
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 5

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

**Procurement Folder:** 1305710
**Procurement Type:** Central Master Agreement
**Vendor ID:** VS0000018765
**Legal Name:** VERTOSOFT LLC
**Alias/DBA:**
**Total Bid:** $0.00
**Response Date:** 11/06/2023
**Response Time:** 12:09
**Responded By User ID:** jay@vertosoft.co
**First Name:** Jay
**Last Name:** Colavita
**Email:** jay@vertosoft.com
**Phone:** 703-568-4703

**SO Doc Code:** CRFQ
**SO Dept:** 0803
**SO Doc ID:** DOT2400000036
**Published Date:** 11/7/23
**Close Date:** 11/9/23
**Close Time:** 13:30
**Status:** Closed
**Solicitation Description:** Auditing SaaS RFQ (81240046)
**Total of Header Attachments:** 5
**Total of All Attachments:** 5

**Department of Administration**
**Purchasing Division**
**2019 Washington Street East**
**Post Office Box 50130**
**Charleston, WV 25305-0130**

# State of West Virginia
# Solicitation Response

| | |
|---|---|
| **Proc Folder:** | 1305710 |
| **Solicitation Description:** | Auditing SaaS RFQ (81240046) |
| **Proc Type:** | Central Master Agreement |

| Solicitation Closes | Solicitation Response | Version |
|---|---|---|
| 2023-11-09 13:30 | SR 0803 ESR11062300000002227 | 1 |

**VENDOR**

VS0000018765
VERTOSOFT LLC

**Solicitation Number:** CRFQ 0803 DOT2400000036

**Total Bid:** 0 **Response Date:** 2023-11-06 **Response Time:** 12:09:37

**Comments:**

**FOR INFORMATION CONTACT THE BUYER**
John W Estep
304-558-2566
john.w.estep@wv.gov

**Vendor**
**Signature X** **FEIN#** **DATE**

**All offers subject to all terms and conditions contained in this solicitation**

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Ln Total Or Contract Amount |
|---|---|---|---|---|---|
| 1 | Cloud-based software as a service | 0.00000 | EA | 464110.800000 | 0.00 |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81162000 | | | |

**Commodity Line Comments:** pricing shown in the unit price is for the total 5 years requested.

**Extended Description:**

Auditing SaaS RFQ (81240046)

# EXHIBIT A - PRICING PAGE

| Auditing Cloud-Hosted SaaS RFQ (81230041) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| LOCATION: BUILDING 5, ROOM A-720, CHARLESTON, WV 25305 | | | | | | | | | |
| **Contract Item Number** | **Description** | **Unit of Measure** | **Estimated Quantity*** | **Year One Unit Cost** | **Optional - Year Two Unit Cost** | **Optional - Year Three Unit Cost** | **Optional - Year Four Unit Cost** | **Optional - Year Five Unit Cost** | **Extended Cost** |
| **Auditing Cloud-Hosted SaaS Subscription / License** | | | | | | | | | |
| 4.1.1, 4.1.2, 4.1.1.2. | Enterprise SaaS Subscription - Must at a minimum include 25 core user licenses, 1500 audits anually, 100 integration workflows (automation) annually, 50 integration monitors (automation) anually and unlimited stakeholders | EA | 1 | $69,000.00 | $74,520.00 | $80,481.60 | $86,920.13 | $93,873.74 | $310,921.73 |
| 4.1.1, 4.1.2, 4.1.1.2.1 | Enterprise SaaS Subscription Per Additional Core User (per license) | EA | 1 | $1,500.00 | $1,620.00 | $1,749.50 | $1,889.57 | $204,073.00 | $6,759.07 |
| **Auditing Cloud-Hosted SaaS Services**** | | | | | | | | | |
| 4.1.3.1 | Initial Cloud-Hosted SaaS Implementation Fee (lump sum) | LS | 1 | $29,500.00 | | | | | $29,500.00 |
| 4.1.3.2 | Initial Cloud-Hosted SaaS Virtual Instructor Led Training (hourly rate) | HR | 4 | $295.00 | | | | | $1,180.00 |
| 4.1.3.3 | Virtual Instructor Led-Training (hourly rate) | HR | 100 | $295.00 | | | | | $29,500.00 |
| 4.1.3.4 | Virtual Adminstrator Training (hourly rate) | HR | 25 | $295.00 | | | | | $7,375.00 |
| 4.1.3.4 | On-Site System Adminstrator Training (hourly rate) | HR | 25 | $395.00 | | | | | $9,875.00 |
| 4.1.5 | Cloud-Hosted SaaS Professional Services Support On-Site Rate (hourly rate) | HR | 100 | $395.00 | | | | | $39,500.00 |
| 4.1.5 | Cloud-Hosted SaaS Professional Services Support Virtual Rate (hourly rate) | HR | 100 | $295.00 | | | | | $29,500.00 |
| | | | | | | **TOTAL AMOUNT OF BID →** | | | **$464,110.80** |

*** The estimated purchase volume for new licenses represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.**

****TRAVEL: Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately. Location: 1900 Kanawha Boulevard E. Building 5, Charleston, WV 25305**

*****Optional Renewals- Year Two through Year Five may be renewed by Change Order upon mutual agreement between the Vendor and Agency.**

