voluntary Voting System Guidelines* (VVSG 1.1)
- Apple iOS and Android accessibility best practices

Test Process

Voatz partnered with the **National Center for Accessible Media** during the design process for their recommendations on accessibility and WCAG 2.1. The resulting apps were systematically evaluated by professional testers with previous WCAG and voting systems experience. Finally, Voatz engaged an **independent voting system testing laboratory (VSTL)** certified in assessing Accessibility compliance to VVSG 1.1. Pro V&V's report dated May 28, 2020, concludes that the Voatz apps conform to applicable federal accessibility requirements.

Voatz for iOS and Android are native smartphone apps, not web applications, so where HTML structure is referenced in WCAG, this report considers the comparable programming conventions to ensure optimal support the following native smartphone assistive capabilities:

- VoiceOver and TalkBack screen readers
- Configurable font sizes and display options
- Voice Control (iOS)
- Speech-to-Text for data entry

Compliance with WCAG 2.1 Guidelines

WCAG Guideline 1.1: Text Alternatives

Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.

Success Criteria	Comment
Non-text Content (Level A): All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below.	**Supports** All non-text content presented to the user has a text alternative.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Success Criteria	Comment
• Controls, Input: If non-text content is a control or accepts user input, then it has a name that describes its purpose. (Refer to Guideline 4.1 for additional requirements for controls and content that accepts user input.) • Time-Based Media: If non-text content is time-based media, then text alternatives at least provide descriptive identification of the non-text content. (Refer to Guideline 1.2 for additional requirements for media.) • Test: If non-text content is a test or exercise that would be invalid if presented in text, then text alternatives at least provide descriptive identification of the non-text content. • Sensory: If non-text content is primarily intended to create a specific sensory experience, then text alternatives at least provide descriptive identification of the non-text content. • CAPTCHA: If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided, and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities. • Decoration, Formatting, Invisible: If non-text content is pure decoration, is used only for visual formatting, or is not presented to users, then it is implemented in a way that it can be ignored by assistive technology.	

WCAG Guideline 1.3: Adaptable

Create content that can be presented in different ways (for example simpler layout) without losing information or structure.

Success Criteria	Comment
1.3.1 Info and Relationships (Level A): Information, structure, and relationships conveyed through presentation can be programmatically determined or are available in text.	**Supports**
1.3.2 Meaningful Sequence (Level A): When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	**Supports**
1.3.3 Sensory Characteristics (Level A): Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, size, visual location, orientation, or sound. Note: For requirements related to color, refer to Guideline 1.4.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Success Criteria	Comment
1.3.4 Orientation (Level AA): Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential. Examples where a particular display orientation may be essential are a bank check, a piano application, slides for a projector or television, or virtual reality content where binary display orientation is not applicable.	**Does not support.** VVSG recommendations conflict with using landscape mode as it reduces the number of candidates displayed on screen.

WCAG Guideline 1.4: Distinguishable

Make it easier for users to see and hear content including separating foreground from background.

Success Criteria	Comment
1.4.1 Use of Color (Level A): Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element. Note: This success criterion addresses color perception specifically. Other forms of perception are covered in Guideline 1.3 including programmatic access to color and other visual presentation coding.	**Supports**
1.4.3 Contrast (Minimum) (Level AA): The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: • Large Text: Large-scale text and images of large-scale text have a contrast ratio of at least 3:1 • Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. • Logotypes: Text that is part of a logo or brand name has no minimum contrast requirement.	**Supports**
1.4.4 Resize text (Level AA): Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality.	**Supports**
1.4.11 Non-text Contrast (Level AA): The visual presentation of the following have a contrast ratio of at least 3:1 against adjacent color(s): • User Interface Components: Visual information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author;	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

• Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.	

WCAG Guideline 2.1: Keyboard Accessible

Make all functionality available from a keyboard.

Success Criteria	Comment
2.1.1 Keyboard (Level A): All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints. Note 1: This exception relates to the underlying function, not the input technique. For example, if using handwriting to enter text, the input technique (handwriting) requires path-dependent input but the underlying function (text input) does not. Note 2: This does not forbid and should not discourage providing mouse input or other input methods in addition to keyboard operation.	**Supports with exception** With VoiceOver (IOS) or TalkBack (Android) enabled, standard gestures (swipe right/left, tap and double-tap), combined with visible navigation focus ensure that precise mouse-like inputs are not required. For jurisdictions requiring use of Voatz' ID verification, a sighted individual can assist a visually-impaired voter by scanning a photo ID and following video 'selfie' instructions, prior to voting without compromising the privacy of the voter's ballot. Bluetooth keyboard use has not been evaluated.
2.1.2 No Keyboard Trap (Level A): If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface, and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away. Note: Since any content that does not meet this success criterion can interfere with a user's ability to use the whole page, all content on the Web page (whether it is used to meet other or not) must meet this success criterion. See Conformance Requirement 5: Non-Interference.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

WCAG Guideline 2.2: Enough Time

Provide users enough time to read and use content.

Success Criteria	Comment
Supports with exception (Level A): For each time limit that is set by the content, at least one of the following is true: • Turn off: The user is allowed to turn off the time limit before encountering it; or • Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or • Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the space bar"), and the user is allowed to extend the time limit at least ten times; or • Real-time Exception: The time limit is a required part of a real-time event (for example, an auction), and no alternative to the time limit is possible; or • Essential Exception: The time limit is essential and extending it would invalidate the activity; or • 20 Hour Exception: The time limit is longer than 20 hours. Note: This success criterion helps ensure that users can complete tasks without unexpected changes in content or context that are a result of a time limit. This success criterion should be considered in conjunction with Success Criterion 3.2.1, which puts limits on changes of content or context as a result of user action.	**Supports**

WCAG Guideline 2.4: Navigable

Provide ways to help users navigate, find content, and determine where they are.

Success Criteria	Comment
2.4.2 Page Titled (Level A): Web pages have titles that describe topic or purpose.	**Supports**
2.4.3 Focus Order (Level A): If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability.	**Supports**
2.4.4 Link Purpose (In Context) (Level A): The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Success Criteria	Comment
2.4.6 Headings and Labels (Level AA): Headings and labels describe topic or purpose.	**Supports**
2.4.7 Focus Visible (Level AA): Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible.	**Supports**

WCAG Guideline 2.5: Input Modalities

Make it easier for users to operate functionality through various inputs beyond keyboard.

Success Criteria	Comment
2.5.1 Pointer Gestures (Level A): All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential. This requirement applies to web content that interprets pointer actions (i.e. this does not apply to actions that are required to operate the user agent or assistive technology).	N/A
2.5.2 Pointer Cancellation (Level A): For functionality that can be operated using a single pointer, at least one of the following is true: • No Down-Event: The down-event of the pointer is not used to execute any part of the function; • Abort or Undo: Completion of the function is on the up-event, and a mechanism is available to abort the function before completion or to undo the function after completion; • Up Reversal: The up-event reverses any outcome of the preceding down-event; • Essential: Completing the function on the down-event is essential. • Functions that emulate a keyboard or numeric keypad key press are considered essential. This requirement applies to web content that interprets pointer actions (i.e. this does not apply to actions that are required to operate the user agent or assistive technology).	N/A
2.5.3 Label in Name (Level A): For user interface components with labels that include text or images of text, the name contains the text that is presented visually. A best practice is to have the text of the label at the start of the name.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

WCAG Guideline 3.1 Readable:

Make text content readable and understandable.

Success Criteria	Comment
3.1.1 Language of Page (Level A): The default human language of each Web page can be programmatically determined.	**Supports**
3.1.2 Language of Parts (Level AA): The human language of each Supportsage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language, and words or phrases that have become part of the vernacular of the immediately surrounding text.	**Supports**

WCAG Guideline 3.2: Predictable

Make Web pages appear and operate in predictable ways.

Success Criteria	Comment
3.2.1 On Focus (Level A): When any component receives focus, it does not initiate a change of context.	**Supports**
3.2.2 On Input (Level A): Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behavior before using the component.	**Supports**
3.2.4 Consistent Identification (Level AA): Components that have the same functionality within a set of Web pages are identified consistently.	**Supports**

WCAG Guideline 3.3 Input Assistance:

Help users avoid and correct mistakes.

Success Criteria	Comment
3.3.1 Error Identification (Level A): If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	**Supports**
3.3.2 Labels or Instructions (Level A): Labels or instructions are provided when content requires user input.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Success Criteria	Comment
3.3.3 Error Suggestion (Level AA): If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.	**Supports**
3.3.4 Error Prevention (Legal, Financial, Data) (Level AA): For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: • Reversible: Submissions are reversible. • Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. • Confirmed: A mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.	**Supports**

WCAG Guideline 4.1: Compatible

Maximize compatibility with current and future user agents, including assistive technologies.

Success Criteria	Comment
4.1.2 Name, Role, Value (Level A): For all user interface components (including but not limited to: form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies. Note: This success criterion is primarily for Web authors who develop or script their own user interface components. For example, standard HTML controls already meet this success criterion when used according to specification.	**Supports**
4.1.3 Status Message (Level AA): In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Compliance with VVSG 1.1 Accessible Voting Standards

Test results excerpted from *Test Report for the Test and Evaluation of Voatz Remote Accessible Ballot Marking System* (May 28, 2020) performed by Pro V&V, an independent, federally-approved Voting System Testing Laboratory (VSTL.)

VVSG 3.3.1 - General Accessibility

Requirement	Description	Comment
3.3.1.a.i	The manufacturer shall supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.	**Supports**
3.3.1.b	When the provision of accessibility for the Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, shall be presented in that alternative format.	**Supports**
3.3.1.c	The support provided to voters with disabilities shall be intrinsic to the Acc-VS. Personal assistive devices of the voter shall not be necessary to operate the Acc-VS correctly. This does not apply to personal assistive technology required to comply with 3.3.4 b.	**Supports**
3.3.1.d	If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the Acc-VS shall provide a secondary means that does not depend on those characteristics.	**Supports**
3.3.1.e	If the Acc-VS generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record then the voting system shall allow the voter to verify that record using the same access features used by the voter to cast the ballot.	**Supports**

VVSG 3.3.2 – Enhanced Visual Interfaces

Requirement	Description	Comment
3.3.2.a	An Acc-VS with a color electronic image display shall allow the voter to adjust the color saturation throughout the voting session while preserving the current votes.	**Supports**
3.3.2.a.i	At a minimum, two alternative display options listed shall be available: 1) black text on white background,2) white text on black background, 3) yellow text on a black background, or 4) light cyan text on a black background.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Requirement	Description	Comment
3.3.2.b	Groups of buttons and controls which perform different functions on the Acc-VS shall be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys in wide use by individuals with disabilities, such as a full alphabetic keyboard when used for purposes other than basic navigation and selection (e.g. entering a write-in candidate name).	**Supports**
3.3.2.c.i	There shall be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively.	**Supports**
3.3.2.c.ii	The system shall allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.	**Supports**

VVSG 3.3.3 – Audio-Tactile Interfaces

Requirement	Description	Comment
3.3.3.a & 3.3.3.a.i	The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.	N/A
3.3.3.b	The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3. • Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations • Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition) • Instructions and feedback for navigation of the ballot • Instructions and feedback for contest choices, including write-in candidates • Instructions and feedback on confirming and changing selections • Instructions and feedback on final submission of ballot	N/A
3.3.3.b.i	The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine. Discussion: For example, if a visual ballot supports voting a straight	N/A

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Requirement	Description	Comment
	party ticket and then changing the choice in a single contest, so must the ATI.	
3.3.3.b.ii	The ATI shall allow the voter to have any information provided by the voting system repeated.	N/A
3.3.3.b.iii	The ATI shall allow the voter to pause and resume the audio presentation.	N/A
3.3.3.b.iv	The ATI shall allow the voter to skip to the next contest or return to previous contests. Discussion: This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether. v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	N/A
3.3.3.b.v	The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	N/A
3.3.3.c.i	The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.	N/A
3.3.3.c.ii	When a voting machine utilize es a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	N/A
3.3.3.c.iii	A sanitized headphone or handset shall be made available to each voter.	N/A
3.3.3.c.iv	The audio system shall set the initial volume for each voting session between 60 and 70 dB SPL.	Not Tested* 3.3.3.c.iv. 3.3.3.c.v, and 3.3.3.c.vi relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Requirement	Description	Comment
3.3.3.c.v	The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	Not Tested*
3.3.3.c.vi	The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.	Not Tested*
3.3.3.c.vii	The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.	**Supports**
3.3.3.c.viii	The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.	**Supports**
3.3.3.d	If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.	**Supports**
3.3.3.e	If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.	**Supports**
3.3.3.f	All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.	N/A
3.3.3.g	On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.	N/A

VVSG 3.3.4 – Enhanced Input and Control Characteristics

Requirement	Description	Comment
3.3.4.a	The Acc-VS shall provide a 3.5 mm industry standard jack used to connect a personal assistive technology switch to the Acc-VS. This jack shall allow only switch data to be transmitted to the voting system. The voting system shall accept switch input that is functionally equivalent to tactile input. All the functionality of the Acc-VS (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, shall also be available through this non-manual input mechanism.	N/A

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Requirement	Description	Comment
3.3.4.b	The Acc-VS shall provide features that enable voters who lack fine motor control or the use of their hands to submit their ballots privately and independently without manually handling the ballot.	**Partially Supports*** * iPhone 6s & higher and iOS 13 &higher support hands-free operation using Voice Control. Android devices do not have this capability yet. However, both devices support limited dexterity with VoiceOver or TalkBack navigation (audio can be turned off.)
3.3.4.c	All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N).	**Supports**
3.3.4.d	The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit.	N/A

VVSG 3.3.5 – Design for Mobility Aids

Requirement	Description	Comment
3.3.5.a	The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.	N/A
3.3.5.1.a	If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum.	N/A
3.3.5.1.b.i 3.3.5.1.b.ii	If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply: • The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches.	N/A

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

Requirement	Description	Comment
	• If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.	
3.3.5.1.b.iii	Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions: • Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction • The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater • Toe clearance shall be 30 inches (760 mm) wide minimum	N/A
3.3.5.1.b.iv	Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions: • Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground. • The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater. • Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. • Knee clearance shall be 30 inches (760 mm) wide minimum.	N/A
3.3.5.c	All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station	N/A
3.3.5.1.c	If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches.	N/A
3.3.5.1.d.i 3.3.5.1.d.ii	If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. • The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches. • If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches.	N/A

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

VVSG 3.3.6 – Enhanced Auditory Interfaces

Requirement	Description	Comment
3.3.6 a	The Acc-VS shall incorporate the features listed under Requirement 3.3.3 c for voting systems that provide audio presentation of the ballot.	**Partially Supports**
3.3.6 b	If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.	**Supports**
3.3.6.c	No voting device shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, shall achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	Not Tested* * These requirements relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized.

VVSG 3.3.8 – English Proficiency

Requirement	Description	Comment
3.3.8.a	For voters who lack proficiency in reading English, the Acc-VS shall provide an audio interface for instructions and ballots as described in 3.3.3 b.	**Supports**

VVSG 3.3.9 – Speech Not Required

Requirement	Description	Comment
3.3.9.a	The voting system shall not require voter speech for its operation.	**Supports**

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-02

12. Attachment I - Full ProV&V Report

6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Phone (256)713-1111
Fax (256)713-1112

Test Report for Test and Evaluation of the Voatz™ Remote Accessible Ballot Marking (RABM) System

Phase 1
Version: 02

Date: 05/28/2020

SIGNATURES

Approved by: Michael L. Walker — 05/28/2020

Michael Walker, VSTL Project Manager — Date

Approved by: Wendy Owens — 05/28/2020

Wendy Owens, VSTL Program Manager — Date

REVISIONS

Revision	Description	Date
00	Initial Release	05/20/2020
01	Updates per manufacturer comments	05/22/2020
02	Updates per manufacturer comments	05/28/2020

Table of Contents

1.0 INTRODUCTION 1

1.1 SCOPE 1
1.2 REFERENCES 2
1.2 TERMS AND ABBREVIATIONS 2

2.0 TESTING OVERVIEW 3

2.1 SYSTEM OVERVIEW 3
2.2 BLOCK DIAGRAMS 4
2.3 TEST CONFIGURATION 5

3.0 MATERIALS REQUIRED FOR TESTING 5

3.1 SOFTWARE 5
3.2 EQUIPMENT 6
3.3 TECHNICAL DATA PACKAGE 6
3.4 TEST SUPPORT MATERIALS 6

4.0 TEST PROCESS AND RESULTS 7

4.1 USABILITY AND ACCESSIBILITY TESTING 7

5.0 CONCLUSION 9

ATTACHMENT A – REQUIREMENTS MATRIX A-1

ATTACHMENT B – VOATZ EBDM RESPONSES B-1

1.0 INTRODUCTION

The purpose of this Test Report is to document the procedures that Pro V&V, Inc. followed to perform the Phase 1 evaluation of the Voatz Remote Accessible Ballot Marking (RABM) System to the applicable requirements in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 and the manufacturer-stated requirements set forth in the system documentation. The RABM is categorized by the VVSG as an Electronically-assisted Ballot Marker (EBM) and is defined by the VVSG as follows:

Accessible Voting Station that produces an executed, human-readable paper ballot as a result, and that does not make any other lasting record of the voter's votes.

The test campaign is being conducted in two phases:

- Phase 1 assesses the RABM's Usability & Accessibility compliance in this Test Report.
- Phase 2 includes all elements of the approved Test Plan inclusive of Phase 1.

Pro V&V Test Plan TP v. 01-02-VTZ-001-01.01 was utilized as the guiding document during test performance. During testing, minor system modifications, such as revised system documentation or software versions, may have been incorporated. This test report reflects Phase 1 testing completed and details the final versions of all technical documentation and system components and supersedes the approved test plan.

Unless otherwise annotated, all testing was conducted at the Pro V&V test facility located in Huntsville, AL, by personnel verified by Pro V&V to be qualified to perform the test

1.1 Scope

The scope of the testing event incorporated a sufficient spectrum of functional tests to verify that the RABM features and applications conform to the defined requirements. Specifically, the testing event had the following goals:

Phase 1

- Usability and Accessibility Review

Phase 2

- Verify that the RABM performs as documented in the provided system technical documentation
- Evaluate the RABM System as it relates to voter experience and transmission of the voter's selection to the jurisdiction.

- Execute system use cases to evaluate system functionality.
- Source Code Review
- Physical Configuration Audit (PCA)
- Functional Configuration Audit (FCA)
- System Integration Testing, including Accuracy Testing and Regression Testing
- Security Testing
- Telecommunications Testing

1.2 References

- Voatz Mobile Elections Platform Proposed Test Plan
- Implementation Statement
- Election Assistance Commission 2015 Voluntary Voting System Guidelines (VVSG) Version 1.1, Volume I, "Voting System Performance Guidelines", and Volume II, "National Certification Testing Guidelines"
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2016 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated July 2016
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Pro V&V, Inc. Quality Assurance Manual, Revision 7.0
- Hunt Engagement Summary
- System Technical Data Package *(A listing of the documents submitted for this test campaign is listed in Section 4.6 of this Test Plan)*

1.2 Terms and Abbreviations

This subsection lists terms and abbreviations relevant to the hardware, the software, or this Test Plan.

"COTS" – Commercial Off-The-Shelf

"EAC" – United States Election Assistance Commission

"EBM" -- Electronically-assisted Ballot Marker

"FCA" – Functional Configuration Audit

"HAVA" – Help America Vote Act

"ISO" – International Organization for Standardization

"PCA" – Physical Configuration Audit

"QA" – Quality Assurance

"TDP" – Technical Data Package

"VSTL" – Voting System Test Laboratory

"VVSG" – Voluntary Voting System Guidelines

2.0 TESTING OVERVIEW

The evaluation of the RABM System addressed each of the test goals in the following manner:

Table 2-1: Testing Overview

Test Goal	Testing Response
Perform a Usability and Accessibility Review	A usability and accessibility review was performed on the submitted system. This review focused on the usability of the system as evaluated against the requirements matrix.

2.1 System Overview

The following sections contain a product description and an overview of the design methodology of the RABM System, as taken from the system technical documentation.

The Voatz Mobile Elections Platform is a configurable, cloud-based Remote Accessible Ballot Marking (RABM) system that:

- Delivers blank ballots to eligible voters
- Allows voters to mark their selections accessibly and verify their selections
- Returns the marked ballots to the jurisdiction according to the statutory provisions of the voter's state.

Jurisdictions can specify the method of returning voted ballots based on their state's statutory requirements and include any state-specific legal documents (such as signed affidavits or checkbox waivers.)

To determine eligibility to vote, voter registration records are incorporated into the Voatz Platform by importing the data. Typically, an indicator in the voter file designates which subset of all voters are eligible to vote remotely. While the Voatz system can remotely confirm the validity of a voter's credentials (e.g. driver's license) and verify the person presenting their credentials is the same person on the credential, it does not by itself determine whether individual

voters are authorized to vote in the current election. This determination must be made by the jurisdiction and indicated in the voter records. Voatz then limits voting to those individuals so designated.

The Voatz RABM system uses all commercial off-the-shelf (COTS) hardware; no proprietary hardware is required. Ballots are marked securely and anonymously via a mobile app on the voter's smartphone—the Voatz Mobile App (VMA).

Marked ballots are returned electronically to the jurisdiction, along with any other required documents. The jurisdiction then prints the returned marked ballots as optical scannable ballots on official ballot stock for tabulation by the primary voting system. Voters receive a password protected ballot receipt that lists their selections and contains an anonymous ID; the jurisdiction receives an identical anonymized copy. Only the voter knows the anonymous ID that is linked to them.

The RABM is categorized by the Voluntary Voting System Guidelines (VVSG) version 1.1 as an Electronically assisted Ballot Marker (EBM) and is defined as follows:

Accessible Voting Station that produces an executed, human-readable paper ballot as a result, and that does not make any other lasting record of the voter's votes on the device.

Voatz has provided responses to a recently issued guidance to election officials regarding electronic ballot delivery and marking circulated by the EAC. The information on the RABM system functionality as provided by Voatz is presented in Attachment B.

2.2 Block Diagram

The process flow of the system is depicted in Figure 1-1.

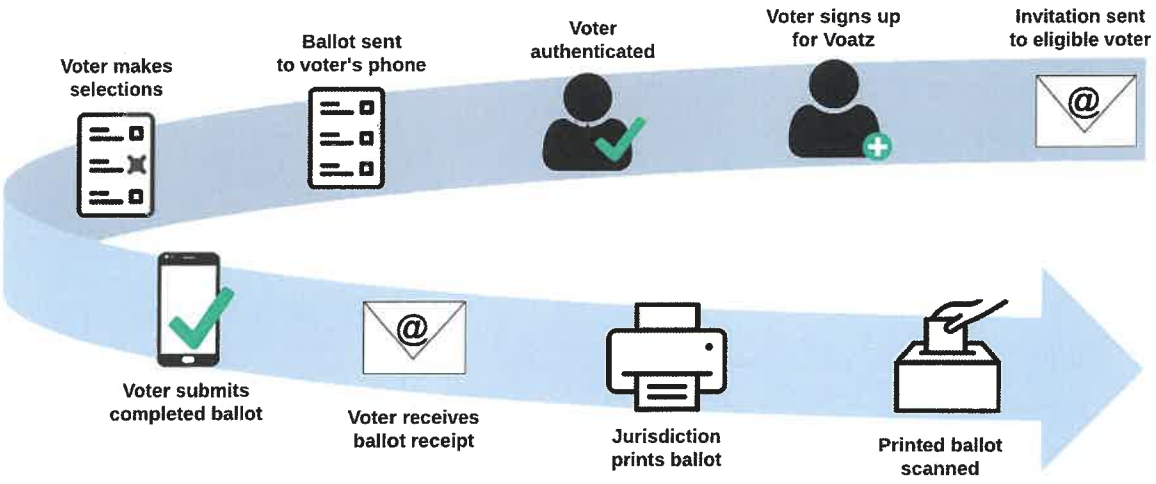
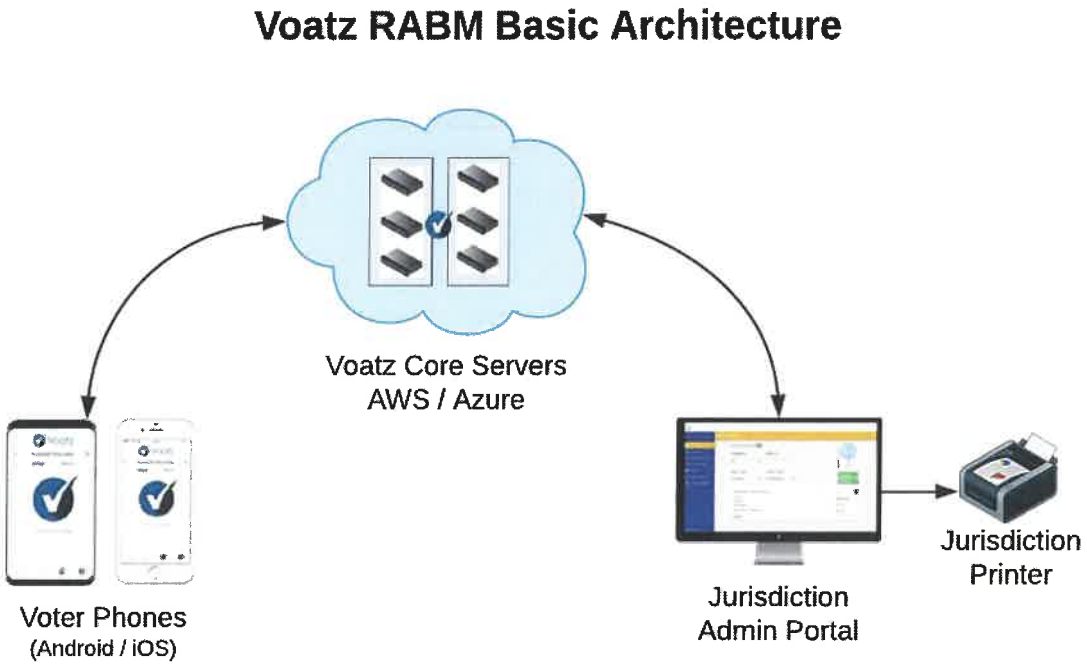


Figure 1-1. RABM Process Flow

2.3 Test Configuration



The testing campaign utilized various models of cell phones, with the Voatz Mobile App (VMA) installed. To access the back-end environment, one Pro V&V laptop was utilized. Ballots generated during testing were printed as optical scannable ballots using an OKI printer.

3.0 MATERIALS REQUIRED FOR TESTING

The following sections list all materials required during the test engagement.

The materials required for testing of the RABM System included all materials to enable the test campaign to occur. This included the applicable hardware and software as well as the TDP, test support materials, and deliverable materials, as described in the following subsections.

3.1 Software

This subsection lists the proprietary and COTS software provided by the manufacturer as part of the test campaign.

Table 3-1. RABM System Software

Firmware/Software	Version
Voatz Mobile App (VMA) for iOS	1.031 (186)
Voatz Mobile App (VMA) for Android	1.1.120 (155)
Voatz Admin Portal	1.0.42

3.2 Equipment

This subsection lists the COTS equipment provided by the manufacturer as part of the test campaign.

For COTS equipment, every effort was made to verify that the COTS equipment has not been modified for use. This was accomplished by performing research using the COTS equipment manufacturer's websites based on the serial numbers for each piece of equipment. Assigned test personnel evaluated COTS hardware, system software and communications components for proven performance in commercial applications other than voting. For smartphones, the device information was compared to the supported configurations in the campaign. Physical external and internal examination was also performed when the easily accessible without the possibility of equipment damage. Hard drives, RAM memory, and other components were examined to verify that the components match the information found on the COTS equipment manufacturer's websites. A factory reset was performed on smartphones prior to testing.

Table 3-2. RABM System Equipment

Component	Model	Serial Number	OS
iPhone 6s	MKRX2LL/A	C6KRL9HVGRY8	iOS 13.3.1
iPhone 6	MG4Q2LL/A	FFMP901MG5MF	iOS 12.4.5
LG Phoenix 4	LM-X210APM	912VTSM766174	Android 8.1.0
Moto e6	XT2005-1PP	352176100933789	Android 9.0
Okidata Printer	432dn-B	AK88034459C0	N/A

3.3 Technical Data Package

A listing of all documents contained in the system TDP relevant to this Phase 1 report is provided in Table 3-3.

Table 3-3. TDP Documents

Document	Description
Vendor Proposed VSTL Usability and Accessibility Test Plan	Provides suggested scope, approach, and criteria of intended testing activities.
System Hardware and Software Specification	Provides detailed specifications of the hardware and software components of the system.

3.4 Test Support Materials

This subsection lists the test materials required to execute the required tests throughout the test campaign.

The following materials were supplied by Voatz to facilitate testing:

- Ballot Paper
- Printer Ink

- Other materials and equipment as required

4.0 TEST PROCESS AND RESULTS

Testing of the RABM System submitted for evaluation was performed to verify that the System conforms to the applicable requirements in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 and the manufacturer-stated requirements set forth in the system documentation. The VVSG 1.1 Requirements Matrix generated for this test campaign was used as a guide to determine the specific tests to be performed. Pro V&V developed test procedures designed to evaluate the system being tested against the stated requirements. The test cases were performed using three types of elections: Primary, General, and Ranked Choice voting. The test procedures were executed independently.

The evaluation area for this test engagement is summarized in the subsection below.

4.1 Usability and Accessibility Testing

The usability testing focuses on the usability of the system being tested. Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter, the product is the RABM, and the task is the correct recording of the voter ballot selections. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the voter selections should be private. Accessibility evaluates the requirements for accessibility. These requirements are intended to address HAVA 301 (a) (3) (B).

Usability and Accessibility Testing included system use cases for the following areas:

- Usability Support
- Cognitive Disabilities
- Perceptual Disabilities
- Interaction Disabilities
- System and Voter Wait Times
- Language Support
- General Accessibility Assistance
- Limited Vision Assistance
- Blind Voter Assistance
- Motor Control Difficulty Assistance
- Limited Hearing Assistance
- English Illiteracy Assistance
- Limited Speech Assistance

Summary Findings

The RABM System was evaluated against the VVSG 1.1 Requirements Matrix generated for this test campaign. Based on the results obtained, the RABM was determined to meet the applicable

Usability and Accessibility requirements. The following observations/exceptions were noted during the review:

Table 4-1 Summary Findings

Requirement	Notes
Usability Review	
Volume I, Section 3.2.3.1 *Privacy at the polls*	
3.2.3.1.a, 3.2.3.1.b, 3.2.3.1.c, 3.2.3.1.d, 3.2.3.1.e	These requirements are not applicable due to there being no polling place.
Volume I, Section 3.2.6.1 *Timing*	
3.2.6.1.a, 3.2.6.1.b, 3.2.6.1.c	Note: Timing was tested concurrent with a simulated load of 500 other users voting.
3.2.6.1.f	The timing of the alert and expiration of session pass. However, there is no poll worker, thus there is no poll worker intervention. The user is required to login again.
Volume I, Section 3.2.7a *Alternative Languages*	
3.2.7a.i.v	Any external reports to be reviewed pending final TDP.
Accessibility Review	
Volume I, Section 3.3.2 *Enhanced visual interfaces*	
3.3.2.c.i, 3.3.2.c.ii	Phone contains capability.
Volume I, Section 3.3.3 *Audio-tactile interfaces*	
3.3.3.a & 3.3.3.a.i	Any external test reports to be reviewed pending final TDP.
3.3.3.b, 3.3.3.b.i, 3.3.3.b.ii, 3.3.3.b.iii, 3.3.3.b.iv. 3.3.3.b.v, 3.3.3.c.i, 3.3.3.c.ii, 3.3.3.3.iii	The system does not contain an ATI; therefore these requirements are not applicable.
3.3.3.c.iv, 3.3.3.c.v, 3.3.3.c.vi	These requirements relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized.
3.3.3.f, 3.3.3.g	These requirements relate to accessible voting stations and are not applicable.
Volume I, Section 3.3.4 *Enhanced input and control characteristics*	
3.3.4.a, 3.3.4.d	These requirements relate to accessible voting stations and are not applicable.
3.3.4.b	Partial Pass - Only on iPhone 6s & higher and iOS 13 & higher support hands-free operation using Voice Control. Android devices do not have this capability yet. However, both devices support limited dexterity with VoiceOver or TalkBack navigation (audio can be turned off.)
Volume I, Section 3.3.5 *Design for mobility aids*	
3.3.5	These requirements relate to accessible voting stations and are not applicable.

Table 4-1 Summary Findings *(continued)*

Requirement	Notes
Volume I, Section 3.3.6 *Enhanced auditory interfaces*	
3.3.6.c	These requirements relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized.
Volume I Section 3.3.10 *Summative Usability Report*	
3.3.10.c.i, 3.3.10.a, 3.3.10.b, 3.3.10.c	Any external test reports to be reviewed pending final TDP.

The results of the evaluation are presented in Attachment A. Each item listed in the table above will have an asterisk in Attachment A.

5.0 CONCLUSION

Based on the results obtained during the test campaign, Pro V&V determined the RABM, as presented for evaluation, meets the Usability and Accessibility requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1, with the clarifications or exceptions noted in Table 4-1.

.

ATTACHMENT A - REQUIREMENTS MATRIX

Table A-1 Usability Review Matrix Requirements

Requirement	Description	Result
	Usability	
3	Usability Requirements	
3.1.1	Purpose	
3.1.1.a	All eligible voters shall have access to the voting process without discrimination.	Pass
3.1.1.a.i	The voting process shall be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed.	Pass
3.1.1.b	Each cast ballot shall accurately capture the selections made by the voter.	Pass
3.1.1.b.i	The ballot shall be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.	Pass
3.1.1.c	The voting process shall preserve the secrecy of the ballot.	Pass
3.1.1.c.i	The voting process shall preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.	Pass
3.2	General usability requirements	
3.2.a and 3.2.b	The voting process shall provide a high level of usability for voters. Accordingly, voters shall be able to negotiate the process effectively, efficiently, and comfortably. The mandatory voting system standards mandated in HAVA Section 301 relate to the interaction between the voter and the voting system:	
3.2.a.1.A	Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall --	
3.2.a.1.A.i	Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted.	Pass
3.2.a.1.A.ii	Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).	Pass
3.2.a.1.A.iii	If the voter selects votes for more than one candidate in a single office:	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.a.1.A.iii.I	Notify the voter that the voter has selected more than one candidate for a single office on the ballot.	Pass
3.2.a.1.A.iii.II	Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office.	Pass
3.2.a.1.A.iii.III	Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.	Pass
3.2.a.1.B	A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A) (iii) by:	
3.2.a.1.B.i	Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office.	Pass
3.2.a.1.B.ii	Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).	Pass
3.2.a.1.C	The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.	Pass
3.2.1	General usability	
3.2.1.a	The voting system shall support voters in the task of effectively completing their ballots.	Pass
3.2.1.b	The features of the voting system shall not contribute to the commission of voter error within the voting session.	Pass
3.2.2	Functional Capabilities	
	The usability of the voting process is enhanced by the presence of certain functional capabilities. These capabilities differ somewhat depending on whether or not the system presents an editable interface within which voters can easily change their votes (typically an electronic screen) or an interface in which voters must obtain a new ballot to make changes (typically a manually-marked paper ballot).	
3.2.2.a	If the voter selects more than the allowable number of choices within a contest, the voting system shall notify the voter of the effect of this action before the ballot is cast and counted.	Pass
3.2.2.c	The voting system shall provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.2.b	The voting system shall allow the voter, at the voter's choice, to submit an undervoted ballot without correction.	Pass
3.2.2.d	If and only if the voter successfully casts or prints the ballot, then the electronic ballot interface or PCOS system shall so notify the voter.	Pass
3.2.2.1	Editable electronic ballot interfaces	
	Voting systems such as DREs and EBMs present voters with an editable interface, allowing them to easily change their votes prior to final casting of the ballot.	
3.2.2.1.a	The electronic ballot interface shall prevent voters from selecting more than the allowable number of choices for each contest.	Pass
3.2.2.1.b	The electronic ballot interface shall provide feedback to the voter, before final casting or printing of the ballot, that identifies specific contests for which the voter has selected fewer than the allowable number of choices (i.e., undervotes).	Pass
3.2.2.1.c	The electronic ballot interface shall provide the voter the opportunity to correct the ballot before it is cast or printed. The electronic ballot interface shall allow the voter to make these corrections without assistance. The corrections to be supported include modifying an undervote and changing a vote from one candidate to another.	Pass
3.2.2.1.d	The electronic ballot interface shall allow the voter to change a vote within a contest before advancing to the next contest.	Pass
3.2.2.1.e	The electronic ballot interface shall provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest(s) currently being presented (whether visually or aurally).	Pass
3.2.2.1.f	If the voter takes the appropriate action to cast a ballot, but the DRE does not accept and record it successfully, including failure to store the ballot image, then the DRE shall so notify the voter and provide clear instruction as to the steps the voter should take to cast the ballot.	Pass
3.2.2.1.g	If the electronic ballot interface generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system shall allow the voter to verify that record using the same access features used by the voter to vote the ballot.	Pass
3.2.2.2	Non-Editable ballot interfaces	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	Non-Editable interfaces, such as manually-marked paper ballots, do not have the same flexibility as do editable interfaces. Nonetheless, certain features are required, especially in the case of precinct-based optical scanners.	
3.2.2.2.a	The PCOS system shall be capable of providing feedback to the voter that identifies specific contests for which the voter has made more than the allowable number of votes (i.e., overvotes).	*Not Applicable*
3.2.2.2.b	The PCOS system shall be capable of providing feedback to the voter that identifies specific contests for which the voter has made fewer than the allowable number of votes (i.e., undervotes). The system shall provide a means for an authorized election official to deactivate this capability entirely and by contest. However, if a ballot is submitted with all the contests on one side left blank, notification to the voter is performed as described in requirement 3.2.2.2 c	*Not Applicable*
3.2.2.2.c	The PCOS system shall be capable of notifying the voter that he or she has submitted a paper ballot that is blank on one or both sides. The system shall provide a means for an authorized election official to deactivate this capability.	*Not Applicable*
3.2.2.2.d	If the PCOS system has notified the voter that a potential error condition (such as an overvote, undervote, or blank ballot) exists, the system shall then allow the voter to correct the ballot or to submit it as is.	*Not Applicable*
3.2.2.2.e	Paper-based precinct tabulators shall be able to identify a ballot containing marginal marks. When such a ballot is detected, the tabulator shall:	*Not Applicable*
3.2.2.2.e.i	Return the ballot to the voter;	*Not Applicable*
3.2.2.2.e.ii	Provide feedback to the voter that identifies the specific contests for which a marginal mark was detected; and	*Not Applicable*
3.2.2.2.e.iii	Allow the voter either to correct the ballot or to submit the ballot "as is" without correction, at the voter's choice.	*Not Applicable*
3.2.2.2.f	Software used to format optical scan ballots shall constrain the size and contrast of all target areas to conform to the following requirements:	*Not Applicable*
3.2.2.2.f.i	The target shall be no less than 3 mm across in any direction	*Not Applicable*
3.2.2.2.f.ii	The contrast ratio between the target area boundaries and the surrounding space shall be no less than 10:1.	*Not Applicable*

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.2.2.g	If the voter takes the appropriate action to cast a ballot, but the PCOS system does not accept and record it successfully, including failure to read the ballot or to transport it into the ballot box, the PCOS shall so notify the voter.	*Not Applicable*
3.2.3	Privacy	
3.2.3	The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.	
3.2.3.1	Privacy at the polls	
3.2.3.1.a	The voting system shall prevent others from determining the contents of a ballot.	*Not Applicable**
3.2.3.1.b	The voting system shall support ballot privacy during the voting session and ballot submission.	*Not Applicable**
3.2.3.1.c	During the voting session, the audio interface of the voting system shall be audible only to the voter.	*Not Applicable**
3.2.3.1.d	The voting system shall issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.	*Not Applicable**
3.2.3.1.e	The voting system shall not issue a receipt to the voter that would provide proof to another of how the voter voted.	*Not Applicable**
3.2.3.2	No recording of alternative format usage	
	When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered. However, in the case of paper ballots, where the interface is the record, some format information is unavoidably preserved.	
3.2.3.2.a	No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.	Pass
3.2.3.2.b	No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.	Pass
3.2.4	Voter instructions, plain language, and information presentation	
	The features specified in this section are intended to minimize cognitive difficulties for voters. Voters should always be able to operate the voting system and understand the effect of their actions. Note that the "should" requirements in this section must be adhered to unless there is strong justification provided for making an exception.	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.4.a	The voting system shall provide instructions for all its valid operations.	Pass
3.2.4.b	The voting system shall provide a means for the voter to get help directly from the system at any time during the voting session.	Pass
3.2.4.c	Instructional material for the voter shall conform to norms and best practices for plain language.	Pass
3.2.4.c.i	Warnings and alerts issued by the voting system shall be distinguishable from other information and should clearly state: The nature of the problem; Whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way; and The set of responses available to the voter.	Pass
3.2.4.c.ii	When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.	Pass
3.2.4.c.iii	The voting system should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.	Pass
3.2.4.c.iv	Each distinct instruction should be separated spatially from other instructions for visual or tactile interfaces, and temporally for auditory interfaces.	Pass
3.2.4.c.v	The voting system should issue instructions on the correct way to perform actions, rather than telling voters what not to do.	Pass
3.2.4.c.vi	The system's instructions should address the voter directly rather than use passive voice constructions.	Pass
3.2.4.c.vii	The voting system should avoid the use of gender-based pronouns.	Pass
3.2.4.d	Consistent with election law, the voting system shall support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices shall be presented in an equivalent manner.	Pass
3.2.4.e	The voting system shall provide the capability to design a ballot with a high level of clarity and comprehensibility.	Pass
3.2.4.e.i	The voting system should not visually present a single contest spread over two pages or two columns.	Pass
3.2.4.e.ii	The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.4.e.iii	The relationship between the name of a candidate and the mechanism used to vote for that candidate shall be consistent throughout the ballot.	Pass
3.2.4.e.iv	The voting system should present instructions near to where they are needed.	Pass
3.2.4.f	The use of color by the voting system shall agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.	Pass
3.2.4.g	When an icon is used to convey information, indicate an action, or prompt a response, it shall be accompanied by a corresponding linguistic label.	Pass
3.2.5	Visual display characteristics	
	The requirements of this section are designed to minimize perceptual difficulties for the voter. Some of these requirements are designed to assist voters with poor reading vision. These are voters who might have some difficulty in reading normal text, but are not typically classified as having a visual disability and thus might not be inclined to use the Acc-VS.	
3.2.5.a	If the voting system uses an electronic display screen as the primary visual interface for the voter, the display shall have the following characteristics:	
3.2.5.a.i	Flicker frequency NOT between 2 Hz and 55 Hz. Does not say "flashing elements" like NIST did? If so maybe one Dell reported concern in settings.	Untested
3.2.5.a.ii	Minimum display brightness: 130 cd/m2	Untested
3.2.5.a.iii	Minimum display darkroom 7×7 checkerboard contrast: 150:1	Untested
3.2.5.a.iv	Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)	Untested
3.2.5.a.v	Minimum display area 700 cm2	Untested
3.2.5.a.vi	Antiglare screen surface that shows no distinct virtual image of a light source	Untested
3.2.5.a.vii	Minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1	Untested

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.5.b	Any aspect of the voting system voter interface that is adjustable by either the voter or poll worker, including font size, color, contrast, audio volume, or rate of speech, shall automatically reset to a standard default value upon completion of that voter's session. For the Acc-VS with an electronic image display, the aspects include synchronized audio/video mode and non-manual input mode.	Pass
3.2.5.c	If any aspect of a voting system is adjustable by either the voter or poll worker, there shall be a mechanism to allow the voter to reset all such aspects to their default values while preserving the current votes.	Pass
3.2.5.d	For all text intended for voters or poll workers, the voting system shall provide a font with the following characteristics	
3.2.5.d.i	Height of capital letters at least: 3.0 mm	Untested
3.2.5.d.ii	x-height of at least: 70% of cap height	Untested
3.2.5.d.iii	Stroke width at least: 0.35 mm.	Untested
3.2.5.e	A voting system that uses an electronic image display shall be capable of showing all information in at least two font sizes:	
3.2.5.e.i	3.0-4.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.35 mm;	Untested
3.2.5.e.ii	6.3-9.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.7 mm; under control of the voter. The system shall allow the voter to adjust font size throughout the voting session while preserving the current votes.	Untested
3.2.5.f	Text intended for the voter should be presented in a sans serif font.	Pass
3.2.5.g	Voting systems using paper ballots or paper verification records shall provide features that assist in the reading of such ballots and records by voters with poor reading vision.	
3.2.5.g.i	The voting system may achieve legibility of paper records by supporting the printing of those records in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm.	Untested
3.2.5.g.ii	The system may achieve legibility of paper records by supporting magnification of those records. This magnification may be done by optical or electronic devices. The manufacturer may either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.	Untested

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.5.h	The colors in the default presentation shall support perception by voters and poll workers with color vision deficiencies, of all text, controls, and infographics or icons on the ballot or ballot interface.	
3.2.5.h.i	The default visual display for voters and poll workers of a voting station with an electronic display shall have a luminosity contrast ratio between the foreground text and background color of at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons. For paper ballots, the contrast ratio shall be at least 10:1 as measured based on ambient lighting of at least 300 lx.	Untested
3.2.5.h.ii	A voting station with an electronic display screen shall have a high contrast mode either as an initial setting or under the control of the voter. If the system allows the voter to adjust contrast during the voting session it shall preserve the current votes. High contrast is a luminosity contrast ratio between the foreground text and background color of at least 20:1. The high contrast mode shall use at least one of the following color combinations: o Black text on a white background o White text on a black background o Yellow text on a black background o Light cyan text on a black background	Untested
3.2.5.i	Color coding shall not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Pass
3.2.6	Voter-interface interaction	
	The requirements of this section are designed to minimize interaction difficulties for the voter.	
3.2.6.a	Voting machines with electronic image displays shall not require page scrolling by the voter. Discussion: This is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the "page." Voting systems may require voters to move to the next or previous "page."	Pass
3.2.6.b	The voting machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.6.c	d. Input mechanisms shall be designed to minimize accidental activation.	Pass
3.2.6.c.i	On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.	Untested
3.2.6.c.ii	No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position.	Pass
3.2.6.1	Timing	
	These requirements address how long the system and voter wait for each other to interact.	
3.2.6.1.a	The initial system response time of the electronic ballot interface shall be no greater than 0.5 seconds.	Pass*
3.2.6.1.b	When the voter performs an action to record a single vote, the completed system response time of the electronic ballot interface shall be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.	Pass*
3.2.6.1.c	The completed system response time during a voter interaction with the visual display of the electronic ballot interface shall be no greater than 10 seconds.	Pass*
3.2.6.1.d	If the electronic ballot interface has not completed its visual response within one second, it shall present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.	Pass
3.2.6.1.e	The electronic ballot interface shall detect and warn about lengthy voter inactivity during a voting session. Each electronic ballot interface shall have a defined and documented voter inactivity time, and that time shall be between two and five minutes.	Pass
3.2.6.1.f	Upon expiration of the voter inactivity time, the electronic ballot interface shall issue an alert and provide a means by which the voter may receive additional time. The alert time shall be between 20 and 45 seconds. If the voter does not respond to the alert within the alert time, the electronic ballot interface shall go into an inactive state requiring poll worker intervention.	Partial Pass*
3.2.7	Alternative languages	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting age population). Thus, election officials must ensure that the voting system they deploy is capable of handling the languages meeting the legal threshold within their districts.	
3.2.7.a	The voting system shall be capable of presenting the ballot, contest choices, review screens, vote verification records, and voting instructions in any language declared by the manufacturer to be supported by the system.	Pass
3.2.7.a.i	The electronic ballot interface should allow the voter to select among the available languages throughout the . voting session while preserving the current votes. When presenting a choice of languages to the voter, the electronic ballot interface shall use the native name of each language.	Pass
3.2.7.a.ii	Information presented to the voter in the typical case of English-literate voters (including instructions, warnings, messages, contest choices, and vote verification information) shall also be presented when an alternative language is being used, whether the language is written or an unwritten language presented aurally.	Pass
3.2.7.a.iii	Any records, including paper ballots and paper verification records, shall have the information required to support auditing by poll workers and others who can read only English.	Pass
3.2.7.a.iv	The manufacturer shall conduct summative usability tests for each of the voting system's supported languages, using subjects who are fluent in those languages but not fluent in English and shall report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
3.2.8	Usability for poll workers	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	Voting systems are used not only by voters to record their votes, but also by poll workers who are responsible for set-up, operation while polls are open, light maintenance, and poll closing. Because of the wide variety of implementations, it is impossible to specify detailed design requirements for these functions. The requirements below describe general capabilities that all systems must support.	Untested
3.2.8.a	Messages generated by the voting system for poll workers in support of the operation, maintenance, or safety of the system shall adhere to the requirements for clarity in Section 3.2.4 "Voter instructions, plain language and information presentation."	Untested
3.2.8.1	Operations	
	Poll workers are responsible for opening polls, keeping the polls open and running smoothly during voting hours, and closing the polls afterwards. Operations may be categorized in three phases: Setup includes all the steps necessary to take the system from its state as normally delivered to the polling place, to the state in which it is ready to record votes. It does not include ballot definition. Polling includes such functions as: • voter identification and authorization; • preparing the system for the next voter; • assistance to voters who wish to change their ballots or need other help; • system recovery in the case of voters who abandon the voting session without having cast a ballot; and routine hardware operations, such as installing a new roll of paper. Shutdown includes all the steps necessary to take the system from the state in which it is ready to record votes to its normal completed state in which it has captured all the votes cast and the voting information cannot be further altered.	
3.2.8.1.a	Voting system setup, polling, and shutdown, as documented by the manufacturer, shall be reasonably easy for the typical poll worker to learn, understand, and perform.	*Not Applicable*
3.2.8.1.b	The manufacturer shall conduct summative usability tests on the voting system using individuals who are representative of the general population and shall report the test results, using the Common Industry Format, as part of the TDP.	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.8.1.b.i	The tasks to be covered in the test shall include setup, operation, and shutdown.	*Not Applicable*
3.2.8.1.b.ii	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable*
3.2.8.1.c	The voting system shall include clear, complete, and detailed instructions and messages for setup, polling, and shutdown.	*Not Applicable*
3.2.8.1.c.i	The documentation required for normal voting system operation shall be presented at a level appropriate for poll workers who are not experts in voting system and computer technology.	*Not Applicable*
3.2.8.1.c.ii	The documentation shall be in a format suitable for use in the polling place.	*Not Applicable*
3.2.8.1.c.iii	The instructions and messages shall enable the poll worker to verify that the voting system o Has been set up correctly (setup); o Is in correct working order to record votes (polling); and o Has been shut down correctly (shutdown).	*Not Applicable*
3.2.8.2	Safety	
	All voting systems and their components must be designed so as to eliminate hazards to personnel or to the equipment itself. Hazards include, but are not limited to: • fire hazards; • electrical hazards; • potential for equipment tip-over (stability); • potential for cuts and scrapes (e.g., sharp edges); • potential for pinching (e.g., tight, spring-loaded closures); and • potential for hair or clothing entanglement.	
3.2.8.2.a	Devices associated with the voting system shall be certified in accordance with the requirements of UL 60950-1, Information Technology Equipment – Safety – Part 1 by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.	Pass
3.2.8.2.b	The certification organization's scope of accreditation shall include IEC/UL 60950-1.	Pass

Table A-2 Accessibility Review Matrix Requirements

Requirement	Description	Result
	Accessibility	
3.3	Accessibility Requirements	pass/fail
3.3.1	General accessibility	
	The requirements of this section are relevant to a wide variety of disabilities.	
3.3.1.a	The of this section are relevant to a wide variety of disabilities. Acc-VS shall be integrated into the manufacturer's complete voting system so as to support accessibility for disabled voters throughout the voting session.	
3.3.1.a.i	The manufacturer shall supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.	Pass
3.3.1.b	When the provision of accessibility for the Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, shall be presented in that alternative format.	Pass
3.3.1.c	The support provided to voters with disabilities shall be intrinsic to the Acc-VS. Personal assistive devices of the voter shall not be necessary to operate the Acc-VS correctly. This does not apply to personal assistive technology required to comply with 3.3.4 b.	Pass
3.3.1.d	If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the Acc-VS shall provide a secondary means that does not depend on those characteristics.	Pass
3.3.1.e	If the Acc-VS generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record then the voting system shall allow the voter to verify that record using the same access features used by the voter to cast the ballot.	Pass
3.3.2	Enhanced visual interfaces	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
	These requirements specify the features of the Acc-VS designed to make the visual interface easier to see, in particular for voters with vision deficiencies, and synchronized with audio for voters with various language, reading, or some cognitive disabilities. In general, low vision is defined as having a visual acuity worse than 20/70. Low (or partial) vision also includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night People with tunnel vision can see only a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the range. People with low vision or color blindness benefit from high contrast and from a selection of color combinations appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required. Note also the general Requirement 3.2.5 h.i. However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual white-out that makes these users unable to distinguish individual letters. Thus, use of non-saturated color options is an advantage for some people. It is important to note that some of the requirements in 3.2.5 "Visual display characteristics" also provide support for voters with certain kinds of vision problems.	
3.3.2.a	An Acc-VS with a color electronic image display shall allow the voter to adjust the color saturation throughout the voting session while preserving the current votes.	Pass
3.3.2.a.i	At a minimum, two alternative display options listed shall be available: 1) black text on white background,2) white text on black background, 3) yellow text on a black background, or 4) light cyan text on a black background.	Pass

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.2.b	Groups of buttons and controls which perform different functions on the Acc-VS shall be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys in wide use by individuals with disabilities, such as a full alphabetic keyboard when used for purposes other than basic navigation and selection (e.g. entering a write-in candidate name).	Pass
3.3.2.c	If the Acc-VS has an electronic image display, the Acc-VS shall provide synchronized audio output to convey the same information as that which is displayed on the screen	
3.3.2.c.i	There shall be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively.	Pass*
3.3.2.c.ii	The system shall allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.	Pass*
3.3.3	Audio-tactile interfaces	
	These requirements specify the features of the Acc-VS designed to not only assist voters who are blind, but also those voters who would benefit from an auditory, rather than a purely visual, interface.	
3.3.3.a & 3.3.3.a.i	The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.	*Not Applicable**

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.b	The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3. • Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations • Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition) • Instructions and feedback for navigation of the ballot • Instructions and feedback for contest choices, including write-in candidates • Instructions and feedback on confirming and changing selections • Instructions and feedback on final submission of ballot	*Not Applicable**
3.3.3.b.i	The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine. Discussion: For example, if a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, so must the ATI.	*Not Applicable**
3.3.3.b.ii	The ATI shall allow the voter to have any information provided by the voting system repeated.	*Not Applicable**
3.3.3.b.iii	The ATI shall allow the voter to pause and resume the audio presentation.	*Not Applicable**
3.3.3.b.iv	The ATI shall allow the voter to skip to the next contest or return to previous contests. Discussion: This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether. v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	*Not Applicable**
3.3.3.b.v	The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	*Not Applicable**
3.3.3.c	All voting stations that provide audio presentation of the ballot shall conform to the following requirements:	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.c.i	The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.	*Not Applicable**
3.3.3.c.ii	When a voting machine utilize es a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	*Not Applicable**
3.3.3.c.iii	A sanitized headphone or handset shall be made available to each voter.	*Not Applicable**
3.3.3.c.iv	The audio system shall set the initial volume for each voting session between 60 and 70 dB SPL.	Untested*
3.3.3.c.v	The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	Untested*
3.3.3.c.vi	The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.	Untested*
3.3.3.c.vii	The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.	Pass
3.3.3.c.viii	The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.	Pass
3.3.3.d	If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.	Pass
3.3.3.e	If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.	Pass
3.3.3.f	All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.	*Not Applicable*

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.g	On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.	*Not Applicable*
3.3.4	Enhanced input and control characteristics	
	These requirements specify the features of the Acc-VS designed to assist voters who lack fine motor control or use of their hands.	
3.3.4.a	The Acc-VS shall provide a 3.5 mm industry standard jack used to connect a personal assistive technology switch to the Acc-VS. This jack shall allow only switch data to be transmitted to the voting system. The voting system shall accept switch input that is functionally equivalent to tactile input. All the functionality of the Acc-VS (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, shall also be available through this non-manual input mechanism.	*Not Applicable**
3.3.4.b	The Acc-VS shall provide features that enable voters who lack fine motor control or the use of their hands to submit their ballots privately and independently without manually handling the ballot.	Partial pass
3.3.4.c	All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N).	Pass
3.3.4.d	The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit.	*Not Applicable**
3.3.5	Design for mobility aids	
	These requirements specify the features of the Acc-VS designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).	
3.3.5.a	The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.	*Not Applicable**
3.3.5	All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements:	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.5.1.a	If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum.	*Not Applicable**
3.3.5.1.b.i 3.3.5.1.b.ii	If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply: • The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches. • If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.	*Not Applicable**
3.3.5.1.b.iii	Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions: • Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction • The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater • Toe clearance shall be 30 inches (760 mm) wide minimum	*Not Applicable**
3.3.5.1.b.iv	Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions: • Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground. • The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater. • Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. • Knee clearance shall be 30 inches (760 mm) wide minimum.	*Not Applicable**

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.5.c	All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station	*Not Applicable**
3.3.5.1.c	If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches.	*Not Applicable**
3.3.5.1.d.i 3.3.5.1.d.ii	If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. • The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches. • If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches.	*Not Applicable**
3.3.6	Enhanced auditory interfaces	
	These requirements specify the features of the Acc-VS designed to assist voters with hearing disabilities.	
3.3.6 a	The Acc-VS shall incorporate the features listed under Requirement 3.3.3 c for voting systems that provide audio presentation of the ballot.	Partial pass
3.3.6 b	If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.	Pass
3.3.6.c	No voting device shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, shall achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	Untested*
3.3.8	English proficiency	
3.3.8.a	For voters who lack proficiency in reading English, the Acc-VS shall provide an audio interface for instructions and ballots as described in 3.3.3 b.	Pass
3.3.9	Speech not required	
3.3.9.a	The voting system shall not require voter speech for its operation.	Pass

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.10	Summative Usability Report	
3.3.10.a	The manufacturer shall submit a report of their summative usability tests on the voting system using individuals who are representative of the general population.	*Not Applicable**
3.3.10.a.i	The report shall be submitted in the Common Industry Format.	*Not Applicable**
3.3.10.a.ii	The report shall contain the results of the summative usability tests.	*Not Applicable**
3.3.10.b	The manufacturer shall conduct summative usability tests on the Acc-VS using individuals with low vision and shall report the test results, using the Common Industry Format, as part of the TDP.	*Not Applicable**
3.3.10.b.i	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
3.3.10.c	The manufacturer shall conduct summative usability tests on the Acc-VS using individuals lacking fine motor control and shall report the test results, using the Common Industry Format, as part of the TDP.	*Not Applicable**
3.3.10.c.i	The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.	*Not Applicable**
3.3.10.c.i	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
	Discussion: Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to encourage early detection and resolution of usability problems. The manufacturer must submit the usability test report to the VSTL as part of their TDP. The VSTL will then check the technical data package to ensure that the report is present and reported in the Common Industry Format and contains the results from a summative usability test.	

ATTACHMENT B – VOATZ EBDM RESPONSES

Electronic Ballot Delivery and Marking

Voatz Remote Accessible Ballot Marking System
Voatz, Inc.

In response to recently-issued guidance to election officials regarding electronic ballot delivery and marking circulated by the Federal Election Assistance Commission (EAC) *, Voatz provides the following information on Voatz functionality.

System Considerations

System Infrastructure

Consideration	Voatz Implementation
How will the voting infrastructure be hosted (i.e., on servers at your facility, in the cloud, etc.)?	Voatz infrastructure is hosted at qualified, professional cloud services providers Microsoft and Amazon.
If you use the cloud, do you have awareness of where will the data be hosted (i.e. outside your jurisdiction, state, or the United States)?	All Voatz critical infrastructure is hosted within the United States at Microsoft Azure™ and Amazon Web Services™ data centers.
Does the system have the capacity to handle the increased load?	Cloud services enable spinning up additional servers on demand. Voatz runs monitored automated load tests daily to assess performance of the server(s) so that additional servers can be commissioned during heaviest load if needed.
What redundancies should be built into the system (i.e., backups, failover system, etc.)?	All Voatz cloud servers have hot standby replacements and are backed up daily.
Who will administer system configuration (i.e., security, load balancing, updates, patches, etc.)?	Voatz IT operations team, with guidance from the cloud providers, handles configuration of load balancing, security patches, etc.

* See: *Electronic Ballot Delivery and Marking Considerations for Election Officials* (as posed by CISA)
https://www.eac.gov/sites/default/files/electionofficials/vbm/eBallot_Delivery.pdf

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-05-26

Electronic Interface / Usability & Accessibility

Consideration	Voatz Implementation
Is the system accessible to voters with specific needs (i.e., visual impairments, disabilities, language, etc.)?	Yes. Voatz apps operate on iOS or Android smartphones and incorporate Apple's and Google's native accessibility features including VoiceOver™, TalkBack™, etc. The Voatz interface and onscreen help are available in English and Spanish. Ballots can be translated into additional languages.
Is the system compatible with mobile devices?	Yes. Voatz apps are designed specifically to operate on Apple iOS v12.4 or higher or Android v8 or higher mobile phones (not other devices).
Is the system compatible with readily available screen readers?	Yes. Voatz runs as native iOS or Android smartphone apps which incorporate Apple's and Google's VoiceOver, TalkBack, as well as other accessibility features.
Is the system accessible with binary personal assistive technologies (i.e., jelly switches, sip-n-puff, etc.)?	Voatz for iOS supports Voice Control hands-free operation. Binary assistive technologies have not been tested but may be adaptable with Bluetooth™.
Do you provide help to voters directly through the electronic ballot delivery system?	Yes. Context dependent, onscreen Help is available in English and Spanish. In addition, Voatz detects if a screen reader is enabled, and provides modified help when necessary.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-05-26

Election Definition Files

Consideration	Voatz Implementation
What file format does your system accept (i.e., HTML, PDF, CSV, etc.)?	Voatz interprets native Electionware™ and ClearVote™ election definition files to transform them into remote accessible ballots. For other vendors, specific scripting routines are used to transform PDF designs into remote accessible ballot formats.
Does your voting system produce ballots in the accepted file types, or do you need software to convert them?	Yes, for supported vendors, fully marked and scannable ballots are available for printing and tabulation by the primary voting system.
What type(s) of audio files does your system use?	Audio files are not required as Apple iOS and Android provide speech to text.
What languages do the ballots need to be presented in?	Determined by jurisdiction. Voatz currently supports English/Spanish EBM interface.

Additional Supplies

Consideration	Voatz Implementation
Do you need to supply additional affidavits and instructions to the voter who votes electronically?	Voatz offers an electronic affidavit with signature or checkbox if required by the jurisdiction- typically for UOCAVA voters.
Will your materials contain labels and self-folding envelopes to mail the ballots back?	No. Ballot return is electronic over secure network and auditable.
Will you provide printable privacy sleeves for the voter to protect the ballot?	Not applicable. Electronic affidavits are stored separately from the returned ballot for privacy and ballots are identified in an anonymized manner.
What auxiliary technologies are required for the voter to complete his or her ballot (i.e., Internet service, email, printer, fax service, specific software, etc.)?	Voatz requires a supported Apple or Android smartphone, an email account, and cellular or Wi-Fi connectivity. No paper, printer or postal service is involved. Auxiliary voting channels should be available for other voters.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-05-26

Ballot Duplication

Consideration	Voatz Implementation
Many ballots generated by an electronic ballot delivery system cannot be directly scanned and tabulated into your voting system. To tabulate ballots using the voting system, the ballots must be printed on paper stock meeting certain specifications. For those ballots, enough blank paper stock will need to be purchased in advance. Jurisdictions may need additional technology (i.e., ballot duplication system, ballot on demand system, etc.) or staff to duplicate electronically generated ballots onto a ballot that can be scanned and duplicated. Depending on the volume of ballots that require duplication, additional staff needs could be significant.	Voatz is rare in its ability to return the ballots electronically to the jurisdiction. After they confirm the voter's affidavit, election officials print marked, scannable ballots directly on ballot stock for tabulation. Election officials do not need to open paper mail. Nor is faxing or hand transcribing required. Voatz supports jurisdiction and/or public post-election auditing of ballots.

Security Recommendations

Vulnerability Scan and Remote Penetration Testing

Recommendation	Voatz Implementation
Because these systems are publicly facing, jurisdictions using an electronic ballot delivery system should request a vulnerability scan and remote penetration test be conducted on the system. Also, for vendor-provided systems, election officials should suggest that their vendor subject the system to a critical product evaluation. These services provide the situational awareness needed to make informed decisions to manage the risks associated with the system and are provided at no cost to election jurisdictions and their private sector partners.	In September 2019, the CISA Hunt and Incident Response Team (HIRT) conducted a proactive hunt operation that included the Voatz internal corporate network, as well as Amazon Web Services (AWS) and Microsoft Azure cloud networks that support the mobile-based election infrastructure. HIRT analysts did not detect threat actor behaviors or artifacts of past activities on the in-scope portions of the Voatz networks. HIRT commended Voatz for their proactive measures in the use of canaries, bug bounties, Shodan alerts, and active internal scanning and red teaming. For more, see: https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-05-26

Web-Based Portals and File Servers

Recommendation	Voatz Implementation
Use security best practices for web and network connected election systems, including two-factor authentication (2FA) for employees and voters.	Yes, Voatz Admin portal uses 2FA for election officials. Voters use Voatz app on smartphones with integrated security features.
Encrypt traffic using secure hypertext transfer protocol (HTTPS) or, if you use a file server, ensure it uses a secure file transfer protocol (SFTP) by supporting transport layer security (TLS) version 1.2.	Yes.
Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.	Yes.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-05-26

6705 Odyssey Drive
Suite C
Huntsville, AL 35806
Phone (256)713-1111
Fax (256)713-1112

Test Report for Test and Evaluation of the Voatz™ Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System

Final
Version: 02

Date: 07/17/2020

SIGNATURES

Approved by: Michael L. Walker
Michael Walker, VSTL Project Manager

07/17/2020
Date

Approved by: Wendy Owens
Wendy Owens, VSTL Program Manager

07/17/2020
Date

REVISIONS

Version	Description	Date
00	Initial Release	07/14/2020
01	Updates per manufacturer comments	07/15/2020
02	Updates per manufacturer comments	07/17/2020

Table of Contents

1.0 INTRODUCTION 1

1.1 SCOPE 1
1.2 REFERENCES 2
1.3 TERMS AND ABBREVIATIONS 3

2.0 TESTING OVERVIEW 3

2.1 SYSTEM OVERVIEW 5
2.2 BLOCK DIAGRAMS 6
2.3 TEST CONFIGURATION 6

3.0 MATERIALS REQUIRED FOR TESTING 7

3.1 SOFTWARE 7
3.2 EQUIPMENT 7
3.3 TECHNICAL DATA PACKAGE 8
3.4 TEST SUPPORT MATERIALS 9

4.0 TEST PROCESS AND RESULTS 9

4.1 USABILITY AND ACCESSIBILITY TESTING 9
4.2 FUNCTIONAL CONFIGURATION AUDIT (FCA) 11
4.3 SYSTEM INTREGRATION 12
4.4 PHYSICAL CONFIGURATION AUDIT (PCA) 12
4.5 SOURCE CODE REVIEW 13
4.6 SECURITY TESTING 13
4.7 TELECOMMUNICATIONS TESTING 13

5.0 CONCLUSION 14

ATTACHMENT A – REQUIREMENTS MATRIX A-1

ATTACHMENT B – VOATZ EBDM RESPONSES B-1

1.0 INTRODUCTION

The purpose of this Test Report is to document the procedures that Pro V&V, Inc. followed to perform the evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System to the applicable requirements in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 and the manufacturer-stated requirements set forth in the system documentation.

The objectives of the evaluation of the Voatz RABDMR were to assess the ability of the system to perform the following tasks:

- Installing, registering, and delivering a ballot to voters using the Voatz Mobile App.
- Voting using the Voatz Mobile App.
- Enforcement of voting checks and ballot validation.
- Accessibility and language support for voters using the Mobile App.
- Compliance with security and privacy requirements when voting using the Mobile App.
- Ability for voters to successfully return their completed ballot.
- Ability of election officials to perform the following actions in the Voatz Admin Portal:
    - Login using 2-factor authentication
    - View election information, including ballots
    - View eligible and signed-up voters
    - View and approve voter-submitted affidavits
    - Download and view anonymized voter-submitted ballots
- Print voter ballots.
- Optionally receive voter ballot receipts and affidavits to a fax machine.

Pro V&V Test Plan TP v. 01-02-VTZ-001-01.01 was utilized as the guiding document during test performance. During testing, minor system modifications, such as revised system documentation or software versions, may have been incorporated. This test report encompasses all aspects of testing (Phase 1 and Phase 2) and details the final versions of all technical documentation and system components and supersedes the approved test plan.

Unless otherwise annotated, all testing was conducted at the Pro V&V test facility located in Huntsville, AL, by personnel verified by Pro V&V to be qualified to perform the test

1.1 Scope

The scope of the testing event incorporated a sufficient spectrum of functional tests to verify that the RABDMR features and applications conform to the applicable requirements.

The test campaign was conducted in two phases:

Phase 1

This portion of testing assessed the RABDMR's Usability & Accessibility compliance *(Reference Pro V&V Test Report TR v. 01-02-VTZ-001-01.02)*.

Phase 2

Phase 2 included all elements of the approved Test Plan inclusive of Phase 1. Specifically, this portion of testing included the following test goals:

- Verify that the RABDMR performs as documented in the provided system technical documentation
- Evaluate the RABDMR System as it relates to voter experience and transmission of the voter's selection to the jurisdiction
- Execute system use cases to evaluate system functionality
- Source Code Review
- Physical Configuration Audit (PCA)
- Functional Configuration Audit (FCA)
- System Integration Testing, including Accuracy Testing and Regression Testing
- Security Testing
- Telecommunications Testing

1.2 References

- Voatz Mobile Elections Platform Proposed Test Plan
- Implementation Statement
- Election Assistance Commission 2015 Voluntary Voting System Guidelines (VVSG) Version 1.1, Volume I, "Voting System Performance Guidelines", and Volume II, "National Certification Testing Guidelines"
- Election Assistance Commission Testing and Certification Program Manual, Version 2.0
- Election Assistance Commission Voting System Test Laboratory Program Manual, Version 2.0
- National Voluntary Laboratory Accreditation Program NIST Handbook 150, 2016 Edition, "NVLAP Procedures and General Requirements (NIST Handbook 150)", dated July 2016
- National Voluntary Laboratory Accreditation Program NIST Handbook 150-22, 2008 Edition, "Voting System Testing (NIST Handbook 150-22)", dated May 2008
- United States 107th Congress Help America Vote Act (HAVA) of 2002 (Public Law 107-252), dated October 2002
- Pro V&V, Inc. Quality Assurance Manual, Revision 7.0

- System Technical Data Package *(A listing of the documents submitted for this test campaign is listed in Section 3.3 of this Test Report)*

1.3 Terms and Abbreviations

This subsection lists terms and abbreviations relevant to the hardware, the software, or this Test Plan.

"COTS" – Commercial Off-The-Shelf

"EAC" – United States Election Assistance Commission

"EBDMR" -- Electronically-assisted Ballot Delivery, Marking and Return

"FCA" – Functional Configuration Audit

"HAVA" – Help America Vote Act

"ISO" – International Organization for Standardization

"PCA" – Physical Configuration Audit

"QA" – Quality Assurance

"TDP" – Technical Data Package

"VSTL" – Voting System Test Laboratory

"VVSG" – Voluntary Voting System Guidelines

2.0 TESTING OVERVIEW

The scope of this testing event incorporated a sufficient spectrum of tests to verify that the RABDMR features and applications conform to the defined requirements. The evaluation of the RABDMR System addressed each of the test goals in the following manner:

Table 2-1: Testing Overview

Test Goal	Testing Response
Perform a Usability and Accessibility Review	This review focused on the usability and accessibility of the system as evaluated against the requirements matrix in Appendix A.
Verify that the RABDMR performs as documented in the provided system technical documentation	This was evaluated during performance of the Functional Configuration Audit. Additionally, a TDP Review was performed
Evaluate the RABDMR System as it relates to voter experience and transmission of the voter's selection to the jurisdiction	This was evaluated during performance of the Functional Configuration Audit.

Table 2-1: Testing Overview *(continued)*

Test Goal	Testing Response
Execute system use cases to evaluate system functionality	This was evaluated during performance of the System Integration Testing.
Source Code Review	The source code submitted by Voatz was reviewed for adherence to applicable requirements and standards.
Physical Configuration Audit (PCA)	A PCA was performed to compare the voting system components and materials submitted for testing against the manufacturer's technical documentation to ensure everything was in agreement and correct.
Functional Configuration Audit (FCA)	A FCA was performed as an exhaustive verification of every system function and combination of functions cited in the manufacturer's documentation.
System Integration Testing, including Accuracy Testing and Regression Testing	The RABDMR was tested to address the integration of the hardware and software. This testing focused on the compatibility of the system software components and subsystems to interface with one another and with other voting system components. Abbreviated Accuracy Testing was performed to verify the system accurately stored election data.
Security Testing	The RABDMR was set up as described in the technical documentation and subjected to security testing. During the execution of this test case, the system was inspected for various controls and measure that were in place to meet the objectives of the security standards.
Telecommunications Testing	The telecommunications testing was performed to determine the capability of the system to transmit and receive data electronically using hardware and software over distances external to a polling place.

2.1 System Overview

The following sections contain a product description and an overview of the design methodology of the RABDMR System, as taken from the system technical documentation.

The Voatz Mobile Elections Platform is a configurable, cloud-based Remote Accessible Ballot Delivery, Marking and Return (RABDMR) system that:

- Delivers blank ballots to eligible voters
- Allows voters to mark their selections accessibly and verify their selections
- Returns the marked ballots to the jurisdiction according to the statutory provisions of the voter's state.

Jurisdictions can specify the method of returning voted ballots based on their state's statutory requirements and include any state-specific legal documents (such as signed affidavits or checkbox waivers.)

To determine eligibility to vote, voter registration records are incorporated into the Voatz Platform by importing the data. Typically, an indicator in the voter file designates which subset of all voters are eligible to vote remotely. While the Voatz system can remotely confirm the validity of a voter's credentials (e.g. driver's license) and verify the person presenting their credentials is the same person on the credential, it does not by itself determine whether individual voters are authorized to vote in the current election. This determination must be made by the jurisdiction and indicated in the voter records. Voatz then limits voting to those individuals so designated.

The Voatz RABDMR system uses commercial off-the-shelf (COTS) hardware; no proprietary hardware is required. Ballots are marked securely and anonymously via a mobile app on the voter's smartphone—the Voatz Mobile App (VMA).

Marked ballots are returned electronically to the jurisdiction, along with any other required documents. The jurisdiction then prints the returned marked ballots as optical scannable ballots on official ballot stock for tabulation by the primary voting system. Voters receive a password protected ballot receipt that lists their selections and contains an anonymous ID; the jurisdiction receives an identical anonymized copy. Only the voter knows the anonymous ID that is linked to them.

Voatz has provided responses to a recently issued guidance to election officials regarding electronic ballot delivery and marking circulated by the EAC. The information on the RABDMR system functionality as provided by Voatz is presented in Attachment B.

2.2 Block Diagram

The process flow of the system is depicted in Figure 1-1.

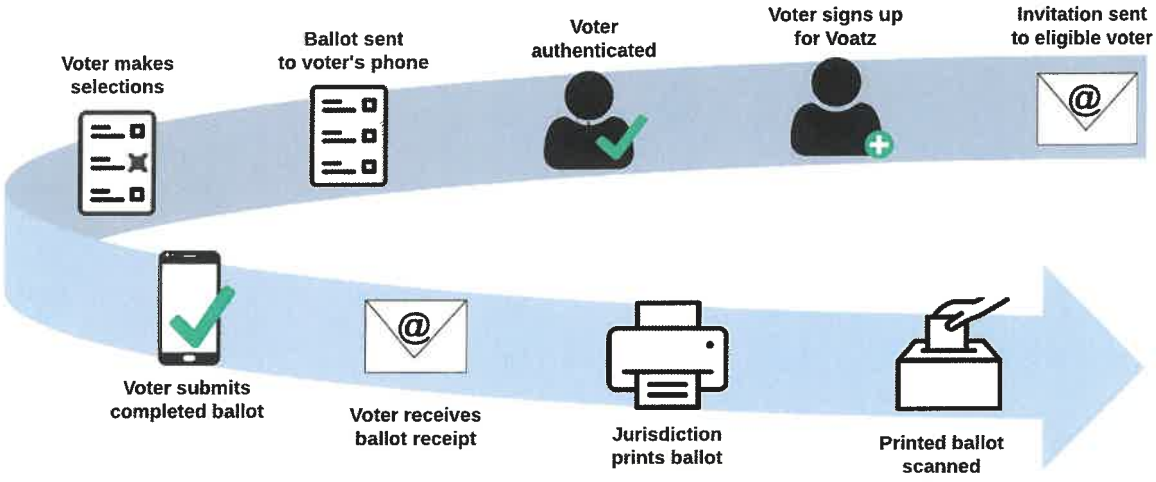
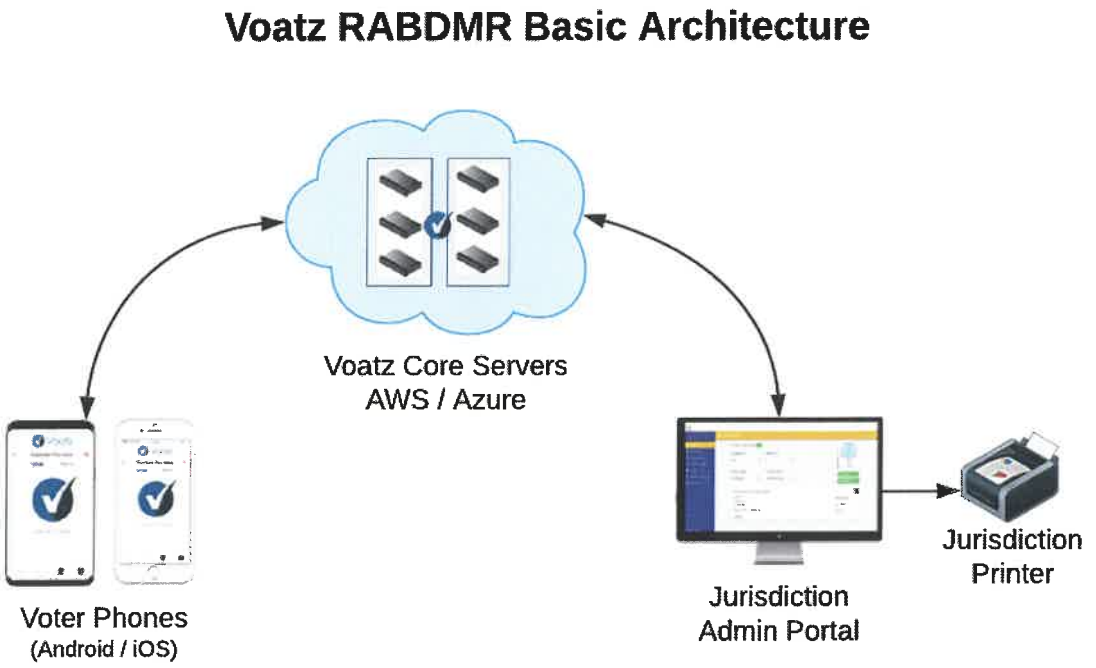


Figure 1-1. RABDMR Process Flow

2.3 Test Configuration



The testing campaign utilized various models of cell phones, with the Voatz Mobile App (VMA) installed. To access the back-end environment, one Pro V&V laptop was utilized. Ballots generated during testing were printed as optical scannable ballots using an OKI printer. An alternate test configuration returned ballots both electronically and via fax.

3.0 MATERIALS REQUIRED FOR TESTING

The following sections list all materials required during the test engagement.

The materials required for testing of the RABDMR System included all materials to enable the test campaign to occur. This included the applicable hardware and software as well as the TDP, test support materials, and deliverable materials, as described in the following subsections.

3.1 Software

This subsection lists the proprietary and COTS software provided by the manufacturer as part of the test campaign.

Table 3-1. RABDMR System Software

Firmware/Software	Version
Voatz Mobile App (VMA) for iOS	1.032 (190)
Voatz Mobile App (VMA) for Android	1.1.124 (159)
Voatz Admin Portal	1.0.48

3.2 Equipment

This subsection lists the COTS equipment provided by the manufacturer as part of the test campaign.

For COTS equipment, every effort was made to verify that the COTS equipment has not been modified for use. This was accomplished by performing research using the COTS equipment manufacturer's websites based on the serial numbers for each piece of equipment. Assigned test personnel evaluated COTS hardware, system software and communications components for proven performance in commercial applications other than voting.

For smartphones, the device information was compared to the supported configurations in the campaign. Physical external and internal examination was also performed when easily accessible without the possibility of equipment damage. Solid State drives, RAM memory, and other components were examined to verify that the components match the information found on the COTS equipment manufacturer's websites. A factory reset was performed on smartphones prior to testing.

Table 3-2. RABDMR System Equipment

Component	Model	Serial Number	OS
iPhone 6s	MKRX2LL/A	C6KRL9HVGRY8	iOS 13.3.1
iPhone 6	MG4Q2LL/A	FFMP901MG5MF	iOS 12.4.5
LG Phoenix 4	LM-X210APM	912VTSM766174	Android 8.1.0
Moto e6	XT2005-1PP	352176100933789	Android 9.0
Okidata Printer	432dn-B	AK88034459C0	N/A
Brother IntelliFAX	FAX2840	U63274C0J773853	N/A

3.3 Technical Data Package

A listing of all documents contained in the system TDP relevant to this report is provided in Table 3-3.

Table 3-3. TDP Documents

Document	Version	Description
Product Summary	---	Statement of the system capability and role in the election eco-system.
Use Procedures	*1.06*	Provides a comprehensive description of the Voatz system for jurisdiction officials. It includes pre-election, election window and post-election procedures, architecture, capabilities, functionality, workflows, logic & accuracy testing, and system security.
Product Datasheet	*1.04*	Supported functionality, system limitations, and other performance characteristics.
Hardware and Software Specification	*1.04*	System hardware and software requirements.
System Test Verification and Specification	*1.03*	Describes the manufacturer's test processes, environment, data, and artifacts.
Configuration for Testing	*1.03*	Describes the configuration actions and resources required to stage a conforming test environment for the system.

Additional ancillary documents, not part of the TDP, were also submitted for review and comment. These documents include:

- Vendor Proposed Test Plan
- Open-SCAP Evaluation Report
- OWASP Security Checklist
- Jmeter 500 User Load Test Summary Report
- Voatz Test Execution Reports (iOS and Android)
- Voatz Admin Portal 1.0.48 Test Execution Report
- Hunt Engagement Summary

3.4 Test Support Materials

This subsection lists the test materials required to execute the required tests throughout the test campaign.

The following materials were supplied by Voatz to facilitate testing:

- Ballot Paper
- Printer Ink
- Other materials and equipment as required

4.0 TEST PROCESS AND RESULTS

Testing of the RABDMR System submitted for evaluation was performed to verify that the System conforms to the applicable requirements in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1 and the manufacturer-stated requirements set forth in the system documentation. The VVSG 1.1 Requirements Matrix generated for this test campaign was used as a guide to determine the specific tests to be performed. Pro V&V developed test procedures designed to evaluate the system being tested against the stated requirements. The test cases were performed using three types of elections: Primary, General, and Ranked Choice voting. The test procedures were executed independently.

The evaluation areas for this test engagement are summarized in the subsections below.

4.1 Usability and Accessibility Testing

The usability testing focuses on the usability of the system being tested. Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary user is the voter, the product is the RABDMR, and the task is the correct recording of the voter ballot selections. Additional requirements for task performance are independence and privacy: the voter should normally be able to complete the voting task without assistance from others, and the voter selections should be private. Accessibility evaluates the requirements for accessibility. These requirements are intended to address HAVA 301 (a) (3) (B).

Usability and Accessibility Testing included system use cases for the following areas:

- Usability Support
- Cognitive Disabilities
- Perceptual Disabilities
- Interaction Disabilities
- System and Voter Wait Times
- Language Support
- General Accessibility Assistance
- Limited Vision Assistance
- Blind Voter Assistance
- Motor Control Difficulty Assistance
- Limited Hearing Assistance
- English Illiteracy Assistance
- Limited Speech Assistance

Summary Findings

The RABDMR System was evaluated against the VVSG 1.1 Requirements Matrix generated for this test campaign. Based on the results obtained, the RABDMR was determined to meet the applicable Usability and Accessibility requirements. The following observations/exceptions were noted during the review:

Table 4-1 Summary Findings

Requirement	Notes
Usability Review	
Volume I, Section 3.2.3.1 *Privacy at the polls*	
3.2.3.1.a, 3.2.3.1.b, 3.2.3.1.c, 3.2.3.1.d, 3.2.3.1.e	These requirements are not applicable due to there being no polling place.
Volume I, Section 3.2.6.1 *Timing*	
3.2.6.1.a, 3.2.6.1.b, 3.2.6.1.c	Note: Timing was tested concurrent with a simulated load of 500 other users voting.
3.2.6.1.f	The timing of the alert and expiration of session pass. However, there is no poll worker, thus there is no poll worker intervention. The user is required to login again.
Volume I, Section 3.2.7a *Alternative Languages*	
3.2.7a.i.v	Any external reports to be reviewed pending final TDP.

Table 4-1 Summary Findings (continued)

Requirement	Notes
Accessibility Review	
Volume I, Section 3.3.2 *Enhanced visual interfaces*	
3.3.2.c.i, 3.3.2.c.ii	Phone contains capability.
Volume I, Section 3.3.3 *Audio-tactile interfaces*	
3.3.3.a & 3.3.3.a.i	Any external test reports to be reviewed pending final TDP.
3.3.3.b, 3.3.3.b.i, 3.3.3.b.ii, 3.3.3.b.iii, 3.3.3.b.iv. 3.3.3.b.v, 3.3.3.c.i, 3.3.3.c.ii, 3.3.3.3.iii	The system does not contain an ATI; therefore these requirements are not applicable.
3.3.3.c.iv, 3.3.3.c.v, 3.3.3.c.vi	These requirements relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized.
3.3.3.f, 3.3.3.g	These requirements relate to accessible voting stations and are not applicable.
Volume I, Section 3.3.4 *Enhanced input and control characteristics*	
3.3.4.a, 3.3.4.d	These requirements relate to accessible voting stations and are not applicable.
3.3.4.b	Partial Pass - Only on iPhone 6s & higher and iOS 13 & higher support hands-free operation using Voice Control. Android devices do not have this capability yet. However, both devices support limited dexterity with VoiceOver or TalkBack navigation (audio can be turned off.)
Volume I, Section 3.3.5 *Design for mobility aids*	
3.3.5	These requirements relate to accessible voting stations and are not applicable.
Volume I, Section 3.3.6 *Enhanced auditory interfaces*	
3.3.6.c	These requirements relate to volume control and audio presentation and were not tested, as they are dependent upon the device being utilized.
Volume I Section 3.3.10 *Summative Usability Report*	
3.3.10.c.i, 3.3.10.a, 3.3.10.b, 3.3.10.c	Any external test reports to be reviewed pending final TDP.

The results of the evaluation are presented in Attachment A.

Note: Each item listed in the table above is marked with an asterisk in Attachment A.

4.2 Functional Configuration Audit (FCA)

The FCA is an exhaustive verification of every system function and combination of functions cited in the manufacturer's documentation. The FCA verifies the accuracy and completeness of the system Technical Data Package (TDP).

Standardized FCA test cases were utilized during testing as well as test cases that focused on the following specific areas:

- Limits Testing (per manufacturer documentation)

- Voting Variations (per manufacturer documentation)
    - General Election
    - Primary Election
        - Open
        - Closed
        - Presidential Primary
    - Ranked Choice Election

Summary Findings

During this area of testing, an evaluation was performed on the RABDMR System as it relates to voter experience and transmission of the voter's selection to the jurisdiction. Additionally, it was verified that the RABDMR performs as documented in the provided system technical documentation.

4.3 System Integration

The system level certification tests addressed the integration of the hardware and software. This testing focused on the compatibility of the voting system software components and subsystems with one another and with other components of the voting system. System Integration testing included the Accuracy Test, which ensures that the voter's encrypted, emailed ballot receipt and jurisdiction's printed ballot match the voter's choices. The Accuracy Test was designed to test the ability of the system to "capture, record, store, consolidate, and report" specific voter selections and absences of a selection.

During test performance, the system was configured as would be for normal field use. Admin portal access was tested in two types of users, "Org Admin" and "Org User."

Summary Findings:

The RABDMR successfully completed the System Integration Test. System use cases were executed to evaluate system functionality. During execution of the test procedure, it was verified that the RABDMR successfully completed the system level integration tests with all actual results obtained during test execution matching the expected results.

The Accuracy Test for this area of testing was conducted on an abbreviated scale. Admin portal access was only tested with the "Org Admin" level control during Accuracy Testing.

4.4 Physical Configuration Audit (PCA)

The Physical Configuration Audit (PCA) compared the voting system components submitted for certification testing to the manufacturer's technical documentation. The purpose of the PCA was to verify that the submitted components matched the manufacturer's technical documentation.

Summary Findings

During execution of the test procedure, the components of the RABDMR were documented by component name, model, serial number, major component, and any other relevant information needed to identify the component. For COTS equipment, every effort was made to verify that the COTS equipment had not been modified for use. Additionally, each technical document submitted in the TDP was recorded by document name, description, document number, revision number, and date of release.

At the conclusion of the test campaign, test personnel verified that any changes made to the software, hardware, or documentation during the test process were fully and properly documented.

4.5 Source Code Review

Pro V&V reviewed the submitted source code to the EAC 2015 VVSG and the manufacturer-submitted coding standards. Prior to initiating the software review, Pro V&V verified that the submitted documentation was sufficient to enable: (1) a review of the source code and (2) Pro V&V to design and conduct tests at every level of the software structure to verify that design specifications and performance guidelines are met.

Summary Findings:

Pro V&V conducted both a manual and automatic source code review for Android and iOS applications. Pro V&V used Android Studio version 4.0.1 for the Android application and Xcode 11.5 for the iOS application. The Android application uses the Kotlin coding standard and the iOS application uses the Swift coding standard. Pro V&V found both code bases to be compliant to their respective standard.

4.6 Security Testing

During the execution of this test case, Pro V&V verified various controls and measures to meet the required security standards including: protection of the critical elements of the voting system; establishing and maintaining controls to minimize errors; protection from intentional manipulation, fraud and malicious mischief; identifying fraudulent or erroneous changes to the voting system; and protecting the secrecy in the voting process.

Summary Findings:

Pro V&V and Voatz decided upon using the OWASP Mobile Application Security Checklist (MASVS Version 1.1.4, MSTG Version 1.1.3) for baseline security testing. Voatz provided the checklist with their findings. Pro V&V used a sample of the test cases to verify the results. Voatz also provided output from the automated Open-SCAP Evaluation Report for Red Hat Enterprise Linux 7 Voatz servers. No security issues were found from the sample test cases.

During the security evaluation, Pro V&V was able to verify that the Voatz RABDMR utilized a Blockchain from the server throughout the remainder of the process.

4.7 Telecommunication Testing

The telecommunications testing determined the capability of the system to transmit and receive data electronically using hardware and software over distances external to a polling place. During testing, both cellular and Wi-Fi transmission were used. The testing ensured that all data transmitted during pre-voting, voting or post-voting activities was transmitted with no alteration or unauthorized disclosure during transmission.

Summary Findings:

During execution of the test procedures, it was verified that the RABDMR successfully completed the applicable telecommunications tests. The system successfully transmitted and received all data with no alteration during pre-voting, voting and post-voting activities.

5.0 CONCLUSION

Based on the results obtained during the test campaign, Pro V&V determined the Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System, as presented for evaluation, meets the applicable requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1, with the clarifications or exceptions noted in Section 4.0.