Jay Colavita

Vendor Signature

Diligent

# Proposal for Audit Software

## PRESENTED TO

**West Virginia Department of Transportation**

## SALES TEAM

**Martina Carstairs, Regional Sales Director**

**Christy Fong, Solutions Consultant**

**Katja Freeman, Principle, Audit Risk Compliance**

**Geoff Thomasson, Director of Advisory Services**

Diligent Corporation
111 West 33rd Street,16th Floor
New York, NY 10120

November 1st, 2022

West Virginia Department of Transportation
Building 5
1900 Kanawha Blvd E
Charleston, WV 25305
Attn: John Estep

RE: Proposal for Audit Software to West Virginia DOT

Dear John and the WVDOT evaluation team,

We understand that selecting an Audit Management tool that meets your needs can be a daunting task. We are excited to participate in this evaluation for audit software and hope to demonstrate via this proposal how Diligent can create a long-standing partnership which aligns with WVDOT's goals.

Thank you for the opportunity to participate in this evaluation. If you have any questions don't hesitate to contact me or my team.

Sincerely,

Martina Carstairs
Regional Sales Director
mcarstairs@diligent.com
604-783-7925

# TABLE OF CONTENTS

# Executive Summary

With over 30 years of experience providing Audit solutions to governments, Diligent's industry leading software allows customers to unlock their potential and have greater efficiency and insight of their audit function.

Diligent builds award-winning, cloud-based Audit, Risk and Compliance software to drive change in some of North America's largest government organizations. We are on a mission to unite and strengthen individuals and entire organizations through our integrated HighBond software platform. With more than 25,000 customer organizations in 130 countries and over 700 government customers in North America, Diligent works to support agencies at any stage in their maturity journey. Whether these professionals are managing audits, assessing risk, measuring controls, monitoring compliance, or testing data, HighBond manages, organizes, and automates the audit workflow.

Diligent will partner with WVDOT to help drive efficiency and program maturity across the Audit function. WVDOT can expect to achieve the following positive business outcomes: increased efficiency, greater visibility, assurance and confidence to leadership, and an increased scope and quality of audits/risk assessments.

## Diligent Facts

Diligent has brought together a wide range of products from ACL, Galvanize and Steele to provide an end-to-end modern governance approach. We are recognized as a leader in many analyst reports, including:

Gartner® FORRESTER® Capterra

## What Makes Us Different

There are many solutions in the market today and choosing a vendor that fits your needs is extremely important. Here are a few reasons that make us a unique vendor:

**Integrated Analytics**

**FedRAMP / IL5 Hosting**

**Audit Domain Expertise**

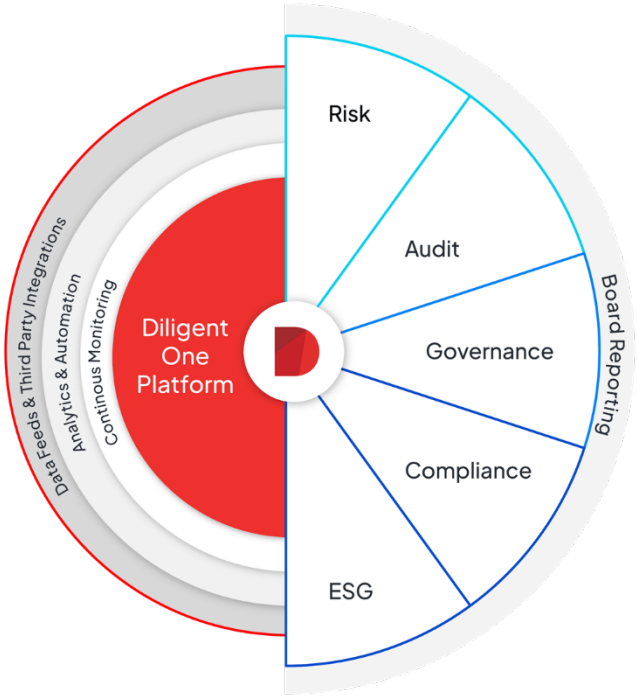
**Unified Platform**

**Robust Reporting Capabilities**

# The HighBond Platform

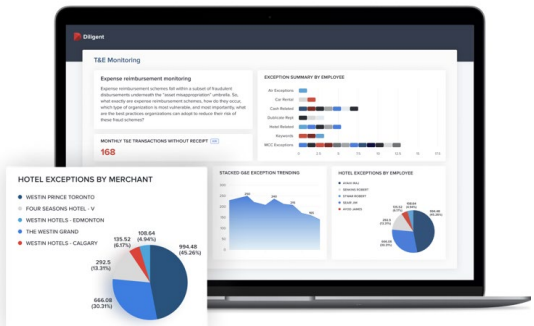
HighBond by Diligent is designed to streamline your audit, risk and compliance activities. Easily oversee grants, manage internal controls, monitor program performance, and protect taxpayer funds and data in a single platform.

More than 700 local and state/provincial governments worldwide have turned to Diligent to address their governance, risk, and compliance challenges. Explore some of the ways our platform can help make your job easier.




**Common Government Use Cases:**

- Audit Workpaper Management
- Program Oversight
- Contracts Oversight
- Whistle Blower Hotline
- Automated Control Monitoring
- Enterprise Risk Management
- Improper Payments
- Grants Oversight
- Fraud Investigations



# Account Team

Your Diligent account team has an extensive audit, risk, technical and domain knowledge and will be able to support you at every step of your evaluation, implemenation and beyond.