ATTACHMENT A - REQUIREMENTS MATRIX

Table A-1 Usability Review Matrix Requirements

Requirement	Description	Result
	Usability	
3	Usability Requirements	
3.1.1	Purpose	
3.1.1.a	All eligible voters shall have access to the voting process without discrimination.	Pass
3.1.1.a.i	The voting process shall be accessible to individuals with disabilities. The voting process includes access to the polling place, instructions on how to vote, initiating the voting session, making ballot selections, review of the ballot, final submission of the ballot, and getting help when needed.	Pass
3.1.1.b	Each cast ballot shall accurately capture the selections made by the voter.	Pass
3.1.1.b.i	The ballot shall be presented to the voter in a manner that is clear and usable. Voters should encounter no difficulty or confusion regarding the process for recording their selections.	Pass
3.1.1.c	The voting process shall preserve the secrecy of the ballot.	Pass
3.1.1.c.i	The voting process shall preclude anyone else from determining the content of a voter's ballot without the voter's cooperation. If such a determination is made against the wishes of the voter, then his or her privacy has been violated.	Pass
3.2	General usability requirements	
3.2.a and 3.2.b	The voting process shall provide a high level of usability for voters. Accordingly, voters shall be able to negotiate the process effectively, efficiently, and comfortably. The mandatory voting system standards mandated in HAVA Section 301 relate to the interaction between the voter and the voting system:	
3.2.a.1.A	Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall --	
3.2.a.1.A.i	Permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted.	Pass
3.2.a.1.A.ii	Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).	Pass
3.2.a.1.A.iii	If the voter selects votes for more than one candidate in a single office:	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.a.1.A.iii.I	Notify the voter that the voter has selected more than one candidate for a single office on the ballot.	Pass
3.2.a.1.A.iii.II	Notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office.	Pass
3.2.a.1.A.iii.III	Provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.	Pass
3.2.a.1.B	A state or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count voting system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A) (iii) by:	
3.2.a.1.B.i	Establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office.	Pass
3.2.a.1.B.ii	Providing the voter with instructions on how to correct the ballot before it is cast and counted (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).	Pass
3.2.a.1.C	The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.	Pass
3.2.1	General usability	
3.2.1.a	The voting system shall support voters in the task of effectively completing their ballots.	Pass
3.2.1.b	The features of the voting system shall not contribute to the commission of voter error within the voting session.	Pass
3.2.2	Functional Capabilities	
	The usability of the voting process is enhanced by the presence of certain functional capabilities. These capabilities differ somewhat depending on whether or not the system presents an editable interface within which voters can easily change their votes (typically an electronic screen) or an interface in which voters must obtain a new ballot to make changes (typically a manually-marked paper ballot).	
3.2.2.a	If the voter selects more than the allowable number of choices within a contest, the voting system shall notify the voter of the effect of this action before the ballot is cast and counted.	Pass
3.2.2.c	The voting system shall provide the voter the opportunity to correct the ballot for either an undervote or overvote before the ballot is cast and counted.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.2.b	The voting system shall allow the voter, at the voter's choice, to submit an undervoted ballot without correction.	Pass
3.2.2.d	If and only if the voter successfully casts or prints the ballot, then the electronic ballot interface or PCOS system shall so notify the voter.	Pass
3.2.2.1	Editable electronic ballot interfaces	
	Voting systems such as DREs and EBMs present voters with an editable interface, allowing them to easily change their votes prior to final casting of the ballot.	
3.2.2.1.a	The electronic ballot interface shall prevent voters from selecting more than the allowable number of choices for each contest.	Pass
3.2.2.1.b	The electronic ballot interface shall provide feedback to the voter, before final casting or printing of the ballot, that identifies specific contests for which the voter has selected fewer than the allowable number of choices (i.e., undervotes).	Pass
3.2.2.1.c	The electronic ballot interface shall provide the voter the opportunity to correct the ballot before it is cast or printed. The electronic ballot interface shall allow the voter to make these corrections without assistance. The corrections to be supported include modifying an undervote and changing a vote from one candidate to another.	Pass
3.2.2.1.d	The electronic ballot interface shall allow the voter to change a vote within a contest before advancing to the next contest.	Pass
3.2.2.1.e	The electronic ballot interface shall provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing a vote on the contest(s) currently being presented (whether visually or aurally).	Pass
3.2.2.1.f	If the voter takes the appropriate action to cast a ballot, but the DRE does not accept and record it successfully, including failure to store the ballot image, then the DRE shall so notify the voter and provide clear instruction as to the steps the voter should take to cast the ballot.	Pass
3.2.2.1.g	If the electronic ballot interface generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system shall allow the voter to verify that record using the same access features used by the voter to vote the ballot.	Pass
3.2.2.2	Non-Editable ballot interfaces	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	Non-Editable interfaces, such as manually-marked paper ballots, do not have the same flexibility as do editable interfaces. Nonetheless, certain features are required, especially in the case of precinct-based optical scanners.	
3.2.2.2.a	The PCOS system shall be capable of providing feedback to the voter that identifies specific contests for which the voter has made more than the allowable number of votes (i.e., overvotes).	*Not Applicable*
3.2.2.2.b	The PCOS system shall be capable of providing feedback to the voter that identifies specific contests for which the voter has made fewer than the allowable number of votes (i.e., undervotes). The system shall provide a means for an authorized election official to deactivate this capability entirely and by contest. However, if a ballot is submitted with all the contests on one side left blank, notification to the voter is performed as described in requirement 3.2.2.2 c	*Not Applicable*
3.2.2.2.c	The PCOS system shall be capable of notifying the voter that he or she has submitted a paper ballot that is blank on one or both sides. The system shall provide a means for an authorized election official to deactivate this capability.	*Not Applicable*
3.2.2.2.d	If the PCOS system has notified the voter that a potential error condition (such as an overvote, undervote, or blank ballot) exists, the system shall then allow the voter to correct the ballot or to submit it as is.	*Not Applicable*
3.2.2.2.e	Paper-based precinct tabulators shall be able to identify a ballot containing marginal marks. When such a ballot is detected, the tabulator shall:	*Not Applicable*
3.2.2.2.e.i	Return the ballot to the voter;	*Not Applicable*
3.2.2.2.e.ii	Provide feedback to the voter that identifies the specific contests for which a marginal mark was detected; and	*Not Applicable*
3.2.2.2.e.iii	Allow the voter either to correct the ballot or to submit the ballot "as is" without correction, at the voter's choice.	*Not Applicable*
3.2.2.2.f	Software used to format optical scan ballots shall constrain the size and contrast of all target areas to conform to the following requirements:	*Not Applicable*
3.2.2.2.f.i	The target shall be no less than 3 mm across in any direction	*Not Applicable*
3.2.2.2.f.ii	The contrast ratio between the target area boundaries and the surrounding space shall be no less than 10:1.	*Not Applicable*

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.2.2.g	If the voter takes the appropriate action to cast a ballot, but the PCOS system does not accept and record it successfully, including failure to read the ballot or to transport it into the ballot box, the PCOS shall so notify the voter.	*Not Applicable*
3.2.3	Privacy	
3.2.3	The voting process shall preclude anyone else from determining the content of a voter's ballot, without the voter's cooperation.	
3.2.3.1	Privacy at the polls	
3.2.3.1.a	The voting system shall prevent others from determining the contents of a ballot.	*Not Applicable**
3.2.3.1.b	The voting system shall support ballot privacy during the voting session and ballot submission.	*Not Applicable**
3.2.3.1.c	During the voting session, the audio interface of the voting system shall be audible only to the voter.	*Not Applicable**
3.2.3.1.d	The voting system shall issue all warnings in a way that preserves the privacy of the voter and the confidentiality of the ballot.	*Not Applicable**
3.2.3.1.e	The voting system shall not issue a receipt to the voter that would provide proof to another of how the voter voted.	*Not Applicable**
3.2.3.2	No recording of alternative format usage	
	When voters use non-typical ballot interfaces, such as large print or alternative languages, their anonymity may be vulnerable. To the extent possible, only the logical contents of their ballots should be recorded, not the special formats in which they were rendered. However, in the case of paper ballots, where the interface is the record, some format information is unavoidably preserved.	
3.2.3.2.a	No information shall be kept within an electronic cast vote record that identifies any alternative language feature(s) used by a voter.	Pass
3.2.3.2.b	No information shall be kept within an electronic cast vote record that identifies any accessibility feature(s) used by a voter.	Pass
3.2.4	Voter instructions, plain language, and information presentation	
	The features specified in this section are intended to minimize cognitive difficulties for voters. Voters should always be able to operate the voting system and understand the effect of their actions. Note that the "should" requirements in this section must be adhered to unless there is strong justification provided for making an exception.	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.4.a	The voting system shall provide instructions for all its valid operations.	Pass
3.2.4.b	The voting system shall provide a means for the voter to get help directly from the system at any time during the voting session.	Pass
3.2.4.c	Instructional material for the voter shall conform to norms and best practices for plain language.	Pass
3.2.4.c.i	Warnings and alerts issued by the voting system shall be distinguishable from other information and should clearly state: The nature of the problem; Whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way; and The set of responses available to the voter.	Pass
3.2.4.c.ii	When an instruction is based on a condition, the condition should be stated first, and then the action to be performed.	Pass
3.2.4.c.iii	The voting system should use familiar, common words and avoid technical or specialized words that voters are not likely to understand.	Pass
3.2.4.c.iv	Each distinct instruction should be separated spatially from other instructions for visual or tactile interfaces, and temporally for auditory interfaces.	Pass
3.2.4.c.v	The voting system should issue instructions on the correct way to perform actions, rather than telling voters what not to do.	Pass
3.2.4.c.vi	The system's instructions should address the voter directly rather than use passive voice constructions.	Pass
3.2.4.c.vii	The voting system should avoid the use of gender-based pronouns.	Pass
3.2.4.d	Consistent with election law, the voting system shall support a process that does not introduce bias for or against any of the contest choices to be presented to the voter. In both visual and aural formats, the choices shall be presented in an equivalent manner.	Pass
3.2.4.e	The voting system shall provide the capability to design a ballot with a high level of clarity and comprehensibility.	Pass
3.2.4.e.i	The voting system should not visually present a single contest spread over two pages or two columns.	Pass
3.2.4.e.ii	The ballot shall clearly indicate the maximum number of candidates for which one can vote within a single contest.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.4.e.iii	The relationship between the name of a candidate and the mechanism used to vote for that candidate shall be consistent throughout the ballot.	Pass
3.2.4.e.iv	The voting system should present instructions near to where they are needed.	Pass
3.2.4.f	The use of color by the voting system shall agree with common conventions: (a) green, blue or white is used for general information or as a normal status indicator; (b) amber or yellow is used to indicate warnings or a marginal status; (c) red is used to indicate error conditions or a problem requiring immediate attention.	Pass
3.2.4.g	When an icon is used to convey information, indicate an action, or prompt a response, it shall be accompanied by a corresponding linguistic label.	Pass
3.2.5	Visual display characteristics	
	The requirements of this section are designed to minimize perceptual difficulties for the voter. Some of these requirements are designed to assist voters with poor reading vision. These are voters who might have some difficulty in reading normal text, but are not typically classified as having a visual disability and thus might not be inclined to use the Acc-VS.	
3.2.5.a	If the voting system uses an electronic display screen as the primary visual interface for the voter, the display shall have the following characteristics:	
3.2.5.a.i	Flicker frequency NOT between 2 Hz and 55 Hz. Does not say "flashing elements" like NIST did? If so maybe one Dell reported concern in settings.	Untested
3.2.5.a.ii	Minimum display brightness: 130 cd/m2	Untested
3.2.5.a.iii	Minimum display darkroom 7×7 checkerboard contrast: 150:1	Untested
3.2.5.a.iv	Minimum display pixel pitch: 85 pixels/inch (0.3 mm/pixel)	Untested
3.2.5.a.v	Minimum display area 700 cm2	Untested
3.2.5.a.vi	Antiglare screen surface that shows no distinct virtual image of a light source	Untested
3.2.5.a.vii	Minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1	Untested

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.5.b	Any aspect of the voting system voter interface that is adjustable by either the voter or poll worker, including font size, color, contrast, audio volume, or rate of speech, shall automatically reset to a standard default value upon completion of that voter's session. For the Acc-VS with an electronic image display, the aspects include synchronized audio/video mode and non-manual input mode.	Pass
3.2.5.c	If any aspect of a voting system is adjustable by either the voter or poll worker, there shall be a mechanism to allow the voter to reset all such aspects to their default values while preserving the current votes.	Pass
3.2.5.d	For all text intended for voters or poll workers, the voting system shall provide a font with the following characteristics	
3.2.5.d.i	Height of capital letters at least: 3.0 mm	Untested
3.2.5.d.ii	x-height of at least: 70% of cap height	Untested
3.2.5.d.iii	Stroke width at least: 0.35 mm.	Untested
3.2.5.e	A voting system that uses an electronic image display shall be capable of showing all information in at least two font sizes:	
3.2.5.e.i	3.0-4.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.35 mm;	Untested
3.2.5.e.ii	6.3-9.0 mm cap height, with a corresponding x-height at least 70% of the cap height and a minimum stroke width of 0.7 mm; under control of the voter. The system shall allow the voter to adjust font size throughout the voting session while preserving the current votes.	Untested
3.2.5.f	Text intended for the voter should be presented in a sans serif font.	Pass
3.2.5.g	Voting systems using paper ballots or paper verification records shall provide features that assist in the reading of such ballots and records by voters with poor reading vision.	
3.2.5.g.i	The voting system may achieve legibility of paper records by supporting the printing of those records in at least two font sizes, 3.0-4.0mm and 6.3-9.0mm.	Untested
3.2.5.g.ii	The system may achieve legibility of paper records by supporting magnification of those records. This magnification may be done by optical or electronic devices. The manufacturer may either: 1) provide the magnifier itself as part of the system, or 2) provide the make and model number of readily available magnifiers that are compatible with the system.	Untested

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.5.h	The colors in the default presentation shall support perception by voters and poll workers with color vision deficiencies, of all text, controls, and infographics or icons on the ballot or ballot interface.	
3.2.5.h.i	The default visual display for voters and poll workers of a voting station with an electronic display shall have a luminosity contrast ratio between the foreground text and background color of at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons. For paper ballots, the contrast ratio shall be at least 10:1 as measured based on ambient lighting of at least 300 lx.	Untested
3.2.5.h.ii	A voting station with an electronic display screen shall have a high contrast mode either as an initial setting or under the control of the voter. If the system allows the voter to adjust contrast during the voting session it shall preserve the current votes. High contrast is a luminosity contrast ratio between the foreground text and background color of at least 20:1. The high contrast mode shall use at least one of the following color combinations: o Black text on a white background o White text on a black background o Yellow text on a black background o Light cyan text on a black background	Untested
3.2.5.i	Color coding shall not be used as the sole means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	Pass
3.2.6	Voter-interface interaction	
	The requirements of this section are designed to minimize interaction difficulties for the voter.	
3.2.6.a	Voting machines with electronic image displays shall not require page scrolling by the voter. Discussion: This is not an intuitive operation for those unfamiliar with the use of computers. Even those experienced with computers often do not notice a scroll bar and miss information at the bottom of the "page." Voting systems may require voters to move to the next or previous "page."	Pass
3.2.6.b	The voting machine shall provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance.	Pass

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.6.c	d. Input mechanisms shall be designed to minimize accidental activation.	Pass
3.2.6.c.i	On touch screens, the sensitive touch areas shall have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches.	Untested
3.2.6.c.ii	No key or control on a voting machine shall have a repetitive effect as a result of being held in its active position.	Pass
3.2.6.1	Timing	
	These requirements address how long the system and voter wait for each other to interact.	
3.2.6.1.a	The initial system response time of the electronic ballot interface shall be no greater than 0.5 seconds.	Pass*
3.2.6.1.b	When the voter performs an action to record a single vote, the completed system response time of the electronic ballot interface shall be no greater than one second in the case of a visual response, and no greater than five seconds in the case of an audio response.	Pass*
3.2.6.1.c	The completed system response time during a voter interaction with the visual display of the electronic ballot interface shall be no greater than 10 seconds.	Pass*
3.2.6.1.d	If the electronic ballot interface has not completed its visual response within one second, it shall present to the voter, within 0.5 seconds of the voter's action, some indication that it is preparing its response.	Pass
3.2.6.1.e	The electronic ballot interface shall detect and warn about lengthy voter inactivity during a voting session. Each electronic ballot interface shall have a defined and documented voter inactivity time, and that time shall be between two and five minutes.	Pass
3.2.6.1.f	Upon expiration of the voter inactivity time, the electronic ballot interface shall issue an alert and provide a means by which the voter may receive additional time. The alert time shall be between 20 and 45 seconds. If the voter does not respond to the alert within the alert time, the electronic ballot interface shall go into an inactive state requiring poll worker intervention.	Partial Pass*
3.2.7	Alternative languages	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	HAVA Section 301 (a)(4) states that the voting system shall provide alternative language accessibility pursuant to the requirements of Section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a). Ideally every voter would be able to vote independently and privately, regardless of language. As a practical matter, alternative language access is mandated under the Voting Rights Act of 1975, subject to certain thresholds (e.g., if the language group exceeds 5% of the voting age population). Thus, election officials must ensure that the voting system they deploy is capable of handling the languages meeting the legal threshold within their districts.	
3.2.7.a	The voting system shall be capable of presenting the ballot, contest choices, review screens, vote verification records, and voting instructions in any language declared by the manufacturer to be supported by the system.	Pass
3.2.7.a.i	The electronic ballot interface should allow the voter to select among the available languages throughout the . voting session while preserving the current votes. When presenting a choice of languages to the voter, the electronic ballot interface shall use the native name of each language.	Pass
3.2.7.a.ii	Information presented to the voter in the typical case of English-literate voters (including instructions, warnings, messages, contest choices, and vote verification information) shall also be presented when an alternative language is being used, whether the language is written or an unwritten language presented aurally.	Pass
3.2.7.a.iii	Any records, including paper ballots and paper verification records, shall have the information required to support auditing by poll workers and others who can read only English.	Pass
3.2.7.a.iv	The manufacturer shall conduct summative usability tests for each of the voting system's supported languages, using subjects who are fluent in those languages but not fluent in English and shall report the test results, using the Common Industry Format, as part of the TDP. In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
3.2.8	Usability for poll workers	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
	Voting systems are used not only by voters to record their votes, but also by poll workers who are responsible for set-up, operation while polls are open, light maintenance, and poll closing. Because of the wide variety of implementations, it is impossible to specify detailed design requirements for these functions. The requirements below describe general capabilities that all systems must support.	Untested
3.2.8.a	Messages generated by the voting system for poll workers in support of the operation, maintenance, or safety of the system shall adhere to the requirements for clarity in Section 3.2.4 "Voter instructions, plain language and information presentation."	Untested
3.2.8.1	Operations	
	Poll workers are responsible for opening polls, keeping the polls open and running smoothly during voting hours, and closing the polls afterwards. Operations may be categorized in three phases: Setup includes all the steps necessary to take the system from its state as normally delivered to the polling place, to the state in which it is ready to record votes. It does not include ballot definition. Polling includes such functions as: • voter identification and authorization; • preparing the system for the next voter; • assistance to voters who wish to change their ballots or need other help; • system recovery in the case of voters who abandon the voting session without having cast a ballot; and routine hardware operations, such as installing a new roll of paper. Shutdown includes all the steps necessary to take the system from the state in which it is ready to record votes to its normal completed state in which it has captured all the votes cast and the voting information cannot be further altered.	
3.2.8.1.a	Voting system setup, polling, and shutdown, as documented by the manufacturer, shall be reasonably easy for the typical poll worker to learn, understand, and perform.	*Not Applicable*
3.2.8.1.b	The manufacturer shall conduct summative usability tests on the voting system using individuals who are representative of the general population and shall report the test results, using the Common Industry Format, as part of the TDP.	

Table A-1 Usability Review Requirements Matrix *(continued)*

Requirement	Description	Result
3.2.8.1.b.i	The tasks to be covered in the test shall include setup, operation, and shutdown.	*Not Applicable*
3.2.8.1.b.ii	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable*
3.2.8.1.c	The voting system shall include clear, complete, and detailed instructions and messages for setup, polling, and shutdown.	*Not Applicable*
3.2.8.1.c.i	The documentation required for normal voting system operation shall be presented at a level appropriate for poll workers who are not experts in voting system and computer technology.	*Not Applicable*
3.2.8.1.c.ii	The documentation shall be in a format suitable for use in the polling place.	*Not Applicable*
3.2.8.1.c.iii	The instructions and messages shall enable the poll worker to verify that the voting system o Has been set up correctly (setup); o Is in correct working order to record votes (polling); and o Has been shut down correctly (shutdown).	*Not Applicable*
3.2.8.2	Safety	
	All voting systems and their components must be designed so as to eliminate hazards to personnel or to the equipment itself. Hazards include, but are not limited to: • fire hazards; • electrical hazards; • potential for equipment tip-over (stability); • potential for cuts and scrapes (e.g., sharp edges); • potential for pinching (e.g., tight, spring-loaded closures); and • potential for hair or clothing entanglement.	
3.2.8.2.a	Devices associated with the voting system shall be certified in accordance with the requirements of UL 60950-1, Information Technology Equipment – Safety – Part 1 by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.	Pass
3.2.8.2.b	The certification organization's scope of accreditation shall include IEC/UL 60950-1.	Pass

Table A-2 Accessibility Review Matrix Requirements

Requirement	Description	Result
	Accessibility	
3.3	Accessibility Requirements	pass/fail
3.3.1	General accessibility	
	The requirements of this section are relevant to a wide variety of disabilities.	
3.3.1.a	The of this section are relevant to a wide variety of disabilities. Acc-VS shall be integrated into the manufacturer's complete voting system so as to support accessibility for disabled voters throughout the voting session.	
3.3.1.a.i	The manufacturer shall supply documentation describing 1) recommended procedures that fully implement accessibility for voters with disabilities and 2) how the Acc-VS supports those procedures.	Pass
3.3.1.b	When the provision of accessibility for the Acc-VS involves an alternative format for ballot presentation, then all information presented to non-disabled voters, including instructions, warnings, error and other messages, and contest choices, shall be presented in that alternative format.	Pass
3.3.1.c	The support provided to voters with disabilities shall be intrinsic to the Acc-VS. Personal assistive devices of the voter shall not be necessary to operate the Acc-VS correctly. This does not apply to personal assistive technology required to comply with 3.3.4 b.	Pass
3.3.1.d	If a voting system provides for voter identification or authentication by using biometric measures that require a voter to possess particular biological characteristics, then the Acc-VS shall provide a secondary means that does not depend on those characteristics.	Pass
3.3.1.e	If the Acc-VS generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record then the voting system shall allow the voter to verify that record using the same access features used by the voter to cast the ballot.	Pass
3.3.2	Enhanced visual interfaces	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
	These requirements specify the features of the Acc-VS designed to make the visual interface easier to see, in particular for voters with vision deficiencies, and synchronized with audio for voters with various language, reading, or some cognitive disabilities. In general, low vision is defined as having a visual acuity worse than 20/70. Low (or partial) vision also includes dimness of vision, haziness, film over the eye, foggy vision, extreme near-sightedness or far-sightedness, distortion of vision, color distortion or blindness, visual field defects, spots before the eyes, tunnel vision, lack of peripheral vision, abnormal sensitivity to light or glare and night People with tunnel vision can see only a small part of the ballot at one time. For these users it is helpful to have letters at the lower end of the font size range in order to allow them to see more letters at the same time. Thus, there is a need to provide font sizes at both ends of the range. People with low vision or color blindness benefit from high contrast and from a selection of color combinations appropriate for their needs. Between 7% and 10% of all men have color vision deficiencies. Certain color combinations in particular cause problems. Therefore, use of color combinations with good contrast is required. Note also the general Requirement 3.2.5 h.i. However, some users are very sensitive to very bright displays and cannot use them for long. An overly bright background causes a visual white-out that makes these users unable to distinguish individual letters. Thus, use of non-saturated color options is an advantage for some people. It is important to note that some of the requirements in 3.2.5 "Visual display characteristics" also provide support for voters with certain kinds of vision problems.	
3.3.2.a	An Acc-VS with a color electronic image display shall allow the voter to adjust the color saturation throughout the voting session while preserving the current votes.	Pass
3.3.2.a.i	At a minimum, two alternative display options listed shall be available: 1) black text on white background,2) white text on black background, 3) yellow text on a black background, or 4) light cyan text on a black background.	Pass

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.2.b	Groups of buttons and controls which perform different functions on the Acc-VS shall be distinguishable by both shape and color. This applies to buttons and controls implemented either "on-screen" or in hardware. This requirement does not apply to sizeable groups of keys in wide use by individuals with disabilities, such as a full alphabetic keyboard when used for purposes other than basic navigation and selection (e.g. entering a write-in candidate name).	Pass
3.3.2.c	If the Acc-VS has an electronic image display, the Acc-VS shall provide synchronized audio output to convey the same information as that which is displayed on the screen	
3.3.2.c.i	There shall be a means by which the voter can disable either the audio or the video output, resulting in a video-only or audio-only presentation, respectively.	Pass*
3.3.2.c.ii	The system shall allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session while preserving the current votes.	Pass*
3.3.3	Audio-tactile interfaces	
	These requirements specify the features of the Acc-VS designed to not only assist voters who are blind, but also those voters who would benefit from an auditory, rather than a purely visual, interface.	
3.3.3.a & 3.3.3.a.i	The vendor shall conduct summative usability tests on the voting system using individuals who are blind. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.	*Not Applicable**

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.b	The accessible voting station shall provide an audio-tactile interface (ATI) that supports the full functionality of the visual ballot interface, as specified in Subsection 2.3.3. • Instructions and feedback on initial activation of the ballot (such as insertion of a smart card), if this is normally performed by the voter on comparable voting stations • Instructions and feedback to the voter on how to operate the accessible voting station, including settings and options (e.g., volume control, repetition) • Instructions and feedback for navigation of the ballot • Instructions and feedback for contest choices, including write-in candidates • Instructions and feedback on confirming and changing selections • Instructions and feedback on final submission of ballot	*Not Applicable**
3.3.3.b.i	The ATI of the accessible voting station shall provide the same capabilities to vote and cast a ballot as are provided by other voting machines or by the visual interface of the standard voting machine. Discussion: For example, if a visual ballot supports voting a straight party ticket and then changing the choice in a single contest, so must the ATI.	*Not Applicable**
3.3.3.b.ii	The ATI shall allow the voter to have any information provided by the voting system repeated.	*Not Applicable**
3.3.3.b.iii	The ATI shall allow the voter to pause and resume the audio presentation.	*Not Applicable**
3.3.3.b.iv	The ATI shall allow the voter to skip to the next contest or return to previous contests. Discussion: This is analogous to the ability of sighted voters to move on to the next contest once they have made a selection or to abstain from voting on a contest altogether. v. The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	*Not Applicable**
3.3.3.b.v	The ATI shall allow the voter to skip over the reading of a referendum so as to be able to vote on it immediately.	*Not Applicable**
3.3.3.c	All voting stations that provide audio presentation of the ballot shall conform to the following requirements:	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.c.i	The ATI shall provide its audio signal through an industry standard connector for private listening using a 3.5mm stereo headphone jack to allow voters to use their own audio assistive devices.	*Not Applicable**
3.3.3.c.ii	When a voting machine utilize es a telephone style handset or headphone to provide audio information, it shall provide a wireless T-Coil coupling for assistive hearing devices so as to provide access to that information for voters with partial hearing. That coupling shall achieve at least a category T4 rating as defined by American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	*Not Applicable**
3.3.3.c.iii	A sanitized headphone or handset shall be made available to each voter.	*Not Applicable**
3.3.3.c.iv	The audio system shall set the initial volume for each voting session between 60 and 70 dB SPL.	Untested*
3.3.3.c.v	The voting machine shall provide a volume control with an adjustable volume from a minimum of 20dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.	Untested*
3.3.3.c.vi	The audio system shall be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.	Untested*
3.3.3.c.vii	The audio presentation of verbal information should be readily comprehensible by voters who have normal hearing and are proficient in the language. This includes such characteristics as proper enunciation, normal intonation, appropriate rate of speech, and low background noise. Candidate names should be pronounced as the candidate intends.	Pass
3.3.3.c.viii	The audio system shall allow voters to control the rate of speech. The range of speeds supported should be at least 75% to 200% of the nominal rate.	Pass
3.3.3.d	If the normal procedure is to have voters initialize the activation of the ballot, the accessible voting station shall provide features that enable voters who are blind to perform this activation.	Pass
3.3.3.e	If the normal procedure is for voters to submit their own ballots, then the accessible voting station shall provide features that enable voters who are blind to perform this submission.	Pass
3.3.3.f	All mechanically operated controls or keys on an accessible voting station shall be tactilely discernible without activating those controls or keys.	*Not Applicable*

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.3.g	On an accessible voting station, the status of all locking or toggle controls or keys (such as the "shift" key) shall be visually discernible, and discernible either through touch or sound.	*Not Applicable*
3.3.4	Enhanced input and control characteristics	
	These requirements specify the features of the Acc-VS designed to assist voters who lack fine motor control or use of their hands.	
3.3.4.a	The Acc-VS shall provide a 3.5 mm industry standard jack used to connect a personal assistive technology switch to the Acc-VS. This jack shall allow only switch data to be transmitted to the voting system. The voting system shall accept switch input that is functionally equivalent to tactile input. All the functionality of the Acc-VS (e.g., straight party voting, write-in candidates) that is available through the conventional forms of input, such as tactile, shall also be available through this non-manual input mechanism.	*Not Applicable**
3.3.4.b	The Acc-VS shall provide features that enable voters who lack fine motor control or the use of their hands to submit their ballots privately and independently without manually handling the ballot.	Partial pass
3.3.4.c	All keys and controls on the accessible voting station shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be no greater 5 lbs. (22.2 N).	Pass
3.3.4.d	The accessible voting station controls shall not require direct bodily contact or for the body to be part of any electrical circuit.	*Not Applicable**
3.3.5	Design for mobility aids	
	These requirements specify the features of the Acc-VS designed to assist voters who use mobility aids, including wheelchairs. Many of the requirements of this section are based on the ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).	
3.3.5.a	The accessible voting station shall provide a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space shall be level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.	*Not Applicable**
3.3.5	All controls, keys, audio jacks and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be within reach as specified under the following sub-requirements:	

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.5.1.a	If the accessible voting station has a forward approach with no forward reach obstruction then the high reach shall be 48 inches maximum and the low reach shall be 15 inches minimum.	*Not Applicable**
3.3.5.1.b.i 3.3.5.1.b.ii	If the accessible voting station has a forward approach with a forward reach obstruction, the following requirements apply: • The forward obstruction shall be no greater than 25 inches in depth, its top no higher than 34 inches and its bottom surface no lower than 27 inches. • If the obstruction is no more than 20 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 44 inches.	*Not Applicable**
3.3.5.1.b.iii	Space under the obstruction between the finish floor or ground and 9 inches (230 mm) above the finish floor or ground shall be considered toe clearance and shall comply with the following provisions: • Toe clearance shall extend 25 inches (635 mm) maximum under the obstruction • The minimum toe clearance under the obstruction shall be either 17 inches (430 mm) or the depth required to reach over the obstruction to operate the accessible voting station, whichever is greater • Toe clearance shall be 30 inches (760 mm) wide minimum	*Not Applicable**
3.3.5.1.b.iv	Space under the obstruction between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground shall be considered knee clearance and shall comply with the following provisions: • Knee clearance shall extend 25 inches (635 mm) maximum under the obstruction at 9 inches (230 mm) above the finish floor or ground. • The minimum knee clearance at 9 inches (230 mm) above the finish floor or ground shall be either 11 inches (280 mm) or 6 inches less than the toe clearance, whichever is greater. • Between 9 inches (230 mm) and 27 inches (685 mm) above the finish floor or ground, the knee clearance shall be permitted to reduce at a rate of 1 inch (25 mm) in depth for each 6 inches (150 mm) in height. • Knee clearance shall be 30 inches (760 mm) wide minimum.	*Not Applicable**

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.5.c	All labels, displays, controls, keys, audio jacks, and any other part of the accessible voting station necessary for the voter to operate the voting machine shall be easily legible and visible to a voter in a wheelchair with normal eyesight (no worse than 20/40, corrected) who is in an appropriate position and orientation with respect to the accessible voting station	*Not Applicable**
3.3.5.1.c	If the accessible voting station has a parallel approach with no side reach obstruction then the maximum high reach shall be 48 inches and the minimum low reach shall be 15 inches.	*Not Applicable**
3.3.5.1.d.i 3.3.5.1.d.ii	If the accessible voting station has a parallel approach with a side reach obstruction, the following sub-requirements apply. • The side obstruction shall be no greater than 24 inches in depth and its top no higher than 34 inches. • If the obstruction is no more than 10 inches in depth, then the maximum high reach shall be 48 inches, otherwise it shall be 46 inches.	*Not Applicable**
3.3.6	Enhanced auditory interfaces	
	These requirements specify the features of the Acc-VS designed to assist voters with hearing disabilities.	
3.3.6 a	The Acc-VS shall incorporate the features listed under Requirement 3.3.3 c for voting systems that provide audio presentation of the ballot.	Partial pass
3.3.6 b	If voting equipment provides sound cues as a method to alert the voter, the tone shall be accompanied by a visual cue, unless the station is in audio-only mode.	Pass
3.3.6.c	No voting device shall cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices. The voting device, measured as if it were a wireless device, shall achieve at least a category T4 rating as defined by [ANSI01] American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19.	Untested*
3.3.8	English proficiency	
3.3.8.a	For voters who lack proficiency in reading English, the Acc-VS shall provide an audio interface for instructions and ballots as described in 3.3.3 b.	Pass
3.3.9	Speech not required	
3.3.9.a	The voting system shall not require voter speech for its operation.	Pass

Table A-2 Accessibility Review Matrix Requirements *(continued)*

Requirement	Description	Result
3.3.10	Summative Usability Report	
3.3.10.a	The manufacturer shall submit a report of their summative usability tests on the voting system using individuals who are representative of the general population.	*Not Applicable**
3.3.10.a.i	The report shall be submitted in the Common Industry Format.	*Not Applicable**
3.3.10.a.ii	The report shall contain the results of the summative usability tests.	*Not Applicable**
3.3.10.b	The manufacturer shall conduct summative usability tests on the Acc-VS using individuals with low vision and shall report the test results, using the Common Industry Format, as part of the TDP.	*Not Applicable**
3.3.10.b.i	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
3.3.10.c	The manufacturer shall conduct summative usability tests on the Acc-VS using individuals lacking fine motor control and shall report the test results, using the Common Industry Format, as part of the TDP.	*Not Applicable**
3.3.10.c.i	The vendor shall conduct summative usability tests on the voting system using individuals lacking fine motor control. The vendor shall document the testing performed and report the test results using the Common Industry Format. This documentation shall be included in the Technical Data Package submitted to the EAC for national certification.	*Not Applicable**
3.3.10.c.i	In addition, the usability test report shall be submitted to the EAC as part of the documentation manufacturers are required to file with the application to test a voting system.	*Not Applicable**
	Discussion: Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to encourage early detection and resolution of usability problems. The manufacturer must submit the usability test report to the VSTL as part of their TDP. The VSTL will then check the technical data package to ensure that the report is present and reported in the Common Industry Format and contains the results from a summative usability test.	

ATTACHMENT B – VOATZ EBDM RESPONSES

Electronic Ballot Delivery and Marking

Voatz Remote Accessible Ballot Delivery, Marking, and Return System
Voatz, Inc.

In response to recently-issued guidance to election officials regarding electronic ballot delivery and marking circulated by the Federal Election Assistance Commission (EAC) [*], Voatz provides the following information on Voatz functionality.

System Considerations

System Infrastructure

Consideration	Voatz Implementation
How will the voting infrastructure be hosted (i.e., on servers at your facility, in the cloud, etc.)?	Voatz infrastructure is hosted at qualified, professional cloud services providers Microsoft and Amazon.
If you use the cloud, do you have awareness of where will the data be hosted (i.e. outside your jurisdiction, state, or the United States)?	All Voatz critical infrastructure is hosted within the United States at Microsoft Azure™ and Amazon Web Services™ data centers.
Does the system have the capacity to handle the increased load?	Cloud services enable spinning up additional servers on demand. Voatz runs monitored automated load tests daily to assess performance of the server(s) so that additional servers can be commissioned during heaviest load if needed.
What redundancies should be built into the system (i.e., backups, failover system, etc.)?	All Voatz cloud servers have hot standby replacements and are backed up daily.
Who will administer system configuration (i.e., security, load balancing, updates, patches, etc.)?	Voatz IT operations team, with guidance from the cloud providers, handles configuration of load balancing, security patches, etc.

[*] See: *Electronic Ballot Delivery and Marking Considerations for Election Officials* (as posed by CISA)
https://www.eac.gov/sites/default/files/electionofficials/vbm/eBallot_Delivery.pdf

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-16

Voatz

Electronic Interface / Usability &Accessibility

Consideration	Voatz Implementation
Is the system accessible to voters with specific needs (i.e., visual impairments, disabilities, language, etc.)?	Yes. Voatz apps operate on iOS or Android smartphones and incorporate Apple's and Google's native accessibility features including VoiceOver™, TalkBack™, etc. The Voatz interface and onscreen help are available in English and Spanish. Ballots can be translated into additional languages.
Is the system compatible with mobile devices?	Yes. Voatz apps are designed specifically to operate on Apple iOS v12.4 or higher or Android v8 or higher mobile phones (not other devices).
Is the system compatible with readily available screen readers?	Yes. Voatz runs as native iOS or Android smartphone apps which incorporate Apple's and Google's VoiceOver, TalkBack, as well as other accessibility features.
Is the system accessible with binary personal assistive technologies (i.e., jelly switches, sip-n-puff, etc.)?	Voatz for iOS supports Voice Control hands-free operation. Binary assistive technologies have not been tested but may be adaptable with Bluetooth™.
Do you provide help to voters directly through the electronic ballot delivery system?	Yes. Context dependent, onscreen Help is available in English and Spanish. In addition, Voatz detects if a screen reader is enabled, and provides modified help when necessary.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-16

Election Definition Files

Consideration	Voatz Implementation
What file format does your system accept (i.e., HTML, PDF, CSV, etc.)?	Voatz interprets native Electionware™ and ClearVote™ election definition files to transform them into remote accessible ballots. For other vendors, specific scripting routines are used to transform PDF designs into remote accessible ballot formats.
Does your voting system produce ballots in the accepted file types, or do you need software to convert them?	Yes, for supported vendors, fully marked and scannable ballots are available for printing and tabulation by the primary voting system.
What type(s) of audio files does your system use?	Audio files are not required as Apple iOS and Android provide speech to text.
What languages do the ballots need to be presented in?	Determined by jurisdiction. Voatz currently supports English/Spanish EBM interface.

Additional Supplies

Consideration	Voatz Implementation
Do you need to supply additional affidavits and instructions to the voter who votes electronically?	Voatz offers an electronic affidavit with signature or checkbox if required by the jurisdiction- typically for UOCAVA voters.
Will your materials contain labels and self-folding envelopes to mail the ballots back?	No. Ballot return is electronic over secure network and auditable.
Will you provide printable privacy sleeves for the voter to protect the ballot?	Not applicable. Electronic affidavits are stored separately from the returned ballot for privacy and ballots are identified in an anonymized manner.
What auxiliary technologies are required for the voter to complete his or her ballot (i.e., Internet service, email, printer, fax service, specific software, etc.)?	Voatz requires a supported Apple or Android smartphone, an email account, and cellular or Wi-Fi connectivity. No paper, printer or postal service is involved. Auxiliary voting channels should be available for other voters.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-16

Ballot Duplication

Consideration	Voatz Implementation
Many ballots generated by an electronic ballot delivery system cannot be directly scanned and tabulated into your voting system. To tabulate ballots using the voting system, the ballots must be printed on paper stock meeting certain specifications. For those ballots, enough blank paper stock will need to be purchased in advance. Jurisdictions may need additional technology (i.e., ballot duplication system, ballot on demand system, etc.) or staff to duplicate electronically generated ballots onto a ballot that can be scanned and duplicated. Depending on the volume of ballots that require duplication, additional staff needs could be significant.	Voatz is rare in its ability to return the ballots electronically to the jurisdiction. After they confirm the voter's affidavit, election officials print marked, scannable ballots directly on ballot stock for tabulation. Election officials do not need to open paper mail. Nor is faxing or hand transcribing required. Voatz supports jurisdiction and/or public post-election auditing of ballots.

Security Recommendations

Vulnerability Scan and Remote Penetration Testing

Recommendation	Voatz Implementation
Because these systems are publicly facing, jurisdictions using an electronic ballot delivery system should request a vulnerability scan and remote penetration test be conducted on the system. Also, for vendor-provided systems, election officials should suggest that their vendor subject the system to a critical product evaluation. These services provide the situational awareness needed to make informed decisions to manage the risks associated with the system and are provided at no cost to election jurisdictions and their private sector partners.	Voatz conducts frequent penetration testing of all its assets. In September 2019, the CISA Hunt and Incident Response Team (HIRT) conducted a proactive hunt operation that included the Voatz internal corporate network, as well as Amazon Web Services (AWS) and Microsoft Azure cloud networks that support the mobile-based election infrastructure. HIRT analysts did not detect threat actor behaviors or artifacts of past activities on the in-scope portions of the Voatz networks. HIRT commended Voatz for their proactive measures in the use of canaries, bug bounties, Shodan alerts, and active internal scanning and red teaming.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-16

Recommendation	Voatz Implementation
	For more, see: https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf

Web-Based Portals and File Servers

Recommendation	Voatz Implementation
Use security best practices for web and network connected election systems, including two-factor authentication (2FA) for employees and voters.	Yes, Voatz Admin portal uses 2FA for election officials. Voters use the Voatz app on compatible iOS and Android smartphones with integrated security features such as biometrics, identity verification and multi-factor authentication.
Encrypt traffic using secure hypertext transfer protocol (HTTPS) or, if you use a file server, ensure it uses a secure file transfer protocol (SFTP) by supporting transport layer security (TLS) version 1.2.	Yes, all traffic is encrypted using TLSv1.2 and the payloads are further encrypted using AES-256 GCM encryption.
Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.	Yes, Voatz has voluntarily submit edits platform and infrastructure for testing by CISA and 3rd party testing laboratories.

Copyright 2020, Voatz, Inc. Visit us online at voatz.com. Updated 2020-07-16

13. Attachment J - Synack Executive Summary

Synack Executive Summary Report: January 27, 2021 - February 04, 2021

Summary

Voatz has completed an extensive penetration test performed by Synack for their Voatz Mobile Voting Application. The data below reflects testing done between January 27, 2021 and February 04, 2021. During the course of the assessment, **0 critical severity, 0 high severity, 2 medium severity and 0 low severity** vulnerabilities were exposed per CVSS standard specification.

105	7	2
Active Researchers	Research Hours	Vulnerabilities

Methodology

The Synack Red Team employs a variety of tools and techniques that closely mimic adversarial tradercraft. Synack researchers cover a full range of testing methodologies which hit known variants of web-based attacks to target issues pertaining to: configuration management, business logic, authentication, authorization, session management, data validation, web services and client-side code. These researchers address the most prevalent security threats facing organizations today, with specific attention being spent on the OWASP Top 10 Project and CWE/SANS Top 25 Most Dangerous Software Errors.

Synack Red Team (SRT)

The SRT is a diverse group of highly skilled security experts, which include top researchers from academia, government, and the private sector. The SRT represents 50 different countries around the world, and hundreds of years of combined testing experience. Many Synack researchers are top producers from over 60 vulnerability disclosure programs, and regularly speak at industry events such as DefCon, AppSec, and Black Hat.

About Synack

Synack was founded by former NSA cyber analysts on a mission to reinvent the penetration testing and security assessment market. Synack facilitates access to the most accomplished white-hat hackers in the world, and rewards them on a solely incentivized basis to discover high-risk vulnerabilities.

Confidential and Proprietary to Synack and Voatz.

14. Attachment J - Resumes of Key Personnel

Richard Catahan – Voatz Canada LTD.

Executive Overview

Richard Catahan is an accomplished Senior Management Professional with over 30 years IT experience in the Public and Private industries. Having managed over 100 Ontario Municipal Elections and over 20 International Elections, Richard is considered a Subject Matter Expert in Online voting, IVR voting, and Datafix integration. Richard, in partnership with Hans Wobbe from Datafix, implemented the largest e-Poll Book for Elections Ontario in 2018.

Richard has been involved in all of the operational aspects of the elections conducted over the past 2 Ontario Municipal Elections (2014, 2018).

His specific areas of focus are:

- Legislative compliance;
- Election processes and procedures;
- Working with both third-party Security and External Auditors;
- Integration with DataFix, ES&S and Gilmore Doculink

Experience

Voatz Canada Limited

VP, Sales Canada

Voatz Canada Limited, North Bay, Ontario, Canada

- Liaise with provincial and Federal jurisdictions in Canada responsible for voting;
- Develop solutions for existing customers;
- Attend speaking engagements to discuss and present online voting;
- Analyze system architecture and recommend improvements;
- Provide requirements for new systems
-

Experience Prior to Voatz Canada LTD.

General Manager, Canada

SCYTL Canada, Toronto, Ontario, Canada (2012-2020)

- Managed 50 personnel, and direct project teams in the successful implementation of projects throughout the project life cycle
- Developed and implemented all IT/Telecommunication Strategic Plan, systems policies, procedures and requirements in accordance with the best business practices.
- Managed all Service Level Agreements (SLA) and monitor project schedules and budgets, and ensure that project milestones are met in a timely manner.

Registrar;IT Manager

Canadore College (2004-2012)

- Managed al Student Records, Registration, Graduation Functions, including transcript evaluations and certifications process to provide maximum service to students while ensuring efficient and effective workflow.
- Serve as ex-officio member for Curriculum Committee.
- Developed Strategic and Process Planning for the Aboriginal Learning Unit.
- Chaired the Committee of Registrars, Admission & Liaison Officers (CRALO) for all Ontario Post-Secondary Institutions.

Contact

www.linkedin.com/in/nimsim (LinkedIn)

Top Skills

Mobile Payments
Mobile Commerce
Software Development

Languages

French (Elementary)
English (Native or Bilingual)
Hindi (Native or Bilingual)

Honors-Awards

Voatz selected for the Techstars Boston 2017 Accelerator Program

Vantiv Challenge Winner @ Money2020 Hackathon 2016

IBM Challenge Winner @ AngelHack Boston 2016

Voatz wins 'The Startup Most Likely to Develop a Cult Following' Award at MIT Enterprise Forum's Startup Spotlight

Voatz wins the Audience Favorite award at Mass Innovation Nights

Patents

System and methods for roaming subscribers to replenish stored value accounts

Nimit Sawhney

Entrepreneur, Co-Founder @ Voatz
Boston, Massachusetts

Experience

Voatz

Co-Founder, CEO
January 2015 - Present
Boston MA

Voatz is a mobile elections platform changing the way the world votes by making it possible to vote with a smartphone or tablet. Powered by military-grade technology secured by blockchain, biometric identification and cryptography, Voatz ensures safe and secure elections while increasing accessibility and citizen engagement.

Since 2016, Voatz has worked with both major political parties, towns, cities, states, universities and non-profits to administer elections. In 2018, Voatz ran the first mobile blockchain vote in US Federal Election history. Specifically, Voatz partnered with the State of West Virginia to empower deployed military and overseas citizens to vote in the 2018 Primary Elections (2 counties) and the 2018 Mid-Term Elections (24 counties). In March 2019, Voatz was selected by the City/County of Denver CO for its 2019 Municipal General & Run-off Elections where its use led to a more than 2x increase in voter participation amongst deployed military and overseas citizen voters. More recently, Utah County (UT) and Jackson County (OR) have selected Voatz for their 2019 elections.

Oberthur Technologies

Director of R&D - Mobile Financial Services Business Line
June 2012 - December 2014 (2 years 7 months)
Waltham MA

• Led the expansion of the R&D team to a group of 25 engineers and managers with dedicated teams for core platform development, professional services, QA and IT support.
• Led the successful implementation and delivery of Czech Republic's first universal mobile payment service (Mobito) in partnership with 4 leading banks and all 3 mobile operators in the country.

• Designed the 4 class projects based on the above & mentored a Senior Level Systems class of 100 students.

Worked on building networked (distributed) applications of the future (emphasis on the interaction of applications and networks) by making use of powerful network processors like the Intel IXP1200:
• Installed and configured the new IXA (Intel Internet Exchange Architecture) programming platform.
• Ported the IXP1200 PCI drivers to work on the Suse Linux platform.

Amdocs
Software Engineer
August 1999 - July 2001 (2 years)
Cyprus, Germany, Austria

• Performed a high-level requirements analysis for developing a new convergent telecom-billing engine.
• Developed routines for handling hierarchical billing of corporate customers, handling paper-bill suppression and Datawarehousing of daily usage data.
• Developed routines for migrating data from external systems (like SAP, Clarify) to the Amdocs data model.
• Trained new employees in C, Pro-C and Data-layer module programming.

Education

Carnegie Mellon University
MS, (Information Networking) Computer Science, Electrical Engg., Business Management, Public Policy · (2001 - 2003)

Harvard Business School
Young American Leaders Program (YALP) · (2019)

Harvard Law School
Program on Negotiation · (2007)

[redacted]

• Led the successful implementation and delivery of a geo-redundant mobile/ landline prepaid recharge solution for Cable & Wireless International in several countries around the world.
• Led the successful implementation and delivery of Caribbean's first cross-border peer-to-peer airtime transfer solution covering 13 nations with 1 million active users.
• Led the successful implementation and delivery of Sierra Leone's first Mobile Money implementation (Splash Cash) – one of the first multi-bank, multi-operator solutions in Africa.

Sr. Software Architect
January 2003 - December 2007 (5 years)
Newton MA

• Developed an XML-based generic reporting framework as part of a distributed inter-carrier financial settlement system in order to facilitate the real-time/batch generation of multi-format reports.
• Developed a Wi-Fi accounting and management system utilizing a Linux server as a WLAN router.
• Developed a .NET plug-in for a RADIUS-based accounting/authorization protocol running on TCP.
• Added real-time charging functionality to the Helix DNA Media Server for streaming pay-per-view audio/video streams to RTSP-compatible mobile-phones/PDAs.
• Designed and developed a .NET based barcode generation and security application for mobile phones.
• Developed a SMS-based account recharging system for the Nokia Series-60 phones using J2ME.
• Provided technical consultancy and support for the Nokia Payment Solution (a white-labeled MoreMagic service) deployed at T-Mobile in Hungary.

School of Computer Science, Carnegie Mellon University
Researcher
September 2001 - December 2002 (1 year 4 months)
Pittsburgh PA

• Developed a non pre-emptive embedded micro-kernel for the Intel XScale 80200 processor.
• Ported the uCOS-II embedded operating system to the XScale 80200 platform.
• Developed device drivers and interrupt handler routines for the serial port, timer and the PCI sound card.

• Designed the 4 class projects based on the above & mentored a Senior Level Systems class of 100 students.

Worked on building networked (distributed) applications of the future (emphasis on the interaction of applications and networks) by making use of powerful network processors like the Intel IXP1200:
• Installed and configured the new IXA (Intel Internet Exchange Architecture) programming platform.
• Ported the IXP1200 PCI drivers to work on the Suse Linux platform.

Amdocs
Software Engineer
August 1999 - July 2001 (2 years)
Cyprus, Germany, Austria

• Performed a high-level requirements analysis for developing a new convergent telecom-billing engine.
• Developed routines for handling hierarchical billing of corporate customers, handling paper-bill suppression and Datawarehousing of daily usage data.
• Developed routines for migrating data from external systems (like SAP, Clarify) to the Amdocs data model.
• Trained new employees in C, Pro-C and Data-layer module programming.

Education

Carnegie Mellon University
MS, (Information Networking) Computer Science, Electrical Engg., Business Management, Public Policy · (2001 - 2003)

Harvard Business School
Young American Leaders Program (YALP) · (2019)

Harvard Law School
Program on Negotiation · (2007)

ANA MARIA QUEVEDO

anamaria.quevedo@voatz.com

Dedicated professional with twenty-one years' experience in the industry of elections, including voting system sales, development of international business opportunities, development, training and support of regional sales forces, system certification and project management. **Responsible for the implementation of national and regional election automation projects of $50Million+**. Strong background in computer technology, Unix and networking (LANs/WANs). Published eVoting research study for automated analysis of audit logs.

EXPERIENCE

Voatz Inc. Boston, MA ***2020- Present***

Account Manager

- Project implementation
- Manage new and existing accounts
- Assist in State system approval efforts
- Recommend customer support policies based on customers' requirements
- Manage election support efforts including help desk staffing and training

Clear Ballot Group, Boston, MA ***2013- 2018***

Customer Success Manager

- Market, sell and implement electronic voting system. Serve as main point of contact with Florida, New York and Maryland customers and prospects
- Manage local customer support partner and consultants
- Assist in State system approval efforts
- Recommend system enhancements based on customers' needs

Modcomp Systems and Solutions, Deerfield Beach, FL ***2011- 2013***

Account Manager

- Market and sell IT infrastructure solutions including network security, wired/wireless networks, data storage, virtualization, content delivery, VoIP, and system implementation services.

Premier Election Solutions (formerly Diebold), Allen, TX ***2007- 2009***

Latin America Sales Manager

- Market and sell election management hardware, software, supplies and services in Latin America
- Identify and contract with local business partners and provide support and training
- Primary point of contact with local partners and election officials
- Assist with development, and evaluation of sales strategies and manage budget for assigned territory
- Provide strategic market, product and competitive input to management
- Rendered assistance with development of systems in accordance with local requirements
- Negotiation of sale and lease contracts for hardware, software, and support services
- Account manager for two electronic voting projects in Colombia

Sequoia Voting Systems, Inc., Boca Raton, FL ***2005- 2007***

Sales Representative

- Territory included Florida, Central America and the Caribbean
- Drafting of RFP responses, conducting sales presentations in two languages, monitoring compliance with procurement requirements and deadlines
- Election support duties throughout the United States. Rendered assistance in California and Florida certification events

Election Systems and Software, Omaha, NE *1998- 2005*

Lead Project Manager, Miami-Dade County, 7,200 touch screen units (2002- 2005)

- Primary company representative in connection with Miami Dade County elections under a $24 Million contract for hardware, software and support services. Responsibilities included system implementation, training county staff, monitoring contract, project accounting and training and management of local partners; and monitoring of project costs to meet budget expectations
- Assist election officials in the conduct of 150 elections

Technical Support Specialist (2000-2002)

- Placer County, CA, project manager: coordinate hardware and software preparation, election programming, ballot layout, pollworker training, election day field support, precinct data transmission and election night tabulation and reporting
- Render technical and site support in numerous automated elections in Texas, California, Missouri, West Virginia, and Louisiana and Broward, Sarasota, Lee, Pasco, and Martin counties in Florida
- Responsible for election programming software and touch screen voting system quality assurance testing

International Sales Director/Lead Project Manager, Caracas, Venezuela (1998- 2000)

- Assist implementation: 7,300 precinct counters throughout 5,800 polling locations countrywide
- Local liaison with Spain based system integrator
- Assistant project manager for a $50 Million precinct voting equipment contract
- Responsible for marketing and sales for South and Central America

Unisys Corporation Venezuela *1989-1998*

Electronic Voting Technical Specialist, Field Engineer and Sales Representative

Nine-year experience in installation, configuration and maintenance of open system servers and peripherals including software, hardware and networking. Served as Unix server specialist (1995-1997). Named 1995 Technician of the Year. Addressed the Venezuelan National Electoral Council and the electoral tribunals of Panama, Ecuador and Costa Rica.

Received on-site training resulting in familiarity with Brazilian electoral system and touch screen technology.

EDUCATION

Florida International University - Miami, FL *2019-2020*

Master's in Cybersecurity

Cumulative GPA 4.0. Graduated summa cum laude

Miami Dade College - Miami, FL *2010-2013*

Bachelor Electronics Engineering Technology

Cumulative GPA 4.0, Dean's list

Johnson Controls and Vera Simpson scholarships.

University of California- Berkeley, CA *Summer 2011*

Team for Research in Ubiquitous Secure Technology (TRUST)

Research in the auditing of electronic voting resulting in the publication of a scientific paper by USENIX conference.

Point Park University - Pittsburgh, PA *1984-1986*

Associate Degree - Electrical Engineering

GPA: 4.0; Dean's List

PERSONAL

Coauthor, Automated *Analysis of Election Audit Logs*; 2012 EVT/USENIX conference publication.

Selected for 2012 Harvard University, Kennedy School of Business Latino Leadership Initiative.

Nominated among the six final candidates for the Distinguished Alumni Award of Point Park University 40th year celebration contest.

Bilingual English and Spanish. Runner: 2011 Boston marathon, finishing time 3:51:35.

Jesse Andrews

Boston, Massachusetts, United States

jesse.andrews89@gmail.com

linkedin.com/in/jessetandrews

Summary

Sales and business development leader with operations experience as a startup early employee. Analyzing new markets, sales approaches, go-to-market planning, winning strategic accounts, and sales hiring all excite me. Former life in banking and private equity.

Experience

Director of Sales and Business Development

Voatz

Feb 2020 - Present (1 year 5 months +)

Consultative solution selling in the election technology space which requires coordination of engineering, lobbying, marketing, media & communications resources to win public procurements and government buyers

Business Development

Voatz

Feb 2017 - Feb 2020 (3 years 1 month)

Business development, business strategy, and financial operations

Investment Associate

HarbourVest Partners

Jul 2014 - Aug 2016 (2 years 2 months)

Evaluate and execute venture capital and buyout fund investment opportunities for a global private equity manager with greater than $40 billion in assets under management - I was lead associate on 20+ commitments representing over $650 million capital committed

Responsibilities include:

• Conduct financial and business due diligence on a wide range of industries (technology, consumer, business services, industrial), author investment memos, and present recommendations to investment committee

• In-person meetings or reference calls with hundreds of top-tier investors, CEOs, and entrepreneurs

• Lead associate responsible for buyout and credit market research and quarterly trend updates for existing and potential investors

• Primary contact for cash flow forecasting assisting Limited Partners project overall private equity exposure for use of marketing future commitments to existing and new investors

• Monitor existing underlying portfolio company exit strategies, growth and return projections

Investment Banking Analyst - Real Estate Syndicated Finance

Wells Fargo

Jul 2013 - Jun 2014 (1 year)

Created comprehensive financial models and valuation analyses on public and private companies to evaluate strategic alternatives for various clients, including the impact of mergers and acquisitions and capital raises

Investment Banking Analyst - Leveraged Finance

Wells Fargo

Jun 2011 - Jun 2013 (2 years 1 month)

Created comprehensive financial models and valuation analyses on public and private companies to evaluate strategic alternatives for various clients, including the impact of mergers and acquisitions and capital raises

Education

University of Florida

Bachelor of Science (B.S.), Finance, General

University of Florida

Master of Science (M.S.), Finance, General

2011 - Present

Skills

Financial Modeling • Finance • Valuation • Capital Markets • Corporate Finance • Project Management • Sales • Elections • Cybersecurity • Enterprise Software

Donald J DeFord

(503) 269-7224 donald.deford@gmail.com Battle Ground, WA

National Election Manager | Senior Business Analyst

With over 20 successful years managing sales and operations teams, and 10 years as an Elections Business Analyst, I have developed a unique skill set that accelerates innovation and communication. I am driven to help election officials and voters find the perfect match of innovation, technology, and productivity. There are many potential industry-changing ideas out there; my greatest aspiration is to help facilitate those ideas to achieve their potential.

Professional Work History

National Sales Manager | Voatz 2020 – Present

Develop a national sales strategy to launch the Voatz voting platform in governmental elections.

- Responsible for developing long-term relationships with national, state, and local elections officials
- Defining strategy for understanding product costs and defining product needs from a customer perspective to assist management team with product roadmap development
- Assessing marketing needs, and developing materials and resources

Sales Director | Smartmatic 2020 – 2020

Brought on the help launch Smartmatic's product lines in the United States. COVID related setbacks in the international elections market forced a stop to current US plans.

Regional Sales Director/Senior Business Analyst | Clear Ballot Group 2015 – 2020

Sales accomplishments

- Joined the company when it had no voting system customers and signed 30 customers, delivering 75% of Oregon's registered voters and 65% in Washington, with 8 new counties working through the contracting process.
- Developed the company's demo process, hardware, and scripts

Business Analyst Accomplishments

- Guided certification, implementation, and third-party integration for our first 12 Ohio customers
- Business analyst for large customers (King, Pierce, Snohomish, Multnomah, Douglas)
- Managed ballot design and layout service for 2019-2020 elections for Ohio and Wisconsin customers
- Developed processes for onboarding new states prior to sales activities

Regional Sales Manager | Everyone Counts 2014 – 2015

Managed sales activities for the company's voting system across northern U.S. states.

- Managed 17 major RFP responses in one year
- Guided the development of an electronic-Poll Book

HAVA Manager | Oregon Secretary of State 2010 – 2014

In a limited duration position, I managed the 'end of life' process for the state's HAVA funds

- Modernized the state voter registration system
- Updated county hardware and software across the state
- Revolutionized voter access for voters with disabilities by implementing the first mobile voting platform

Field Sales/Sales Manager/Trainer | Eli Lilly/Novo Nordisk/Rhone-Poulenc Rorer 1995 – 2008

Field sales manager for various pharmaceutical companies. Sales and technology trainer for the West Coast.

- Top 1% in sales three times, and always in the top 10%
- Managed nine new product launches-over 125% to quota in all nine
- Rookie of the year, trainer of the year, president's club (3 times) and many other awards and recognitions

Education

Bachelor of Arts in Business Communication | Jones International University 2002

- **Honors:** Cum Laude (GPA: 3.9/4.0)

Contact

www.linkedin.com/in/linda-hutchinson-boston (LinkedIn)

Top Skills

Software Project Management
SaaS
Testing

Certifications

Blockchain User Certification
Cyber Risk Management

Patents

System and methods for calculating and predicting near term production cost, incremental heat rate, capacity and emissions of electric generation power plants based on current operating and optionally atmospheric conditions.

Linda Hutchinson

Director of QA & Compliance
Boston, Massachusetts

Summary

Proven track record in the design, testing, scheduling and delivery of quality software products to enterprise, multinational and GovTech clients. Led all phases of productization from concept prototypes to successful SaaS and enterprise-wide client/server deployments. Real-world Cybersecurity experience and continuing education. Experienced technical manager and project leader.

Experience

Voatz
Director of Quality Assurance & Compliance
February 2019 - Present
Boston, Massachusetts

Direct testing of Voatz' mobile voting platform in use in five US states. Serve as Agile product owner and ensure compliance with federal voting standards and accessibility guidelines. Partner with scrum team in planning and scoping sprints. Collaborate with senior management on executing corporate growth strategies.

Clear Ballot Group
Director of Quality Engineering
October 2015 - January 2019 (3 years 4 months)
Greater Boston Area

Directed all testing of the ClearVote voting system which achieved the fastest ever initial US federal certification. Led QA team in establishing in house software and hardware testing methods for six GovTech products. Partnered with third party federal testing laboratories to ensure products met accuracy, usability, scalability, security and accessibility requirements of states' election officials. Clear Ballot Group was selected as a GovTech Top 100 winner in 2018 for its success in bringing innovation and transparency to the election industry.

IBM
Advisory Software Engineer

2006 - September 2015 (9 years)
Greater Boston Area

Led multiple quality engineering projects at Kenexa, an IBM company. Devised new test methodologies for BrassRing SaaS recruiting software serving global clients. Specified and validated migration of applicant tracking and resume data into new database platform. With development architect, migrated to open source search engine resulting in $3MM in cost savings while increasing both reliability and performance. In partnership with a localization vendor, tested translation and internationalization of software for European and Asian markets. Ensured compliance with PII privacy regulations. Partnered with DevOps on seamless, staged deployments in US and European data centers.

BrassRing
Quality Engineering Architect consultant
2002 - 2006 (4 years)
Waltham, MA

Served as technical project leader for KenexaBrassRing SaaS recruiting solution serving global clients. Led teams of two to seven engineers in developing ten thousand new test cases for growing product. Served as cross-departmental project manager for migration of millions of resumes to new search platform. Established method of back-end validation of full-text search functionality. Designed automation for execution prior to deployments.

Lotus Development
Senior Quality Engineering Manager - Lotus Notes
1987 - 1996 (9 years)

Directed Lotus Notes Quality Engineering responsible for all testing of the software on multiple client/server platforms of product with 60 million users. Led test automation, network/platform certifications, scalability, performance benchmarking, localization, UI and system testing Grew department(s) to 100 employees to efficiently meet rapidly growing product requirements on across multiple platforms while achieving highest employee satisfaction/ retention. Helped ensure successful deployment at selected Fortune clients. Nominated by peer managers to direct corporate QA Managers Task Force. Partnered with Development (Iris Associates) and Product Management in scheduling and implementing new Notes releases. Established certification Lab and automation strategy. With software architect, devised method to accurately scale testing for each platform while minimizing risk and expediting new products to market.

Education

The University of Connecticut

Bachelors, IMJR

The Commonwealth Institute

Certificate, Entrepreneurship/Entrepreneurial Studies · (2000 - 2001)

Harvard Kennedy School

Certificate, Cybersecurity · (2018 - 2018)

Dolan Murvihill

503 830 4363
dmurvihill@gmail.com
https://github.com/dmurvihill
(LinkedIn)

Experienced software engineering leader obsessed with building great teams that build great products. Laser-focused on increasing the product's value to the user as quickly and as steadily as possible, by creating a culture of care and support that carries the team over obstacles.

Confident individual contributor to API servers, data pipelines, DevOps infrastructure, and the web. Production code currently running in Java, Scala, Python 2 and 3, SQL, TypeScript, and JavaScript. Academic and hobby code in many more, including C. Strongest in functional and OO paradigms. Comfortable in the AWS console and AWS command line. Terraform user. Have set up about a dozen continuous integration pipelines using Jenkins and CircleCI.

Experience

Voatz, Boston, MA

2018-present Software Engineer

- Led the design and development of the Voatz Web App, a web portal that voters use to participate in Voatz elections. Stack: Angular, Node.js, Terraform, AWS Lambda.
- Actively worked as a senior resource to develop the team. Reached out to team members who needed support, interviewed candidates for senior technical positions, and drove essential process maturity improvements.
- Created the company's 2021-2024 resource needs forecast for its product development, testing, and documentation needs. Based on one-sentence market penetration objective set by CEO for 2024, worked with the team to identify required changes to the software, used established evidence-based techniques to estimate required product development effort and from there the headcount of the required organization, and developed a four-year, $4M budget proposal covering engineering, QA, documentation, DevOps, and product design, for presentation to investors, resulting in a $6M funding raise.
- Wrote the company's software development security policy for ISO 27001 certification. Led an incident response team consisting of staff from the junior to the executive level in responding to a simulated data breach.
- Designed and implemented the performance test architecture for the Voatz API server; wrote the test procedure, coded the test plan in JMeter and supporting scripts in Python, specified the hardware platform, set up continuous integration pipelines for performance testing the server and for testing the test harness itself, developed a JSON "cover sheet" format that enables fully reproducible test results, and trained others to execute the tests. Interfaced with ProV&V, a federally-accredited voting system test lab, to verify the app remained human-usable under its maximum load.
- Developed a voter-verifiable digital receipt for the first ballots submitted by mobile phone in any United States election — a "game changer" for public trust in our ballots, according to the state election director.
- Designed and implemented a web app in TypeScript to enable voters and auditors to compare the voter's receipt with the official ballot that was scanned at the precinct. Successful deployment resulted in client receiving the National Association of Election Officials' Democracy Award.
- Design and manage systems for the electronic management of personally identifiable information.

EverQuote, Cambridge, MA

2017-2018 Senior Quantitative Software Engineer
2015-2017 Quantitative Software Engineer

- Co-creator and architect of the EverQuote Real-Time Bidder, a high-throughput real-time ad buyer, and its associated data pipeline. Developed the API layer and bidding logic using the Twisted event-driven networking engine for Python 2. Interfaced with MySQL for operational data and for auction records. Set up Spark transformations through Databricks to make advanced queries available to the advertising analysts. Created configuration files for Fluentd and other dependencies, and wrote the scripts that provisioned the server and started the application. Managed deployments and operations in the AWS console. Interfaced with auction organizers to solve interoperability issues.
- Design and manage systems for the electronic management of personally identifiable information.

Voter Choice Massachusetts, Boston, MA

Early member and volunteer leader, and then staff member, of Voter Choice Massachusetts, a Ranked Choice Voting advocacy organization.

2018 Grassroots Organizer

- Founded the Greater Boston chapter, developing over a dozen volunteer leaders and organizers. Conducted our first statewide volunteer census and plotted our members across the state.

2017-2018 Regional Chapters Director
2016-2017 Live Outreach Director

- Assumed a volunteer leadership role at the beginning of the Massachusetts Ranked Choice Voting 2020 movement. Oversaw field outreach across five regions, involving 30 volunteers at over 12 events each month, which resulted in email list growth from an initial 250 to over 8000 in the first year, and monthly active volunteers from 3 to about 100. Constantly developed and fine-tuned field messaging in response to voter feedback and news events.
- Later, coordinated six active chapters across the state, consisting of hundreds of active volunteers. Advised chapter leads, represented the statewide organization at chapter meetings from Brewster to Pittsfield, and developed volunteer engagement programming and training.
- Routinely led outreach teams in the field, including at state party conventions where there was considerable time pressure and the team would exceed 30 volunteers.

Resilient Systems, Cambridge, MA

2014 Software Engineering Intern

Developed a prototype integration between Co3 Systems (now IBM Resilient) and the ArcSight Security Information and Event Management platform. Java 8. **VMware**, Palo Alto, CA

2013 Software Engineering Intern

Developed kdauto, a tool to facilitate debugging of Windows core dumps by executing several command line Windows debugging tools and collating the results. Python 3. **Intel**, Hillsboro, OR

2012 Software Engineering Intern

Wrote a user manual for the Intel ASIC Emulation Module, a programmable emulator for development of custom integrated circuits that interface with standard Intel CPU sockets. Product shipped with manual to the customer, Groupe Bull, in 2012. LibreOffice Writer.

Education

Worcester Polytechnic Institute Worcester, MA
B.S., Computer Science, May 2015

- Co-developed Checksims, a similarity detector that uncovered dozens of previously undetected cases of plagiarism in introductory CS and EE classes (Heon and Murvihill 2015).
- With a team of four, developed a detailed set of criteria for moving the election process for faculty committees to a web-based, electronic system; and made recommendations (Fogel *et al.* 2013)
- Coursework and extracurricular activity heavily slanted toward cryptography and information security, including several graduate-level cryptography courses.

Orlando Alomá, FMVA®

San Juan, Puerto Rico | 787-637-6459
alomaborlando@gmail.com
linkedin.com/in/orlando-aloma/

Professional Experience

VOATZ — Boston, USA May 2019 - Present

Assistant Project Manager — Navigated numerous duties to deliver exceptional products and successfully implement mission-critical projects.

- Hosted Project Management meetings and gathered necessary information and project requirements
- Served as the Technical Lead of the Project Management Team advising about our products and their capabilities
- Assisted with Project Implementation & Managed Active Projects
- Conducted product training for government and private sector clients
- Managed communication to/from C-level management when isolated issues arose during an election and communicated a solution to Customer Support Agents
- Attended product meetings to keep up with product enhancements and provide information about upcoming projects
- Created documentation & videos to match upcoming election requirements
- Performed training and updated documentation for Customer Support Agents
- Provide tier 2 & 3 support to Customer Support Agents
- Periodically assisted with QA tasks like Regression Testing & Product Testing

Management Associate

- Spearheaded a project to identify an opportunity to collaborate with the 2020 Census Opportunity Project and pitched the idea to the Deputy Director of the Census Bureau.
- Collaborated with Project Managers to develop elaborated plans including all necessary product features and functions for projects.
- Performed Product Demos to potential clients and government regulators such as Thomas Greg & Sons from Colombia and EAC Commissioner Donald Palmer.
- Teamed with the Product Owner to evaluate alternatives to make quick and informed decisions in difficult situations.
- Led Quality Assurance Testing on iOS and Android mobile apps and implemented a Regression Testing spreadsheet with 500+ Test Cases resulting in a 20% decrease in testing time.

Advisor Experience

Airblock Tech. (Start-Up), Board of Advisors — Boston, USA September 2019 – Present

- Researched Zero Equity funding strategies by studying the field of Accelerator Programs and SBIR Grants.
- Advised on the decision-making strategy to choose a Blockchain protocol and infrastructure.
- Teamed up with the CEO and CTO to pitch to Angel Investors.

Skills and Certifications

Other Languages: Spanish (Native).
Certifications: Financial Modeling & Valuation Analyst (FMVA®, CFI, 2020), Private Equity and Venture Capital Course Certification (Università Bocconi on Coursera, 2018), Blockchain Revolution for the Enterprise Specialization (INSEAD on Coursera, 2019), PwC Pitch Challenge 2019.
Mastered Tools: PitchBook, Excel, Capital IQ, SQL, Power Point, Word, JIRA, Slack, Dropbox.
Personal Interests: Entrepreneurship, Technology, Financial Markets, Trading, Tennis, Traveling, Rock Climbing.

Education

Master of International Business & Finance August 2019
HULT INTERNATIONAL BUSINESS SCHOOL— Boston, USA

Bachelor of Business Administration in Finance August 2017
FLORIDA ATLANTIC UNIVERSITY— Boca Raton, USA

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Summary

COO, Technical, Program, Project and Product manager/director steering multi-stage high complexity initiatives within a large matrix organization from concept to full deployment in an Agile/Waterfall environments.
Deliver top quality results on time and within budget. Tactical strategist, who adeptly bridges the gap between clients and infrastructure/development teams, builds and sustains strong, collaborative cross-departmental working relationships to meet mission-critical objectives.
Strong understanding of technology operations and project management from ground up.
Plan and monitor CAPEX/OPEX budgets between $100K to $20 Million.
Proactively managed teams between 25-75 resources by demonstrating strong, decisive leadership with sound, practical and participative management style.
Core strengths in Project Delivery, Product Design, Relationship/Vendor/Change Management, PMO Governance
Technical and infrastructure knowledge.
Work in several industry domains including Public Sector, Energy, B2B.

Experience

Konnech – Michigan, US (Remote)

World-wide Technical Director	**D. START**	**9/2020**
	D. END	**ACTUAL**
Performed functions	**Manage a department of over 70 engineer distribute between Australia, India, China, Brazil and US** Managing the company's technological plans. **Lead the strategy for technology platforms, partnerships and external relationships** **Create overall technology standards and practices and ensure adherence** Track, analyze and monitor technology performance metrics Oversee all system design and changes in system architecture **Envisioning how different forms of technology will be used throughout the company.** Researching ways the company's technological assets can be improved **Creating networking safeguards that prevent security breaches and keep client information confidential.** **Assessing new technologies are appropriate for the company to use.** Ensuring technologies currently in use are efficient and making changes wherever necessary (I reduced company cloud infrastructure year cost over 300.000 in less than 3 months) Work closely with Marketing, Business Development and Operations to define and deliver new products and enhancements **Analyze RFPs, estimate cost and generate business and technically proposals** **Direct report to CEO**	
Technical environment	- .Net, Vue, Js, Python, SQL Servers, - JIRA, Xray, SharePoint, Gitlab, Jenkins - Office Package (Excel, Power Point, Word, Visio, PPM)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Xtremis – Barcelona, Spain

COO	D. START	2/2020
	D. END	ACTUAL
Performed functions	**Design and implement long and short term business strategies, plans and procedures.** **Manage over 30 resources.** Set comprehensive goals for performance and growth. Establish policies that promote company culture and vision. **Oversee daily operations of the company and the work of executives (IT, Marketing, Sales, Finance and Operations.).** Lead employees to encourage maximum performance and dedication. Evaluate performance by analyzing and interpreting data and metrics. ISO 9001 Cerification. Generate a network of partners and suppliers. Providers/Partner management Client Management. Cashflow Management. **Generate business and technically proposals** **Direct Report to CEO**		
Technical environment	- JS, Angular, Python, Oracle, React, Maven, Java, PHP, Heroku - JIRA, Testrail, SharePoint, Github, Codeship, Saleforce - Office Package (Excel, Power Point, Word)		

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Scytl Secure Electronic Voting – Tampa, Florida (US)

Program Manager	**D. START**	**10/2017**
	D. END	**1/2020**
Projects Description	• **2018 Election Ontario, Partnership with Datafix** o Deliver a pollbook product for 2018 Ontario Election o Execute 2018 Ontario Provincial Election • **2018 Ontario Municipalities Elections** o Deliver an online voting and IVR systems for 2018 Municipal elections o Deliver a Telephone voting system for 2018 Municipal elections o **Execute and manage 103 Municipal elections (Markham, Newmarket, Sarnia….)** Directing and manage all the Online voting election projects delivered in North America for Public and private sectors by Scytl.	
Performed functions	**- Project Estimation** **- Program Planning** **- Providers/Partner Management** **- Client/partners Expectations management** - Change Request Management **- Cashflow Management** **- Lead the Develop and QA team** - Specifying acceptance criteria **- Release Planning** - Quality Report - User story design - Documentation - Helping the team to continuously improve their process. - Project Closing and Delivery management **- Change Request management** **- Deploy Plan** **- Working close with Presale team generating RFP responses and cost estimation for project opportunity**	
Technical environment	- Java, JS, Angular, Python, Oracle, Ansible, Maven, Splunk - JIRA, Testrail, SharePoint - Office Package (Excel, Power Point, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Product Manager (Online Voting system)	**D. START**	**03/2017**
	D. END	**01/2018**
Performed functions	**- Design Product Roadmap** - Evaluate new requirement - Design product architecture **- Release Planning** - Documentation **- Manage Product Backlog** **- Report to management and stakeholders**	
Technical environment	- Java, JS, Angular, Python, Oracle, Ansible, Maven, Splunk, Sonar - JIRA, Redmine Testrail, SharePoint - Office Package (Excel, Power Point, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Project & Technical Manager	**D. START**	**03/2017**
	D. END	**10/2017**
Projects name and description	Delivery of customized Online voting solutions for up to 150.000 voters integrated with external and internal systems (Voter list manger, IVRs, credential delivery systems, Authentication providers) in order to accomplish client requirement. **United States projects:** - IDB (Inter-American Development Bank) - OAS Staff Association - Election Trust (Partner) - College Board **Canada projects:** - APEGA (Association of Professional Engineers and Geoscientists of Alberta) - CPA (Chartered Professional Accountants of Ontario) - ACTRA National (Alliance of Canadian Cinema, Television and Radio Artists) - ACTRA Toronto (Alliance of Canadian Cinema, Television and Radio Artists) **South America:** - Medellin Municipality Referendum **Europe projects:** - Ajuntamiento Girona (Girona Municipality) - SGAE (Sociedad General de Autores y Editores) - COIGI (Col·legi Oficial d'Infermeres/ers de Girona)	
Performed functions	**- Project Estimation** **- Manage project stakeholders** **- Project Planning** **- Price Negotiation with 3rd Parties** **- Provider manager** **- Manage Client Expectations** - Solution Design - Change Request Management **- Lead the Develop and QA team** - Specifying acceptance criteria **- Release Planning** - Quality Report - User story design - Documentation **- External Auditor Management** - Helping the team to continuously improve their process. - Report to management and stakeholders - Project Closing and Delivery management **- Change Request management** **- Deploy Plan**	
Technical environment	- Java, JS, Angular, Python, Oracle, Ansible, Maven, Splunk - JIRA, Testrail, SharePoint - Office Package (Excel, Power Point, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Scytl Secure Electronic Voting – Barcelona, Spain

Product Owner (Candidate Manager)	**D. START**	**04/2015**
	D. END	**03/2017**
Product Description	The Candidates Manager is a solution to be delivered to several clients, each of those with different ways of working with the Election **Candidates.** That's the reason we developed a flexible system from the very beginning so the different elections types. The Final solution has a configurable workflow for approval of a register candidate, configurable by an admin form when the election is created in the platform.	
Performed functions	- Solution Design - **Manage the Develop and QA team** - Coordinate with UI/UX team - Acceptance criteria definition - **Release Planning** - **Road Map** - Quality report - User story design - Documentation - Helping the team to continuously improve their process. - **Manage Product Backlog** - Report to management and stakeholders	
Technical environment	- PHP, python, MySQL, Fabric - AGM, ALM, PPM - Office Package (Excel, PowerPoint, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Product Owner (Credential Delivery OTL)	**D. START**	**04/2015**
	D. END	**03/2017**
Product Description	The Credential Delivery is a solution used in to deliver credential in a secure way to voters all around the world. Using different method as OTL or SMS. The system has been developed taking in account all the different requirement of the elections all around the world, creating a configurable and flexible solution that fits the need of all the customers. The main product features are: - integration with the Online voting - send credentials via different flow in order to keep the delivery secured - credential recovery - User management for Client use	
Performed functions as a consultant	- Solution Design - **Manage the Develop and QA team** - Coordinate with UI/UX team - Acceptance criteria definition - **Release Planning** - **Road Map** - Quality report - User story design - Documentation - Helping the team to continuously improve their process. - **Manage Product Backlog** - Report to management and stakeholders	
Technological environment	-Java, JS, Oracle, Fabric -AGM, ALM, PPM -Office Package (Excel, Ppt, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Project and Technical Manager	**D. START**	**06/2015**
	D. END	**03/2017**
Projects Description	Delivery of customized online voting solution with Scytl systems and integrations with external providers for one shot licences and long term **United States Projects:** - Election Trust (Partner) **Canadian Projects:** - OECTA (Ontario English Catholic Teachers' Association (OECTA) **French Projects:** - French Primary elections **Norway Projects (Partnership with NVTC):** - Nord-Odal Municipal Referendum) - South-Odal Municipal Referendum) - Lørenskog Municipal Referendum) **Iceland Project:** - Register Iceland and partnership with Advania **Spanish Projects**: - MC MUTUAL (Insurance) - UPV (University Valencia) - COFB (Pharmaceutic association) - OpenSeneca (Partner) **Malaysia Projects:** - RSPO (Roundtable on Sustainable Palm Oil) **South Africa:** - Pollmed (Partner with Tata motors)	
Performed functions	- Deploy manger - Manage the developing team and QA team **- Validation of requirements and changes** **- Control of estimates** **- Solution Design** **- Provider management** **- Partnership management** - Quality Report - Management of deliveries and follow-up meetings - User story design - Operation and installation - Security Audit **- Effort Estimations** **- Change Request management** **- Delivery management** **- Mange Internal and external teams**	
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Fabric, Django - Office Package (Excel, Word)	

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Technical Manager	D. START	02/2014
	D. END	06/2015
Projects Description	Delivery of customized online voting solution with Scytl systems for the following clients **Canadian Projects:** - Quality Control Council of Canada - Shawanaga (Canadian First Nation) - White River First Nation - Nunavut Employees Union - PCAA (Progressive Conservative Association of Alberta) - Uniform 111 (Drivers Association) - AMAPCEO (Association of Management, Administrative and Professional Crown Employees of Ontario) **French Projects:** - MIF (Interior Ministry of France) - IRIS (Partner) - **German Projects:** - SPD (Social Democratic Party of Germany) **Spanish Projects**: - COAC (Architect association Catalonia) - CESCA (University Catalunya) - URV (University Rovira and Virgil) - CIXUG (University Galicia) - MC DONALDS (Owners association) - CDC (Catalunya Democrat Party) - JNC (Joventut Nacionalista de Catalunya, political Organization) - COAM (Architect association Madrid) - **India Projects:** - Gujarat (Partner with Tata motors)		
Performed functions	- Deploy in DEMO environment, Pre-Production Environment, Production Environment with Fabric scripts - Manage the developing team and QA team **- Validation of requirements and changes** **- Control of estimates** **- Solution Design** - Quality Report - Management of deliveries and follow-up meetings - User story design - Travel to Clients for operation and installation - Auditors **- Effort Estimations** **- Change Request management** **- Delivery management** **- Mange Internal and external teams**		
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Fabric, Django - Office Package (Excel, Word)		

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Description of the projects	**2014 Ontario municipalities Elections** (18 Municipalities) Electronic Voting Solutions integrate with an external IVR system (Datatel) and Voter list Manager (Datafix), login transforms and Web crossing login
Performed functions	- System Operation - User acceptance test plan and execution - Election Support - Electoral Consultant for Electronic Voting - DB Scripting - **Auditors management**
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Fabric, Django, Spunk - Office Package (Excel, word)
Projects Description	**Electoral Management System for Ecuador 2014 Elections business processes for the modules Post electoral and Logistic**
Performed functions as a consultant	- Deploy in DEMO environment - Manage the developing team and QA Team - Validation of requirements and changes - Control of estimates - Quality Report - Management of deliveries and follow-up meetings with management - Customization of the system s - User story design - Travel to Peru, for Training the Peru Team
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Fabric, Django - Package Office (Excel, word, MS Project, SharePoint)
Projects Description	UNED: e-voting Platform
Performed functions	- Validation of requirements and changes - Control of estimates - Reporting of quality internal - Management of deliveries and follow-up meetings with management - Customization of the system s - User story design
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python - Office Package (Excel, word)
Projects Description	**Libya Election result consolidation System**
Performed functions	- Deploy the application in Production Environment - Develop Changes in the system -DB Analysis - Automation of Testing with Selenium - Stress test with Jmeter - Bug Fixing in python Django - System Operation: Travel to Libya - **Team Management**

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Django, Fabric, Spunk - Office Package (Excel, word, MS Project, SharePoint)

Description of the project	Denmark OLVP (Online Voting Platforms)
Performed functions	-Design of a complex project based in 3 applications: 1- Candidate Manager (PHP and python) after the project the application has been introduced to Scytl portfolio product, SAAS architecture 2- Credential delivery (by mail or SMS), after the project the application has been introduced to Scytl portfolio product, SAAS architecture 3- Customization of the online voting Platforms - Manage the developer team and the QA team for create a Custom solution for this client. - Develop web service for cast votes by phone, and integration with 3rd parties - Internal Auditor Management - Deploys in Pre and Pro environments - Manage external parties as Help desk and IVR locate in Canada
Technical environment	- Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Jmeter, Fabric, AngularJS, Spunk - Office Package (Excel, word, MS Project, SharePoint)

Team Leader	**D. START**	**8/2013**
	D. END	**2/2014**

Projects Description	Electoral Management System for Ecuador 2014 Elections business processes for the modules Post electoral and Logistic
Performed functions as a consultant	- Deploy in DEMO - Manage the developing team - Validation of requirements and changes - Control of estimates - Quality Reporting - Management of deliveries and follow-up meetings with management - Customization of the system s - User story design - Mange internal and external teams
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python, Jmeter, Fabric, Django - Office Package (Excel, word)

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Projects Description	UNED: Evoting Platform
Performed functions as a consultant	- Validation of requirements and changes - Control of estimates - Reporting of quality internal - Management of deliveries and follow-up meetings with management - Customization of the system s - User story design
Technical environment	- SQL, Oracle, JS, Java, Selenium, Test Rail, Redmine, Postman, Soap UI, Eclipse, Python - Office Package (Excel, word)

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Previous Experience

IT CONSULTANT	D. START	06 2011
	D. END	07/2013

Company	Indra
Customer	Project Zeus INDRA / Gas Natural Fenosa
Projects Description	ERP performed by Indra for the integral management of the business of GNF in Spain, Italy and Latin America, with a size of 600 people.
Performed functions such as QA Manager	- Meetings with Natural Gas service providers to establish a real test plan - Hire the necessary support - Quality assurance, coordinate test plan and treat the effects of user - Defense of the project in the face of the customer. - Weekly Reporting internal and customer - Implementation of simulator of tests for interfaces with satellite systems through queues MQ, with ACTIVEMQ in the environment of pre-production - Analysis and evaluation (proof of concept) of tools test automation project, selection of this and official presentation to the project team. - Trainer of automation tester for Selenium IDE and FlexMonkium, creating documentation (Videos of classes and PowerPoints) tools. - Responsible for the design and development of a web application in JAVA and HTML for the launch of test cases automated with direct reporting to the corporate Testlink tool and creation of defects in JIRA/MANTIS automated with the possibility of video recording of the execution of the test cases. - Estimation of time, efforts and personnel required for the Project tasks. - Design of methodologies for the execution of the test plan. - Audit of quality of the application regarding the standards stipulated by the style guide.
Performed functions such as PMO	- Validation of Projects - Validation of the performance of the project teams - Validation of requirements changes - Control of estimates - Reporting of quality internal and external - Management of deliveries and follow-up meetings with management and BP. -Design of the conceptual map of the system -Milestone planning
Technical environment	- Microsoft Project, Jira, Testlink, Redmine, MS Share Point and other management tools, staff, efforts and temporary estimate (the company INDRA active) -Software used: Selenium IDE, Selenium RC, Imacros, Test Complete, SVN, ActiveMQ, Active Presenter, VMWARE, Toad. -Interfaces with systems SAP MM, SAP MQ, SAP ECOFI, SAP GNS, Documentum, Dazel, SAU, VIKING, IVR, SIEBEL (CRM), EDITRAN, FTPU, Helplines, SIFCO, GIS, NORMA, distribution Portal, SGL WEB - Office Package (Visio, Access, Excel, PowerPoint, Word)
Contacts	INDRA: Alvaro Arguiñarena, Energy Manager, aarguinarena@indra.es INDRA: Pablo Fernández, Project Manager, pfpuente@indra.es EFRON: José Antonio González Díaz, FreeLancer, jagonzalezdiaz@gmail.com EFRON: Martin Sarro, Freelance, martinsarro@hotmail.com

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Project ERP consultant Freelance	**D. START**	**03/2012**
	D. END	**10/2012**

Company	**NUXE-Spain Makeup /Cosmetic sector**
Customer	**NUXE-Spain**
Projects Description	Design and parameters to adapt ERP Navision to the customer's business processes
Performed functions as a consultant	- Preparation of project documents: Plan of resources/matrix of responsibilities, timetable, plan of quality, catalogue of risks testing/Plan / Plan mitigation and contingency, communication Plan, drop Plan of Hummers, training Plan - Provision of requirements and scope - Management of change requests - Estimation of time, efforts and personnel required for the tasks. - Management tools necessary for communication between clients and suppliers (SharePoint, Testlink) - Control of the monthly and quarterly delivery of hours/rates for all resources
Technical environment	- Microsoft Project, Navision, SQL and other tools of personnel management, efforts and time estimation. - Office Package (Visio, Access, Excel, PowerPoint, Word) - EDI module
Contacts	NUXE: Sara Laso, Office Manager, slaso@nuxe.com NUXE: Helena Sola, Business Analyst, hsola@nuxe.com

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

SYSTEMS ENGINEER Intern	D. START	07/2009
	D. END	06 2011

Company	**La Salle**
Functions performed	- Maintenance and management of the systems used by the Department and the rest of the University -Trainer of University tools - Manager of the master's fellows - Classroom management - CAU students ONLINE - In charge of procurement of infrastructure of the Department and head of infrastructure projects
Projects Description	Of the final project with which it is possible to transmit live face-to-face students Online and record them for later playback. The project consists of the installation of all the necessary systems (servers, video storage, installation of environmental microphones, equalizers, timely network creation, deployments the necessary software, Ipcams) and its subsequent configuration.
Technical environment	- Moodle, MySQL, Telenet, Wireshark, AutoCAD, HTML, VMWARE - IPCAM, Roter, Swich, CISCO - Amplifiers, equalizers, microphones environmental sound - Patchpanels, table blends, Video servers, H264, Streaming Video - Pack Office (Visio, Access, Excel, PowerPoint, Word)
Contacts	LaSalle: Raquel Oneca, head of Department, roneca@salle.url.edu La Salle: Jordi Monfulleda. Systems engineer, jmonfulleda@salle.url.edu

Simulation Engineer NVH in A + (IDIADA) Intern	D. START	06/2008
	D. END	12/2008

Projects Description and functions implemented	- Real analysis and simulated acoustic (noise and vibration, NVH) of the Seat Ibiza 5 doors, in a multidisciplinary and international English-speaking environment - Adaptation of the model in AutoCAD to your meshing in EMF - Designs and execution of the tests Test for the actual model, analysis of results - Execution of the Test's test in the dummy model adapted to the actual results obtained by the model
Technical environment	- Nastran, Pastran, AutoCAD, C - Pack Office (Visio, Access, Excel, PowerPoint, Word) - Aniconic Room

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

INTERNSHIP IN VIDEO	D. START	09/2008
	D. END	07/2009
Company	**Salle La, Bonoloto, Meteo channel**	
Projects Description, functions implemented	- Video editing for customers of the University - Configuration of video to the live systems - Camera - Engineer of continuity	
Technical environment	-Patch Panels, H264, cameras, VideoPremie, Video signals, H262, H264, DVB (DVB-SI, DVB-T2/C/S2, DVBSubtitle, DVB-CI, CCU, MATRIX. Teletext, HbbTV, MPEG.	

Education

Bachelor

TITLE	**Telecommunication Engineer** La Salle University Barcelona	2010

Masters

TITLE	**Master Information Technologies Business Administration (MGTI/MITBA)** La Salle University Barcelona http://beslasalle.salleurl.edu/en/master-gestion-tecnologias-informacion-presencial-barcelona	2011
TITLE	**Master In Project Management certified by the PMI (MUDP/MPM),** La Salle Barcelona University Barcelona (scholarship) https://www.salleurl.edu/en/education/master-science-project-management	2012

Certificates and Courses

COURSES	1,2,3,4 By CISCO ACADEMY CCNA	2012
CERTIFICATE	Scrum Manager Certified, PUE, 15 PDU for PMI	2012
CERTIFICATE	PMI Agile Certified Practitioner (PMI-ACP), PMI	2014
COURSE	Estructura del Conocimiento en la gestión de proyectos, NETMIND, 35 PDUs for PMI	2011
COURSE	Scrum Manager Course	2012
COURSE	Integration CAD-CAM systems by the University of Oviedo	2004

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

Technical Knowledge

Tools

OTHER PROGRAMS & EXPERTISE	Level	Years
MS office	High	10
MS Project	High	7
MS SharePoint	High	5
TestRail	Medium	5
Redmine	High	8
Mantis	High	2
Jira	High	5
Testlink (test cases management tool)	High	2

OTHER PROGRAMS & EXPERTISE	Level	Years use
Git (Version Control)	High	6
CVS, SVN and Perforce (Version Control)	High	5
Installation and configuration of computers, IT	High	3
MATLAB (for modeling systems and digital control)	High	3
SPSS (statistical applications on databases and spreadsheets)	Basic	0.5
SeleniumRC, Selenium IDE, TestComplete, Imacro, FlexMonkey, FlexMonkium (test automation tools)	High	3.5
Sonar, PMD, Checkstyle, coverage (QA Tools code)	Basic	3
Jenkies, Hudson (continuous integration tools)	Medium	6

Software

DATABASES	Level	Years
Oracle (SQL, JDBC, Hibernate and using toad)	High	6
MySQL (SQL, JDBC, Hibernate and with direct consultations from console), Maria DB	Medium	4
PostgreSQL	High	4
SQL Server	Medium	2
NO relational Database (CouchBD, MongoDB)	Medium	3
Access (from the interface itself with forms) and Visual Basic	Medium	3

Luis Nabergoi Punete
Barcelona Spain
Tel +34 637 596 120

PROGRAMMING LANGUAGES	Level	Years
Java, J2EE, Java script	Medium	6
Web programming, Xml, Html 5, CSS,	Medium	6
WebLogic / Tomcat	Medium	5
Flex	Basic	0.5
Assembler (Motorola 68 k), assembler (8086)	Basic	1
Python, Django	Medium	7
Visual Basic 6.	Medium	2
C and C++ (with environments C ++ Builder, Eclipse and Visual Studio 2005)	Medium	3

OPERATING SYSTEMS	Level	Years
Windows level user and general administration	High	10
Linux-level programming in c Shell	Medium	6
Mac OS	High	6

Elections / Cyber

Incident Response Plan

For additional questions please contact the IT Ops Team at <phone number>

CONFIDENTIAL: DO NOT SHARE IN PUBLIC FORUMS

Version 1.x January 2021

Table of Contents:

SECTION 1: Protocol

1. Goals, Guidebook on Key Stakeholders
2. Cyber Incident Communications Flowchart
3. Cyber Incident Reporting Document Template
4. Contact Information / Escalation Matrix
5. Information Sharing Policy

SECTION-2: Communications Strategy

SECTION-1: Protocol

Goals:

The primary goals of this protocol include:

1. **Share** timely, relevant, and actionable **information** throughout the relevant team members and with our clients.
2. **Educate** the clients wherever necessary about security threats, probabilities, vulnerabilities, controls and responses.
3. **Create a secure information-sharing environment** that enables the availability and flow of accurate, timely, and relevant information, intelligence, and incident reporting.
4. **Connect client election officials** with support organizations, services, and products if needed.

Guidebook on Key Stakeholders <this section will be replaced with country specific version in place of the USA sample below>:

The responsibilities of key stakeholders include:

1. **Local entity or jurisdiction** that receives threat or vulnerability information from a private sector source or other information resource that affects the election sector typically shares any threat or exposure with their state office through established reporting channels.