**Martina Carstairs** | Regional Sales Director

- 4 years in public sector tech sales
- Manage and support Diligent's southeast government customers
- Extensive Government procurement experience

**Christy Fong** | Solutions Engineer

- 6 Years of IT Project Management experience
- Responsible for demonstrations and customizations of HighBond
- Detailed public sector knowledge

**Katja Freeman** | Principal, Audit, Risk Compliance

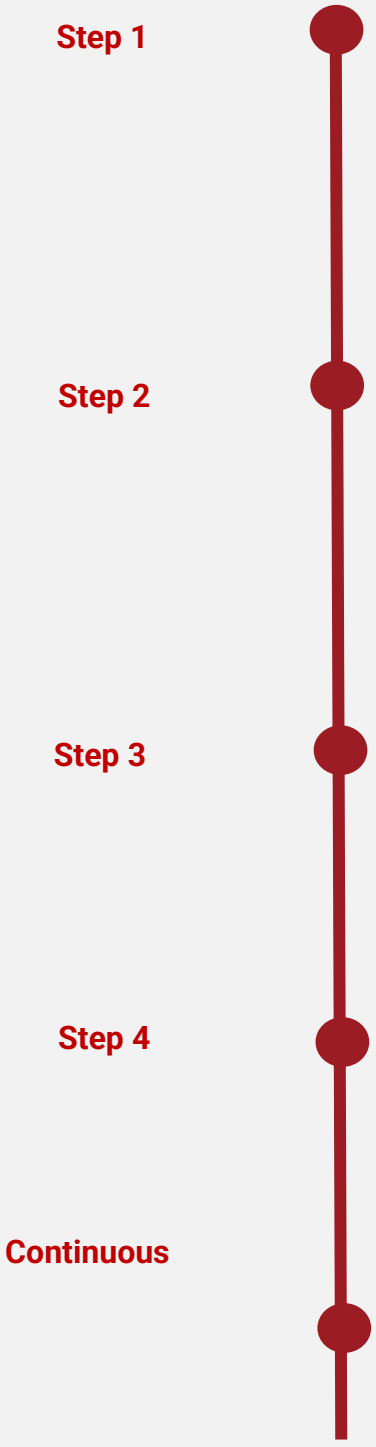
- 10 years at the City and County of Denver, most recently held position as the Audit Director
- 15 years of performance audit, analytics, and policy experience
-

**Geoff Thomasson** | Director, Advisory and Consulting

- 10 years of audit and risk experience
- KPMG
- Certified Public Accountant (CPA)

# Implementation Strategy

Change can be difficult, and although our platform is intuitive, the nature of our customers work can be complex. We provide an integrated learning approach, developed by education specialists with decades of experience to engage and enable teams.




## Requirements Gathering

- Planning and oversight
- Kick-off calls and introductions
- Mutually acceptable project plan
- Gather detailed requirements of the customer

## Prototyping

- Interview subject matter experts
- Review requirements
- Build customized HighBond prototype based on customers' needs
- Review and validate prototype with key stakeholders

## Training and Enablement

- Diligent will develop a robust training plan
- Diligent will execute on training with virtual, instructor led courses.

## Post Enablement Support

- Diligent will verify the solution is working as intended and make any final changes as required
- Diligent will hand-off to the Customer Success team and Client Partner

Because Diligent is a configurable platform and not built completely from the ground up, this allows our implementation times to shorten, allowing our customers to be up and running within a matter of weeks.

## Experienced Onboarding Team

We pride ourselves in providing an implementation team that has extensive audit and risk backgrounds. Our Diligent customer success teams comprises of our Adoption Managers who average 10 years of Audit experience who will be there to ensure you have a successful onboarding with HighBond.

After the initial implementation, we provide a dedicated resource called a Client Partner who is there to help execute on your short and long term vision with the platform, increase usage and adoption, and provide recommendations from other customers they've seen in the industry.

We anticipate that the implementation team to comprise of 3-5 individuals who will work with WVDOT's subject matter experts to ensure you are fully implemented and successfully using the platform with an estimated timeline of 8-12 weeks.

**Imad Jebara** | VP, Global Customer Operations

- 13 years of audit and risk experience
- KPMG
- Certified Public Accountant (CPA), Masters of Business Administration (MBA)

**Geoff Thomasson** | Director, Advisory and Consulting

- 10 years of audit and risk experience
- KPMG
- Certified Public Accountant (CPA)

**Jimmy Shapira** | Advisory and Consulting Manager

- 4 years of audit experience
- Deloitte
- Extensive customer onboarding experience

# Diligent Security

At Diligent, we take security seriously, especially for our government customers who in many cases manage sensitive data. We are one of the only cloud hosted FedRAMP vendors on the market.

Every person, team, and organization using our service expects their data to be secure, available, and handled according to strict confidentiality and privacy principles at all times—and we understand how important this is.

We have built our global business on the trust our customers place in our ability to safeguard their data and continue to maintain that trust through our security and compliance initiatives and culture of continuous improvement.

## Our commitment

We are committed to providing a robust and secure service that protects our customers' data.

We provide our service to customers, and we also use it ourselves—storing our corporate data in our products. We do so knowing that our platform is built upon industry-leading security technology, refined principles and practices, and ongoing investments in security training, testing, independent audits, expert consulting, and advanced tooling.

We are committed to providing all necessary documentation to make our customers comfortable, including our SOC2, ISO27001, Penn Testing, CAIQ, BCP's and more.