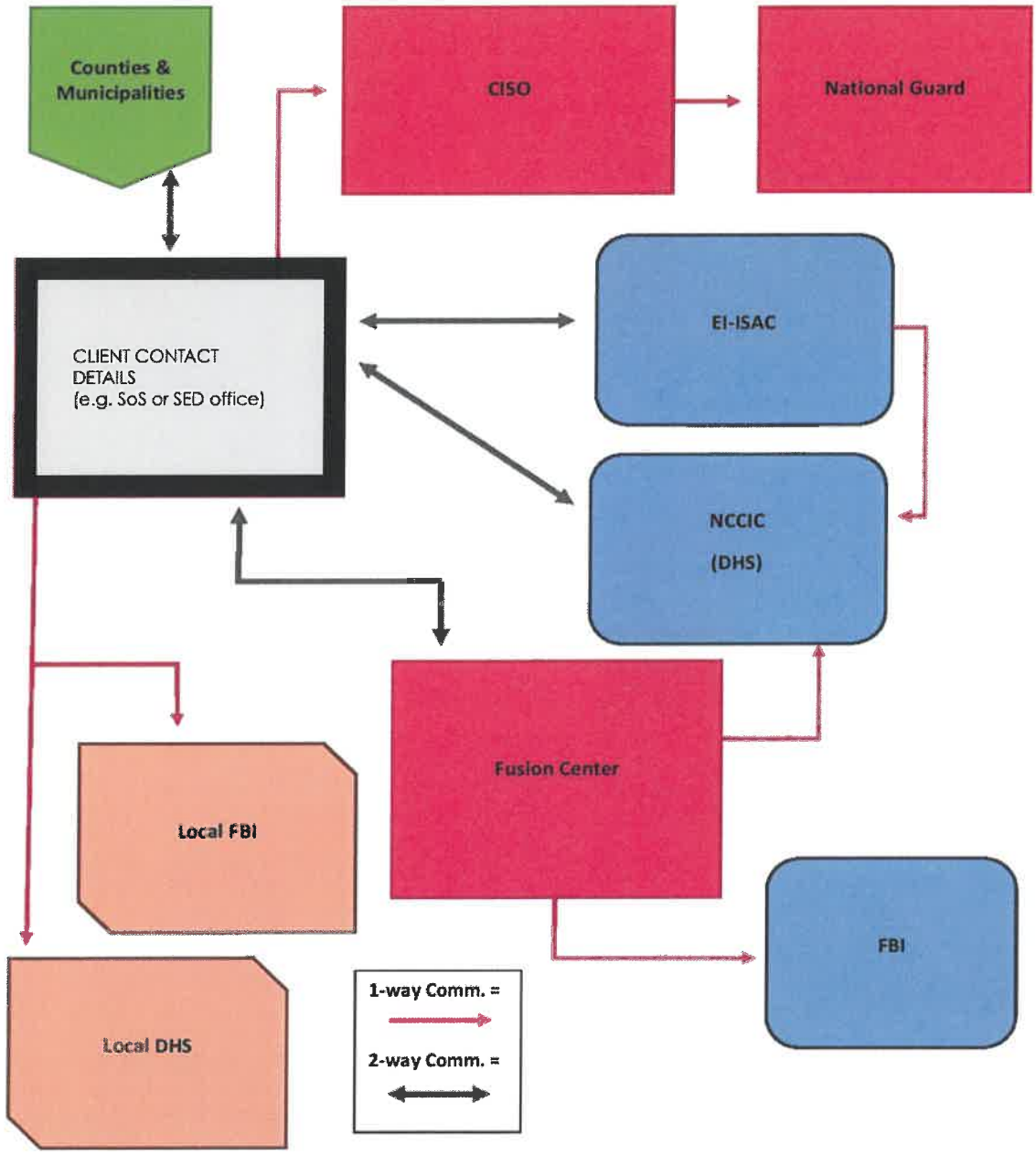
2. **Each state election official** is responsible for compiling and maintaining an updated State Incident Notification Contact List and will share that list with the EIS. This contact list includes state and local election contacts, CIOs, CISOs, fusion center contacts, state or regional DHS contacts, and applicable vendors.

3. **Department of Homeland Security** (DHS) works with other federal agencies representing law enforcement and the intelligence communities to identify, declassify whenever possible and as necessary, and make available any actionable threat information regarding the election sector in a timely manner. As necessary, DHS will relay classified information to any affected state or local election official with appropriate security clearance as soon as practical.

4. **EI-ISAC** will share threat information immediately with the Department of Homeland Security National Cybersecurity & Communications Integration Center (NCCIC), the Federal Bureau of Investigation (FBI) and relevant state or local entities using existing reporting mechanisms, concurrently as above, in a timely and actionable manner.

Cyber Incident Communications Flow Chart

<*this section will be replaced with country specific diagram in place of the USA sample below*>



Cyber Incident Reporting Document Template

<*template below is customized per client scenarios*>

Voatz

UOCAVA Mobile Voting Platform Security Incident Report (Sample)

CONFIDENTIAL

Copyright © 2018 by Voatz, Inc.
All Rights Reserved.

(Version 1.0 DRAFT - Last updated: November 26, 2018)

Cyber Incident Contact Information / Escalation Matrix

<*to be filled with the client specific information below*>

Organization	Contact (Title)	Phone(s)	Email
Voatz	Customer Support Team	\ - mobile	info@voatz.com
	IT Ops Team	\ - mobile	Itops.sec@voatz.com
Client	TBD	\ - direct \ - mobile	Client CISO Contact
Advisory Team	-	-	\
Local Law Enforcement	\ (Special Agent, Local Division)	\ - office	\

Information Sharing Policy

The communication policy for passing cyber threat intelligence to any third parties is as follows:

All cyber threat intelligence must be:

a. Reviewed by multiple personnel and validated as reasonably accurate and relevant;
b. If possible, allocated a traffic light protocol (https://www.us-cert.gov/tlp);
c. Allocated a threat severity rating (low, normal, high);
d. Communicated to the Client's office first if specific to a certain client;
    i. Primary POC:
e. Clients may, at their discretion, relay the intelligence to a third-party including DHS.

SECTION-2: Communication Strategy

Table of Contents:

1. *How to Use this Communications Plan*
2. *Guidelines for Communicating with the Media*
3. *Cyber Incident Escalation Decision Process*
4. *Crisis PR and Q&A*
5. *Appendix (TBD): Scenario Planning & Materials*
    a. *Scenario 1: Limited number of election server nodes compromised, no impact on election outcome*
    b. *Scenario 2: Incident impedes voting process/operations*
    c. *Scenario 3: Unsuccessful attempt to break-in*
    d. *Scenario 4: False rumors circulate on social media.*

How To Use This Communications Plan

This section includes:

- **Guidelines for Communicating with the Media:** This section provides practical guidance on communicating with the public via the media in a cyber-crisis.

- **Escalation Guidelines:** This table provides guidance on how to differentiate between high, medium, and low severity incidents and how to respond to each type.

- **Crisis PR Plan and Q&A:** Provides a response to be shared with media or other stakeholders if an interim statement is required while more complete information is gathered and a more thorough response is prepared.

Suggested Guidelines For Communication With Media

- **In most situations, a designated PR professional from the Voatz team or the Client Jurisdiction side should be fronting this aspect.**

- **Establish trusted media relationships before an incident.** Doing so will allow you to have more open conversations in the middle of the crisis. It will also mean that reporters have a baseline understanding of "normal" levels of cyber activity and less likely to make a big story out of a non-incident.

- **It is important to communicate with the public via the media.** Cyber incidents, especially in the elections arena, will be covered aggressively by both the cyber security beat reporters and the political beat reporters. You need to talk with both. If you don't, you risk having others tell your story, and it will likely be more hyperbolic and less factual than the actual story.

- **Focus your media responses on incident response—not the incident details or the agency.** The media will want to know how bad the incident is and whose fault it was. You are not obligated to weigh in on those questions. The best way to demonstrate competence is to be laser- focused on addressing the issue quickly and getting back to regular business.

- **Reporters will press for details on the incident, but avoid succumbing to pressure.** Assume everything you say is on the record, reflecting on the incident and the organization. As above, focus on the response.

- **Be aggressive about correcting errors by countering with the facts.** Reporters will seek information from a range of analysts and sources that may not be well informed. Quickly reach out to reporters to correct errors, and provide context, to prevent misinformation from spreading.

- **Avoid saying "no comment." It leaves the impression you have something to hide.**
  For example, instead of responding "no comment" to a question about incident details, you can say: "Cyber investigations take time, and will provide more information when we can." You can also explain, if appropriate, why it would be irresponsible to speculate before having all the facts.
  Speak about issues as directly as possible and avoid "wiggle words" like "so far as we know."

- **Work with journalists to counter misinformation.** Misinformation can easily spread from social media to traditional media outlets. Journalists may unknowingly re-post or quote messages that originated with fake accounts. Work with journalists before and during elections to provide accurate information and encourage them to ignore misinformation.

Cyber Incident Decision & Escalation Guidelines

The first critical decision you will need to make is whether there is a cyber incident, and if so, what the scale of it appears to be (at that point in time). Below is a guide to help make that determination, but you will need to use common sense and situational factors in making the final decisions about what the appropriate scale and next steps for escalation are in a given incident. ***Contact the IT Ops Team if you have any doubts about how to proceed.***

Severity of Incident	Key Considerations / Actions	Potential Key Communications Materials
Low Cyber incident that involves no PII and / or minor system disruptions that will likely not be visible to the public or affect the elections process.	• Prioritize stakeholders • Determine if formal notification to client is required • Communications to team members to get second opinions • Necessary communications to be determined based on the incident.	• Holding statement, in case of leak • Peer communication / email, if needed • Other necessary communications to be determined based on the incident.
Medium Cyber incident resulting in the loss or compromise of voter data or server nodes, but formal notification obligations may not be triggered. The issue begins to become public.	• Prioritize stakeholders • Determine if formal notification to client is required. • Determine if broader public communication is appropriate to maintain trust in the election system.	• Notification letters, if needed • Peer communication / email • Media statement and FAQ • Voter Communications • Jurisdiction election director communications / email • Website / social media materials
High Cyber incident that triggers local or international reporting obligations, affects a large amount of voter information, or is destructive to election operations	• Prioritize stakeholders • Determine if broader public communication is appropriate. • Determine what contact information we have for those affected. • Fulfill all client-reporting requirements.	• Notification letter(s) • Peer communication/email • Voter communications • Website / social media materials • Media materials • Legislator / policymaker materials • Jurisdiction election director communications / email • State Elections official talking points • Local County Elections official talking points

Crisis PR and Q&A

The draft holding statement and Q&A/FAQ will provide a basis for communications about any election-related, state-level cyber incident. They can be used as interim messages while additional facts are gathered. Answers to the Master Q&A can be used in conjunction with the scenario-specific Q&As and the Crisis PR plan prepared by the Voatz/Client Jurisdiction PR Teams.

General Cyber Incident Holding Statement

We are investigating a potential cyber incident affecting [NAME SYSTEMS, IF APPROPRIATE]. This incident may [DESCRIPTION OF POSSIBLE EFFECTS].

Our team is coordinating with [client contact and relevant law enforcement agency or agencies]. As you know, cyber investigations can take time, and we want to ensure that all information we provide is accurate. We will provide more information when we can.

The integrity of our election systems is the top priority for Voatz and we are working around the clock to address this matter as quickly as possible.

Master Q&A

Please refer to this PR document template <customized per client>.

tugboat logic

Voatz, Inc.

Information Security Program

November 22, 2021

Table of Contents

Table of Contents 2
InfoSec Policies 9
A.6 Organization of Information Security 10
Voatz, Inc. Internal Audit Policy 10
1.0 Purpose 10
2.0 Scope 10
3.0 Policy 10
A.6.2.1 Mobile Device Management 11
Voatz, Inc. Mobile Device Management Policy 11
1.0 Purpose 11
2.0 Scope 11
3.0 Policy 11
A.7 Human Resource Security 14
Voatz, Inc. Personnel Security Policy 14
1.0 Overview 14
2.0 Purpose 14
3.0 Scope 14
4.0 Policy 14
5.0 Enforcement 15
A.8 Asset Management 16
Voatz, Inc. IT Asset Management Policy 16
1.0 Overview 16
2.0 Purpose 16
3.0 Scope 16
4.0 Definitions 16
5.0 Policy 16
6.0 Enforcement 17
7.0 Responsibilities 17
8.0 References 18
A.9 Access Control 19
Voatz, Inc. Access Control Policy 19
1.0 Purpose 19
2.0 Scope 19
3.0 Business Requirements 19
4.0 User Access Management 20
5.0 User Responsibilities 21
6.0 System and Application Access Control 22
A.10 Cryptography 24
Voatz, Inc. Acceptable Encryption Policy 24
1.0 Purpose 24
2.0 Scope 24
3.0 Policy 24
4.0 Compliance and Exceptions 25
A.11 Physical and Environmental Security 26
Voatz, Inc. Physical and Environmental Security Policy 26
1.0 Overview 26
2.0 Purpose 26
3.0 Scope 26
4.0 Policy 26
5.0 Enforcement 27
A.12 Operations Security 28
Voatz, Inc. Operations Security Policy 28

1.0 Purpose 28
2.0 Scope 28
3.0 Business Requirements 28
4.0 Operational Procedures and Responsibilities 28
5.0 Protection from Malware 29
6.0 Backup 29
7.0 Logging and Monitoring 29
8.0 Control of Operational Software 29
9.0 Technical Vulnerability Management 29
10.0 Information Systems Audit 29
11.0 Enforcement 29
A.13 Communications Security 32
Voatz, Inc. Network Security Policy 32
1.0 Purpose 32
2.0 Scope 32
3.0 Definitions 32
4.0 Policy 32
5.0 Requirements 32
6.0 Enforcement 33
A.14 System Acquisition, Development and Maintenance 34
Voatz, Inc. Software Development Security Policy 34
1.0 Purpose 34
2.0 Scope 34
3.0 Business Requirements 34
4.0 Enforcement 35
5.0 Customer Notification 35
A.15 Supplier Relationships 37
Voatz, Inc. 3rd Party Vendors and Assessment Policy 37
1.0 Introduction 37
2.0 Scope 37
3.0 Managing Outsourcing Risks 37
4.0 Formal Outsourcing 37
5.0 Vendor Selection and Due Diligence 37
6.0 Contractual Issues 38
7.0 Sensitive Information 38
8.0 Informal Outsourcing 38
9.0 Third Party Physical Access and Operational Control 38
10.0 Risk Assessment 39
11.0 Enforcement 39
Appendix A: Vendor Compliance Survey 39
A.16 Information Security Incident Management 40
A.17 Information Security Aspects of Business Continuity Management 44
Voatz, Inc. Business Continuity Plan Policy 44
1.0 Purpose 44
2.0 Scope 44
3.0 Business Requirements 44
4.0 Enforcement 45
A.18 Compliance 46
Voatz, Inc. Information Security/Sensitivity 46
1.0 Purpose 46
2.0 Scope 46
3.0 Policy 46
4.0 Customer Information Handling 48
5.0 Exceptions and Enforcement 49
AC1 - Visitor Office Access 50

Voatz, Inc. Visitor and Contractor Premises Access Policy 50
1.0 Purpose 50
2.0 Scope 50
3.0 Policy 50
5.0 Responsibility 51
6.0 Penalties 51
AC4 - Mobile Device Encryption 52
Voatz, Inc. Mobile Device Encryption Policy 52
1.0 Purpose 52
2.0 Scope 52
3.0 Definitions 52
4.0 Policy 52
5.0 Enforcement 53
AC5 - Passwords 54
Voatz, Inc. Password Policy 54
1.0 Overview 54
2.0 Purpose 54
3.0 Scope 54
4.0 Definitions 54
5.0 Policy 54
6.0 Enforcement 56
AC6 - Remote Access 57
Voatz, Inc. Remote Access Policy 57
1.0 Purpose 57
2.0 Scope 57
3.0 Definitions 57
4.0 Policy 57
5.0 Enforcement 58
AC7 - VPNs 59
Voatz, Inc. Virtual Private Network (VPN) Policy 59
1.0 Purpose 59
2.0 Scope 59
3.0 Policy 59
4.0 Enforcement 59
AC9 - Server Security 60
Voatz, Inc. Server Security Policy 60
1.0 Purpose 60
2.0 Scope 60
3.0 Definitions 60
4.0 Policy 61
5.0 Enforcement 62
AC10 - Database Credentials 63
Voatz, Inc. Database Credentials Policy 63
1.0 Purpose 63
2.0 Scope 63
3.0 Definitions 63
4.0 Policy 63
5.0 Enforcement 64
AM1 - Equipment Disposal 65
Voatz, Inc. Equipment Disposal 65
1.0 Overview 65
2.0 Purpose 65
3.0 Scope 65
4.0 Policy 65
5.0 Enforcement 66

AU2 - Customer Support 67
Voatz, Inc. Customer Support and SLA Policy 67
1.0 Definitions 67
2.0 Customer Support 67
4.0 Service Management 67
5.0 Customer Requirements (SLA) 68
AU3 - Email Retention 69
Voatz, Inc. Email Retention Policy 69
1.0 Purpose 69
2.0 Scope 69
3.0 Policy 69
4.0 Enforcement 69
Backup and Restoration 70
Voatz, Inc. Backup and Restoration Policy 70
1.0 Purpose 70
2.0 Scope 70
3.0 Policy 70
Bring Your Own Device (BYOD) 72
Voatz, Inc. Bring Your Own Device (BYOD) Policy 72
1.0 Purpose 72
2.0 Scope 72
3.0 Expectation of Privacy 72
4.0 Policy 72
Data Retention and Disposal 74
Voatz, Inc. Data Retention and Disposal Policy 74
1.0 Purpose 74
2.0 Scope 74
3.0 Roles and Responsibilities 74
4.0 Retention of Data 74
5.0 Data Disposal 75
6.0 Suspension of Disposal in Event of Litigation or Claims 75
Disciplinary Policy 76
Voatz, Inc. Disciplinary Policy 76
1.0 Purpose 76
2.0 Scope 76
3.0 Communication of Disciplinary Action 76
IC1 - Email Use 77
Voatz, Inc. Email Use Policy 77
1.0 Purpose 77
2.0 Scope 77
3.0 Policy 77
4.0 Enforcement 78
IC2 - Email Authentication 79
Voatz, Inc. Email Authentication 79
1.0 Purpose 79
2.0 Scope 79
3.0 Policy 79
4.0 Enforcement 79
IC3 - Internet Usage 80
Voatz, Inc. Internet Usage 80
1.0 Summary 80
2.0 Internet Services 80
3.0 Usage Policies 80
4.0 Enforcement 82

IC6 - Removable Media 83
Voatz, Inc. Removable Media Policy 83
1.0 Overview 83
2.0 Purpose 83
3.0 Definitions 83
4.0 Scope 83
5.0 Policy 83
6.0 Enforcement 83
IC7 - Wireless Communication 84
Voatz, Inc. Wireless Communication Policy 84
1.0 Overview 84
2.0 Scope 84
3.0 Definitions 84
4.0 Policy Statement 84
5.0 Enforcement 85
IC8 - Workstation Security 86
Voatz, Inc. Workstation Security Policy 86
1.0 Purpose 86
2.0 Scope 86
3.0 Definitions 86
4.0 Policy 86
5.0 Enforcement 87
IC13 - Processing Integrity 88
Voatz, Inc. Processing Integrity Policy 88
1.0 Purpose 88
2.0 Scope 88
3.0 Definitions 88
4.0 Policy 88
5.0 Exceptions and Enforcement 89
Internal Privacy Policy 91
Voatz, Inc. Internal Privacy Policy 91
1.0 Purpose 91
2.0 Scope 91
3.0 What Personal Information we Collect 91
4.0 Individual's Responsibility to Inform Voatz, Inc. of Changes 92
5.0 How we Use Personal Information 92
6.0 How we Share Personal Information 93
7.0 Information Security/Data Protection 93
8.0 Information Retention 93
9.0 Individual Rights in Connection with Personal Information 93
10.0 Changes to this Privacy Notice 94
OM1 - Product/Services Scope 95
Voatz, Inc. Product/Service Scope Policy 95
1.0 Purpose 95
2.0 Scope 95
3.0 Program Review and Renewal 95
OM2 - Information Security Management System (ISMS) Policy 96
Voatz, Inc. Information Security Management System (ISMS) Policy 96
1.0 Voatz ISMS 96
2.0 Purpose 96
3.0 Scope 96
4.0 General ISMS Policy Statements 96
5.0 Program Review and Renewal 97
OM4 - Acceptable Use 98
Voatz, Inc. Acceptable Use Security Policy 98

1.0 Overview 98
2.0 Purpose 98
3.0 Scope 98
4.0 Policy 98
5.0 Enforcement 101
OM5 - Clean Desk 102
Voatz, Inc. Clean Desk Policy 102
1.0 Overview 102
2.0 Purpose 102
3.0 Responsibility 102
4.0 Scope 102
5.0 Policy 102
6.0 Enforcement 103
OM6 - Environmental Protection 104
Voatz, Inc. Environmental Protection Policy 104
1.0 Purpose 104
2.0 Principles and Policies 104
OM7 - Equality and Diversity 105
Voatz, Inc. Equality and Diversity 105
1.0 Policy 105
2.0 Our Commitment 105
3.0 Responsibilities of Management 105
4.0 Responsibilities of Staff 106
5.0 Third Parties 106
6.0 Related Policies 106
7.0 Rights of Disabled People 106
8.0 Monitoring 106
9.0 Grievances and Disciplinary Action 107
10.0 Review 107
OM8 - Corporate Ethics 108
Voatz, Inc. Corporate Ethics and Social Responsibility 108
1. Overview 108
2. Purpose 108
3. Scope 108
4. Policy 108
5. Enforcement 109
Privacy Policy for Websites 110
Voatz, Inc. Privacy Policy 110
Voatz, Inc. Privacy Policy (per voatz.com/privacy) 110
Risk Assessment and Risk Treatment Methodology 113
Voatz, Inc. Risk Assessment and Risk Treatment Methodology 113
1.0 Overview 113
2.0 Purpose 113
3.0 Scope 113
4.0 Definitions 113
5.0 Criteria for Performing Risk Assessments 114
6.0 Risk Assessment Process 114
7.0 Risk Management and Risk Treatment 114
8.0 Monitor and Review 114
9.0 Statement of Applicability (SOA) 115
10.0 Risk Treatment Plan 115
RM1 - Risk Assessments 116
Voatz, Inc. Risk Assessment Policy 116
1.0 Purpose 116
2.0 Scope 116

3.0 Policy 116
4.0 Risk Management 116
5.0 Enforcement 118
SO4 - Change Control and Configuration Management 119
Voatz Change Control & Configuration Management Policy 119
1.0 Purpose 119
2.0 Scope 119
3.0 Process/ Guidelines 119
4.0 Exceptions 120
5.0 Enforcement 120

InfoSec Policies

A.6 Organization of Information Security

The organization conducts Internal Audits on its existing policies and controls in order to ensure the best level of service to its customers.

Voatz, Inc. Internal Audit Policy

1.0 Purpose

Voatz is a small company and has no separate internal audit function. As a small company, internal audits are conducted informally as self assessments by Voatz IT Ops who will regularly review and test controls as a part of continuous improvement approach towards Voatz security posture.

Voatz IT Ops collaborates with other teams as necessary to oversee internal policies and procedures to ensure that they are operating effectively.

2.0 Scope

This policy applies to all Voatz, Inc. internal policies and procedures.

3.0 Policy

Voatz, Inc. is committed to maintaining a risk-based, efficient, effective and economical internal audit function. Accordingly, Voatz conducts regular internal reviews on their policies and controls regardless of SOC2/ISO audits. These reviews include the following:

- Evaluation of systems, processes and controls related to internal functions.
- Evaluation of new technologies being adopted by Voatz, Inc..
- Documentation of control failures and deficiencies, proposed corrective action plans for newly identified issues, and progress reports for the corrective action plans
- Tracking status by providing information and evidence to demonstrate actions taken to date, outlining actions still to be taken, and a revised implementation date if required.

A.6.2.1 Mobile Device Management

This policy defines procedures and restrictions for connecting mobile devices to organization's corporate network.

Voatz, Inc. Mobile Device Management Policy

1.0 Purpose

This policy defines procedures and restrictions for any and all end users with legitimate business use connecting mobile devices to Voatz, Inc.'s corporate network, digital resources, and data. The mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablets
- Portable media devices
- Laptop/notebook/ultrabook computers
- Wearable computing devices
- Any other mobile device capable of storing corporate data and connecting to a network

The primary goal of this policy is to protect the integrity of the confidential client and business data that resides within Voatz, Inc.'s technology infrastructure, including internal and external cloud services. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it could potentially be accessed by unauthorized resources.

A breach of this type may result in loss of information, damage to critical applications, loss of revenue, damage the Voatz, Inc.'s public image, breach our data privacy requirements, and violate data privacy laws.

2.0 Scope

- All employees, contractors, or personnel using a mobile device connected to Voatz, Inc.'s corporate network, and/or capable of backing up, storing, or otherwise accessing corporate data of any type, must adhere to this policy. Failure to do so will result in immediate suspension of that user's account, disciplinary action, and possibly termination of employment.
- All mobile devices, whether owned by Voatz, Inc. or owned by employees that have access to corporate networks, data and systems are governed by this mobile device management policy.
- Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorization by Voatz, Inc. IT Ops must be obtained.
- Applications used by employees on their own personal devices that store or access corporate data, such as cloud storage applications, are also subject to this policy.

3.0 Policy

3.1 Technology and Security Requirements

- Devices must be updated on a regular basis and use the latest OS available.
- If the user is storing passwords in the device, an encrypted password store must be used.
- Devices must be configured with a secure password that complies with Voatz, Inc.'s password policy. This

password must not be the same as any other credentials used within the organization. Employees agree never to disclose their passwords to anyone.

- Device must lock itself with a password or PIN if it's idle for five (5) minutes.
- Only devices managed by IT or authorized by IT will be allowed to connect directly to the internal corporate network.
- These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management (MDM) software whenever possible.
- Any attempt to contravene or bypass the MDM implementation will result in immediate disconnection from all corporate resources, and there may be additional consequences in accordance with Voatz, Inc.'s overarching security policy.
- All personal mobile devices attempting to connect to the corporate network through the internet will be inspected by Voatz, Inc.'s IT department. Devices that are not supported by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.
- When remote, devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection.
- Devices must have endpoint protection/anti-malware installed. Where possible this is supplied by Voatz IT Ops.

3.2 User Requirements

- Users may only load corporate data that is essential to their role onto their mobile device(s).
- Users must report all lost or stolen devices to Voatz, Inc. IT Ops immediately.
- If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with Voatz, Inc.'s incident handling process.
- Devices must not be "jailbroken" or "rooted"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources. Installation of applications from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact IT.
- Devices must be kept up to date with manufacturer or network provided patches. As minimum patches should be checked weekly and applied at least once a month.
- Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
- Devices must be encrypted in line with Voatz, Inc.'s compliance standards.
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in the body text or as an attachment, they must notify Voatz, Inc. IT Ops immediately.
- The user is responsible for the backup of their own personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

*To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

3.3 Remote Wipe

Mobile devices with the organization provided MDM solution gain the capability of being wiped remotely by Voatz, Inc. IT Ops department.

When a remote wipe is initiated by the user or the IT department, the user's mobile device will be wiped of all data and settings. Wiping data, documents, files, settings, and applications in the event a device is lost, stolen, or compromised in any way is critical to protecting our company and it's confidential data.

If a user requests a remote wipe all data stored on that device will be deleted. It is recommended that users backup their personal data frequently to minimize loss if a remote wipe is necessary.

A remote wipe will only be initiated if IT Ops/Security deems it appropriate. Examples of situations requiring remote wipe include, but are not limited to:

- Device is lost, stolen or believed to be compromised
- Device contains an app known to contain a critical security vulnerability that could expose the organization to harm
- Device is found to be non-compliant with company policy
- Device inspection is not granted in accordance with company policy
- Device belongs to a user that no longer has a working relationship with Voatz, Inc..
- The user decides they no longer wish to participate in accordance with this Mobile Device Management Policy.
- Termination of employment in which the user has not already cleared all Voatz, Inc. data by another method approved by IT.

A.7 Human Resource Security

Organization members understand their roles and responsibilities around security and privacy.

Voatz, Inc. Personnel Security Policy

1.0 Overview

Organizations need to set expectations around security for each employee and the different roles within the organization.

2.0 Purpose

This policy establishes the organization personnel security policy, for managing risks from personnel screening, onboarding, termination, transfer and management. The personnel security policy helps the organization implement security best practices with regard to personnel processes and events.

3.0 Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by the organization and covers all personnel.

4.0 Policy

4.1 Personnel Security Procedures

Voatz adheres to a formal personnel security procedure that addresses purpose, scope, roles, responsibilities, management commitment, and coordination.

4.2 Position Categorization

The organization shall:

- Document all roles and make job descriptions available.
- Assign a risk designation to all positions.
- Establish screening criteria for individuals filling those positions.
- Conduct performance evaluations and review and revise position risk designations on an annual basis.

4.3 Personnel Screening

The organization must screen individuals prior to access to sensitive information. In addition, the organization must rescreen individuals every seven years.

4.4 Personnel Onboarding

The organization must upon personnel start:

- Provide onboarding guidance via handbook, intranet, etc.
- Obtain a signed NDA and prior inventions agreement
- Obtain signed employment agreement with security and privacy expectations

4.5 Personnel Termination

The organization must upon personnel termination:

- Terminate information asset access.
- Conduct exit interviews.
- Retrieve all security-related organizational information system-related property.
- Retain access to organizational information and information assets formerly controlled by terminated personnel.

4.6 Personnel Transfer

The organization must review logical and physical access to information assets and facilities when personnel are re-assigned or transferred to other positions within the organization.

4.7 Third-Party Personnel Security

The organization must:

- Establish personnel security requirements including security roles and responsibilities for third-party providers.
- Document personnel security requirements.
- Monitor provider compliance.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.8 Asset Management

The organization closely manages IT systems and the data that they contain from purchase to disposal.

Voatz, Inc. IT Asset Management Policy

1.0 Overview

Asset management is the process of receiving, tagging, documenting, and disposing of equipment. It is important to maintain up to date inventory and asset controls to ensure that equipment locations and dispositions are understood. Lost or stolen equipment can contain sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

2.0 Purpose

This policy provides procedures and protocols supporting effective organizational asset management specifically focused on electronic devices.

3.0 Scope

This policy applies to all organization members.

4.0 Definitions

"IT Asset" - refers to anything (tangible or intangible) that has value to an organization, including, but not limited to, a computing device, IT system, IT network, IT circuit, software (both a installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards), as well as people and intellectual property (including software).

5.0 Policy

5.1 Asset Types

The following asset types are subject to tagging and tracking:

- Desktop workstations
- Laptop computers
- Mobile Devices (Tablet devices, Smartphones)
- Printers, copiers, fax machines, and multifunction print devices
- Scanners
- Servers (on-premise, cloud, remote)
- Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), wireless access points, and storage)
- Memory devices

5.2 Asset Value

Assets of value less than $250 shall not be tracked, including computer components such as smaller peripheral devices, keyboards or mice. Assets, which store data, regardless of cost, shall be tracked as part of a computing device or as a part of network attached storage. These assets include:

- Network Attached Storage (NAS), Storage Area Network (SAN) or other computer data storage
- Temporary storage drives
- Tape or optical media with data stored on them including system backup data

5.3 Asset Tracking Requirements

The following procedures apply to asset management activities:

- All IT assets purchased by the organization tracked must be tracked in a central location.
- An asset-tracking database shall be created to track assets. It shall minimally include:
  - Make, model, and descriptor
  - Serial Number
  - Location
  - Type of asset
  - Owner
  - Department
  - Disposition
- All assets must be assigned to individual users or to a department who will be responsible for their care and security at all times whether they are in use, storage or movement.

5.4 Acceptable Use and Management

All assets purchased by the organization are the property of Voatz, Inc. and will be deployed and utilized in a way that is deemed most effective for addressing the organization's need and objectively demonstrated value for money.

Individual users or departments will be held responsible for protecting the IT assets that have been assigned to them against physical or financial loss whether by theft, mishandling or accidental damage by using appropriate physical security measures.

Additionally, users will ensure any software installed on devices is legitimately purchased and licensed for the use made of it.

5.5 Asset Disposal and Repurposing

Refer to the established AM1 - Equipment Disposal Policy for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

6.0 Enforcement

Any actual or suspected violation of this policy must be reported to Information Technology via the most suitable channel.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Responsibilities

Voatz IT Ops is responsible for implementing this policy. This team will be responsible for:

- Coordinating IT asset audit activities and updating and maintaining the accuracy of the asset inventory
- Checking IT equipment is returned in the same configuration as expected;
- Administrating the control and security of IT equipment held in stock for issuing and awaiting reissue or disposal;
- Ensuring that all IT equipment is returned to Voatz upon replacement or when the holder leaves the organization
- Ensuring that any IT asset that is retired is disposed of according to the Equipment Disposal policy
- Giving appropriate advice to users on the correct handling of IT assets; and
- Reporting any incorrect disposal or misuse of an IT asset

End users issued with IT assets will be responsible for:

- Retaining responsibility for IT equipment issued to them until it has been returned to Voatz IT Ops for redeployment or disposal;
- Reporting the loss or theft of IT asset immediately to Voatz IT Ops;
- Ensuring that IT assets are not moved to another location or transferred to another person without the consent of Information Technology;

- Reporting any defects and returning IT assets immediately that are not operating normally to Information Technology;
- Returning all IT equipment to Voatz IT Ops upon replacement, when it is no longer required for business or when the holder leaves the organization.

8.0 References

- AM1 - Equipment Disposal Policy

A.9 Access Control

The organization actively manages risks around user account management, access enforcement and monitoring, separation of duties, and remote access.

Voatz, Inc. Access Control Policy

1.0 Purpose

This policy ensures access to information assets and systems within Voatz, Inc.'s corporate and election environments is actively managed in accordance with the principles of least privilege.

2.0 Scope

The scope of this policy is applicable to all information assets and systems owned or operated by, or on behalf of,Voatz, Inc. to include on-premises and cloud assets. This includes information processed by Voatz, or its suppliers, on behalf of Voatz' customers.

All users (Voatz, Inc. employees, contractors, vendors or others) of Voatz' systems are responsible for adhering to this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.0 Business Requirements

Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

The control of access to Voatz' information assets is a fundamental part of a defense in depth approach to information security. In order to protect the confidentiality, integrity and availability of valuable assets effectively, a comprehensive mix of physical and logical controls shall be implemented.

The access control measures implemented shall be appropriate to the business requirements. These requirements may depend on factors such as:

- The security classification of the information stored and processed by a particular system or service;
- Relevant legislation that may apply e.g. Data protection legislation;
- The regulatory frameworks in which Voatz and its systems operate;
- Contractual obligations to external third parties;
- The threats, vulnerabilities and risks involved

Business requirements shall be established as part of the requirements-gathering stage of new or significantly changed systems and services and shall be incorporated in the resulting design.

In addition to the specific requirements, a number of general principles will be used when designing access controls for Voatz' systems and services. These are:

- Defense in Depth – security shall not depend upon any single control but be the sum of a number of complementary controls;
- Least Privilege – the default approach taken shall be to assume that access is not required, rather than to assume that it is. In particular, all access to election infrastructure and election data shall be limited to those individuals that have a business or legal need-to-know;
- Need to Know – access is only granted to the information required to perform a role, and no more. The default setting of the access control system has to be "deny-all";
- Need to Use – users will only be able to access physical and logical facilities required for their role.

The following table illustrates at a high level who is authorized to access which systems:

System type	Who typically requires access
Corporate network	Voatz team members
On-premise collaboration systems	Voatz team members with a need to use the system concerned.
Cloud-based collaboration systems (e.g. Jira, Dropbox, Confluence, Slack)	Voatz team members with a need to use the service concerned.
Critical corporate systems (e.g. finance)	A restricted set of Voatz team members with a need to use the system concerned.
Elections Systems	A restricted set of Voatz team members with a need to use the system concerned.

All Voatz team members have access to the Voatz Corporate network via secured access to Voatz dedicated wireless network (when on premises) or via Voatz Corporate VPN when working remote. Access to additional services (e.g., Jira, Confluence, Dropbox, Slack) is granted on an as needed basis, depending on the role of the user and managed through an LDAP server/service.

4.0 User Access Management

4.1 User Registration and De-registration

Voatz IT Ops is responsible for registering and de-registering users. They shall establish and maintain an agreed process for the registration and de-registration of users. The process shall ensure that:

- The request to register or de-register a user has come from someone with appropriate authority and shall be auditable.
- A record of the request and the action taken is kept for audit purposes.
- De-registration of users is done in a timely manner.

Each user shall be assigned a unique user account with a unique username that is not shared with any other user and is associated with a specific user.

Generic and shared users (where an account is used by more than one person) should not be created unless there is a valid business reason, e.g. test users that are used exclusively for system testing. Any generic or system accounts shall have an identified owner who must ensure such accounts are reviewed regularly.

4.2 User Access Provisioning

Voatz IT Ops is responsible for assigning and revoking access rights for all user types to all systems and services. They shall establish and maintain agreed upon processes for managing the user access rights. These shall ensure that:

- Requests to assign or revoke access have come from someone with appropriate authority, in writing (via email, ticket or similar method that is clearly linked back to the requesting party).
- The request is in line with the principles described in section 3.0 above, ensuring that the requested access is in line with the roles and responsibilities of the user.
- Requests are sufficiently granular, e.g. being specific about which folders, channels, groups or similar the user should be granted access to within an application or system.
- The request is actioned in a timely manner, especially in the case of a revocation.
- Access is granted on a permanent or temporary basis as appropriate. Where temporary access only is required, then temporary only should be granted.
- A record of the request and the action taken is kept for audit purposes.

Access to critical corporate and election systems shall be managed and controlled by the Voatz IT Ops Super User(s).

4.3 Management of Privileged Access Rights

The allocation and use of privileged access rights shall be restricted and controlled.

[A limited number of people in Voatz have privileged access rights[SP1] . These are directly controlled by Voatz CEO and CTO]

[SP1]Is this generic to all systems - collaboration, critical corporate and election systems. How is the list of who has these controls managed, e.g. is their a list? who manages it? I've uploaded a list to dropbox that we'd initially uploaded as evidence for the controls for this policy.

4.4 Management of Secret Authentication Information of Users

The allocation of secret authentication information shall be controlled through a formal management process.

[Users select their own passwords. Where Voatz IT Ops issues initial passwords, these are sent out of band and users are asked [SP1] to change their passwords and any default passwords.]

[SP1]Are they asked or forced to change their passwords? - A bit of both. We ask them to change it but for employee accounts managed by LDAP the passwords expire every 60-90days and everyone is forced to change them.

4.5 Review of User Access Rights

User access rights shall be reviewed by Voatz IT Ops periodically to ensure that user access is consistent with user roles and in line with the principles described in section 3.0 above.

In addition access to systems and applications shall be reviewed under the following conditions:

- A new user requires access for the purpose of fulfilling job responsibilities
- An existing user has a change in job function requiring a change in role and privileges
- A user ceases to have a particular role, leaves Voatz or no longer needs access to the system or application

4.6 Removal or Adjustment of Access Rights

Voatz IT Ops are responsible for ensuring that the access rights are removed or adjusted as required based on changes in a user's role, status or access requirements. The applies to all users – employees, contractors and other authorized third parties.

When a user leaves Voatz under normal circumstances access shall be removed at the close of business on the user's last working day. It is the responsibility of HR (for employees and contractors) and the relationship manager (for authorized third parties) to notify Voatz IT Ops that the user is leaving and request the suspension of access rights.

When there is a perceived risk (e.g. termination of employment on disciplinary grounds) removal of access may be actioned sooner.

User accounts shall initially be suspended or disabled only, for a period of 90 days prior to deletion.

5.0 User Responsibilities

5.1 Use of Secret Authentication Information

Users are responsible and accountable for safeguarding personal authentication information, passwords and other secrets. Such information shall not be written down or stored in a manner that could be accessible to others.

[Users are asked to select strong passwords/passphrases of a certain minimum length; not to store passwords ; to use a password manager; to implement multi-factor authentication wherever possible[SP1] .]

[SP1]This should not be a user responsibility but enforced by the organisation-

6.0 System and Application Access Control

6.1 Information Access Restriction

Voatz aims for a layered approach to manage access to corporate and elections assets which includes:

- Disabling all ports or services on critical assets not needed.
- Setting access control lists for systems components to default deny all unless privilege to a particular function is explicitly allowed.
- Implementing multi-factor authentication and strong passwords on accounts wherever possible.
- Reserving the right to disconnect devices or disable services without notification.
- Not permitting the use of shared account credentials.
- Ensuring credentials (including passwords, pin, tokens, etc) are not hardcoded in source code, configurations files, or stored any other insecure location.
- Permitting use of guest/anonymous and temporary accounts only in the test environment
- Limiting access to data labelled sensitive or confidential.

All Voatz, Inc. systems must enforce approved authorizations for access to the system in accordance with applicable policy and users requiring access must receive approval directly from the system/application owner.

Voatz follows least privilege when granting access to information and application system functionality.

Additionally, access to information/data deemed sensitive or confidential is limited based on a need to know.

Read-only access is granted to most users, while functions that allow users to create, modify, or delete information is restricted to designated super users/admins. (E.g., Only admins can create or delete code repositories, while developers are restricted to adding new code, and editing existing code. Only a super admin or designated alternate with super admin access can push code to the live/production environment.

6.2 - Secure Log-on Procedures

Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.

[Users must enable multi-factor authentication for all internal applications [SP1] and third party applications used for internal operations (e.g. Slack, Dropbox, mail, etc.)]

[SP1]Is this true? Certainly I would expect MFA for some systems but not necessarily all, especially when being access from within the company network or over VPN.

For Team collaboration tools (Jira, Confluence) no MFA

For Slack, Dropbox, Zoho (mail) Users are asked to enable MFA

6.3 - Password Management System

Password management systems shall be interactive and shall ensure quality passwords.

[Voatz does not have a Password Management System][SP1]

[SP1]This needs to be addressed.

6.4 - Use of Privileged Utility Programs

Access to utility programs should be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of a named project or change.

Utility programs capable of overriding system or application controls must be implemented using the following principles where possible and appropriate:

- Where possible and appropriate privileged utility programs must incorporate multi-factor authentication (MFA);
- Utility programs must have secure authentication mechanisms that use identification, authentication and authorization and accounting/audit procedures;
- Utility programs must be limited to the minimum practical number of trusted, authorised users;

- Where possible role-based access control and constrained interfaces must be used to provide granular access to privileged utility programs;
- All utility program usage must be logged.

[Need a list of Privileged Utility programs- Currently Sophos Endpoint Protection; Nessus (Vulnerability Scanner but we're not running credentialed scans (need to confirm)]

6.5 - Access Control to Program Source Code

Source code shall be managed using on-premise repositories that segregate the code into the major parts of the service - Frontend (mobile apps, web application), Backend (server, database, blockchain). Developers shall be grouped according to their areas of responsibility and only been given access in the necessary repositories.

Once source code is ready for production (after successful completion of QA/testing) a single super user has the necessary access to push code into production.

The following principles must be adhered to where possible:

- Program source code must not be held in operational systems where possible;
- Accountable and responsible asset and system owners must establish procedures to manage program source code and program source code;
- Support personnel must not have unrestricted access to program source libraries;
- Updates to program source code and associated items, and the issuing of program sources to programmers must only be performed in line with established procedures and after appropriate authorization has been received;
- Audit logs must be maintained for all accesses changes to program source code;
- Maintenance and copying of program source code must be performed in line with applicable Change Control Procedure

A.10 Cryptography

The organization utilizes the latest commercially accepted encryption protocols.

Voatz, Inc. Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope

This policy applies to all Voatz, Inc. employees and affiliates.

3.0 Policy

3.1 Encryption Method and Application

All Voatz, Inc. encryption shall be done using approved cryptographic modules. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Voatz, Inc.'s key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows. All private keys for encryption must be password protected and not stored in the clear on systems.

Encryption shall be implemented in:

- All web applications via the most secure version of SSL/TLS
- Device/file encryption i.e. partial disk encryption and full disk encryption
- During data transmission between and among infrastructure components
- During sensitive data transmission over public networks
- storage on disk, particularly secrets and user passwords
- App/client source code to secure voter data and selections
- App/client communication with back end infrastructure

3.2 Proprietary Encryption Algorithms

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts and approved by Voatz, Inc. IT Ops. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

3.3 Data Protection

- **Data at rest:**
  - All Voatz, Inc. and customer data deemed a secret shall be stored in an encrypted manner.

- **Data in motion:**
  - All data sent or received outside of Voatz, Inc. data centers and cloud environments (corporate and elections networks) shall be encrypted for transmission.
  - Where possible, data exchanged inside the Voatz, Inc. network should be encrypted

3.4 Digital Signature

- Digital signatures can be used on documents as proof of identity. All digital signatures shall only use algorithms approved by IT Ops.

3.5 User Passwords

- Where applicable, user passwords shall be stored in a secure manner by using HMAC with hash.
- All user passwords should be salted on a per secret basis.
  - The salt should be random.
  - The salt size should be the same length as the output of the hashing function.
  - The salt should not be considered a secret.

*** Voatz, Inc. shall not use other algorithms/hashing functions other than those specified in the controls.

3.6 Key Management

Key management should be planned which will include secure key generation, use, storage, distribution, recovery, and removal. Currently, Voatz does not store or distribute keys. Key generation and exchange is a part of the mobile application initial handshake between the smartphone clients, and back end servers, however, once a shared secret is established, the keys are automatically deleted.

- **Generation:**
  - Cryptographic keys must be generated and stored in a secure manner that prevents loss, interception, theft, or compromise.
  - Key generation must be seeded from an industry standard random number generator.
- **Key Removal:**
  - Key removal shall occur after an archival phase and after adequate analysis to ensure that loss of that key will not correspond to loss of data or other keys.

4.0 Compliance and Exceptions

All vendors must be evaluated for their compliance with Voatz, Inc. encryption policy.

Any exceptions to the policy must have written approval from Information Technology.

A.11 Physical and Environmental Security

The organization protects managed systems and personnel from unauthorized access and from natural and human caused damage or destruction.

Voatz, Inc. Physical and Environmental Security Policy

1.0 Overview

The Physical Security and Environmental Policy is implemented in order to ensure the safety of the organization systems as well as physical resources and personnel on the organization premises.

2.0 Purpose

The purpose of the Physical and Environmental Security Policy is to establish controls to prevent unauthorized physical access to assets and protect them from damage, interruption, misuse, destruction and/ or theft or from damage, destruction and/ or interruption due to environmental factors such as fire, humidity, water, power outage, etc.

3.0 Scope

The Physical Security and Environmental Policy applies to all organization systems, facilities and personnel. Where assets are located on premise, Voatz will leverage and verify existing controls implemented by the shared office space provider in addition to any controls Voatz has implemented within its internal office space. Where assets are in remote environments, Voatz will leverage the controls in place by the third party datacenter or cloud service provider.

Elements of our on-premise physical and environmental security are reliant on our shared office space host. Our provider requires access badges for anyone entering office areas. Visitors must sign in at visitor control at the entrance which is monitored by security guards. Cameras are controlled by our host and monitor activity throughout the building. Voatz is located in a dedicated, locked office space.

4.0 Policy

4.1 Physical Access Authorization

- Develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
- Establish a process to review, approve, and issue credentials for facility access.
- Remove individuals from the facility access list when access is no longer required.

4.2 Physical Access Control

The organization will control entry/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).

- Maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
- Employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
- Perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.
- Establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.

- Change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

4.3 Access Control for Transmission Medium

The organization shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).

4.4 Monitoring Physical Access

Review physical access logs at a defined frequency and upon occurrence of security incidents.

4.5 Power Equipment and Cabling

Place power equipment and cabling in safe locations to prevent environmental or human damage and destruction.