**FAQ:**

- Hosted on AWS
- SOC 2 provided with a Mutual NDA in place
- FedRAMP and IL5 authorized
- Multi-layered security environment following the principles of least privilege
- Customers have full ownership of user access controls

aws partner network
Advanced Technology Partner

FedRAMP

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

# Procurement Options

We are committed to providing our customers with the smoothest procurement process we can. Whether it is submitting an RFP, purchasing directly, or going through a reseller we can support a wide range of procurement options.

In our experience with public sector, procuring through a state-approved contract via a reseller makes the procurement process much smoother.

Diligent solutions can be purchased on the following contracts within West Virginia:

1. Omnia Partners
    a. **Insight**
2. TIPS Cooperative
    a. **Vertosoft**
3. Sourcewell
    a. **SHI**

# Current Customers

Diligent has been providing audit, risk compliance solutions to state/local government transit customers for over 30 years and works with over 700 government agencies across the United states.

1

# Specification

*Response on behalf of Diligent Corporation*

Martina Carstairs

Email: mcarstairs@diligent.com | Phone: 604-783-792

# SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Department of Transportation (WVDOT) to purchase Auditing Cloud-hosted SaaS to be utilized by the West Virginia Transportation Auditing Division.

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

   **2.1. "Contract Item"** means the list of items identified in Section 3.1 below and on the Pricing Pages.

   **2.2. "Pricing Pages"** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A, and used to evaluate the Solicitation responses.

   **2.3. "SaaS"** means Software as a Service

   **2.4. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

   **2.5. "Working Papers"** means audit documentation is an essential element of audit quality. The process of preparing and reviewing audit documentation contributes to the quality of an audit. Audit documentation serves to (1) provide the principal support for the audit report, (2) aid auditors in conducting and supervising the audit, and (3) allow for the review of audit quality"

3. **QUALIFICATIONS:** Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

   **3.1.** Vendor must provide, upon request, documentation showing their experience with having successfully completed implementation of an existing Auditing Cloud-hosted SaaS with workflows within an organization of similar size and complexity or larger than WVDOT.

   **3.2.** Vendor must provide, upon request, proof as an authorized reseller of the proposed Auditing Cloud-hosted SaaS or a Sole Source letter if the Cloud-hosted SaaS is proprietary to the vendor before contract award.

   **3.3.** Vendor must provide, upon request, proof their proposed solution is ISO 27001 certified (SOC-2).

Table of Contents

1.0 General Auditing Cloud-hosted Saas Operating Requirements

**1.1 Cloud-hosted Saas must have the capability to store hundreds of audit files per fiscal year.**

HighBond is a Cloud-based solution, and the user can store unlimited number of audit files per fiscal year.

**1.2 Cloud-hosted SaaS must have the capability to create and maintain a library of findings and create templates by individual client or engagement.**

Yes, Diligent is able to create and maintain a library of findings and create templates by individual client or engagement.

**1.3 Cloud-hosted Saas must include a subscription for up to a minimum of twenty-five (25) users in the audit work papers system concurrently from multiple locations, allow for at least one thousand five hundred (1500) audits annually, allow at least one hundred (100) automated integration workflows annually, allow at least fifty (50) automated integration monitors annually and must include unlimited stakeholders.**

Yes, HighBond allows up to a minimum of 25 users access to audit work papers. There is no limit to the number of audits and the user can have an unlimited number of automated integration workflows

1.3.1 **Cloud-Hosted SaaS must have the ability to add additional core user licenses as requested and purchased by the Agency**.

Yes, HighBond allows the user to add an unlimited number of core user licenses to the platform

**1.4 Cloud-hosted Saas must have the capability for the client to create work papers, audit programs, reports, and templates for use.**

Yes, licensed users can create work papers, audit programs, reports, and templates.

**1.5 Cloud-hosted Saas must filter work papers by client, engagement type, fiscal year, or by auditor.**

Yes, HighBond provides filter functionality including by client, engagement type, fiscal year, or by the auditor.

**1.6 Cloud-hosted SaaS must support and integrate with agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu (PDF) programs for searching, retrieval and saving of documents.**

Yes, HighBond provides full integration with Microsoft Office Suite and Google Workspace. Currently, there is no direct integration with Adobe Acrobat Professional and Bluebeam Revu, but we can help to search, retrieve, and save the documents by connecting to those platforms and importing the documents to HighBond.

**1.7 Cloud-hosted Saas must be compatible with states Google email system.**

HighBond is compatible and allows the user to send the request and notification to the Google email system.

**1.8 Cloud-hosted Saas must have the ability to assign hierarchy of roles for users**

Yes, HighBond provides the user with the ability to assign a hierarchy of roles. The system is governed via role-based access. Each user is assigned a role at the time of provisioning which defines baseline access. Additional access can be granted on an ad hoc basis at the discretion of a user with a higher permission level.

**1.9 Cloud-hosted Saas must have the capability of add/alter client information, auditors, approvers, reviewers, and administrative personnel.**

Yes, HighBond provides the capability to add/alter client information, auditors, approvers, reviewer, and administrative personnel. These can all be archived through the user setting.

**1.10 Cloud-hosted Saas must be able to create assignments to specific users.**

Yes, HighBond allows the user to create and assign assignments to specific users. All the assignment progress can also be tracked directly on the platform.