4.6 Emergency Shutoff

Provide the ability to shut off power to data center during an incident.

- Place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.
- Implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.

4.7 Data Center Emergency Power

The organization has uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power loss.

4.8 Data Center Fire Protection

The organization shall install and maintain fire detection and suppression devices that are supported by an independent power source.

- Use fire detection devices/systems that activate automatically and notify emergency personnel and emergency responders in the event of a fire.
- Use an automatic fire suppression system if/when the data center is not staffed on a continuous basis.

4.9 Data Center Temperature and Humidity Controls

The organization has automatic temperature and humidity controls in facilities to prevent fluctuations potentially harmful to processing equipment.

- Use temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

4.10 Data Center Water Damage Protection

The organization protects processing equipment from damage resulting from flooding or water leakage.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.12 Operations Security

Policy to ensure organization operational processes meet information security requirements and objectives

Voatz, Inc. Operations Security Policy

1.0 Purpose

The purpose of this policy is to guide Voatz, Inc. to plan, implement and control the operational processes needed to meet information security requirements, address risks, and implement plans to achieve information security objectives as identified in the Voatz Information Security Policy.

2.0 Scope

This policy covers all Voatz, Inc. operations and functional areas.

3.0 Business Requirements

Voatz, Inc. will operate in a manner that meets its Information Security Objectives. As listed in the Information Security Policy, these objectives include:

- Operating a voting platform that meets the confidentiality, integrity and availability requirements of jurisdictions around the world
- Continuously improving the Voatz service by keeping technology up to date, employing additional security controls where these make sense to maintain a strong security posture a
- Proactively managing risks.

Voatz, Inc. processes are designed to meet information security requirements of its corporate and elections operations.

The following environments are involved with Voatz Operations:

- Corporate Environment (on-premise employee laptops and on-premise servers including JIRA, Confluence, etc.and some test servers in AWS and Azure)
- Mobile/Elections Environment (including the app, cloud hosted core servers, databases, blockchain)

4.0 Operational Procedures and Responsibilities

4.1 Operating Procedures

Voatz has both on-premise and cloud (remote) based information processing facilities. On-premise facilities support the operation of the corporate network/infrastructure and are jointly protected by controls of our hosting provider and Voatz implemented access controls. Voatz leverages the security of cloud providers for the cloud based information processing facilities. Voatz shall implement controls to ensure the correct and secure operation of both its corporate and elections infrastructure. This shall include:

- Documented operating procedures with defined owners covering the key operational tasks
- Defined change management processes (see XXX) ensuring that change, whether to systems or business processes, is only introduced in a controlled and secure manner
- Clear separation of development, test and production environments to ensure that only authorized changes can be made in each environment in line with each environment's purpose.
- Monitoring and planning to ensure that environments (especially production) can support the required performance.

5.0 Protection from Malware

A defense in depth approach shall be taken to protect Voatz from malware including, as a minimum:

- **Firewalls**: these shall be installed at all points where internal networks are connected to the internet. Further requirements on firewall configuration and maintenance are contained in the Communications Security Policy.
- **Anti-virus**: this shall be installed on all key devices including firewalls, proxy servers, all servers and all end-user devices
- **Threat monitoring**: information about emerging threats shall be obtained from appropriate sources and necessary action taken, e.g. ensuring that users are alerted proactively of potential attacks.
- **Security Awareness Training**: as phishing it is a major delivery mechanism for malware, Voatz conducts regular security awareness training.

6.0 Backup

Voatz implements data lost prevention polices on its corporate network to detect the exfiltration/movement of sensitive information to destinations outside of the environment. (need to check - currently dlp enabled on in Sophos endpoint management console for laptops monitored by Sophos agents but not sure about the rest of the network)

7.0 Logging and Monitoring

Voatz centralized collection of logs captures events from sources on the corporate and elections infrastructure. Logging activities have also been configured to trigger alerts for unusual or suspicious activity. (need to verify if alerting is in place)

8.0 Control of Operational Software

Voatz monitors systems to detect unauthorized access and modification. (Need to confirm this is true and to what extent. Probably need to establish a baseline first and detect deviations from normal). Additionally Voatz has documented Backup and Recovery procedures and checklists to ensure in the event of an incident, operational systems are able to perform with minimum disruption. Voatz also follows least privilege to limit the access to critical systems and limit the ability to make changes.

9.0 Technical Vulnerability Management

Voatz, Inc. conduct regular vulnerability scans for all internal and external assets to identify known vulnerabilities. (need to verify)

Voatz also engages external security experts to conduct penetration testing.

Voatz receives information regarding vulnerabilities from multiple external sources to include vendor security advisories, public sources, vulnerability databases, and vulnerabilities reported via the Voatz bug bounty program.

Voatz limits lateral movement through the network by implementing least privilege and segregating the network into corporate and elections, and further into development, test, and production environments with limited and monitored access across. (need to verify)

10.0 Information Systems Audit

For hosts in production, scans and other audit activities must be scheduled to run during times that minimize disruption to live events. Logging is automated and backup jobs are scheduled to run during off hours.(need to verify)

11.0 Enforcement

It is every one's responsibility to ensure operational security of Voatz, Inc. and its products or services. Failure to do so may be subject to disciplinary action, up to and including termination of employment.

Controls

A.12.1.1 - Documented Operating Procedures

[See procedures associated with this policy]

A.12.1.2 - Change Management

[See procedures associated with this policy]

A.12.1.3 - Capacity management

[Some load testing conducted on elections infrastructure to ensure performance for elections of various sizes. Additional monitoring for capacity, performance, and load is done by Nagios installed on corporate network.]

A.12.1.4 - Separation of development, testing and operational environments

[There is some separation but the boundary is not clear, perhaps due to the way the app stores handle Beta and Test version of the app and how those are connected to their respective live versions. Prior to this, need to understand the separation of the environments we do have control over.][SP1]

[SP1]The level of required separation should be defined, i.e. what is the team not allowed to do in terms of connecting environments together.

Also if there are cases where there is not strict separation the required controls/mitigation in place to protect each environment should be s

[Still need to investigate.]

A.12.2.1 Controls against malware

[Employee laptops have enterprise anti-malware/endpoint protection installed and servers are running a capability that detects changes as indicators of the presence of malware. Need info on product.]

A.12.3.1 Information backup

[See Voatz Business Continuity and Disaster Recovery Plan and Procedures]

A.12.4.1 Event logging

[We have it to some extent but probably need more - need to check]

A.12.4.2 Protection of log information

[Not sure where this is stored-Need to check]

A.12.4.3 Administrator and operator logs

[Need to double check what is being logged]

A.12.4.4 Clock synchronization

[See updated control language]

A.12.5.1 Installation of software on operational systems

[See procedures associated with this policy]

A.12.6.1 Management of technical vulnerabilities

[See procedures associated with this policy]

A.12.6.2 Restrictions on software installation

[See procedures associated with this policy]

A.12.7.1 Information systems audit controls

[Currently use graylog for centralized logging. Need info on what we audit/log in each environment, how long the

logs are stored, how they are protected, etc.][SP1]

[SP1]I think this requirement is more around how operational processes are audited and ensuring that the audits do not impact the ongoing business.

[Don't believe current operational process are audited. Would the post elections audit fall under this?]

A.13 Communications Security

Voatz, Inc. provides a protected, interconnected computing environment through the use of securely configured network devices to meet organizational missions, goals, and initiatives.

Voatz, Inc. Network Security Policy

1.0 Purpose

The purpose of this policy is to ensure the availability and reliability of network devices to ensure safe and secure connections to the information assets owned by Voatz, Inc..

2.0 Scope

This policy applies to all network devices, (includes switches, firewalls, and wireless access points) that are owned and managed by Voatz, Inc..

3.0 Definitions

IPsec- Internet Protocol Security- a secure network protocol suite that authenticates and encrypts the packets of data sent over an Internet Protocol network. IPsec can automatically secure applications at the IP layer.
MFA- Multi-Factor Authentication- a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

4.0 Policy

- Network devices owned and managed by Voatz, Inc. must be configured securely and designed to secure network traffic between trusted and untrusted network zones.
- Every network device deployed in the Voatz, Inc. network shall be appropriately configured and meet security requirements for their individual purposes (internal, public facing)
- All traffic and protocols should be expressly denied except for those necessary for business purposes
- All the traffic to and from a particular list of IPs and Domains (Blacklisted) should be denied at the Firewall Level

5.0 Requirements

5.1 Physical Security

Network devices must be located in a locked room and not accessible to unauthorized personnel. Devices must have adequate cooling, a reliable power supply and/or plugged into a right-sized uninterruptible power supply (UPS). Wireless access points should either be in a locked room or located high on the ceiling where it would be obvious if someone were physically accessing the device.

5.2 Privilege Access Control

- Privileged access to prevent configuration changes should be restricted to authorized personnel only.
- Passwords shall follow strong password mechanisms outlined under the Password Guidelines.
- Access control shall be used to provide separate authentication, authorization, and accounting services for network-based access.
- A Privileged Access Management solution can control credentials accessing the device and commands that can be executed when a session is initiated, providing a complete audit of both commands and sessions.

5.3 Enable logging

Logging should be enabled, also include log configuration changes, preferably back to a central source like a Syslog server or a centralized log management platform.

5.5 Backup network device configuration

Network device configuration is backed up regularly whenever configuration changes are made each day or every week to a central source. The central backup source shall be secured as well.

5.6 Switch security

Switch ports shall be locked down by configuring port security features allowing access only to the first authorized device connecting to that port.

5.7 Wireless access points security

Wireless points shall be secured in accordance with the Voatz, Inc. Wireless Communication Policy.

5.8 Network design and audits

- Network design shall allow legitimate traffic to flow through the appropriate zones, segments and/or resources and unwanted traffic detected and dropped. Firewalls, VPNs, Virtual Local Area Networks (VLANs) and/or Access Control Lists (ACLs) shall be implemented to achieve the same.
- Development/testing, production, and corporate resources should not be in the same network segments.
- The network diagram should provide an overview of network devices deployed, network traffic flows and should identify physical and/or logical security controls that are in place to direct legitimate traffic and detect & drop unnecessary or unwanted traffic.
- Firewall policies and ACLs shall be tested to ensure that the traffic is permitted or denied according to the firewall rule. Network shall be audited based on the network diagram by conducting vulnerability scans and penetration tests on strategic areas in the network and mitigating identified high risks.

5.9 Encrypt sensitive network traffic

Appropriate encryption and authentication methods should be used for the transmission of sensitive data and remote access.

5.10 Develop and maintain expertise

Ensure that network support personnel are adequately trained in implementing and supporting a secured network infrastructure through training and drills.

5.11 Patching

Network devices shall be patched and updated on a documented, regular, and timely schedule.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.14 System Acquisition, Development and Maintenance

The organization designs and builds software with security and privacy as design principles.

Voatz, Inc. Software Development Security Policy

1.0 Purpose

This policy ensures that information security is an integral part of information systems across the entire software development lifecycle. This includes requirements for information systems which provide services over public networks and provides for secure methodologies during the design and implementation of Voatz, Inc. products and services.

2.0 Scope

This policy covers all Voatz, Inc. Engineering and Operations groups during design, implementation, deployment and maintenance of Voatz, Inc. products and services.

3.0 Business Requirements

All activity associated with the development of in-house software that will run on production systems and the configuration of key systems must ensure:

- Security is embedded in all stages of the SDLC to include requirements analysis, design, implementation, testing, release, and ongoing operations/maintenance.
- All code and systems configurations are reviewed and approved through a formal process
- Software development follows a consistent methodology
- All application/program debugging interfaces or backdoors utilized in development or testing must be deleted or disabled before software is moved into production.
- All changes, both scheduled and unscheduled, will be logged, documented, and handled according to the **Change and Configuration Management Policy.**

3.1 Security Requirements

Security requirements must be established during the overall product requirements gathering and design phases. The following security concerns should be considered:

- Type of information processed (e.g., PII) by the application and how it is transmitted, processed, and stored
- User roles and access to front and backend components
- Authentication mechanisms
- Functionality, Security, Usability Tradeoffs
- Resilience of application against fraudulent use, harmful activity, inadvertent error, and other threats
- Use case and threat modeling
- Use of 3rd party libraries

Risks will be reviewed by a cross functional team that includes development, security/IT Ops, and any others as needed per project and related features.

3.2 Development Methodology

To ensure that code is developed in a secure manner and that the security controls are implemented throughout every stage, Voatz, Inc. development methodology includes:

- Testing of the application's security features
- Ensuring secure coding standards are followed (need reference)
- Manual and automated code analysis

- Independent third party code review and penetration testing
- Quality Assurance Testing

3.3 Code and Configuration Reviews

During implementation and maintenance, all source code and system configurations must be reviewed and approved before deployment by a team member who did not participate in implementing the change.

Reviews may be manual or automated and include review of planned changes and potential vulnerabilities that could be exploited by an attacker or expose the system to remote exploits (e.g., opening a port, enabling a service).

Exceptions must be documented in Jira and approved by Voatz CEO or CTO.

4.0 Enforcement

Any employee found to have knowingly or intentionally added vulnerabilities to the source code or configuration of Voatz, Inc. products or services may be subject to disciplinary action, up to and including termination of employment.

5.0 Customer Notification

As currently available products and services are regularly assessed and reviewed, if a high-risk vulnerability is found, Voatz, Inc. will create a plan to address the issue. No notification will occur until a resolution is generally available to customers.

Controls Notes

A.14.1.1 - Information Security Requirements Analysis and Specification
The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.

[This currently comes from clients/contracts/rfp or internal determination (I think we need to have formal process for gathering/identifyng requirements and a system baseline to work from).]

A.14.1.2 - Securing Application Services on Public Networks
Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

[The mobile app has built-in protections that detect whether the voters' device is connected to an insecure/unsafe network and prevent the use of the app. Any services between the clients and backend are encrypted in transit via TLS (need version and need to determine if the handshake and encrypted tunnel are applicable here).

All data is sent via TLS. All communications between the mobile app and Voatz backend are encrypted with ECDH providing the initial key exchange to establish a session and then encrypting subsequent communications with AES-GCM

TLS also for web applications (VWA, admin portals) but not sure of anything beyond that]

A.14.1.3 - Protecting Application Services Transactions
Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

[Same as previous]

A.14.2.1 - Secure Development Policy
Rules for the development of software and systems shall be established and applied to developments within the organization.

[Don't believe we have rules in place . . . generally, the development is done and security checked throughout - is this a language specific checklist?]

A.14.2.2 - System Change Control Procedures
Changes to systems within the development lifecycle shall be controlled by the use of formal change control

procedures.

[Actual changes managed via change control and well documented, however, the introduction of proposed changes not very formal - i.e. process where a proposed change is clearly described, rationale provided, pros/cons to current processes, clear explanation of what needs to be done and why prior to deciding to proceed with a change.]

A.14.2.3 - Technical Review of Applications after Operating Platform Changes
When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

[I think we do this]

A.14.2.4 - Restrictions on Changes to Software Packages
Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.

[Would this refer to the apk/ipa files?]

A.14.2.5 - Secure System Engineering Principles
Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.

[Some documentation, but somewhat adhoc- need to create a checklist/procedure, maybe? i.e.

1. Ensure all unused ports and services are closed/disabled

2. Validate user supplied input, etc.]

A.14.2.6 - Secure Development Environment
Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life cycle.

[Pretty sure we do this (see also control A.9.4.5 - Access Control to Program Source Code: Voatz source code is developed on developer's laptops, stored in on-premise repositories. Developers are grouped by the following: Frontend (mobile apps, web application), Backend (server, database, blockchain). Repository accounts are configured so that developers only have access to repositories pertaining to their group for the development through test phases of development. Access to repository accounts enforce MFA and require strong passwords.

Control needed (DLP): How to prevent developer from cloning the code

Control needed (Monitoring logins, pull requests, code updates, and downloads): How to do this

Once source code is ready for production, a single super user with an admin account has the access to push the code to the live environment.]

A.14.2.8 - System Security Testing
Testing of security functionality shall be carried out during development.

[We do this]

A.14.2.9 - System Acceptance Testing
Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

[Unit testing vs acceptance testing vs verification/validation? Test team does complete a series of tests(could call them acceptance tests) related to any customizations for new clients/new requirements prior to the apps being pushed to live.]

A.14.3.1 - Protection of Test Data
Test data shall be selected carefully, protected and controlled.

[We have test accounts which can get cleared manually. We've done load testing and can set up test elections but not sure we use test data extensively.]

A.15 Supplier Relationships

The organization actively manages risks around 3rd party vendors and their access to Voatz, Inc. data.

Voatz, Inc. 3rd Party Vendors and Assessment Policy

1.0 Introduction

This document contains guidelines that should be followed to maintain the security of organization information systems and data when Voatz, Inc. enters into any arrangement with a third-party vendor.

2.0 Scope

This policy should be understood by any member of Voatz, Inc. who seeks to source a service from a third party that would give them direct access to organization data. This may involve services run on systems outside of the organization in the cloud or where support agreements give the third-party access to organization systems or data.

3.0 Managing Outsourcing Risks

Prior to outsourcing or allowing third party access to the organization's non-public information or systems, the risks involved must be clearly identified and documented and approved by leadership as acceptable to Voatz, Inc..

4.0 Formal Outsourcing

Where a service is formally outsourced, a process must be contractually in place to ensure that information security standards are in place, maintained and reported on. A duty to report any breaches in security should be formally included in any contract, and the frequency and timeliness of reports should be included within any contract.

5.0 Vendor Selection and Due Diligence

The process of selecting a third-party service provider must include due diligence of the third party in question, a risk assessment and a review of any proposed terms and conditions to ensure that Voatz, Inc. is not exposed to undue risk.

This process may involve advice from members of the organization with expertise in contract law, IT, information security, data protection and human resources. For any potential high-risk new vendor, the review process may include, but is not limited to the following as appropriate:

- Review of open source information (media, webpage, privacy policies, etc.)
- Comprehensive security review (may be conducted by questionnaire, includes primary contractor and any subcontractors, datacenters and all locations Voatz data will be stored/processed)
- Previous breach history and steps taken to mitigate incidents
- Breach notification process (i.e. vendor will notify Voatz within 72 hours of discovery of breach affecting Voatz data)
- Vendor financial data
- Insurance review (cyber insurance, liability)
- Business model review
- Background check
- Operational review
- Certification and audit reports (SOC 2, NIST, ISO 27001, or others applicable to service provided)
- Contract issues and legal review
- Data retention and destruction policies

This process must also include the consideration of any information security policies or similar information available from the third party and whether they are acceptable to Voatz, Inc..

6.0 Contractual Issues

All third parties who are given access to the organization's non-public information or systems must agree to the following terms in any agreement:

- Compliance with Voatz, Inc.'s Information Security Policy
- Appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier; and
- Confidentiality obligations where a third party is given access to the Voatz, Inc.'s non-public information
- Secure access routes and access rights required for maintenance based on the principle of least privilege Full auditing of all actions

7.0 Sensitive Information

A **Privacy Impact Assessment (PIA)** is essential at the outset of any project that will potentially involve sensitive information such as personal data being accessed by a third party. A comparison between a potential cloud service and an onsite service should be included if an onsite offering is available.

Any outsourcing arrangement involving the transfer of sensitive information to a third party must include the acceptance of the organization's standard personal data processing terms. All systems that process or store Voatz, Inc. sensitive information must maintain an automated audit trail that documents system security events as well as any event that results in the access, modification, and /or deletion of Voatz, Inc. sensitive information.

Upon termination of the Agreement with Voatz, Inc., or at any time prior to the reuse or repurposing of media used to store or process Voatz, Inc. sensitive information, the vendor shall sanitize the media or destroy the sensitive information in its possession in accordance with acceptable standards for such destruction.

Third-party vendors must ensure all personnel receive regular security awareness training and are apprised of the requirements outlined within this policy.

Control Condition: The following control is required if the organization does business with or handles data of customers from the European Union.

If the outsourcing involves the transfer of personal data outside the European Economic Area (EEA), it must only be to a country or territory that ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. There are avenues for countries outside of the EU to address this (Ex. U.S. and the Privacy Shield framework).

8.0 Informal Outsourcing

Commercial and free cloud providers offer convenience and simplicity for services such as email and storage. However, there are risks to their use since unlike formal outsourcing where Voatz, Inc. negotiates the terms and conditions of a contract and carries out formal assessments and retains rights of intellectual property, users of free services must accept the provider's terms and conditions. Accordingly, Voatz employees will notify IT Ops prior to using cloud service providers to store, transmit, or process sensitive data.

9.0 Third Party Physical Access and Operational Control

Voatz, Inc. has secure areas where significant information assets are stored. Prior to a third party accessing these areas, a risk assessment should be performed and include the following details:

- Who the party is and the contractual arrangements (Need to Know)
- What information systems the third party may have access to (Need to Know)
- What information they could potentially access (Least Privilege)
- If supervision or monitoring is required
- If there are any other measures that could be taken to mitigate risk

Where a third-party vendor has operational access to the Voatz, Inc. product such as hosting provider, these requirements apply:

- All personnel accessing the Voatz, Inc. network or system must undergo annual cybersecurity training. The training documentation must be disclosed to Voatz, Inc..
- Vendors must have a formal, documented process for granting and revoking access to all systems that interact

with the Voatz, Inc. network or systems. All access to the Voatz, Inc. systems must be audited by the vendor and those audit records be maintained and made available to Voatz, Inc. upon request.

10.0 Risk Assessment

All vendors will be evaluated for their risk to the organization. Risk associated with new vendors should be assessed prior to signing a contract. All third-party vendor risk should be assessed annually. Vendors handling critical data/functions should be evaluated more frequently.

Third-party vendors should do an impact assessment ranking for the risk. The impact assessment rating will be based on a combination of the risk Impact, Probability of Occurrence ratings for the risk.

Reporting Lines

All vendors will disclose their reporting lines within Voatz, Inc., and designated organization primary and technical contacts are assigned to them based on their assessed risk levels.

11.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Appendix A: Vendor Compliance Survey

This document is designed to act as an aid to ensure that all areas of information security and privacy are included when checking a potential cloud service provider (CSP) for software as a service (SaaS).

A.16 Information Security Incident Management

Voatz, Inc.'s response to situations that threaten the security or privacy of confidential information shall ensure events and activities associated with those events are properly identified, contained, investigated, and remedied.

Incident Response Policy

1.0 Overview
It is critical to the organization that incidents that threaten the security or privacy of critical information are properly identified, contained, investigated, and remedied.

The purpose of this policy is to provide an effective response to incidents that threaten the confidentiality, integrity, and availability of digital assets, information systems, and the networks that deliver information. The policy provides a process for documentation, reporting, response, and communication and establishes responsibility for each step in the process of addressing security incidents.

2.0 Scope
This policy applies to all members of the organization and all Voatz systems. Members include employees, guests, and contractors. Systems include computing or network devices owned, leased, or otherwise controlled by the organization. This includes both the Voatz corporate network and Voatz systems providing election insfrastructure. Additionally, incidents involving sensitive/confidential information apply to any computing or network device, regardless of ownership, on which confidential or restricted information is stored by Voatz or on behalf of Voatz or by which access to confidential or restricted information might be gained.

3.0 Policy

3.1 Voatz Election Infrastructure Policy

Elections sytems have been designated as critical infrastructure https://fas.org/sgp/crs/misc/IF10677.pdf. Accordingly, the compromise or suspected compromise of any aspect of the Voatz Election Infrastructure will be immediately reported to the CEO of Voatz and to Voatz IT Ops who will convene an incident response team. If possible, the initial notification should, at a minimum, include the following information:

- Who discovered the potential compromise
- Date/time of the discovery
- Description of what occurred and what was observed when the activity was noticed.
- List of the component(s) of the Voatz platform affected/involved (function, hostname, IP address if available)
- Type of data exposed if applicable (such as PII, credentials, voter information, etc.)

Voatz leadership will direct remediation and recovery efforts and reach out to external incident response and investigation resources as necessary.

If has been determined an incident has occurred, and external notifications need to be made, Voatz leadership will designate one individual to provide the initial notification and updates throughout the duration of the incident. The incident response team will proceed with the same steps to remediate incidents affecting the corporate network listed below in section 3.2.

3.2 Voatz Corporate Network Policy
Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the organization must be reported to Voatz, Inc. IT Ops. Anyone with knowledge, or a reasonable suspicion, of an incident which violates the confidentiality, integrity, or availability of digital information, will make an immediate report to Voatz, Inc. IT Ops.

Voatz, Inc. IT Ops, in collaboration with other appropriate staff, shall determine if a reported incident IS or IS NOT a confidential information security incident.

If the incident IS NOT considered a confidential information security incident, the incident shall be referred to the appropriate staff who shall insure that the incident is handled and documented in accordance with the procedures described herein.

If the Voatz, Inc. IT, in collaboration with other appropriate staff, determines that the incident IS a confidential data security incident, an Incident Response Team is formed. The purpose of the Incident Response Team is to determine a course of action to appropriately address the incident. The security lead shall designate the

membership of the Incident Response Team. Membership will include appropriate individuals from IT, offices with responsibility for the compromised data, and an executive.

It is the responsibility of the Incident Response Team to assess the actual or potential damage to the organization caused by the security incident, and to develop and execute a plan to mitigate that damage. Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

The Incident Response Team should review, assess, and respond to the incident for which it was formed according to the following factors, in decreasing order of priority:

Safety - Incidents affecting human life or safety receive the highest priority. Only after the safety of all affected people has been secured will the team address other aspects of the incident.

Urgent concerns - Departments may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Appropriate IT staff shall be available for consultation in such cases.

Scope - Work to promptly establish the scope of the incident and to identify the extent of systems and data affected.

Containment - After life and safety issues have been resolved, identify and implement actions to mitigate the spread of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the network.

Preservation of evidence - Develop a plan to identify and implement steps for the preservation of evidence, consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information. Preservation of evidence should be addressed as quickly as possible in order to restore availability of the affected systems as soon as practicable.

Investigation - Investigate the root causes and circumstances of the incident, and determine future preventative actions.

Risk mitigation - Identify and recommend strategies to mitigate the risk of harm arising from this incident.

Lessons Learned - Once the incident has been resolved, the teams involved will review lessons- learned to update this policy and implement any additional security measure to reduce the risk of re-occurrence.

If, in the judgment of the security lead, the incident might reasonably be expected to cause significant harm to the subjects of the data or to the organization, the team will determine whether the organization should make best efforts to notify individuals whose personally identifiable information might have been at risk due to the incident. In making this determination, the following factors shall be considered:

- Legal duty to notify
- Length of compromise
- Human involvement
- Sensitivity of compromised data
- Existence of evidence that data were compromised
- Existence of evidence that affected systems were compromised for reasons other than accessing and acquiring data

Additional factors recommended for consideration by members of the Incident Response Team:

- IT shall maintain a log of all confidential information Security Incidents, recording the date, type of confidential information affected, number of subjects affected (if applicable), summary of the reason for the breach, and

corrective measures taken.

- IT shall issue a report for every confidential information security incident describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.
- IT shall provide annually to the executive team a report containing statistics and summary-level information about all known confidential information security incidents, along with recommendations and plans to mitigate the risks that led to those incidents.

4.0 Definitions

Malware - Any software designed with malicious intent including software that performs actions different from those advertised. Examples include, but aren't limited to:

- Viruses
- Worms
- Trojan horses
- Spyware/Keyloggers
- Ransomware
- Bots (Botnets)
- Rootkits
- Malware embedded with attachments (i.e. macros)

Security Incident - Any event that threatens the confidentiality, integrity, or availability of organization systems, applications, data, or networks. Examples of organization systems, applications, data, and networks include, but are not limited to:

- Servers(On prem, Cloud)
- Endpoints (Desktop computers, Laptop computers, Workstations)
- Mobile devices (Smartphones, Tablets)
- Mobile app and code
- Web Portals
- Network equipment (Firewalls, Switches, Routers)
- Data held by third parties with whom Voatz has a contract to store/process/transmit data

Examples of Security Incidents include, but aren't limited to:

- Unauthorized access to Voatz corporate or elections infrastructure (Includes access to third party infrastructure with whom Voatz has a contract to store/process/transmit data)
- Loss of data integrity (e.g. votes modified)
- Intentionally targeted but unsuccessful unauthorized access (e.g. Brute force password cracking attempts)
- Accidental disclosure of Confidential Data (e.g. voter id/registration verification info, pins, or vote selections, database compromise)
- Infection by malware (Including bots participating in a botnet and/or making outbound C2 connections to malicious attacker infrastructure)
- Denial-of-service (DoS)/Distributed Denial of Service(DDoS) attack
- Theft or loss of an organization system (Laptop containing source code)
- The theft or physical loss of computer equipment known to store SSNs or other PII (date of birth, address, etc.)

- Loss or theft of tablets, smartphones or other mobile device
- A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party
- A firewall accessed by an unauthorized entity
- The act of violating an explicit or implied security policy
- A virus or worm uses open file shares or other vector (such as phishing) to infect hosts and spread to other computers
- An attacker runs an exploit tool against a vulnerable/exposed system to gain access to a server's password file or any other part of the system.
- Compromised Accounts

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.17 Information Security Aspects of Business Continuity Management

Voatz, Inc. has a Business Continuity Plan that ensures that the organization can quickly recover from natural and man-made disasters while continuing to support customers and other stakeholders.

Voatz, Inc. Business Continuity Plan Policy

1.0 Purpose

The purpose of this policy is to ensure Information security continuity is embedded in the organization's business operations and provides guidance on how to ensure continuous secure operations during any adverse event affecting Voatz, Inc. assets.

2.0 Scope

This policy applies to all information systems owned or operated by Voatz, Inc.. It also applies to the entire IT infrastructure of Voatz, Inc. and all employees, contractors, and third-party vendors, who have access to IT assets of Voatz, Inc. and may be bound by contractual agreements.

3.0 Business Requirements

Voatz must be resilient and be able to operate in the event of a planned or unplanned loss, interruption, or disruption. Furthermore, Voatz must be able to sustain its security posture during an adverse event and recover gracefully from the event. To accomplish this the organization will:

- Create a Business Continuity Plan that includes Preparedness activities, Backup and Restore procedures as well as Disaster Recovery Strategy
- The Business Continuity Plan may be activated during normal business hours and after hours, with and without warning based on the severity of the triggering event.
- The organization will conduct exercises at least annually to test the ability to restore information and systems from backups

3.1 Plan Design and Development

The plan focuses on maintaining the operation of critical business functions, compiling resource requirements, and identifying alternatives available for recovery.

Response plan and procedures include:

- Evacuation and safety of personnel
- Notification of disaster internally and externally (phone and email)
- Initial damage assessment
- Activating recovery team and Review of recovery strategies for implementation
- Activating Business Continuity Action Plan
- Status notifications

3.2 Testing

The organization performs the following types of BCP tests on an annual basis:

- Structured walkthrough: step by step review of BCP plans
- Simulation: Conduct scenario-based practice execution of plans.
- Full interruption test: Full-scale operational test including a shutdown of primary site and recovery of business operations

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Controls

A.17.1.1. Planning information security continuity

[I think this is covered in the Business Continuity and Disaster Recovery Plan but may need more detail for instance around requirements during election windows.]

A.17.1.2 Implementing information security continuity

[Covered in Business Continuity and Disaster Recovery Plan]

A.17.1.3 Verify, review and evaluate information security continuity

[Covered in Business Continuity and Disaster Recovery Plan]

A.17.2.1 Availability of information processing facilities

[I believe this is in place. See tables in Business Continuity and Disaster Recovery plan that show failover options. In some cases, there are hot spares, and for others, the option to move to a different environment (e.g. from AWS to Azure) to sustain availability]

A.18 Compliance

The organization understands how to determine what information is sensitive and how to handle each level of sensitive information. This includes public, company confidential, personally identifiable information (PII), and 3rd party confidential information.

Voatz, Inc. Information Security/Sensitivity

1.0 Purpose

Voatz, Inc. maintains a strong commitment to information security. This Information Security/Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Voatz, Inc. without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this section.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries and third-party affiliates.

Voatz, Inc. personnel are encouraged to use common sense judgment in securing Voatz, Inc. information to the proper extent. This includes ensuring confidential documents aren't left in conference rooms or on printers, and not leaving laptops/smartphones that may have sensitive data unattended. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact IT Ops.

3.0 Policy

3.1 Data Classification Levels

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Voatz, Inc. information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the information in question.

Level 1: Confidential Data Requiring Notification

Confidential Data Requiring Notification includes any information that Voatz, Inc. has a contractual, legal or regulatory obligation to safeguard in the most stringent manner. This applies to data pertaining to Voatz corporate and Elections operations. In some cases, disclosure, loss, or modification of this data would require the company to notify the affected individual and state or federal authorities.

The company's obligations will depend on the particular data and the relevant contract or laws. Individuals working with the following types of data must consult with **IT Ops** to ensure they meet all of the requirements of their data type:

- Personally Identifiable Information (PII) covered under Massachusetts General Law chapter 93H and 201 CMR 17, including an individual's name plus the individual's Social Security Number, driver's license number, or financial account number.
- Personal Data covered under the European General Data Protection Regulation (GDPR).
- Personal Data covered under the California Consumer Privacy Act as of January 1, 2020.
- "Criminal Background Data" that might be collected as part of an application form or a background check.
- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA), which sets standards for protection of medical records and patient data. See the HIPAA Policy for details.
- Controlled Unclassified Information required to be compliant with NIST 800.171.

- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements.
- U.S. Government Classified Data

Contractual obligations to other firms must be addressed on per company basis depending on what was agreed.

Level 2: Confidential

Confidential data is information that is proprietary in nature and should not be disclosed to others. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Examples of Internal data include: Internal correspondence, planning documents, technical specifications, product code and meeting minutes; contact lists that contain information that is not publicly available; and procedure documentation that should remain private. Passwords, Private Keys and System Keys are a special type of Level 2 data. Any unauthorized disclosure or loss of Confidential data must be reported to **IT Ops**.

Level 3: Public/Unrestricted

Unrestricted data is public data information that may be disclosed to any person regardless of their affiliation with the company. The Unrestricted classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. Public data may be shared with a broad audience both within and outside the company, and no steps need be taken to prevent its distribution.

Examples of Unrestricted data include: press releases, and other general information that is openly shared.

3.2 Data Protection Standards

Each classification of data has different requirements for protection throughout the lifecycle of use.

Users are expected to use good judgement, in case of any uncertainty about classification level of any data, the Information Security Team should assist in making the decision.

Collection

- Collection of Level 1 data about individuals must be approved by Voatz IT Ops.
- Reduce or eliminate collection of Level 1 and Level 2 data when not required for business functions.
- There are no restrictions on collection of Level 3 data.

Access

- Access to Level 1 and Level 2 data requires approval of the Voatz IT Ops.
- Avoid accessing or using Level 1 data whenever possible and do so from as few different devices as possible. Restricted information access must be immediately removed from any person that no longer requires that access as part of their job function.
- Access to Level 2 data should be provided as required for business devices used to access sensitive (non-Public) information and decides must meet minimum security standards.

Sharing

- If you are uncertain if a piece of Level 1 information should be shared, escalate the request to IT Ops. This information may be shared only for need-to-know business purposes and only as approved.
- Note: Non-disclosure and other types of agreements (business associate agreements) may be necessary. Such agreements or agreement forms must be approved by **the CEO.**
- In case of uncertainty of the confidentiality of a piece of data, escalate the request to IT Ops. Information may be shared only for business purposes.
- Level 2 data can be shared with employees as needed and shared with vendors/third-parties as approved by IT Ops head.

Auditing

Each unit or department must conduct periodic reviews of where Level 1 and Level 2 data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify that procedures for removing access are documented and accurate.

Incident Reporting

Any unauthorized disclosure or loss of Level 1 or Level 2 information must be reported to Voatz IT Ops.

Storage

Individual access controls are required for electronic information. Physical security is generally used, and information shall be stored in a physically secured computer. Level 1 data must be stored in an encrypted manner. Acceptable Encryption policy provides standards for encryption of data at rest. Inventories of Level 1 and Level 2 data and the Voatz, Inc. system used for said information must be maintained.

Data Retention

- Data shall be retained for as long as is necessary to provide the service to the client. After the retention period is over or upon specific request by the client, data shall be destroyed in accordance with Destruction and Disposal defined in this policy.

Destruction and Disposal

IT Ops maintains and shall enforce a detailed list of approved destruction methods appropriate for each type of information stored, whether in physical storage media or in database records or backup files. When systems containing data are decommissioned, they must follow the following destruction policy:

- Paper documents containing Level 1, Level 2 information shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by a security screened personnel. (CIC provides)
- Level 1 and Level 2 information on electronic files and data on Reusable Electronic Storage Devices should be reliably erase or physically destroy media using DOD Standard for Secure Data Sanitation (DOD 5220.22M). Functional electronic media that can be overwritten using a secure erase tool then may be recycled or disposed of. Non-functional electronic media (damaged disk drives) must be physically destroyed.
- Devices such as Printers, Copiers, Multifunction office machines often contain hard drives which must be properly erased, or “wiped”, prior to leaving Voatz, Inc. control (returned to the vendor, sent to surplus, donated, disposed of, etc.). (CIC)

Do not destroy records that are the subject of a litigation hold or that must be retained.

The specific deletion or destruction process may be carried out either by an employee or internal/external service providers. All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements, and all data disposal is subject to applicable provisions under relevant data protection laws.

Unless specified, no controls are required for Level 3 data.

4.0 Customer Information Handling

All customer information is treated as Level 1 data and should be handled in accordance with this policy.
All workstations accessing customer information must follow Voatz, Inc. **Workstation Security Policy** at all times.

Customer information shall be retained as per the customer agreement or for as long as it is required for it’s understood purpose.

Data Retention

Customer data will be retained only for as long as **Voatz, Inc.** needs it to fulfil the purpose for which data has been collected. Customers can submit data deletion requests in case of termination, cancellation, expiration or other conclusion of the agreement. Data shall be deleted within 30 days of a data deletion requests.

Security Review

Voatz, Inc. may provide customers with the right to review Voatz, Inc.'s security controls annually for the entire period that Voatz, Inc. processes, stores or otherwise has access to Customer Confidential Information. Voatz, Inc. may provide customers with access to independent audit reports that have been performed on Voatz, Inc.. If issues are found during a customer review of Voatz, Inc.'s security controls, Voatz, Inc. will file a remediation plan with the customer within thirty (30) days following the completion of such a review, and Voatz, Inc. will remediate each such

issue in a timely manner in accordance with a remediation schedule agreed to by the parties.

Security Incidents

Voatz, Inc. shall notify customers of any information security breach involving Customer Confidential Information, including any security breach at or involving a Contractor's systems, hardware, equipment, devices or premises computers or otherwise involving a Contractor's personnel; Voatz, Inc. shall provide notification of any such incident promptly, but in no event later than seven (7) days (or if such incident involves Customer's Sensitive Information, in no event later than three (3) days) following the date Voatz, Inc. first becomes aware of such an incident.

Application Vulnerabilities

Voatz, Inc. shall notify customers of any high-risk vulnerabilities or defects found within products or services within 72 hours of remediation of those defects. Voatz, Inc.

5.0 Exceptions and Enforcement

CEO/IT Ops is authorized to grant exceptions to the requirements set forth in this document. Requests for exceptions shall be initiated through a *request email, ticket, etc.* Any exception granted will require a thorough review of the situation and will be based on the implementation of appropriate compensating controls.

Some data may be subject to specific protection requirements under a contract or grant, or according to a law or regulation not described here, in those circumstances, the most restrictive protection requirement should apply.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

AC1 - Visitor Office Access

The organization tracks and controls visitor access to facilities and assets.

Voatz, Inc. Visitor and Contractor Premises Access Policy

1.0 Purpose

The purpose of this document is to provide guidance for visitors on Voatz, Inc. premises, as well as for employees sponsoring visitors at Voatz, Inc..

2.0 Scope

This policy applies to all visitors to any premise of Voatz, Inc., and to employees who sponsor visitors.

3.0 Policy

Voatz, Inc. corporate office is located in facility hosted by a third party office space provider, CIC. This policy provides guidance for Voatz employees who sponsor visitors and covers how to complete short and long term visitor in-processing. Additionally, it outlines the expectations with regards visitors who will have access to the corporate office space and network resources.

4.1 Parking

Visitors of any duration may use any available public parking garages within the vicinity. Voatz does not have designated parking.

4.2 Check-In

All Visitors must report to the security desk/visitor control at the building entrance to check-in.

If a Voatz employee needs to sponsor a visitor(s), they will inform visitors ahead of time to bring a US Drivers License or State ID with them on the day of their arrival. Additionally, Voatz employees acting as sponsors will need to provide contact information for each visitor to the security desk.

Visitors may be asked to present government-issued photo identification at time of check-In. For mult-day visitors, a photograph will be taken at the time of badge pickup when they arrive on Day 1.

Visitors must be met by their Voatz employee sponsor at the time of Check-In.

Unless otherwise authorized, visitors must be accompanied by their employee sponsor at all times when in common office areas.

A Visitor cannot sponsor another visitor.

4.3 Visitor Logs

Visitors will be asked to sign-in at visitor control. Voatz sponsors will also ensure visitors sign-in once they arrive at the Voatz office. Voatz will also keep a log of visitors.

4.4 Visitor Badges

Visitor Badges issued must be worn at all times. Visitors requiring access to locked areas should arrange times with their sponsor and Voatz IT Ops.

For long term visitors, contractors, or other affiliates requiring access to Voatz facilities for more than a day,

sponsors will contact CIC at helpmeboston11@cic.com and Voatz IT Ops at least two weeks prior to visitor's arrival to request temporary badges.

4.5 Photographs and Cameras

Visitors are not permitted to take photographs inside of Voatz, Inc. premises, unless discussed specifically with sponsoring employees. If employees have any questions about the suitability of photographs, they should consult the Human Resources Department and/or IT OPs.

4.6 Information Disclosure

Visitors should not request information that does not pertain to their visit or the work being performed, confidential or otherwise. Requests for corporate documents, customer information, financial projections, comments on any matter currently under litigation, future products or future corporate direction, or requests for information or statements in the name of the company (as might be requested by a reporter or a lawyer) will be reported to Voatz, Inc. IT Ops or directly to the CEO.

4.7 Emergency Evacuation

In the event of an emergency, it is the sponsoring employee's responsibility to ensure that the Visitor is present and accounted for at the designated evacuation point. Visitors will not leave the property until it is confirmed with IT Ops or Human Resources that they have successfully evacuated the building.

4.8 Network or System Access

Visitors or other affiliates that require internet network access can freely access the CIC Public Wireless Network.

Visitors who require access to Voatz production IT networks will need permission from their employee sponsor and IT Ops, who will arrange for temporary credentials with Voatz, Inc.. Part of this procedure will require the Visitor to review the Acceptable Use Policy. After credentials are arranged, activities on the network will be subject to the Acceptable Use Policy. Visitor use of employee credentials (i.e. sharing of passwords) is not permitted under any circumstances.

Remote Access to Voatz, Inc. networks are governed by the Voatz, Inc. Remote Access Policy.

5.0 Responsibility

This document is maintained jointly by the Human Resources Department and Voatz, Inc. IT Ops.

6.0 Penalties

Violation of any of the requirements in this policy by any employee will result in suitable disciplinary action, up to and including prosecution and / or termination.

Violation of any of the requirements in this policy by any Visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

AC4 - Mobile Device Encryption

The organization requires encryption of sensitive data on phones, laptops, tablets and other mobile devices.

Voatz, Inc. Mobile Device Encryption Policy

1.0 Purpose

This document describes requirements for encrypting sensitive data at rest on Voatz, Inc. mobile devices.

2.0 Scope

This policy applies to any mobile device issued by Voatz, Inc. or used for Voatz, Inc. business which contains sensitive data owned by Voatz, Inc..

3.0 Definitions

Term	Definition
Cleartext	Unencrypted data
Full disk encryption	Technique that encrypts an entire hard drive, including operating system and data
Key Phrase	Used to encrypt or decrypt data
Remote wipe	Software that remotely deletes data stored on a mobile device.

4.0 Policy

All mobile devices, including laptops containing sensitive data owned by Voatz, Inc. must use an approved method of encryption to protect data at rest.

Unless approved by Voatz, Inc. IT Ops, users are expressly forbidden from storing sensitive Voatz, Inc. data on devices that are not issued or supported by Voatz, Inc..

4.1 Laptops

Laptops must employ disk encryption with an approved software encryption package. No sensitive Voatz, Inc. data may exist on a laptop in cleartext.

4.2 Cell phones and Tablets

Any sensitive Voatz, Inc. data stored on a cell phone or tablet must be saved to an encrypted file system using Voatz, Inc.-approved(in the future) software. Voatz, Inc. shall also employ remote wipe technology (now or in the future) to remotely disable and delete any data stored on Voatz, Inc. cell phones or tablets which are reported lost or stolen.

4.3 Keys

All keys used for encryption and decryption must meet complexity requirements described in Voatz, Inc.'s Password Protection Policy.

4.4 Loss and Theft

The loss or theft of any mobile device containing sensitive Voatz, Inc. data must be reported immediately.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC5 - Passwords

Organization members use strong passwords.

Voatz, Inc. Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. This means that all Voatz, Inc. employees (including contractors and vendors with access to Voatz, Inc. systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Voatz, Inc. facility, has access to the Voatz, Inc. network, or stores any non-public Voatz, Inc. information.

4.0 Definitions

Application Administration Account: Any account that is for the administration of an application (e.g., Oracle database administrator, System administrator).

5.0 Policy

5.1 General

- Whenever possible, use 2-Factor Authentication (2FA) or 2-Step Authentication.
- All production system-level passwords must be part of the Voatz, Inc. IT Ops administered global password management database.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be shared between users without specific business reasons and must be managed by a centralized enterprise password management system.
- End user passwords shall be conveyed to staff in a secure manner and end users shall be required to change their initial password to something that adheres to the policy and is known only to that user.
- All user-level and system-level passwords must conform to the guidelines described below.

5.2 Guidelines

5.2.1. General Password Construction Guidelines

Passwords are used for various purposes at Voatz, Inc.. All users should be aware of how to select strong passwords.

When implemented, users may use a randomly generated password from a password generator/manager (i.e. 1Password, LastPass). If no password manager is in use, users must create their own strong passwords. Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Minimum length of 8 random characters but ideally no less than 12
- Passwords should NEVER be “Password” or any derivation.
- The password should **not** be:
  - A single word/phrase found in a dictionary (in any language).
  - A common usage word like computer terms and names, commands, sites, commands, sites, companies, hardware, software.
  - Names of family, pets, friends, co-workers.
  - Birthdays and other personal information such as address and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Same as passwords/phrases used on personal accounts (e.g. email, online banking, social media).
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- Administrative passwords should be 15 (semi-random) characters long.

5.2.2. Passphrases

Passphrases can be used as an alternative to passwords. They are an easy way to remember complex passwords. They can be based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TsmyB1wy2Rmmr!" or some other variation.
NOTE: Do not use any of these examples as a secret!

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

5.2.3. Use of Passwords and Passphrases for Remote Access Users

Access to the Voatz, Inc. network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

5.3 Password Protection Standards

- Do not use the same password for Voatz, Inc. accounts as for other non-Voatz, Inc. access (e.g., personal online accounts, etc.).
- Where possible, don't use the same password for various Voatz, Inc. access needs. For example, select one password for an Engineering system and a separate password for an IT system.
- Select separate passwords to be used for different system (Mac, Windows, Linux, etc.) accounts.
- Do not share Voatz, Inc. passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Voatz, Inc. information.
  - Don't reveal a password over the phone to ANYONE.
  - Don't send a password in an email message.
  - Don't talk about a password in front of others.
  - Don't hint at the format of a password (e.g., "my family name").
  - Don't reveal passwords on questionnaires or security forms Don't share passwords with family members.
  - Don't reveal a password to co-workers while on vacation.
- Do not use the "Remember Password" feature of applications (browsers, email clients, etc.).
- Do not write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including phones or tablets) without encryption. Do not insert passwords into unencrypted email messages or other forms of electronic communication.
- If an account or password is suspected to have been compromised, report the incident to Voatz, Inc. IT and change all passwords immediately.
- Password cracking or guessing may be performed on a periodic or random basis by Voatz, Inc. IT Ops or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Users shall NOT share passwords with other users/employees. If such a demand is made, users shall point to this policy or direct it to their supervisor or IT Ops.