**1.11 Cloud-hosted Saas must have the capability to retrieve prior audit information from agency owned Teammate Software. This information would reference prior completed set of working papers for a particular entity.**

Yes, Diligent provides the capability to retrieve prior audit information from other agencies. During the implementation phase, we will retrieve the information for our users, the user also has the ability to add/import files on their own by utilizing our importing tool.

**1.12 Cloud-hosted Saas must have the capability to convert past audit work papers from agency owned current TEAMMATE software.**

Yes, Diligent provides the ability to convert past audit work papers from agency-owned current Teammate software.

**1.13 Cloud-hosted Saas must allow users have the capability to view, alter and create multiple workpapers at the same time.**

Yes, HighBond allows users to have the capability to view, alter, and create multiple work papers at the same time.

**1.14 Cloud-hosted Saas must have evidence of workpaper completion and review by whom and the date completed.**

Yes, HighBond provides the full audit trail. The work paper completion date and review by whom the information will be recorded and saved on the platform.

**1.15 Cloud-hosted SaaS must have controls over workpaper sharing and have the capability for different employees to alter same work paper.**

Yes, the user will have full control over work paper sharing and have the capability for employees to alter the same work paper.

**1.16 Cloud-hosted SaaS must allow peer review team to view work papers.**

Yes, HighBond allows the peer review team to view the work paper. The system is governed via role-based access. Each user is assigned a role at the time of provisioning which defines baseline access. Additional access can be granted on an ad hoc basis at the discretion of a user with a higher permission level.

**1.17 Cloud-hosted Saas must have the capability to leave reviewer comments notes for work paper corrections that can be removed by reviewer.**

Yes, HighBond provides the "to-do" tab to allow the user to leave reviewer comments notes for work paper corrections that can be removed by a reviewer.

**1.18 Cloud-hosted Saas must have indicators that work papers have been altered and needs reviewed.**

Yes, HighBond provides the indicators that work papers have been altered and needs reviewed. The reviewer can also assign the next review directly through the platform.

**1.19 Cloud-hosted Saas must have the capability to reference or link support documents**

Yes, HighBond allows the user to add a hyperlink to reference and to link support documents. The support documents can also be added, edited, and saved directly to the platform.

**1.20 Cloud-hosted Saas must automatically generate audit reports to agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu with indicators of each engagement in progress.**

One-click reports (including Final Audit reports) are available throughout the platform. In addition to the out-of-the-box one-click reports, custom one-click reports can be created to meet West Virginia Depart's needs. The report can be provided in PDF, Word, Excel, and PowerPoint formats.

**1.21 Cloud-hosted Saas must have the capability to run macros in agency owned Microsoft Office Suite software while in the audit Cloud-hosted SaaS system.**

Yes, HighBond provides full integration with Microsoft Office Suite.

**1.22 Cloud-hosted SaaS must have the capability to lock down work papers and have the capability of removing this lock this if necessary.**

Yes, HighBond allows the user to lock down work papers and change them into "read-only". The user can also remove the lock if necessary.

**1.23 Cloud-hosted Saas must have the capability to access multiple clients working files at the same time.**

HighBond does not allow multiple users to access the same working files at the same time. This is designed on purpose to prevent the user to overwrite the changes by the other user.

**1.24 Cloud-hosted Saas must have the ability to spell and grammar-check text fields.**

Yes, the spell and grammar check are built into the browser.

**1.25 Cloud-hosted Saas must have the capability to store client files on an external hard drive.**

Yes, HighBond allows users to store client files on an external hard drive.

**1.26 Cloud-hosted Saas must have the capability to tick mark or reference agency owned Acrobat Adobe Professional or Bluebeam PDF software.**

Yes, HighBond allows the user to tick mark or reference agency-owned Acrobat Adobe Professional or Bluebeam PDF software.

**1.27 Cloud-hosted Saas must have indicators that work paper has been changed after reviewer sign off.**

Yes, the changes after the reviewer's sign-off can be noted and recorded. HighBond also allows the user to change the working paper to "read-only" after signing off by the preparer to prevent editing by the reviewer.

**1.28 Cloud-hosted Saas must have the capability to run reports to compile data information such as number of audits completed, number of audits in progress, number of findings issued, audit hours per engagement, audit hours per auditor, audit hours per fiscal year for a section and for entire Division.**

Yes, HighBond's storyboard allows the user to compile data information including the number of audits completed, number of audits in progress, number of findings issued, audit hours per engagement, audit hours per auditor, and audit hours per fiscal year for a section and for the entire Division. HighBond's dashboards are user-friendly, and we also offer executive reporting through our
Interactive Storyboards (dashboards) can be used to aggregate all compliance data through visualizations, written commentary, and drill-through capabilities to raw compliance data. Storyboards are configurable and shareable via email or link to various stakeholders.

**1.29 Cloud-hosted Saas must have a dedicated audit workflow process and pages for each audit with configurable sections for planning, fieldwork, reporting, etc in a straightforward to navigate user interface.**

Yes, HighBond provided a dedicated audit workflow including planning, fieldwork, and reporting.

**1.30 Cloud-hosted Saas must provide the ability for end-users to configure reporting dashboards straightforward without the need for vendor support or enchantment.**

Our digital interactive storyboards (dashboards) track real-time risk and compliance information captured in the system using data visualization, accompanied by commentary, with drill-through capabilities to raw data, whereby individual records can be further investigated and assigned to appropriate personnel for action. Users can also configure custom dashboards or modify template dashboards that can be shared via email or a link to stakeholders.