5.4 Application Development Standards

Application developers must ensure their software contains the following security precautions.
Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC6 - Remote Access

Access to organization resources from outside organization networks for business purposes is closely managed and protected.

Voatz, Inc. Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Voatz, Inc.'s network from any host. These standards are designed to minimize the potential exposure to Voatz, Inc. from damages which may result from unauthorized access and use of Voatz, Inc. resources. Damages include the exposure/loss of sensitive customer or company confidential data, intellectual property, damage to public image, damage to critical Voatz, Inc. internal systems, etc.

2.0 Scope

This policy applies to all Voatz, Inc. employees, contractors, vendors, and agents with Voatz, Inc.-owned or personally-owned computer or workstation used to connect to the Voatz, Inc. secured network. This policy applies to remote access connections used to do work on behalf of Voatz, Inc., including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, all physical and wireless modes of network connections.

3.0 Definitions

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection and dialing into an internet service provider (ISP). Being on a Voatz, Inc.-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

Remote Access: Any access to Voatz, Inc.'s corporate network through a non-Voatz, Inc. controlled network, device, or medium.

Split-tunneling: Simultaneous direct access to a non-Voatz, Inc. network (such as the Internet, or a home network) from a remote device while connected into Voatz, Inc.'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

4.0 Policy

4.1 General

- It is the responsibility of Voatz, Inc. employees, contractors, vendors, and agents with remote access privileges to Voatz, Inc.'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Voatz, Inc..

4.2 Requirements

- Secure remote access must be strictly controlled. Access must be approved by Voatz, Inc. IT Ops. Employees agree to never disclose their passwords to anyone.
- Voatz, Inc. employees and contractors with remote access privileges must ensure that their Voatz, Inc.-owned or personal computer or workstation, which is remotely connected to Voatz, Inc.'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Voatz, Inc. employees and contractors with remote access privileges to Voatz, Inc.'s corporate network must not use non-Voatz, Inc. email accounts or other external resources to conduct Voatz, Inc. business, thereby

ensuring that official business is never confused with personal business.
- All remote computer equipment used for business interests, whether personal or company-owned, must display reasonable physical security measures. Computers will have installed whatever antivirus software deemed necessary by Voatz, Inc.'s IT Ops.
- All hosts that are connected to Voatz, Inc. internal networks via remote access technologies must use the most up-to-date software, this includes personal computers, smartphones, network devices, IoT devices, etc.
- Personal equipment that is used to connect to Voatz, Inc.'s networks must meet the requirements of Voatz, Inc.-owned equipment for remote access.
- All remote access connections must include a “time-out” system. In accordance with Voatz, Inc.'s security policies, remote access sessions for all SSH sessions will time out after 30 minutes of inactivity and will terminate after unlimited hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter company networks.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC7 - VPNs

Organization members understand when and how to use virtual private networks.

Voatz, Inc. Virtual Private Network (VPN) Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Remote Access via Virtual Private Network (VPN) connections to the Voatz, Inc. corporate network.

2.0 Scope

This policy applies to all Voatz, Inc. employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing the VPN to access the Voatz, Inc. network.

3.0 Policy

Approved Voatz, Inc. employees and authorized third parties (customers, vendors, etc.) may utilize the VPN. Further details may be found in the Voatz, Inc. Remote Access Policy.

Additionally,

- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Voatz, Inc. internal networks.
- VPN should be controlled by a strong authentication method. Initial configuration will be done by Voatz, Inc. IT OPs and users will be responsible for selecting a strong password after initial login.
- When actively connected to the corporate network, VPNs will force all traffic to and from their workstation over the VPN tunnel.
- VPN gateways will be set up and managed by Voatz, Inc. IT Ops.
- All devices connected to Voatz, Inc. internal networks via VPN must use the most up-to-date endpoint protection software that is the corporate standard; this includes personal computers.
- Users of computers that are not Voatz, Inc.-owned equipment must configure the equipment to comply with Voatz, Inc.'s VPN, Security, and Network policies. Contact IT Ops for details.
- Only Voatz, Inc. IT Ops-approved VPN clients may be used.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Voatz, Inc.'s network, and as such are subject to the same rules and regulations that apply to Voatz, Inc.-owned equipment, i.e., their machines must be configured to comply with Voatz, Inc. IT's Security Policies.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC9 - Server Security

The organization manages, configures and protects organization servers and hosts based on industry best practices.

Voatz, Inc. Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Voatz, Inc.. Effective implementation of this policy will minimize unauthorized access to Voatz, Inc. proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by Voatz, Inc., and to servers registered under any Voatz, Inc.-owned internal network domain.

Based on the type of servers, such as Cloud Managed Systems, Cloud Managed Instances or Physical Servers, the policy for handling patching, configuration, backups, and monitoring shall vary. See the table below.

	Cloud Managed System	Cloud Managed Instance	Physical Servers (On-prem)	Physical Serviers (Remote Datacenter)
Infrastructure Ownership	Service Provider	Service Provider	Voatz, Inc.	Voatz, Inc.
Configuration & Backup	Managed by Provider	Managed by Voatz, Inc.	Managed by Voatz, Inc.	Managed by Voatz, Inc.
Monitoring	Managed by Provider	Managed by Voatz, Inc.	Managed by Voatz, Inc.	Managed by Voatz, Inc.
Patch Management	Managed by Provider	Managed by Voatz, Inc.	Managed by Voatz, Inc.	Managed by Voatz, Inc.
Decommissioning	Not Applicable	Not Applicable	Applicable	Applicable

3.0 Definitions

Intrusion Detection System (IDS): A system that monitors network traffic for malicious activity.

Intrusion Prevention System (IPS): A network security prevention technology that examines network traffic flow to detect and prevent vulnerability exploits.

SSH (Secure Shell): SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

IPSec (Internet Protocol Security): IPSec is a suite of protocols for securing IP communications by authenticating and encrypting each IP packet of a data stream.

4.0 Policy

4.1 Ownership and Responsibilities

All servers deployed at Voatz, Inc. must be the responsibility of corporate IT Ops. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Voatz, Inc. IT Ops. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Voatz, Inc. IT.

At a minimum, the following information is required to be documented and tracked along with a primary and alternate point of contact (system owner) for each server:

- Server contact(s) and location, and a backup contact.
- Hardware and Operating System/Version.
- Main functions and applications, if applicable.
- Type of data processed and sensitivity
- Criticality of a server to mission
- Configuration changes for production servers must follow the appropriate change management procedures.
- Backups

Policy Conditions:

- Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run the Cloud services) is the responsibility of the host or provider in the case of Cloud Managed Systems and Cloud Managed Instances and servers hosted in remote data centers.
- Physical security and maintenance of the infrastructure (hardware, software, networking, and facilities that run a server) is the responsibility of Voatz, Inc. in the case of on-premise physical servers being used.

4.2 General Configuration and Backup Guidelines

Operating System configuration should be in accordance with approved Voatz, Inc. IT guidelines. Services and applications that will not be used must be disabled where practical.

- Access to services should be logged and protected through access-control methods.
- The most recent security patches must be installed on the system as soon as practical..
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use the least privilege to perform a function. Do not use root/admin accounts when a non-privileged account is sufficient.
- Privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- The production servers shall be backed up on a regular basis, ideally once a day.
- Critical servers should have hot spares on standby.

Policy Conditions:

- Configurations and backups for Cloud Managed Systems shall be managed by the provider.
- Configurations and backups for Cloud Managed Instances (virtual machines) and Physical Servers shall be managed by Voatz, Inc. in accordance with the Server Security Policy.

4.3 Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- Logs are accessible only to appropriate applications and trusted users.
- Review of logs will only be done with read-only access tools (e.g., view, more, less, graphical web tools for accessing/filtering logs, etc.).
- All security related logs will be kept a minimum of 30 days.
- Security-related events will be reported to Voatz, Inc. IT Ops, who will review logs and escalate incidents as necessary. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

    - Port-scan attacks
    - (Distributed) Denial of Service attacks
    - Evidence of actual or attempted unauthorized access to privileged accounts or compromised credentials
    - Anomalous occurrences that are not related to specific applications on the host.
    - Malware infections (botnet activity, outbound connections to malicious C2 servers, ransomware, crypto miners)
    - Loss or breach of sensitive data.
- The server shall also be monitored for capacity requirements and resource utilization.

Policy Conditions:

- Logging and monitoring for Cloud Managed Systems shall be managed by the provider.
- Logging and monitoring for Cloud Managed Instances and Physical Servers shall be managed by Voatz, Inc. in accordance with the Server Security Policy.

4.4 Patch Management

All servers under Voatz, Inc. will be maintained with the latest security patches to their operating systems and applications.

All critical patches (operating system, security, third party application) must be applied as soon as practically possible, ideally no later than 48 hours of public release. Patches for high issues/vulnerabilities must be applied within thirty (30) calendar days after public release for any critical production server. All other patches must be rolled out within ninety (90) calendar days. Any low priority patches will be installed on a case-by-case basis. All patches should be tested on development systems before being rolled out to production, where possible. Approvals for exemptions to this timeline shall be granted by IT Ops.

IT Ops/Security is responsible for performing a vulnerability scan on systems after each patch window to show that the patches were installed correctly. Clean vulnerability scan reports should be reviewed periodically.

Policy Conditions:

- Patch Management for Cloud Managed Systems shall be managed by the provider.
- Patch Management for Cloud Managed Instances and Physical Servers shall be managed by Voatz, Inc. in accordance with the Server Security Policy.

4.5 Decommissioning a Server

Policy Condition:

- A “final” backup shall be made before decommissioning the server. This backup is kept for a year and then will be permanently deleted.
- The data on the servers must be completely destroyed using industry standard data destruction technology before the machine is taken out of service. The machine should be labeled accordingly.

4.6 Compliance

Security Audits will be performed and managed by Voatz, Inc. IT Ops. Voatz, Inc. IT Ops will present findings to the appropriate team for remediation or justification.

Every effort will be made to prevent audits from causing operational failures or disruptions.

Policy Conditions:

- Applicable to Cloud Managed Systems and Cloud Managed Instances.
- Voatz, Inc. shall obtain and review ISO 27001/SOC 2 or equivalent compliance certificates for all Cloud Servers as made available by the cloud service providers.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AC10 - Database Credentials

The organization uses strong passwords and protects credentials for databases using industry best practices.

Voatz, Inc. Database Credentials Policy

1.0 Purpose

Systems running on Voatz, Inc.'s managed networks often require the use internal databases. In order to access any internal databases, a system must authenticate to the database by presenting acceptable credentials. Database usernames and passwords (i.e., database credentials) must be securely stored and retrieved.

2.0 Scope

This policy applies to all entities that will access Voatz, Inc. production databases.

3.0 Definitions

Credentials: Something you know (e.g., a password or passphrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print), and/or something you have (e.g. hardware token, smart card).

Hash: An algorithmically generated number that identifies a datum or its location.

Lightweight Directory Access Protocol (LDAP): a set of protocols for accessing information directories.

Production: Software that is being used for a purpose other than when software is being implemented or tested.

4.0 Policy

4.1 General

In order to maintain the security of Voatz, Inc.'s internal databases, access by software programs must be granted only when authenticated. The credentials used for this authentication must not reside in the program's source code in clear text. Database credentials must not be stored in a location that can be accessed by unauthorized parties.

Clients with unique schemas must have unique passwords.

4.2 Storage of Database Credentials

Database credentials shall be stored only in an encrypted manner. Refer to the **Acceptable Encryption Policy** for encryption standards and protocols.

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be exposed or world readable.
- Database credentials may reside on the database server. In this case, a hash of the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the documents tree of a web server.
- Passwords or passphrases used to access a database must adhere to the **Password Policy**.

4.3 Retrieval of Database Credentials

- If stored in a file that is not source code, database credentials must be read from the file immediately prior to use. Following database authentication, the memory containing the username and password must be released or cleared at the earliest opportunity.
- The scope into which database credentials may be stored must be separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

4.4 Access to Database Usernames and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the **Password Policy**.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

AM1 - Equipment Disposal

The organization appropriately disposes of equipment that contains sensitive information.

Voatz, Inc. Equipment Disposal

1.0 Overview

Technology equipment often contains parts that cannot simply be thrown away because they could contain information someone outside of the company should not have access to and may contain hardware components harmful to the environment. Proper disposal of equipment is both environmentally responsible and often required by privacy laws. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Voatz, Inc. data, some of which is considered sensitive. In order to protect data, all storage mediums must be properly erased before being disposed of. Simply deleting or formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until it has been overwritten by a new file. Therefore, special secure data deletion/destruction tools must be used to securely erase data prior to equipment disposal.

2.0 Purpose

This policy has been developed to define the requirements for proper disposal of technology equipment at Voatz, Inc..

3.0 Scope

This policy applies to all technology equipment owned by Voatz, Inc. including company issued laptops, tablets, and mobile phones.

4.0 Policy

4.1 Technology Equipment Disposal

When technology assets reach the end of their useful life they should be sent to Voatz IT Ops for proper disposal.

Source code, business data, personally identifiable information, other sensitive, confidential, and/or non-public data must be reliably erased and/or destroyed from any electronic device before the device is transferred out of the organization's control or before being transferred from one individual to another. Failure to do so might pose a significant risk to the organization since data can often be easily recovered with freely available tools. In all cases, the following standard should be followed when making those decisions:

- Voatz IT Ops shall evaluate each device to determine if the device should be sanitized or if the data on the device needs to be retained and transferred elsewhere for long term storage.
- No devices containing personally identifiable information or confidential information (see Data Classification policy) shall be disposed of unless sanitization is complete.
- Data that must be retained and transferred to another device must be done in consultation with Voatz IT Ops.
- If equipment must be transferred offsite for disposal, software and data deemed to be the property of Voatz, Inc. must be removed from devices prior to transfer of equipment from the organization.

Selection of data destruction methods should be based on the sensitivity of the data being destroyed. Methods may include those procured in-house use and the use of off-site secure data destruction services provided by vetted third parties as necessary.

- **Erasing/overwriting**
  - Erasing by overwriting is an acceptable method of scrubbing data that is not sensitive or requires safeguarding. Multiple passes should be performed with random overwrite patterns – not just all zeros or another single character. A minimum of three (3) overwrites is required; additional overwriting is recommended depending upon the sensitivity of the data to be erased.

- **Degaussing**
  - Degaussing is a form of demagnetizing where the magnetic charge of an object is reset to a magnetically neutral state, in effect erasing all the data previously written to the hard drive or tape.
- **Destruction**
  - In case the data cannot be overwritten or when degaussing is not possible, hard drives should be physically destroyed. For drives that are defective, dead, or sufficiently unresponsive that they do not complete at least a three overwrite minimum, physical destruction is required.

Voatz IT Ops will place a sticker on the equipment case indicating the performance of disk wipe including the date and initials of the technician who performed the disk wipe.

Equipment which is working, but has reached the end of its useful life to Voatz, Inc., should be returned to Voatz IT Ops for refresh/disposal.

Where applicable, prior to leaving Voatz, Inc. premises, all equipment must be recorded as removed from Voatz IT Ops inventory and having been transferred to the approved receiving party. Voatz IT Ops will obtain a **certificate** of **data destruction** for any off-site secure data or equipment destruction services.

4.2 Voatz, Inc. Ramifications

Failure to properly dispose of technology equipment can have several negative ramifications to Voatz, Inc. including exposure of personal /sensitive information in violation of data protection and privacy regulations, fines, negative customer perception, damage to reputation, and costs to notify constituents of data loss or inadvertent disclosure.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any exceptions to the policy must be approved by Voatz IT Ops in advance.

AU2 - Customer Support

Customers are important to Voatz, Inc.. Voatz, Inc. provides Customer Support to support its customers.

Voatz, Inc. Customer Support and SLA Policy

1.0 Definitions

Response time: time elapsed between when the customer creates the incident report (help desk ticket) and when the initial response is sent to the end user (requester).

Resolution time: time window since the incident is initially reported and when the issue is resolved. The resolution time includes troubleshooting efforts, ticket escalation and time required to obtain additional information from the end user -if necessary.

2.0 Customer Support

Voatz, Inc. knows that providing the best possible support to our customers is critical to our mission.

3.1 Service Scope

The following services are covered:

- Account management
- Project implementation services
- Assistance with voter education material
- Election services including ballot preparation, voter file imports, administration portal management, electronic ballot transmission, post-election audits
- System training: remote or onsite
- Help desk support during business hours with extended coverage during the voting window as required by the customer.

3.2 Contact Information

Voatz provides a dedicated hot line and a customized email address for help desk services. The voter may find these support resources via a help menu within the app or on the jurisdiction-specific web landing page (including app download instructions, video tutorials, contact information, and more).

- **Email:** support@voatzsupport.zendesk.com
- **Help Desk Telephone Number:** 1-617-514-2713
- **Web:** https://www.voatz.com/contact

4.0 Service Management

Voatz assigns an Account Manager to each county and jurisdiction in which the Voatz solution is in place. On election day and other critical shared deadlines, our help desk handles all support requests so that each request is triaged promptly as it comes to Voatz based on the stage of the election cycle, the severity of the issue and the number of likely voters affected. There are five stages to the delivery and management of our services:

- Web-based Training
- Ballot preparation
- Voting window
- Vote Consolidation
- Post-Election Audit

Additionally, Voatz may provide on-site support services based on customer requirements. Leveraging hotline/email help desk services alongside in-person resources, Voatz can successfully manage all critical deadlines from customers. Customers must schedule on-site support services two months in advance.

5.0 Customer Requirements (SLA)

Some contracts provide for Service Level Agreement (SLA) requirements. The agreed-upon response and resolution time measures ensure that the services rendered meet customer requirements. Voatz support personnel configure the SLA metric in the help desk tool and monitor that the service performance adheres to the customer's Service Level Agreement response and resolution time requirements.

Voatz shall meet the customer support schedules contemplated in the executed contract. Support staff shall be assigned accordingly.

AU3 - Email Retention

The organization retains email messages critical to the business and in accordance to local regulations.

Voatz, Inc. Email Retention Policy

1.0 Purpose

The information covered in this policy includes the retention of information that is stored or shared via email or instant message/chat.

2.0 Scope

Any email that contains Voatz, Inc. administrative, fiscal/financial, sensitive/confidential correspondence, or information relevant to Voatz platform as critical infrastructure may be considered a record that falls under this policy.

3.0 Policy

Voatz, Inc. administrative correspondence includes, though is not limited to, communication of established company policy, including holidays, time card information, dress code, workplace behavior and legal issues such as intellectual property inquiries or violations.

Voatz, Inc. Fiscal/Financial Correspondence is all information related to revenue and expenses for the company or employee payroll information.

Voatz, Inc. Sensitive/Confidential correspondence covers information that relates to the techncial details of the Voatz platform, personally identifiable information, and anything else not for public release.

Voatz, Inc. Correspondence with regards the Voatz platform as critical elections infrastructure, per DHS, include email related to development, vulnerabilities, updates and status reports.

Voatz follows best practices by retaining correspondence depending on data. Currently, messages deleted from an inbox are also deleted from mail servers. Voatz uses other means to record and retain information including dropbox, slack.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Backup and Restoration

The organization actively manages risks associated with data loss by defining a sound backup regime for all the data services.

Voatz, Inc. Backup and Restoration Policy

1.0 Purpose

The purpose of this policy aims to provide means to:

- To define and apply a clear backup and restore standard for all corporate information systems.
- To define backup and recovery standards per data prioritization.
- To prevent the loss of data in the case of accidental deletion or corruption of data, system failure, or disaster.

2.0 Scope

This policy applies to all information systems owned or operated by Voatz, Inc.. It also applies to the entire IT infrastructure of Voatz, Inc. and all employees, contractors, and third-party vendors, who have access to IT assets of Voatz, Inc. and may be bound by contractual agreements.

3.0 Policy

- All user-level and system-level information maintained by Voatz, Inc. shall be backed up periodically. The backup media (if exists) and backup copies shall be stored with sufficient protection and proper environmental conditions.
- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The backup and recovery process for each system along with defined roles and responsibilities must be documented and periodically reviewed.
- Physical access controls implemented at offsite backup storage locations (if applicable) must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest sensitivity level of information stored.
- Backup copies of operating systems and other critical information system software shall not be stored in the same location as the operational software.
- Backups must be periodically tested to ensure that they are recoverable and verify data integrity.
- Access to backup data/ media must be reviewed annually or when an authorized individual leaves Voatz, Inc..
- Backup information shall be selectively used to restore information system functions as a part of the business continuity process.
- Procedures between Voatz, Inc. and the offsite backup storage vendor(s) must be reviewed at least annually.
- All backup data must be stored encrypted using strong encryption mechanisms.
- Voatz, Inc. IT Ops is responsible for the backup of corporate information systems.

3.1 Review and Testing

Voatz will carry out annual Testing to verify the effectiveness of the plan, train the DR team on what to do in actual disaster scenarios and highlight areas where the plan needs to be improved. Backup restores are also tested annually to ensure the integrity of the backups in case of a disaster.

The organization performs the following types of BCP tests on an annual basis:

Structured walkthrough: step by step review of the following plans:

Business Continuity Plan and controls	See Tugboat
Incident Response Plan (TBL-501 Incident Response) and controls	See Tugboat

Each functional representative will ensure critical data is backed-up to a secure location

Function Area	Critical Data Backup Strategy
Leadership	Dropbox, NAS
Software Engineering/Developers	BitBucket, JIRA, Confluence on-prem
Sales and Customer Success	Dropbox, NAS
Project Management	Dropbox, NAS
IT Ops and Security	Dropbox, NAS
QA and Testing	Dropbox, NAS
Business Development	Dropbox, NAS
HR and Finance	Dropbox, NAS
Product Design and Management	Dropbox, NAS
Documentation/Technical Writing	Tugboat (exports), Dropbox, NAS

Simulations: Conduct scenario-based practice execution of plans

Scenario	Strategy for Backup/Failover site
Loss of power to CIC building	Full-scale (can table-top it to start) operational test including a shutdown of primary site (CIC) and recovery of business operations and restore from backup at alternate site
Cloud providers hit with denial of service	All Voatz traffic routed to alternate Cloud providers
Jira/Confluence (Primary-On Prem) is down	Jira/Confluence (Backup-On Prem)
BitBucket (Primary -On Prem) is down	BitBucket (Backup-On Prem)
Firewall (Primary- on prem) is down	Firewall (Hot spare is on prem)
VPN down	No remote access to corporate network
Wi-Fi down (CIC)	No wireless access to corporate network
Primary LDAP Server Down (on-prem)	LDAP Backup (also on prem)

Bring Your Own Device (BYOD)

This policy is intended to protect the security and integrity of organization's data and technology infrastructure when employees are using their personal device(s) to connect to organization's corporate network.

Voatz, Inc. Bring Your Own Device (BYOD) Policy

1.0 Purpose

This document provides guidelines and acceptable practices for the use of personally-owned devices by Voatz, Inc. employees to access Voatz, Inc.'s resources.

2.0 Scope

This policy is for all staff using personally owned devices to store, access, carry, transmit, receive or use Voatz, Inc.'s information or data, whether on an occasional or regular basis.

This policy is intended to protect the security and integrity of Voatz, Inc.'s data and technology infrastructure.

Limited exceptions to the policy may occur due to variations in devices and platforms.

3.0 Expectation of Privacy

Voatz, Inc. will respect the privacy of individuals's personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

4.0 Policy

4.1 Acceptable Use

- Voatz, Inc. defines acceptable business use as activities that directly or indirectly support the business of Voatz, Inc..
- Employees are expected to follow Voatz, Inc.'s acceptable use policy when using their devices to perform business activities.

4.2 Devices and Support

- The following devices are supported:
  - iPhones
  - iPads
  - MacBooks
  - Android
  - Windows
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Connectivity to the Voatz network is supported by Voatz IT Ops; employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.
- Devices that are not on the Voatz, Inc.'s list of supported devices are not allowed to connect to the network.
- Employees shall ensure that password/pin/biometric locks are enabled on their devices.
- Employees shall ensure that they are using the latest OS in their devices.

- Devices must be encrypted in line with Voatz, Inc.'s compliance standards.

4.3 Risks/Liabilities/Disclaimers

- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Voatz, Inc. reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to Voatz IT Ops within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of Voatz, Inc. and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- Voatz, Inc. reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.
- Voatz, Inc. retains the right to remotely wipe all data from a device in the event of employee termination, data or policy breach, in compliance with the Mobile Device Management Policy, where applicable.

Data Retention and Disposal

This policy is about the organization's approach for data retention and secure disposal.

Voatz, Inc. Data Retention and Disposal Policy

1.0 Purpose

The purpose of this policy is to mitigate threats of non-compliance with regulatory, legal and contractual requirements regarding data retention and disposal policies.

2.0 Scope

This policy applies to all data assets of Voatz, Inc., whether owned or provided by a third party. Voatz, Inc. data assets include, without limitation: Intellectual Property (IP), Personally Identifiable Information (PII) for employees, customers, other third parties, Business Sensitive Information (BSI), financial information, other non-public data or information assets deemed the property of Voatz, Inc..

3.0 Roles and Responsibilities

3.1. Data Owners

Data Owner is the person who is ultimately responsible for the data and information being collected and maintained by his or her department or division. All data within Voatz, Inc. must be assigned a Data Owner, either directly or indirectly through their roles and responsibilities in the organization. The responsibilities of the Data Owners include defining data retention and destruction requirements and making sure they are enforced.

3.2. Data user

Person or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to such data use.

4.0 Retention of Data

4.1 Retention of Business Sensitive and Financial Information

Voatz, Inc.'s Business Sensitive and Financial Information is retained in accordance with the schedule provided below.

Data/Record Types	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
General Ledgers	Permanent
Annual Audit Reports and Financial Statements	Permanent
Bank Statements	7 years
Chart of Accounts	Permanent
Stock and Bond records	Permanent
Contracts and Leases	7 years after expiration
Correspondence (legal)	Permanent
Employee Payroll Records	Permanent
Contractor Payment Records	7 years

Data/Record Types	Retention Period
Insurance Records	Permanent
Invoices to Customers	5 years
Invoices from Vendors	5 years
Employee Expense reports	7 years
Board Meeting Minutes	Permanent
Electronic Documents	Depend on subject matter
Legal files and papers	7 years after close of matter
Risk Assessment reports	5 years

4.2 Retention of PII

All PII data shall be retained for as long as there is a business purpose or a legal requirement to do so.

4.3 Retention of Customer Data

All active Customer Data shall be retained for as long as the Customer continues to be an active Customer of Voatz, Inc. or unless a request has been made by the active Customer for the deletion of data.

All Customer Data, after termination of contract, must be retained in accordance with the contractual agreement between Customer and Voatz, Inc..

Customer Data retention policies may be implemented against Customer Data on an ad-hoc basis as may be agreed between Voatz, Inc. and Customer.

5.0 Data Disposal

5.1 Customer Data Disposal

Disposal of customer data will be carried out in accordance with the contractual agreement between Voatz, Inc. and Customer. In the absence of any contractual agreement, an automatic script or manual removal (for ad-hoc requests) is initiated on Voatz, Inc. platform containing customer data. This activates a full hard delete of customer data on the platform.

5.2 Other Data Disposal, including Voatz, Inc. Business Sensitive Information

All electronic documents containing Voatz, Inc. business sensitive information must be purged upon reaching its' retention life span.

All printed material must be shredded prior to disposal.

6.0 Suspension of Disposal in Event of Litigation or Claims

In the event Voatz, Inc. is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Voatz, Inc. or the commencement of any litigation against or concerning Voatz, Inc. such employee shall inform the Senior Management and any further disposal of documents shall be suspended until such time as the Senior Management, with the advice of counsel, determines otherwise. The Senior Management shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of data.

Disciplinary Policy

The organization has implemented a disciplinary process in order to deal with instance(s) of indiscipline including (but not limited to) non-compliance to information security policies and procedures by users.

Voatz, Inc. Disciplinary Policy

1.0 Purpose

Voatz is a small, innovative company and in that spirit, we do not wish to provide a litany of prohibited behaviors nor an enumeration of all possible disciplinary actions. We trust employees to be professionals, use their good judgment, refer to the code of conduct and ethics as a guide when uncertain of how to act, and be proactive in initiating contact with their manager and/or HR directly to address any questions or concerns.

2.0 Scope

This policy applies to all employees of {organisation.name}. It also applies to direct and indirect contractors of {organization.name} who have agreed to the contractual terms and conditions of {organization.name}.

This policy applies to all our employees regardless of employment agreement (full time, intern, volunteer, contractor, etc.) or rank. We encourage employees to consult with their managers or HR, if they have doubts or questions.

3.0 Communication of Disciplinary Action

Formal disciplinary action may be justified in certain circumstances. In those situations, the person facing the disciplinary action should be notified in writing, wherever applicable. Such communications shall include (at a minimum):

- Description of incident and violation
- Required corrective action
- Potential consequences of repeating the violation and failure to take corrective action (if this is the first notification, next steps are to inform Voatz HR and the CEO)
- Voatz CEO and HR must be cc'd if more than one communication has already been made. (Please note, Voatz is a small company and this notification is meant for situational awareness so that leadership can assess the situation and offer insight and resources, such as additional training, mentoring, other opportunities to improve, etc.). The intent is not to use this as a threat.

Voatz CEO will make any further disciplinary determinations.

IC1 - Email Use

Employees and contractors representing Voatz, Inc. with a Voatz, Inc. email address approach all external email with professionalism and integrity in mind.

Voatz, Inc. Email Use Policy

1.0 Purpose

When email goes out from Voatz, Inc., the general public will tend to view that message as an official policy statement from Voatz, Inc.. Employees and contractors representing Voatz, Inc. with Voatz, Inc. email addresses need to approach all external email with professionalism and integrity in mind.

2.0 Scope

This policy covers appropriate use of any email sent from Voatz, Inc. email addresses and applies to all employees, vendors, and agents operating on behalf of Voatz, Inc..

3.0 Policy

3.1 Prohibited Use

Employees represent the company whenever they use their corporate email address. The Voatz, Inc. email system shall NOT to be used for:

- The creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- Signup for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Intentionally spam other people's emails, including their coworkers.

Employees who receive any email messages with insulting or discriminatory content from any Voatz, Inc. employee should report the matter to their supervisor immediately.

3.2 Appropriate Use

Employees are allowed to use their corporate email for work-related purposes without limitations. For example, employees can use their email to:

Communicate with current or prospective customers and partners.

Log in to purchased software they have legitimate access to.

Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.

Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

3.3 Email Security

All employees must follow the password guidelines and password protection standards specified under the Password Policy.

Employees shall always be vigilant to catch emails that carry malware or phishing attempts. Employees shall undergo phishing training and be instructed to:

- Avoid opening attachments and clicking on links when content is suspect.
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.

If an employee remains unsure about the safety of an email, they can reach out to their supervisors or IT Ops.

3.4 Personal Use

Using a reasonable amount of Voatz, Inc. resources for personal email is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters from Voatz, Inc. email accounts are prohibited. Virus or other malware warnings and mass mailings from Voatz, Inc. shall be approved by IT Ops before sending. These restrictions also apply to the forwarding of mail received by Voatz, Inc. employees.

3.5 Forwarding

Employees are discouraged from auto-forwarding email from their Voatz, Inc. account to external destinations. Exceptions must be approved by IT Ops.

3.6 Monitoring

Voatz, Inc. employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Voatz, Inc. may monitor messages without prior notice. Voatz, Inc. is not obliged to monitor email messages.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IC2 - Email Authentication

Email sent from organization domains are authenticated using standard protocols such as SPF, DKIM and DMARC.

Voatz, Inc. Email Authentication

1.0 Purpose

To protect the Voatz, Inc. brand and guard against potential phishing targets. When email goes out from Voatz, Inc., the general public will tend to view that message as an official policy statement from Voatz, Inc.. If a message is not authenticated through SPF, DKIM and DMARC, a third party could spoof the organization's domain(s) and send malicious and erroneous email messages as if they were from the organization.

2.0 Scope

This policy covers the need to authenticate any email sent from Voatz, Inc. email addresses and applies to all employees, vendors, and agents operating on behalf of Voatz, Inc..

3.0 Policy

3.1 SPF - Sender Policy Framework

Sender Policy Framework (**SPF**) is an email validation protocol designed to detect and block email spoofing by providing a mechanism to allow receiving mail exchangers to verify that incoming mail from a domain comes from an IP Address authorized by that domain's administrators. SPF is set up for all of Voatz email sending hosts.

3.2 DKIM - DomainKeys Identified Mail

DomainKeys Identified Mail (**DKIM**) is an email authentication method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain and signed cryptographically by that domain with it's private key. DKIM is set up for all of Voatz email sending hosts.

3.3 DMARC - Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (**DMARC**) is an email-validation system designed to detect and prevent email spoofing. It is intended to combat certain techniques often used in phishing and email spam, such as email messages with forged sender addresses that appear to originate from legitimate organizations. DMARC counters the illegitimate usage of the exact domain name in the From: field of email message headers. DMARC reports provide details about the effectiveness DKIM and SPF implementations. DMARC is set up for all Voatz domains. Voatz enforces a DMARC reject policy so that unauthenticated/suspicious messages sent using the Voatz domain are not delivered.

3.4 Monitoring

Voatz, Inc. regularly reviews and updates organization domains, 3rd party senders, and authentication settings to ensure that all domains are authenticated. Voatz receives monthly DMARC Aggregate Reports from multiple providers.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IC3 - Internet Usage

Organization members use the organization internet connection responsibly and appropriately.

Voatz, Inc. Internet Usage

1.0 Summary

This Internet usage policy applies to all users (including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Voatz, Inc. dedicated and password protected corporate wifi network.

2.0 Internet Services

Access to the Internet will be provided to users to support business activities.

2.1 User Services

2.1.1 Internet Services Provided

The following standard Internet services will be provided to users:

- Email and Chat: Send/receive messages to/from the Internet (with or without attachments).
- Full access to the Internet

Management reserves the right to add or delete services as business needs change or conditions warrant.

2.2 Request & Approval Procedures

Access to the dedicated and password protected corporate wifi network will be provided to users to support business activities.

Requests must be made through Voatz, Inc. IT Ops.

3.2.1 Removal of Privileges

The privileges granted to users must be reevaluated by Voatz, Inc. IT Ops annually, or upon departure of an employee (for any reason). In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

3.0 Usage Policies

3.1 Resource Usage

Access to the dedicated and password protected corporate wifi network will be approved and provided only if reasonable business needs are identified. User Internet access requirements will be reviewed periodically to ensure that continuing needs exist.

3.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet.

Examples of acceptable use of the Internet for performing job functions include:

- Web applications for business and limited personal purposes.
- Communication between employees and non-employees for business purposes
- IT technical support downloading software upgrades and patches
- Review of possible vendor web sites for product information
- Reference regulatory or technical information
- Research

3.3 Personal Usage

All users of the dedicated and password protected corporate wifi network should be aware that the network is monitored for both inbound and outbound traffic and logs are periodically reviewed. Using company computer resources to access the Internet for personal purposes or choosing to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" is done so at their own risk. The company is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

3.4 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits conducting a business enterprise, political activity, stalking, bullying, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information for which there is not a need-to-know.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or linking of company web sites to other internet sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation of, posting, transmission, or voluntary receipt of unlawful, libelous, offensive, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees.

3.5 Software Licenses and Copyrights

The company supports strict adherence to software vendor license agreements. When at work or when company computing or networking resources are used, copying of software in a manner inconsistent with the vendor's license is forbidden. Questions regarding lawful versus unlawful copying should be referred to Voatz, Inc. IT Ops for review.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

3.6 Expectation of Privacy

3.6.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly. Management reserves the right to examine any email, files, directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

3.6.2 Email Confidentiality

Users should be aware that clear text email is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an email message is transmitted it may be altered. Deleting an email from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

3.7 Maintaining Corporate Image and Goodwill

3.7.1 Representation

When using company resources to access and use the Internet users must realize they represent the company.

3.7.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, social media service, or similar service. Any posting of materials must be approved by the CEO.

3.7.3 Creating Web Sites

All company pages are owned by, and are the ultimate responsibility of Voatz, Inc..

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from Voatz, Inc. IT Ops.

3.8 Periodic Reviews

To ensure compliance with and appropriateness of this policy, periodic reviews will be conducted. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

4.0 Enforcement

Violations of the Voatz, Inc. Internet usage Policy can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation.

IC6 - Removable Media

The organization is aware of the risks of removable media in both loss of data and potential inbound attacks. Utilization of removable media is done carefully.

Voatz, Inc. Removable Media Policy

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. It is important to utilize removable media carefully.

2.0 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by Voatz, Inc. and to reduce the risk of acquiring malware infections on computers operated by Voatz, Inc..

3.0 Definitions

Removable Media: Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players, etc.; removable hard drives ; optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by Voatz, Inc..

Encryption: A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information: Information, which, if made available to unauthorized persons, may adversely affect Voatz, Inc., its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers and , financial information,

Malware: Software of malicious intent/impact such as viruses, worms, and Spyware.

4.0 Scope

This policy covers all computers and servers operating in Voatz, Inc..

5.0 Policy

Voatz, Inc. staff may only use Voatz, Inc. IT Ops approved removable media in their work computers. If issued/approved by Voatz, Inc. IT Ops, removable media may not be connected to or used in computers that are not owned or leased by the Voatz, Inc. . Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the Voatz, Inc. Acceptable Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by Voatz, Inc.-exception procedures.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IC7 - Wireless Communication

The organization uses wireless devices and infrastructure responsibly.

Voatz, Inc. Wireless Communication Policy

1.0 Overview

The purpose of this policy is to secure and protect the information assets owned by Voatz, Inc., partners and customers. Voatz, Inc. grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Voatz, Inc. network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by Voatz, Inc. IT are approved for connectivity to Voatz, Inc. networks.

2.0 Scope

All employees, contractors, consultants, and other temporary workers at Voatz, Inc., including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Voatz, Inc. must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to Voatz, Inc. networks or reside on Voatz, Inc. sites that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones and tablets. This includes any form of wireless communication device capable of transmitting packet data.

The IT Department must approve exceptions to this policy in advance.

3.0 Definitions

Voatz, Inc. network: A wired or wireless network that provides connectivity to corporate services.

Corporate connectivity: A connection that provides access to Voatz, Inc. networks.

Information assets: Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.

MAC address: The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

4.0 Policy Statement

4.1 General Requirements

All wireless infrastructure devices that reside at Voatz, Inc. sites and connect to Voatz, Inc. networks, or provide access to information classified as Voatz, Inc. Confidential (requiring notification or otherwise) must:

- Abide by the standards specified in the Voatz, Inc. **Wireless Communication Policy**.
- Be installed, supported, and maintained by an approved support team.
- Use Voatz, Inc. approved authentication protocols and infrastructure.
- Use Voatz, Inc. approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.1. Labs

Policy Condition – for lab environments.

If/when the organization has a lab, all lab wireless infrastructure devices that provide access to Voatz, Inc. Confidential, Voatz, Inc. Highly Confidential, or Voatz, Inc. Restricted information must adhere to this section.

Lab and isolated wireless devices that do not provide general network connectivity to the Voatz, Inc. network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Voatz, Inc.Voatz, Inc. **Internal Lab Security Policy**.
- Not interfere with wireless access deployments maintained by other support organizations.

Wireless data in transit should be encrypted. Encryption controls and policies are defined by the **Acceptable Encryption Policy**.

4.2 Access Points

All wireless Access Points connected to all internal networks must be registered and approved by IT Ops. They shall be installed and configured to comply with Voatz, Inc. Network Security Policy. The Voatz owned and managed access points shall be subject to periodic penetration tests and audits.

4.3 SSIDs

Policy Condition – shared building.

Internal Corporate networks' SSIDs should be hidden.

The SSIDs shall be configured so that it does not contain any identifying information about the organization, such as company name, division title, employee name or product identifier.

A separate SSID is configured for all Personal Mobile phones which will be on a completely different network and won't be able to access any internal resources.

4.4 Access to Wireless Networks

Access shall be granted according to the user's role. Voatz, Inc. is responsible for maintaining the confidentiality, integrity, and availability of its resources and must manage the roles accordingly. Access to the Voatz, Inc. corporate network through any device not on site must use remote access authentication through the Voatz VPN.

4.5 Passwords

All passwords to the wireless infrastructure and wireless network should follow the **Password Policy**.

Guest Wi-Fi is managed by the office space hosting provider.

5.0 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Voatz, Inc..

IC8 - Workstation Security

The organization protects laptops and workstations and their contents using industry best practices.

Voatz, Inc. Workstation Security Policy

1.0 Purpose

The purpose of this policy is to provide guidance for workstation security for Voatz, Inc. workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

2.0 Scope

This policy applies to all Voatz, Inc. employees, contractors, workforce members, vendors and agents with Voatz, Inc.-owned or personal workstations connected to the Voatz, Inc. network.

3.0 Definitions

Workstations: Includes laptops, desktops, tablets, smart phones, PDAs, computer-based equipment containing or accessing customer information and authorized home workstations accessing the Voatz, Inc. network.

4.0 Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorized users.

Workforce members using workstations shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.

Voatz, Inc. will implement physical and technical safeguards for all workstations that access electronic protected customer or sensitive corporate information to restrict access to authorized users.

The following procedures shall be in force to manage technical, physical and administrative controls and safeguards for Voatz, Inc. workstations:

4.1 Physical Safeguards

Physical access to workstations shall be restricted to authorized personnel only. Employees shall prevent unauthorized viewing of information on a screen by:

- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Ensuring workstations are used for authorized business purposes only.
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Ensuring that screens/monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Enabling lockout after 30 minutes of inactivity.
- Complying with all applicable password policies and procedures.
- Not leaving laptops or other devices unattended in public spaces

4.2 Operational Safeguards

Employees shall use workstations for authorized business purposes only and only approved personnel may install software on workstations. The following operational safeguards shall be implemented:

- Ensuring that latest OS and software updates are installed.
- Never installing unauthorized software on workstations.
- Complying with the Anti-Virus policy.
- Ensuring that workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by using highest generally accepted wireless security encryption standard (i.e. WPA2, etc.).
- Install and enable security features such as firewalls, anti-virus and anti-malware software.

4.3 Management and Administration

Voatz IT Ops shall ensure that all workstations have all critical security updates patched and installed in a timely manner. Additional Voatz IT Ops will install endpoint protection (including anti-virus, anti-ransomware, disk encryption, etc) on all Voatz owned workstations.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IC13 - Processing Integrity

Voatz, Inc. ensures that system processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Voatz, Inc. Processing Integrity Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for processing integrity for the products defined in the scope outlined in control **OM1.1 - Processing Integrity Scope**.

This policy should ensure the following with regard to Voatz mobile elections platform data:

- Procedures exist to prevent, or detect and correct, processing errors.
- System inputs are measured and recorded completely, accurately, and in a timely manner.
- Data is processed completely, accurately, and a timely manner.
- Data is stored and maintained completely, accurately, and in a timely manner for its specified life span.
- System output is complete, accurate, and distributed to meet the entity's processing integrity commitments and system requirements.
- Modification of data, other than routine transaction processing, is authorized and processed to meet with the entity's processing integrity commitments and system requirements.

2.0 Scope

This policy applies to all products defined in the scope outlined in control **OM1.1 - Processing Integrity Scope**.

3.0 Definitions

Data Inputs: The source data that is sent into a processing system.

Data Processing: The act of collecting data inputs into a system, manipulating in some fashion, and providing data outputs. Example: Performing financial transactions.

Data Outputs: The resulting data that is provided by a data processing system.

4.0 Policy

4.1 Data Inputs

Voatz, Inc. implements policies and procedures over system **inputs** to ensure data is complete, valid, accurate, timely, and authorized to meet the organization's objectives. This includes the following:

- System inputs include the following:
  - Voter data file sent directly to Voatz by election officials
  - Voter list (includes PII protected under Policy **IC4 - Information Security/Sensitivity)**
    - Name (First, Middle, Last)
    - Ballot ID
    - Address (City, State, Zip)
    - Date of birth
    - Passport number, license number or other proof of identity
    - Voter/precinct mapping
    - Voter ID or Number (Jurisdiction-based)
    -

    - Voter information provided directly from voters via support channels
    - Voter information provided directly by voters while using Voatz app
        - ID Scan
        - Mobile Number and Email Address during user sign-up
        - Geolocation
        - Device Data
    - Ballots coded by precinct sent directly to Voatz by election officials
        - Convert from PDF or Ballot Definition File (BDF) format to JSON using ClearBallot Converter
        - Alternatively, ballots are generated in ClearDesign, then used by Voatz Ballot Ops to generate a BDF

4.2 Data Processing

Voatz, Inc. implements policies and procedures over system **data processing** to ensure data is complete, valid, accurate, timely, and authorized to meet the organization's objectives. This includes the following items:

- Data processing specifications and activities required to meet Voatz objectives, including:
    - Ballot proofing
    - Automated scripts to validate ballot-to-JSON conversion
    - Upload JSON files to test version of admin portal
    - Create events and organizations for each jurisdiction
- The following detects and correct errors during data processing:
    - Voatz team proofs the events, voter lists, and ballots in the portal
    - Finalized events and ballots are loaded into the live (or Test) version of the admin portal
    - Authorized election officials do a final proof (sign off)
    - Election goes live (event is active/election window starts/voters sign up and vote using app)

4.3 Data Outputs

Voatz, Inc. implements policies and procedures over system **outputs** to ensure data is complete, valid, accurate, timely, and authorized to meet the organization's objectives. This includes the following:

- System outputs:
    - Digital ballot automatically generated and printed for each mobile ballot submitted
    - Votes recorded electronically on blockchain and audit portal
    - Real-time, voter-verified receipts or aninymous ID generated to allow jurisdictions and citizens to conduct a post-election audit
    - Digitally tabulated/reported votes for private organization elections
        - Conveyed via email, spreadsheet, or private Slack channel
- Accuracy and completeness to ensure votes cast are counted once and counted correctly is accomplished by:
    - Post-election audits via the Voatz audit portal and blockview
    - Audit portal digital lockbox requires credentials of two authorized jurisdiction representatives
    - Paper ballot contains information that can be used in an audit
    - Audits facilitate final vote tabulation and election reporting
- All data is protected (covered in Policy **IC4 - Information Security/Sensitivity**)

5.0 Exceptions and Enforcement

CEO/IT is authorized to grant exceptions to the requirements set forth in this document. Requests for exceptions shall be initiated through a request email, Jira ticket, etc. Any exception granted will require a thorough review of the situation and will be based on the implementation of appropriate compensating controls.

Some data may be subject to specific processing requirements under a contract or grant, or according to a law or regulation not described herein. In those circumstances, the most restrictive protection requirements should apply.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Penalty for deliberate or inadvertent violation of this policy: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

References:

https://linfordco.com/blog/processing-integrity/

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf

Internal Privacy Policy

Demonstrate the organization's commitment to safeguarding and appropriately handling our employees' and contractors' personal information.

Voatz, Inc. Internal Privacy Policy

1.0 Purpose

The purpose of this policy is to satisfy the notification regulatory requirements as well as to demonstrate Voatz, Inc.'s commitment to safeguarding and appropriately handling our employees and contractors personal information.

This Internal Privacy policy ensures that Voatz, Inc.:

- Complies with data privacy requirements and follows good practices
- Informs employees and contractors of their privacy rights and Voatz, Inc.'s information handling practices.

2.0 Scope

The Internal Privacy Policy applies to all employees, workers and contractors of Voatz, Inc. (collectively referred to as "Individuals"). It applies to all data that the company holds relating to identifiable individuals and it describes how Voatz, Inc. collects and uses personal information during and after their working relationship with Voatz, Inc..

Voatz, Inc. has decided to apply the highest regulatory standards in dealing with personal information uniformly across all our offices, regardless of regulatory requirements, while at the same time complying with any specific, local privacy requirements.

3.0 What Personal Information we Collect

Personal information means any information about an individual from which that person can be identified. It does not include information where the identity has been removed (anonymous information).

We collect, store and use the following categories of personal information:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Dates of birth, marriage and divorce.
- Gender.
- Marital status and dependents.
- Next of kin, emergency contact and death benefit nominee(s) information.
- Social Security Number and other government/state-issued IDs.
- Bank account details, payroll records and tax status information.
- Salary and benefits information.
- Start date, leaving date.
- Location of employment or workplace.
- Relevant proof of identification to verify your identity and personal details (e.g. passport, driving license).
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Compensation history.
- Performance and appraisal information.
- Disciplinary and grievance information.
- Information about the use of our information and communications systems.
- Accident book, first aid records, injury at work and third party accident information.
- Information about convictions/allegations of criminal behavior.
- Evidence of right to work and/or immigration status.

Voatz, Inc. typically collects personal information about employees, workers and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider.

Voatz, Inc. will sometimes collect additional information from third parties, including former employers, credit

reference agencies or other background check agencies.

Voatz, Inc. may collect additional personal information in the course of job-related activities throughout the employment period or life of the contract.

Voatz, Inc. limits the collection of personal information to what is strictly necessary to establish, manage or terminate the employment or contractual relationship with its workers. If Voatz, Inc. needs to collect additional personal information for reasons outside establishing, managing or terminating the employment or contractual relationships, we will notify the appropriate individuals in advance, in writing and obtain their consent, in writing.

Applicable privacy legislation may allow us to collect personal information about individuals without their consent, in specific circumstances, such as investigations or legal proceedings.

4.0 Individual's Responsibility to Inform Voatz, Inc. of Changes

It is important that the personal information we hold about our workers is accurate and current. Individuals are responsible for keeping Voatz, Inc. informed if their personal information changes during their working relationship with us.

5.0 How we Use Personal Information

Voatz, Inc. will only use personal information as permitted by the applicable legislation.

Most commonly, Voatz, Inc. will use personal information in the following circumstances:

- Making a decision about recruitments or appointments.
- Determining the terms of working agreements.
- Checking that individuals are legally entitled to work in the jurisdiction.
- Paying individuals and, if applicable, deducting tax and any other social contributions.
- Providing employment-related benefits including:
    - Occupational Sick, Adoption, Maternity, Paternity, Shared Parental and Annual leave
    - Salary, including any pay awards or allowances
    - 401K
    - Advances of salary
- Liaising with benefit providers, providing information about changes to employment.
- General administration of the employment or work contract.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary and compensation.
- Assessing qualifications for a particular job/task, including decisions about promotions.
- Gathering evidence and dealing with grievances, disciplinary matters etc.
- Making decisions about continued employment or engagement.
- Making arrangements for the termination of working relationships.
- Education, training and development requirements.
- Dealing with legal disputes involving Voatz, Inc. workers, including accidents at work.
- Ascertaining workers fitness to work, managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor workers business and personal use of Voatz, Inc.'s information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorized access to Voatz, Inc. computer and electronic communications systems and preventing malicious software distribution.
- To conduct information analytics studies to review and better understand employee retention and attrition rates.
- Dealing with any subject rights requests.
- To provide employment references, at workers' request.
- To carry Voatz, Inc.'s HR-related investigations, solving internal disputes etc.

Voatz, Inc. will only use personal information to establish, manage, or terminate employment or contractual relationships.

If Voatz, Inc. needs to use personal information for an unrelated or new purpose, Voatz, Inc. will notify the appropriate individual and obtain their consent for the new purpose. Individuals always have the right to withdraw

their consent at any time.

Please note that Voatz, Inc. will, if necessary, process personal information without the individual's knowledge or consent as allowed by the applicable privacy legislation, in specific circumstances, such as investigations or legal proceedings.

6.0 How we Share Personal Information

We share your personal information with third parties if it's:

- required by law, and
- necessary to establish, manage or terminate the working relationship

Voatz, Inc. does not sell the personal information of any employees or contractors. Voatz, Inc.'s third-party service providers are only permitted to process personal information for specified purposes and in accordance with instructions as required by contractual obligations and are required to take appropriate security measures to protect personal information in line with applicable privacy legislation.

6.1 Third-party Service Providers Voatz, Inc. Uses

These are entities which Voatz, Inc. contracts to support activities for HR and payroll purposes:

- Payroll (ADP)
- 401K (American Century Investments)
- Background Investigation(Insert provider name)
- Recruitment agencies (AngelList Recruit)

7.0 Information Security/Data Protection

Voatz, Inc. has put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

In addition, Voatz, Inc. limits access to personal information to those employees, contractors and other third parties who have a business need to know. They will only process personal information on Voatz, Inc. instructions.

Voatz, Inc. has put in place procedures to deal with any suspected information security breaches and will notify affected individuals and any applicable regulator of a suspected breach where legally required to do so.

8.0 Information Retention

Voatz, Inc. will only retain personal information for as long as necessary to fulfill the purposes it was collected for, including satisfying any legal, accounting or reporting requirements.

To determine the appropriate retention period for personal information, Voatz, Inc. considers the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of personal information, the purposes for which we process personal information and whether those purposes can be achieved through other means, and the applicable legal requirements.

Voatz, Inc. will retain and securely destroy the personal information of former employees, workers or contractors in accordance with defined timelines or applicable laws and regulations.

9.0 Individual Rights in Connection with Personal Information

Under certain circumstances, by law, individuals have the right to:

- Request access to personal information (commonly known as an "information subject access request"). This enables individuals to receive a copy of the personal information Voatz, Inc. holds about individuals and to check that Voatz, Inc. is lawfully processing it.
- Request correction of the personal information that Voatz, Inc. holds. This enables individuals to have any incomplete or inaccurate information Voatz, Inc. holds corrected.
- Request erasure of personal information. This enables individuals to ask Voatz, Inc. to delete or remove personal information where there is no good reason for continuing to process it.
- Right to withdraw consent. In the limited circumstances where individuals have provided consent to the

collection, use and transfer of personal information for a specific purpose, individuals have the right to withdraw consent at any time. Once Voatz, Inc. has received notification of consent withdrawn, Voatz, Inc. will no longer process information for the purpose or purposes the individual originally agreed to.

To exercise any of these rights, please email hr@voatz.com.

Individuals also have the right to lodge a complaint to the responsible authority in their jurisdiction.

10.0 Changes to this Privacy Notice

Voatz, Inc. may update this policy at any time and will provide individuals with a new policy when substantial updates are made. Voatz, Inc. will also notify individuals in other ways from time to time about the collection, use and sharing of personal information.

Any questions about this policy have to be directed to hr@voatz.com.

OM1 - Product/Services Scope

Voatz, Inc.'s Information Security Program pertains to the following products and services.

Voatz, Inc. Product/Service Scope Policy

1.0 Purpose

This policy defines the products and services covered by Voatz, Inc.'s Information Security Program.

2.0 Scope

Voatz, Inc.'s Information Security Program covers the following products and/or services

- Voatz Corporate Operations and Personnel
- Voatz Elections Infrastructure that has been designated as Critical Infrastructure

3.0 Program Review and Renewal

Voatz, Inc.'s scope of product and services will be reviewed on an annual basis by the **CEO** and **IT Ops.**

OM2 - Information Security Management System (ISMS) Policy

Voatz, Inc. utilizes the "Tugboat Logic Virtual CISO Platform Platform" to manage InfoSec policies, provide security awareness training, implement and document security controls, and track compliance with customers, 3rd party vendors, independent auditors, and regulatory agencies.

Voatz, Inc. Information Security Management System (ISMS) Policy

1.0 Voatz ISMS

Voatz, Inc. utilizes the **Tugboat Logic Virtual CISO Platform Platform** to manage its ISMS.

2.0 Purpose

The purpose of this document is to outline the approach Voatz will take to ensure the security of the processes, technology, data/information, and people involved in the development, operation, administration, maintenance and delivery of the Voatz mobile platform.

3.0 Scope

These policy statements cover all Voatz, Inc. information and information systems and apply to all Voatz, Inc. employees, contractors, and other users of Voatz, Inc. information and information systems.

4.0 General ISMS Policy Statements

The Voatz Mobile Platform hosts political and non-political elections and is committed to protecting its data and that of its customers. To achieve this, the company has implemented security and privacy protections throughout its corporate and elections infrastructure.

Voatz ISMS covers the following components of the Voatz Mobile Elections Platform:

- Corporate Infrastructure which includes the employees involved with and systems used create, deploy, maintain and store the source code and proprietary information pertaining to Voatz mobile apps, web based portals, and other Voatz products
- Elections Infrastructure which consists of software applications that support elections operations including, client applications (ios, android apps), core server, web servers, database, and blockchain.
- Sensitive Elections Information to include voter PII (including personal information and information about/from their devices) provided as voter files, entered by voters during mobile app onboarding and identity verification, and completed ballot selections made by voters as they participate in the election.
- Involved election set up including Ballot Definition File, Voter File, Ballot Styles received from Elections Officials
- Post-election Infrastructure supporting audits in establishing/generating a tamper resistant record, completed ballots, and proof of ballot accuracy which includes the blockchain, ballot receipt, anonymous ID, and jurisdiction/election industry support for paper ballot

With elections infrastructure having been designated as critical infrastructure by the Department of Homeland Security, Voatz strives to take a methodical approach to identify risks associated with each of these components, evaluate the potential for threats/threat actors to exploit flaws or vulnerabilities in these components, an take the necessary action to protect individual privacy as well as the confidentiality, integrity, and availability of Voatz, Inc. resources and data.

5.0 Program Review and Renewal

This Information Security Management System policy shall be evaluated on an ongoing basis by the **CEO** and **ITOps**.

OM4 - Acceptable Use

Organization members are informed about what they can and cannot do with company resources.

Voatz, Inc. Acceptable Use Security Policy

1.0 Overview

Voatz, Inc.'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Voatz, Inc.'s established culture of openness, trust and integrity. Voatz, Inc. maintains a strong commitment to information security. Voatz, Inc. systems and networks, to include information, electronic and computing devices, company issued computer equipment, mobile devices, software, storage media, network accounts providing electronic mail, internet access, and other services must be protected from illegal or damaging actions by individuals either knowingly or unknowingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of information and information/computer systems at Voatz, Inc.. These rules are in place to protect the employee and Voatz, Inc.. Inappropriate use exposes Voatz, Inc. to risks including virus attacks, compromise of systems and services, and legal issues.

Effective security is a team effort involving the participation and support of every Voatz, Inc. employee and affiliate who deals with information and/or information systems. This Acceptable Use Policy is intended to outline the approved use of company resources while conducting Voatz business or interacting with internal networks and business systems.

All employees, contractors, consultants, temporary, and other workers at Voatz, Inc. are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Voatz, Inc. policies and standards, and local laws and regulation.

3.0 Scope

The information covered in these guidelines includes, but is not limited to, information that is stored or shared via any means. This includes: electronic information, information on paper/hardcopy, and information shared using a telephone and video conferencing. This policy applies to all equipment that is owned or leased by Voatz, Inc. . This policy applies to employees, contractors, consultants, temporaries, and other workers at Voatz, Inc. including all personnel affiliated with third parties.

It is the responsibility of every user with access to Voatz, Inc. property and resources to know these guidelines, and to conduct their activities accordingly. Additionally, users should refer to Voatz, Inc. policy IC4-Information Security/Sensitivity for additional guidance on information sensitivity and classification.

4.0 Policy

4.1 General Use and Ownership

All requests for access to Voatz, Inc. networks and systems must be approved by Voatz, Inc. IT Ops.

While Voatz, Inc.'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Voatz, Inc.. Because of the need to protect Voatz, Inc.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Voatz, Inc..

Employees and contractors will be removed from access to all Voatz, Inc. systems and networks upon the day of termination or earlier.

4.1.1 Voatz, Inc. proprietary information stored on electronic and computing devices whether owned or

leased by Voatz, the employee or a third party, remains the sole property of Voatz.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Voatz, Inc. proprietary information.

4.1.3 You may access, use or share Voatz, Inc. proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. if there is any uncertainty, employees should consult their supervisor or manager or Voatz, Inc. IT Ops.

4.1.5 For security and network maintenance purposes, authorized individuals within Voatz, Inc. may monitor equipment, systems and network traffic at any time.

4.1.6 Voatz, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

Information or data should be classified according to Voatz, Inc. policy IC4-Information Security/Sensitivity guidance on information sensitivity and classification. Examples of confidential information include but are not limited to: source code, corporate strategies and diagrams, competitor sensitive, employee personal information, trade secrets, technical specifications, and customer lists. Employees should take all necessary steps to prevent unauthorized access to this information by ensuring:

- 4.2.1 All laptops that connect to the Voatz internal network and VPN must be approved by Voatz IT Ops.

  4.2.2 Providing access to Voatz property/resources to another individual, either deliberately or through failure to secure its access, is prohibited.

  4.2.3 Postings by employees from a Voatz email address to external/public sites must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Voatz, unless posting is in the course of business duties.

  4.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

  4.2.5 Creating strong passwords and keep them secure. Do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed at least quarterly, and user level passwords should be changed at least every six months.

  4.2.6 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.

  4.2.7 Use encryption of information in compliance with Voatz, Inc.'s Acceptable Encryption Use Policy.

  4.2.8 Because information contained on portable computers is especially vulnerable, special care should be exercised and disk encryption is recommended.

  4.2.9 All systems used by the employee that are connected to the Voatz, Inc. Internet/Intranet/Extranet, whether owned by the employee or Voatz, Inc., shall have approved virus-scanning/endpoint protection software with a current virus database unless approved by IT Ops.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Voatz, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Voatz, Inc.-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited:

4.4.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Voatz.

4.4.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Voatz or the end user does not have an active license is strictly prohibited.

4.4.3. Accessing data, a server or an account for any purpose other than conducting Voatz business, even if you have authorized access, is prohibited.

4.4.4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.4.5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.4.6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.4.7. Using a Voatz computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.4.8. Making fraudulent offers of products, items, or services originating from any Voatz account.

4.4.9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.4.10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.4.11. Port scanning or security scanning is expressly prohibited unless prior notification to Voatz IT Ops is made.

4.4.12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty (e.g. internal security assessments).

4.4.13. Circumventing user authentication or security of any host, network or account (except as part of conducting internal security assessments)

4.4.14. Introducing honeypots, honeynets, or similar technology on the Voatz network without written approval from Voatz IT Ops.

4.4.15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.4.16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or remotely via the Internet.

4.4.17. Providing information about, or lists of, Voatz employees to parties outside Voatz.

4.5 Email and Communications Activities

4.5.1. When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to Voatz IT Ops.

4.52. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to

individuals who did not specifically request such material (email spam).

4.5.3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4.5.4. Unauthorized use, or forging, of email header information.

4.5.5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.5.6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.5.7. Use of unsolicited email originating from within Voatz's networks of other service providers on behalf of, or to advertise, any service hosted by Voatz or connected via Voatz's network.

4.6 Blogging

4.6.1. Blogging by employees, whether using Voatz's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Voatz's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Voatz's policy, is not detrimental to Voatz's best interests, and does not interfere with an employee's regular work duties. Blogging from Voatz's systems is also subject to monitoring.

4.6.2. Voatz's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Voatz confidential or proprietary information, trade secrets or any other material covered by Voatz's Confidential Information policy when engaged in blogging.

4.6.3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Voatz and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Voatz's Non-Discrimination and Anti-Harassment policy.

4.6.4. Employees may also not attribute personal statements, opinions or beliefs to Voatz when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Voatz. Employees assume any and all risk associated with blogging.

4.6.5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Voatz's trademarks, logos and any other Voatz intellectual property may also not be used in connection with any blogging activity.

5.0 Enforcement

Any exception to the policy must be approved by Voatz IT Ops in advance.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

OM5 - Clean Desk

Organization members keep their workspaces neat and organized while protecting sensitive information.

Voatz, Inc. Clean Desk Policy

1.0 Overview

The purpose for this policy is to establish a culture of security and trust for all employees at Voatz, Inc.. An effective clean desk effort involving the participation and support of all Voatz, Inc. employees can greatly protect paper documents that contain sensitive information about employees, customers, partners and vendors.

2.0 Purpose

The reasons for a clean desk policy are:

- A clean desk can produce a positive image when our customers/partners visit the organization.
- It reduces the risk of a security incident as confidential information will be locked away when unattended and cannot be seen or taken.
- Sensitive documents left in the open can be stolen by a malicious entity.

3.0 Responsibility

All staff, employees and entities working on behalf of Voatz, Inc. are subject to this policy

4.0 Scope

- At known extended periods away from your desk, such as a lunch break, sensitive working papers are expected to be placed in locked drawers.
- At the end of the workday employees are expected to put away all sensitive media and documents. Voatz, Inc. provides locking desks and filing cabinets for this purpose.
- Employees who work from home are expected to take reasonable precautions as well. Sensitive documents and materials should be stored in a safe space such as a filing cabinet or a locked desk when not in use.
- Sensitive documents and materials that are no longer needed must be shredded or otherwise securely disposed of.

5.0 Policy

- Always clear workspace before leaving for long periods of time.
- If you are unsure of whether a duplicate piece of sensitive documentation should be kept - it will probably be better to place it in the secured shred bin unless you have been told to retain certain material for legal reasons or believe it may be covered soon by a legal requirement to retain it.
- Consider scanning paper items and filing them electronically on secured systems.
- Use the secure shredding bins for sensitive documents when they are no longer needed. Do **not** place them in the trash or recycling bin.
- Lock your desk and filing cabinets at the end of the day.
- Lock away portable computing devices such as laptops or phones.
- Treat mass storage devices such as USB drives as sensitive and secure them in a locked drawer.
- If you do not have a locking drawer system, Voatz, Inc. IT Ops can store sensitive documents and equipment for you.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

OM6 - Environmental Protection

Voatz, Inc. acknowledges a responsibility to the environment, and we express our commitment toward implementing practices that will promote environmental sustainability.

Voatz, Inc. Environmental Protection Policy

1.0 Purpose

Voatz, Inc. acknowledges a responsibility to the environment, and we express our commitment toward implementing practices that will promote environmental sustainability. The following policy governs the management of the environmental aspects of our company, with specific focus on the conservation of resources and the reduction of waste.

This policy relates to how all operations in Voatz, Inc. will be continually reviewed and improved upon, so that we can integrate environmental and social considerations into our everyday practices.

Voatz, Inc. will strive to raise awareness in the partner, customer and supplier communities and encourage participation and provide training of employees in environmental matters.

2.0 Principles and Policies

- Comply with or exceed local, state and federal regulations governing the environment, and actively look for ways to improve on these guidelines.
- Work toward the conservation of energy, water and resources in all of our operations.
- Strive to better understand both the direct and indirect impact that our practices may have on the environment.
- Promote environmental awareness throughout all operations of the company.
- Provide training/newsletters/posters to staff on implementing our sustainable policies.
- Dispose of waste thoughtfully, and develop an attitude of "reducing, recycling and reusing."
- Lessen our environmental impact by purchasing environmentally-friendly products and services.
- Work with our entire supply chain in order to gain mutual benefits of incorporating environmentally sustainable goals into everyday business.
- Annually review our business practices, and determine whether each practice is suitable in an environmental context.
- Independently audit our practices, and determine whether our goals have been reached.
- One of the most significant areas that a company like Voatz, Inc. can help the environment is in a reduction of printing and paper use. Voatz, Inc. personnel will only print documents when absolutely necessary. Personal preference in working with paper is not considered a necessity.

OM7 - Equality and Diversity

Voatz, Inc. recognizes that discrimination and victimization is unacceptable and that it is in the interest of the organization and its employees to utilize the skills of the total workforce.

Voatz, Inc. Equality and Diversity

1.0 Policy

Voatz, Inc. recognizes that discrimination and victimization is unacceptable and that it is in the interest of the organization and its employees to utilize the skills of the total workforce. It is the aim of the organization to ensure that no member or job applicant receives less favorable facilities or treatment (either directly or indirectly) in recruitment or employment on grounds of age, disability, gender / gender reassignment, marriage / civil partnership, pregnancy / maternity, race, religion or belief, sex, or sexual orientation (the protected characteristics).

Our aim is that our workforce will be truly representative of all sections of society and each employee feels respected and able to give of their best.

We oppose all forms of unlawful and unfair discrimination or victimization. To that end the purpose of this policy is to provide equality and fairness for all in our employment.

All employees, whether part-time, full-time or temporary, will be treated fairly and with respect. Selection for employment, promotion, training or any other benefit will be on the basis of aptitude and ability. All employees will be helped and encouraged to develop their full potential and the talents and resources of the workforce will be fully utilized to maximize the efficiency of the organization.

Our staff will not discriminate directly or indirectly, or harass customers or clients because of age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, and sexual orientation in the provision of the organization's goods and services.

This policy and the associated arrangements shall operate in accordance with statutory requirements. In addition, full account will be taken of any guidance or Codes of Practice issued by the Equality and Human Rights Commission, any Government Departments, and any other statutory bodies.

2.0 Our Commitment

- To create an environment in which individual differences and the contributions of all our staff are recognized and valued.
- Every employee is entitled to a working environment that promotes dignity and respect to all. No form of intimidation, bullying or harassment will be tolerated.
- Training, development and progression opportunities are available to all staff.
- To promote equality in the workplace which we believe is good management practice and makes sound business sense.
- We regularly review our employment practices and procedures to ensure fairness.
- Breaches of our equality policy will be regarded as misconduct and could lead to disciplinary proceedings.
- The policy will be monitored and reviewed annually.

3.0 Responsibilities of Management

Responsibility for ensuring the effective implementation and operation of the arrangements will rest with the organization management. Directors / Managers will ensure that they and their staff operate within this policy and arrangements, and that all reasonable and practical steps are taken to avoid discrimination. Each manager will ensure that:

- all their staff are aware of the policy and the arrangements, and the reasons for the policy;
- grievances concerning discrimination are dealt with properly, fairly and as quickly as possible;
- proper records are maintained.

Human Resources will be responsible for monitoring the operation of the policy in respect of employees and job applicants, including periodic departmental audits.

4.0 Responsibilities of Staff

Responsibility for ensuring that there is no unlawful discrimination rests with all staff and the attitudes of staff are crucial to the successful operation of fair employment practices. In particular, all members of staff should:

- comply with the policy and arrangements;
- not discriminate in their day to day activities or induce others to do so;
- not victimize, harass or intimidate other staff or groups who have, or are perceived to have one of the protected characteristics.
- ensure no individual is discriminated against or harassed because of their association with another individual who has a protected characteristic.
- inform their manager if they become aware of any discriminatory practice.

5.0 Third Parties

Third-party harassment occurs where an organization employee is harassed, and the harassment is related to a protected characteristic, by third parties such as clients or customers. Voatz, Inc. will not tolerate such actions against its staff, and the employee concerned should inform their manager / supervisor at once that this has occurred. Voatz, Inc. will fully investigate and take all reasonable steps to ensure such harassment does not happen again.

6.0 Related Policies

All employment policies and arrangements have a bearing on equality of opportunity. The organization policies will be reviewed regularly and any discriminatory elements removed.

7.0 Rights of Disabled People

The organization attaches particular importance to the needs of disabled people.

Under the terms of this policy, managers are required to:

- make reasonable adjustment to maintain the services of an employee who becomes disabled, for example, training, provision of special equipment, reduced working hours. (NB: managers are expected to seek advice on the availability of advice and guidance from external agencies to maintain disabled people in employment);
- include disabled people in training/development programs;
- give full and proper consideration to disabled people who apply for jobs, having regard to making reasonable adjustments for their particular aptitudes and abilities to allow them to be able to do the job.

8.0 Monitoring

The Company deems it appropriate to state its intention not to discriminate and assumes that this will be translated into practice consistently across the organization as a whole.

We will maintain information on staff who have been involved in certain key policies: Disciplinary, Grievance and Bullying & Harassment.

Where appropriate, equality impact assessments will be carried to ascertain the effect of the Company policies and our services / products may have on those who experience them.

The information collected from will be treated as confidential and it will not be used for any other purpose.

If assessments show that the organization, or areas within it, are not representative, or that sections of our workforce are not progressing properly within the organization, then an action plan will be developed to address these issues. This will include a review of recruitment and selection procedures, organization policies and practices as well as consideration of taking legal Positive Action.

9.0 Grievances and Disciplinary Action

Employees have a right to pursue a complaint concerning discrimination or victimization via human resources.

Discrimination and victimization will be treated as disciplinary offenses and they will be dealt with under the organization disciplinary procedure.

10.0 Review

The effectiveness of this policy and associated arrangements will be reviewed annually under the direct supervision of management.

OM8 - Corporate Ethics

The organization values ethics trust and integrity throughout our business practices.

Voatz, Inc. Corporate Ethics and Social Responsibility

1. Overview

Voatz, Inc.'s purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Voatz, Inc. employee.

Voatz, Inc. is committed to protecting employees, customers, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Voatz, Inc. addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Voatz, Inc. will not tolerate any wrongdoing or impropriety at anytime. Voatz, Inc. will take the appropriate measures to act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. Purpose

The company's purpose for authoring a publication on ethics is to emphasize the employee's and customer's expectation to be treated with fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Voatz, Inc., including all personnel affiliated with third parties.

4. Policy

4.1 Executive Commitment to Ethics

- The Executive Management Team within Voatz, Inc. must set a prime example. In any business practice, honesty and integrity must be top priority for executives.
- Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the workforce.
- Executives must disclose any conflicts of interest regarding their position within Voatz, Inc..

4.2 Employee Commitment to Ethics

- Voatz, Inc. employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.
- Every employee needs to apply effort and intelligence in maintaining ethical values.
- Employees must disclose any conflicts of interest regarding their position within Voatz, Inc..
- Employees will help Voatz, Inc. to increase customer and vendor satisfaction by providing quality products and timely responses to inquiries.

4.3. Company Awareness

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- Voatz, Inc. will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

- Voatz, Inc. will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director, VP needs to consistently maintain an ethical stance and support ethical behavior.
- Employees at Voatz, Inc. should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.5. Unethical Behavior

- Voatz, Inc. will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications. Employees will not participate in any acts of corruption, bribery or other illegal behavior.
- Voatz, Inc. will not tolerate harassment or discrimination.
- Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code & technical information integral to the success of our company will not be tolerated.
- Voatz, Inc. will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- Voatz, Inc. employees will not use corporate assets or business relationships for personal use or gain.

5. Enforcement

- Any infractions of this code of ethics will not be tolerated and Voatz, Inc. will act quickly in correcting the issue if the ethical code is broken.
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Privacy Policy for Websites

The generic use and disclosure of personal information that is collected from the individuals online, through websites

Voatz, Inc. Privacy Policy

Voatz, Inc. Privacy Policy (per voatz.com/privacy)

Last Updated: May 6, 2018

At Voatz, we take your privacy and the security of your information very seriously. This Privacy Policy ("***Policy***") covers Voatz owned or operated services, including voatz.com, the Voatz App, the VEM App, and any services offered via the Site (collectively, the "***Services***"). This Policy is incorporated into, and is part of, our Terms of Service available at https://voatz.com/legal/ which govern your access to the App and your use of the Site and/or Services. Unless otherwise defined herein, capitalized terms shall have the meaning assigned to such terms in the Terms of Service. If you have any questions regarding this Policy please contact us at privacy@voatz.com. The Policy describes the types of information we gather from people visiting our Site and from individual users ("***you***" or "***users***") interacting with our App and how we use, transfer, and secure such information. By accessing our Site or using any Services, you agree to be bound by this Policy. This Policy does not govern information we receive from third parties. If you do not agree to the terms of this Policy, please do not use the Site, or any of our Services. Each time you use any Site, or any Services, the current version of this Privacy Policy will apply. Accordingly, when you use any Site or Services, you should check the date of this Policy (which appears at the top) and review any changes since you last reviewed the Policy.

1. **Types of Information We Collect**
   We may collect two types of information from users of our Sites and Services: "***Personal Information***," which is information that you provide that can be used to identify you (such as name, email address, mobile number, etc.), and "***Aggregate Information***," which is information that cannot be used to identify you (such as frequency of visits to the Site, browser type, device type, etc.)

   1. **Personal Information Collected**
      1. We collect Personal Information from you that you voluntarily provide to us when you use our Sites and Services. For example, you may provide us with your email address, name, mobile number, or other Personal Information.

      2. We do not control your use of our Sites and Services to share Personal Information with others. If you choose to share information publicly through our Site or Services such that it is available to other users please understand that we cannot control the actions of third parties who could collect this information.

   2. **Collection of Personal Information by Third Parties**
      1. Some links on our Site may redirect you to third party websites and services that we do not operate. The privacy practices of these websites and services will be governed by their own policies. We make no representation or warranty as to the privacy policies of any third parties, including the providers of third party applications. If you are submitting information to any such third party through our Site or Services, you should review and understand that party's applicable policies, including their privacy policy, before providing your information to the third party.

   3. **Aggregate Information Collected**
      1. Aggregate Information is information that does not identify you. Aggregate Information may be collected when you visit our Site or interact with our Services, independent of any information you voluntarily enter. We may collect, use, store, and transfer Aggregate Information without restriction.

      2. For example, when you visit our Site, some information is automatically collected. Such information could include your operating system, the site from which you linked to us ("***referring page***"), the name of the website you choose to visit immediately after ours (called

the "***exit page***"), information about other websites you have recently visited, browser (software used to browse the internet) type and language, device identifier numbers, your site activity, and the time and date of your visit. Although we do our best to honor the privacy preferences of our visitors, we are not able to respond to Do Not Track signals from your browser at this time.

4. **Use of "Cookies"**
    1. Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your web browser to help us identify you when you come to our Site. You have choices with respect to cookies. By modifying your browser preferences, you have the choice to accept all cookies, to be notified when a cookie is set, or to reject all cookies. If you choose to reject all cookies you may be unable to use those aspects of our Sites that require registration in order to participate. You can learn more about cookies and how they work at www.allaboutcookies.org. You can always disable cookies through your browser settings. Doing so, however, may disable certain features on our Sites. You can opt-out from third party cookies that are used for advertising purposes on the NAI website at http://www.networkadvertising.org/managing/opt_out.asp.

5. **Analytics**
    1. We may use third parties, such as Google Analytics or other analytics providers, to analyze traffic to a Site. Google Analytics does not create individual profiles for visitors and only collects aggregate data. To disable Google Analytics, please download the browser add-on for the deactivation of Google Analytics provided by Google at http://tools.google.com/dlpage/gaoptout?hl=en. To learn more about privacy and Google Analytics, please consult the Google Analytics overview provided by Google at http://www.google.com/intl/en/analytics/privacyoverview.html. You may find additional information about Google Analytics at http://tools.google.com/dlpage/gaoptout?hl=en. You have the option to opt out of Google's use of cookies by changing your settings through Google Ad Settings via the Google advertising opt-out page at http://www.google.com/policies/technologies/ads/.

    2. We may also use cookies, pixels, beacons, or other web tracking technologies to track the amount of time spent on our Sites or social media and whether or not certain content was viewed. We may work with a third party to collect and process this information for us, based on our instructions and in compliance with this Privacy Policy.

2. **Sharing of Personal Information with Third Parties**
    1. We may transfer Personal Information to third parties for the purpose of providing the Services. For example, we may transfer your Personal Information to third party service providers to (i) provide functionality made available on the Site or via the Services (ii) communicate with you about future offerings. These third party service providers are not authorized to retain, share, store or use the Personal Information for any purposes other than to provide the services they have been hired to provide.

    2. We may also elect to transfer your Personal Information to third parties to: (i) to comply with a legal requirement, judicial proceeding, court order, or legal process served on Voatz; (ii) to investigate a possible crime, such as fraud or identity theft; (iii) in connection with the sale, purchase, merger, reorganization, liquidation or dissolution of Voatz; (iv) when we believe it is necessary to protect the rights, property, or safety of Voatz or other persons, or (v) as otherwise required or permitted by law, including any contractual obligations of Voatz.

3. **Corrections/Information Removal/Opt-Out**
    1. You can request that any Personal Information stored by us to be deleted at any time by contacting us at privacy@voatz.com. We may require you to provide certain information to verify that it is you making the request. However, we will not delete information that we are required to retain in order to comply with applicable laws and regulations.

    2. If you no longer wish to receive our newsletter and promotional communications, you may opt-out of receiving them by following the instructions included in each communication.

4. **Children and Privacy**
    1. We do not knowingly collect Personal Information from children in connection with the features of our Sites or Services. If we become aware that an individual under the age of 13 has provided personally identifiable information through our Sites or Services, we will immediately remove the individual's personally identifiable information from our files.

5. **How Does Voatz Protect My Information**
    1. We take the security of your Personal Information very seriously. We use state of the art administrative, physical, and technical safeguards to secure the Personal Information you share with us. Despite these safeguards and our additional efforts to secure your information, We cannot promise or guarantee that hackers, cybercriminals, or other unauthorized third-parties will not be able to defeat our security and improperly collect, access, steal, or modify your Personal Information but we do try our very best to make sure that never happens.

    2. Any email or other communication purporting to be from one of our services or websites asking you to provide sensitive information via email, should be treated as unauthorized and suspicious and should be reported to us immediately by emailing privacy@voatz.com.

6. **Site And Services Intended For Use By United States Citizens &/or Residents Only At This Time**
    1. Voatz provides its Sites and Services for the purpose of creating an enjoyable experience for users residing within the United States and for citizens of the United States residing or traveling overseas. The laws governing the collection and use of information within the United States may be different from the laws of your country of residence or travel.

7. **Will We Change This Privacy Policy?**
    1. Each time you use our Site or Services the current version of the Policy will apply. When you use our Site, you should check the date of this Policy (which appears at the top of the Policy) and review any changes since the last version. Our business changes frequently and this Policy is subject to change from time to time. Unless stated otherwise, our current Policy applies to all information that we have about you. We will not materially change our policies and practices to make them less protective of your privacy without the consent of affected customers.

8. **How Do You Contact Us?**
    1. To contact us with your questions or comments regarding this Policy or the information collection and dissemination practices of this website, please email us at privacy@voatz.com.

9. **Governing Law**
    1. This Policy is governed by the laws of the State of Massachusetts, U.S.A. without giving effect to any principles of conflict of law.

Risk Assessment and Risk Treatment Methodology

The organization provides a foundation for the effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified. Also refer to RM1-Risk Assessments Policy

Voatz, Inc. Risk Assessment and Risk Treatment Methodology

1.0 Overview

An effective risk management process is an important component of a successful information security program. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. This guideline provides a foundation for the effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within Voatz, Inc..

2.0 Purpose

The principal goal of the risk management process is to protect the Voatz, Inc. and its ability to perform its mission, not only its information assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the information security experts who operate and manage the information security system; but as an essential management function of the Voatz, Inc. asset owners and their asset custodians.

The objective of Information risk management is to identify and assess the risks to which Voatz, Inc.'s information is exposed. The purpose of this guideline is to help Voatz, Inc. carry out an effective risk assessment and risk treatment keeping in mind the following objectives:

- Identify the risks that could cause the loss of confidentiality, integrity and/or availability of the information
- Identify the risk owners
- Define criteria for assessing consequences and assessing the likelihood of the risk
- Define how the risk will be calculated
- Define criteria for accepting risks

3.0 Scope

Risk assessments (RAs) can be conducted on any entity within Voatz, Inc. or any outside entity that has signed a third party agreement with Voatz, Inc.. This methodology document is applicable to all operations, products, services, information assets, information systems that are owned and operated by Voatz, Inc., including (but not limited to) applications, databases, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

4.0 Definitions

Risk - Risk is a function of the likelihood of a given threat source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

Acceptable level of Risk - Voatz, Inc. aims to reduce the risk level of all its information and information processing assets/processes to an acceptable level, such that critical business is not affected. At all times there should remain a "Risk Level" for any given asset/process that is below an "Acceptable Risk Level" as set by the management. "Acceptable Risk is the risk level that the management is prepared to accept as business risk".

Risk Assessment - The process of identifying risks to assets/processes and determining the probability of occurrence, the resulting impact and additional safeguards that would mitigate this impact is part of Risk

Management.

Risk Management - The total process of identifying, controlling and mitigating information security-related risks. It includes risk assessment, cost-benefit analysis, and the selection, implementation, test and security evaluation of safeguards.

Threat - The potential for a threat source to exercise either accidentally trigger or intentionally exploit a specific vulnerability.

Vulnerability - Vulnerabilities are weaknesses associated with an asset. These may be exploited by a threat causing an unwanted incident that may result in loss, damage or harm to the business. (Vulnerability in itself doesn't cause harm; it is merely a condition or set of conditions that may allow a threat to affect an asset)

Likelihood - How often the risk event might happen (e.g. per procedure/episode or within a specified timeframe).

Risk Score - A measurement of the risk useful for assessing the priority for control measures for the treatment of different risks.

5.0 Criteria for Performing Risk Assessments

Risk assessments must be conducted across the whole organization covering all key business processes. Such assessments are required to be performed while building Voatz, Inc.'s information security management system in order to identify risks and threats that could emerge from the processes, the people or the information systems that are in place. In addition, risk assessments must be reviewed and performed:

- Before new processes or activities are introduced.
- Before significant changes are introduced to existing processes, activities or product
- For any changes in legislation, regulations or contractual obligations
- For any changes in the business model or significant change in organizational structure
- For any changes in suppliers
- For any major technological changes
- Following an incident that has significantly impacted the organization and its customer
- Following results from internal audit activities (if required)

6.0 Risk Assessment Process

Refer to RM1 - Risk Assessments for Voatz, Inc. Risk Assessment Policy

7.0 Risk Management and Risk Treatment

Refer to RM1 - Risk Assessments for Voatz, Inc. Risk Assessment Policy

8.0 Monitor and Review

The risk management process should be an iterative process and should be the subject of a structured monitoring and review process. For risk assessments associated with the whole of the scheme or individual business units, the review process will be built into the business planning process. In relation to project-based risk assessments, the risk treatment plan provides the project manager with a tool to continuously monitor project improvement through the implementation of the plan.

The output from the risk assessments is to be used as input to the business planning processes as well for internal assessments/ audits, to develop the assessment/ audit plans. Risks should be monitored and reviewed on an ongoing basis by the respective risk owners, and the risk treatment plan updated to reflect the current status of the risk and the controls identified.

9.0 Statement of Applicability (SOA)

The Statement of Applicability (ISO 27001 Clause 6.1.3 d) is the main link between the risk assessment & treatment and the implementation of your information security and should:

- Identify the controls that are necessary for reasons other than any identified risks (Example: because of legal or contractual requirements, because of other processes, etc.). Justify the inclusion and exclusion of controls from Annex A, as well as the inclusion of controls from other sources.
- Record a summarized form of applicable controls (114 from Annex A, plus any additional ones), to present to management and to keep it up to date.
- Document whether each applicable control is already implemented or not.

Statement of Applicability provides auditors with guidance to understand the organization's security approach and to check whether Voatz, Inc. has implemented controls in the way that was planned.

10.0 Risk Treatment Plan

As an output of the risk treatment process, the Risk Treatment Plan must be written after the Statement of Applicability, because this document defines the controls that need to be implemented, given a comprehensive picture of information security, considering not only the result of risk treatment, but also legal, regulatory, and contractual requirements, other business needs, etc. Management and risk owners should review this plan on a periodic basis (preferably quarterly) or in case of any recent security events and make recommendations to reduce risk and improve quality with Voatz, Inc. processes.

RM1 - Risk Assessments

The organization institutes regular risk assessments and uses industry best practices in remediation.

Voatz, Inc. Risk Assessment Policy

1.0 Purpose

To empower Voatz, Inc. IT Ops to perform periodic information security risk assessments for the purpose of determining areas of vulnerability in corporate operations, products and services, and to initiate appropriate remediation.

The risk management process ensures risks to Voatz are identified and mitigated by integrating security into its operations. Accordingly, Voatz, Inc. regularly assesses internal and external risks as they affect information confidentiality, integrity, and availability across Voatz operations.

2.0 Scope

Risk Assessments can be conducted on any entity within Voatz, Inc. or any outside entity that has signed a Third-Party Agreement with Voatz, Inc.. Risk assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of Voatz, Inc. IT Ops. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Voatz, Inc. IT Risk Assessment Team in the development of a remediation plan.

Voatz, Inc. is committed to taking a risk-based approach to managing its organizational risk. This means that when policies or mitigations are proposed they should be weighted between the cost and benefit.

Voatz, Inc. seeks to proactively and continuously monitor and anticipate risks through threat research and ongoing systems monitoring. Several technical controls are in place to track vulnerabilities, threats, and other activities that pose a risk to Voatz operations. Additionally, Voatz conducts ongoing gaps analysis and implements additional controls as necessary to address identified and emerging risks.

Voatz will review this document and identified risks annually.

4.0 Risk Management

4.1 Risk Assessment

Voatz, Inc. engages in an annual risk assessment to evaluate its organizational risk. It evaluates all of the areas that may have significant adverse impact to its organization.

Voatz, Inc. must have a mitigation plan for all Critical and High risks.

Once risks are identified, the Voatz team evaluates the likelihood and impact of risk to Voatz, Inc. operations. Risk assessments are an ongoing component of Voatz processes with impacts are rated low, medium, or high.

4.1.1 Third-Party Vendor Risk

All vendors will be evaluated for their risk to the organization. Vendors will be specifically evaluated if they have the following characteristics:

- Access to Voatz, Inc. sensitive information.
- Operational responsibilities for Voatz, Inc. product offering.
- Component responsibilities for Voatz, Inc. product offering.
- Operational responsibilities for Voatz, Inc. internal operations.

Voatz, Inc. **Third-party Vendors and Assessment Policy** establishes the policy and controls for third-party risk assessments.

4.1.2 Threat and Vulnerability Identification

As a part of the risk assessment, Voatz identifies threats to the organization as well as vulnerabilities to which the organizational information systems may be exposed.

Threat identification requires an examination of threat sources and events, includes the identification of adversary threat capabilities, and intentions.

4.1.3 Risk Determination and Analysis

Voatz determines risk by considering the likelihood that known threats are able to exploit identified vulnerabilities, whether the organization is able to effectively detect such efforts and and the adverse impacts if such exploitations occur and are successful.

Voatz takes a threat-oriented and asset/impact-oriented approach to analyze risk. Key data includes the identification of information assets, threat sources capable of creating threat events that negatively affect the confidentiality, integrity, and availability of those assets, and vulnerabilities associated with Voatz corporate and elections infrastructure environment on which those assets are stored, transmitted and protected.

This information is used to determine overall risk as a combination of likelihood of exploitation of vulnerabilities and the impact of such exploitation.

4.2 Risk Qualification

Voatz, Inc. identifies all key risks and applies the following for evaluating the likelihood and impact of risk:

EXPOSURE		IMPACT		
		HIGH	MEDIUM	LOW
LIKELIHOOD OF ATTACK	HIGH	EXTREME	HIGH	MEDIUM
	MEDIUM	HIGH	MEDIUM	LOW
	LOW	MEDIUM	LOW	SLIGHT

4.3 Risk Treatment

Voatz shall review internal and external feedback annually (or in case of any recent security events) to improve quality with Voatz, Inc. and Voatz, Inc. products with regards to approaches for treating identified risks.

Voatz leadership is responsible for deciding to how to address each risk (whether to Avoid/Eliminate, Reduce/Mitigate, Share/Transfer, or Retain/Accept).

Cybersecurity insurance (or other relevant insurance) should be in place to mitigate the financial impact of a breach or other incident.

4.4 Risk Reporting

Risk Assessments are conducted annually. Voatz documents and tracks risk throughout their processes and mitigation efforts.

4.5 Continuous Risk Monitoring

Continuous monitoring helps determine the ongoing effectiveness of Voatz risk response measures. Additionally, monitoring helps identify risk-impacting changes to Voatz corporate and elections infrastructure affecting information assets.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

SO4 - Change Control and Configuration Management

The organization closely manages process changes and system configurations to ensure availability and integrity of those processes and systems.

Voatz Change Control & Configuration Management Policy

1.0 Purpose

The purpose of this policy is to ensure availability & reliability of applications and resources for internal and external users.

2.0 Scope

This policy applies to all computing resources, hardware (workstations, laptops, servers, network equipment, access points, switches, routers, security equipment, firewalls, intrusion detection systems, intrusion protection systems) and software (operating systems, desktop applications, server applications, security applications, antivirus, data loss prevention, productivity applications, business critical/ customer facing applications) that are owned and managed by Voatz. Where applicable, this change control and configuration management policy will align with the team's software development life cycle and Agile processes.

3.0 Process/ Guidelines

3.1 Change Management Process

The following requirements shall be met in the Change Management Process:

- All changes, both scheduled and unscheduled, will be documented and tracked.
- Stakeholders shall be informed of all upcoming application and system changes that impact system availability or operations.
- Regular planned changes shall be minimally communicated to all the stakeholders on a monthly basis.
- Unplanned outages shall be communicated immediately to stakeholders with regular updates on progress towards the resolution and resumption of service.
- All medium- and high-impact changes, whether scheduled or unscheduled, and whether successful or unsuccessful, must be reviewed.
- All medium- and high-impact changes must receive appropriate approval before being released.

All changes shall be classified as follows:

- Low impact
- Medium impact
- High impact

Process for all changes:

1. Create a ticket requesting the change.
2. Approval by stakeholder.
3. Implement the change.

All high impact changes shall have a rollback plan.

3.2 Change Review

A post-implementation Change Review shall be conducted for all high impact, company-wide changes. The review shall answer questions including but not limited to the following:

- Did the change have the desired effect?
- Are there any shortcomings or undesired effects?
- If there are problems, how should they be addressed?

3.3 Documentation

All identified changes shall be requested by entering requested functionality into the organization's change tracker (Jira). The change requester shall provide the necessary information to identify the basic requirements associated with the change like information about the requestor, request date and reason for request.

3.4 Approvals

The stakeholder shall review the description and requirements for the changes and evaluate the following before approval:

- Impact on business continuity and contingency plans
- Risk involved in making the change
- Business impact and resource assessment
- Evaluate the technical feasibility of the change and the whole impact of the change in terms of:
  - Performance
  - Capacity
  - Security
  - Operability

3.5 Code Changes

The Code Change process is as described in the following steps:

1. A ticket is created requesting the change.
2. The Internal QA process is completed by the Development Team.
3. The change must first be executed internally and run and tested internally.
4. Once the approval process is completed, the changes are pushed out to customers.

3.6 Denials

The stakeholder may deny or postpone a scheduled or unscheduled change for reasons including, but not limited to:

- Inadequate change planning or unit testing
- Lack of stakeholder acceptance (where applicable)
- System integration or interoperability concerns
- Missing or deficient roll-back plans
- Security implications and risks
- Timing of the change negatively impacting key business processes
- Timeframes do not align with resource scheduling (e.g. late-night, weekends, holidays, or during special events).

4.0 Exceptions

Any exception should be signed off by **the stakeholder.**

5.0 Enforcement

Voatz IT Ops is responsible for the implementation and enforcement of this policy.