**1.31 Cloud-hosted Saas must provide the ability for WVDOT to update configuration of interface key field names, layout and attributes without requiring vendor assistance.**

HighBond allows the user to update the configuration of interface key field names, layouts, and attributes without requiring vendor assistance.

**1.32 Cloud-hosted Saas must accommodate any file size or file type with very small data load latency issues.**

HighBond provides and accommodates an unlimited number of file attachments. Each file size limit is 1 GB.

**1.33 Cloud-hosted Saas must integrate with agency-owned Microsoft Power BI report and visualization software.**

Yes, HighBond has full integration with Microsoft Power BI report and visualization software.

2.0 Auditing Cloud-hosted Saas Security Requirements

**2.1 Cloud-hosted Saas Servers must be replicated and load-balanced across data centers and regions.**

HighBond utilizes a combination of Route 53, AWS CloudFront, AWS Shield, AWS WAF, AWS Guardduty, Application Load balancers, and distributed infrastructure within AWS. Amazon CloudFront distributes traffic across multiple edge locations and filters requests. CloudFront also supports geoblocking, which you can use to prevent requests from particular geographic locations from being served. Data is stored and replicated across state-of-the-art data centers operated by Amazon Web Services (AWS). Specifically, data is physically stored in RDS databases on AWS EBS storage blocks attached to dedicated Amazon EC2 server instances. Our system is provided from the following regions: North America (US), North America (Canada), Europe (Germany), Asia Pacific (Singapore), Asia Pacific (Australia), South America (Brazil), Africa (South Africa), GovCloud (US Federal), and GovCloud (US SLED).

**2.2 Cloud-hosted Saas must take backups at a minimum of every four to eight hours and ensure an RPO of four hours.**

Yes, all changes performed in the system are reflected in real-time. Changes to documentation are also synced in real time via online editing.

**2.3 Cloud-hosted Saas must save daily encrypted database backups that are also stored in encrypted, redundant, and versioned storage.**

Yes, all regional equipment is fully redundant data is replicated or backed up to alternate regional locations in case of failure.

In addition to this real-time redundancy, we back up all customer data, including field data and attached documents that are stored in your account within the system.

A full backup of the entire system database is run hourly, daily, and weekly for a one-year period, for the purpose of restoring data integrity due to systemic or database failure, but not for the purpose of restoring user-deleted data.

All data and backups are encrypted at the storage level AND the file level. Backups expire and are automatically deleted after a year. HighBond cannot manually delete customer data from backups.

**2.4 Cloud-hosted Saas must have built in redundancies at the regional, datacenter, hardware, container, and data levels.**

All regional equipment is fully redundant and data is replicated or backed up to alternate regional locations in case of failure. In addition to this real-time redundancy, Diligent backs up all customer data, including field data and attached documents that are stored in your account within the system. A full backup of the entire system database is run hourly, daily, and weekly for a one-year period, for the purpose of restoring data integrity due to systemic or database failure, but

not for the purpose of restoring user-deleted data. Diligent utilizes AWS Availability zones which are physically separated data centers within one region. All data centers are at least 6 miles away from each other.

**2.5 Cloud-hosted Saas must be able to export all data and files to common formats such as CSV.**

Yes, all formats are supported including PDF, XLS, CSV, and DOC. All data elements can be extracted from within the HighBond platform.

**2.6 Cloud-hosted Saas must be accessible and have full functionality from web browsers (eg: Chrome, Edge Firefox)**

Yes, HighBond supports all web browsers (i.e. Edge Firefox, Chrome & Safari, etc.)

**2.7 Cloud-hosted SaaS servers must have 24/7/365 physical security monitoring.**

All product systems are monitored 24/7 for security & availability. In the event of any service interruption, alerts are delivered via email, text message, and phone call to system admins and management. We actively monitor our solutions for availability and performance to a 99.9% + average uptime. Diligent HighBond utilizes AWS Availability zones, which are physically separated data centers within one region. All data centers are at least 6 miles away from each other.

**2.8 Cloud-hosted Saas must have single sign-on ability and work with State owned Active Directory.**

Yes, HighBond provides a single sign-on ability, and an Active directory may be used.

**2.9 Cloud-hosted Saas must have an out of the box role-based pennission(s) or allow for custom roles to restrict what can be viewed or edited down to field level.**

The system is governed via role-based access. Each user is assigned a role at the time of provisioning which defines baseline access. Additional access can be granted on an ad hoc basis at the discretion of a user with a higher permission level.

**2.10 Cloud-hosted SaaS must have the ability for two-factor authentication.**

Two-factor authentication and multi-factor authentication can be provided to the HighBond solution via the customer's identity provider through SSO integration via SAML 2.0

**2.11 Cloud-hosted Saas must have data protection and at a minimum have end-to-end TLS 1.2 encryption or better.**

We provide strong encryption of all data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security)

protocol supporting only the strongest encryption algorithms, including AES (Advanced Encryption Standard) with up to 256-bit key lengths.

Encryption at rest is achieved by leveraging AWS storage encryption, which also relies on the AES encryption algorithm with strong 256-bit keys.

By using TLS version 1.2, an encrypted communication channel between the end-user web browser and the HighBond service is established, ensuring the confidentiality and integrity of all data transmissions from end to end.

**2.12 Cloud-hosted Saas must have storage encryption and protect all WVDOT auditing files, databases and backups with at least AES-256 bit encryption or better before being written to permanent disk storage.**

We provide strong encryption of all data in transit and at rest. Encryption in transit is achieved via the industry-standard TLS (Transport Layer Security) protocol supporting only the strongest encryption algorithms, including AES (Advanced Encryption Standard) with up to 256-bit key lengths.

Encryption at rest is achieved by leveraging AWS storage encryption, which also relies on the AES encryption algorithm with strong 256-bit keys.

**2.13 Cloud-hosted Saas must encrypt all wire transmissions and use hashing controls for sensitive data (passwords), have data loss capabilities at the firewalls and email and utilize TLS for encryption for data in transit and AES for encryption of data at rest.**

All regional equipment is fully redundant and data is replicated or backed up to alternate regional locations in case of failure. In addition to this real-time redundancy, Diligent backs up all customer data, including field data and attached documents that are stored in your account within the system. A full backup of the entire system database is run hourly, daily, and weekly for a one-year period, for the purpose of restoring data integrity due to systemic or database failure, but not for the purpose of restoring user-deleted data. Diligent utilizes AWS Availability zones which are physically separated data centers within one region. All data centers are at least 6 miles away from each other.

**2.14 Cloud-hosted SaaS must use NIST-compliant data sanitization procedures to securely delete data requested by WVDOT that has reached the end of use life.**

At Diligent, we build security into our software. Secure coding best practices are strictly followed.Diligent bases its ISMS on NIST and ISO27001.

Common application layer vulnerabilities, including all OWASP Top 10 vulnerabilities, are explicitly addressed at all stages of the SDLC using industry-standard counter-measures, such as explicit sanitization of all user input, use of parameterized queries, and use of secure libraries. All code changes are controlled and approved and must go through strict peer review and Quality Assurance (QA) testing prior to production deployment.

**2.15 Cloud-hosted Saas audit trails must be strictly monitored to ensure performance, availability, and security.**

A full audit trail exists for all objects in HighBond to monitor to ensure performance, availability, and security.

**2.16 Cloud-hosted Saas audit trails must have audit logs that track every data change made in the system against an authenticated user.**

A full audit trail exists for all objects in HighBond that track every data change made in the system against an authenticated user.

**2.17 Cloud-hosted Saas audit trail must have every successful or failed attempt to access WVDOT Saas Cloud-hosted instance. This data must be recorded and viewable by WVDOT/WVOT.**

All platform activity is captured through event logs and can be reported on, charted, and exported. The audit trail provides every successful or failed attempt to access the platform. Logs are kept until deleted by the client.

3.0 Training & Implementation

**3.1 Vendor must implement, configure, build and setup proposed cloud- hosted Saas for WVDOT.**

Yes, Diligent will implement, configure, build and set up the proposed cloud-hosted Saas for WVDOT.

**3.2 Vendor shall provide the Agency with virtual training within five (5) working days of Cloud-hosted Saas implementation.**

Yes, Diligent can provide the Agency with virtual training within five working days of Cloud-hosted Saas implementation. We will work together based on the WVDOT timeline and provide all support needed.

**3.3 Vendor shall provide on-going training rates for virtual instructor led training.**

Yes, Diligent will provide ongoing training for virtual instructor-led training. Diligent also provides our training academy and helps docs for additional support. Diligent Academy is our online training resource complete with on-demand courses, video tutorials, and certification programs designed to help professionals leverage the entire HighBond platform and obtain CPE credits. Diligent Academy is designed to help increase the skill set of HighBond users to effectively use the software. Diligent offers a certification program which is an effective way to validate HighBond and Analytics skills. Certified users are able to join a group of GRC professionals and a growing network of HighBond power users to exchange questions and experiences. Further, HighBond certification programs are free with a customer's software subscription. Additionally, core HighBond courses are available for traditional classroom delivery from a HighBond expert. Users can access our comprehensive Help Docs (help.highbond.com), which provides them with self-serve and help-style product information, new release announcements, FAQs, and comprehensive quick start and solution guides. Help Docs is supported in English, German, Spanish, French, Portuguese, Japanese, and Chinese. Every ACL subscription includes access to self-help resources in 'Community', a site that allows users to participate in self-help forum discussions, log support tickets with our Support team, and access various free and premium content resources such as tools & templates, a catalog of risks scenarios, an analytics test script library, how-to tutorials, and online courses with CPE credit to name a few.

**3.4 Vendor shall provide on-going training rates for virtual and on-site administrator training.**

Diligent provides ongoing training through an online academy and on-site administrator training can be provided through customer success partners.

Online Academy
Catalog of self-paced online training courses that are NASBA self-study QAS

compliant for CPE credits through Diligent Academy. The online Diligent Academy features on-demand courses, video tutorials, and certification programs designed to help professionals leverage the entire HighBond and Rsam platform and obtain NASBA-compliant CPE credits. Diligent Academy is designed to help increase the skill set of HighBond users to effectively use the software. Diligent offers a certification program which is an effective way to validate platform skills. Certified users are able to join growing groups of professionals and an extensive network of HighBond power users to exchange questions and experiences. Further, HighBond certification programs are free with a customer's software subscription.

Customer success partners and experts with domain knowledge
Customer success plans that provide "beyond technical support" level service through a dedicated Client Partner and Customer Success Manager. Client Partners work closely with customers to help them with their IT RM maturity roadmap including determining the appropriate implementation phases, setting/measuring KPIs for their IT RM program performance, and bringing in the right resources to make sure they are successfully evolving their IT RM journey. Client Partners are a complementary (i.e. included with the subscription) advisory service for customers and are comprised of individuals with extensive consulting (e.g. Big 4) and domain (e.g. cybersecurity) expertise.

Diligent Online Community
Access to interact and share in the Diligent Community platform with like-minded professionals in nearly 6,300 organizations globally. Users can connect, share, and learn from other governance, risk, and compliance professionals, access tools and templates, obtain training and take self-directed learning, and view Diligent's comprehensive Help Docs.

4.0 Technical Support

**4.1 Vendor shall provide technical support for the Cloud-hosted Saas utilizing a primary technical support phone number, ticket portal or primary technical support email address.**

Yes, each client is assigned a dedicated account team and there are various levels of technical support available. The primary technical support phone number and primary technical support email address will be provided.

**4.2 Vendor shall provide a minimum response time of two (2) hours call back for support requests during normal business hours of 8:00 a.m. through 5:00 p.m. Eastern Standard Time Monday through Friday excluding WV state holidays.**

Diligent support teams operate on 24/5 basis (5 days a week, 24 hours, Sunday 3pm to Friday 5pm PST), and 24x7 for online case submission and Diligent Global Community.

CALLS: 99% of all support calls are typically answered in four rings by one of over 320 dedicated support team members. 95% of issues are resolved on the first call.

EMAIL / SUPPORT DESK: Average email/support desk response time = <1 business day.

Please see our Support details here:
https://www.wegalvanize.com/docs/legal/galvanize-master-subscription-agreement.pdf

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Centralized Request for Quote**
**Info Technology**

| | |
|---|---|
| **Proc Folder:** | 1305710 |
| **Doc Description:** | Auditing SaaS RFQ (81240046) |
| **Proc Type:** | Central Master Agreement |
| **Reason for Modification:** | Addendum No. 1 |

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2023-11-01 | 2023-11-07 13:30 | CRFQ 0803 DOT2400000036 | 2 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :** Vertosoft, LLC

**Address :**

**Street :** 1602 Village Market Blvd, Suite 320

**City :** Leesburg

**State :** VA **Country :** United States **Zip :** 20175

**Principal Contact :**

**Vendor Contact Phone:** **Extension:**

**FOR INFORMATION CONTACT THE BUYER**
John W Estep
304-558-2566
john.w.estep@wv.gov

**Vendor Signature X** Jay Colavita **FEIN#** 81-3911287 **DATE** 11.6.2023

**All offers subject to all terms and conditions contained in this solicitation**

## ADDITIONAL INFORMATION

Addendum No. 1

To move the bid opening date from 11/02/2023 to 11/07/2023. The bid opening time remains at 1:30 pm.

See attached pages.

| INVOICE TO | SHIP TO |
|---|---|
| DEPT. OF TRANSPORTATION<br>1900 KANAWHA BLVD E,<br>BLD. 5 RM-720<br><br>CHARLESTON WV<br>US | DEPT. OF TRANSPORTATION<br>1900 KANAWHA BLVD E,<br>BLD. 5 RM-720<br><br>CHARLESTON WV<br>US |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Cloud-based software as a service | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81162000 | | | |

**Extended Description:**
Auditing SaaS RFQ (81240046)

## SCHEDULE OF EVENTS

| Line | Event | Event Date |
|---|---|---|
| 1 | Technical questions due by 2:00 pm | 2023-10-25 |

# SOLICITATION NUMBER: DOT2400000036
# Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

**Applicable Addendum Category:**

[X] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

**Description of Modification to Solicitation:**

1. **To move the bid opening date from 11/02/2023 to 11/07/2023. The bid opening time remains at 1:30 pm.**

**Additional Documentation:** Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

**Terms and Conditions:**

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

**ADDENDUM ACKNOWLEDGEMENT FORM**
**SOLICITATION NO.: DOT24000000367**

**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. 6 |
| [ ] | Addendum No. 2 | [ ] | Addendum No. 7 |
| [ ] | Addendum No. 3 | [ ] | Addendum No. 8 |
| [ ] | Addendum No. 4 | [ ] | Addendum No. 9 |
| [ ] | Addendum No. 5 | [ ] | 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 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.

Vertosoft, LLC

Company

Jay Colavita

Authorized Signature

11.6.2023

Date

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

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

**State of West Virginia**
**Centralized Request for Quote**
**Info Technology**

| | |
|---|---|
| **Proc Folder:** | 1305710 |
| **Doc Description:** | Auditing SaaS RFQ (81240046) |
| **Proc Type:** | Central Master Agreement |
| **Reason for Modification:** | |

| Date Issued | Solicitation Closes | Solicitation No | Version |
|---|---|---|---|
| 2023-10-19 | 2023-11-02 13:30 | CRFQ 0803 DOT2400000036 | 1 |

**BID RECEIVING LOCATION**

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

**VENDOR**

**Vendor Customer Code:**

**Vendor Name :** Vertosoft, LLC

**Address :** 1602

**Street :** Village Market Blvd, Suite 320

**City :** Leesburg

**State :** VA **Country :** United States **Zip :** 20175

**Principal Contact :** Jay Colavita

**Vendor Contact Phone:** 571-707-4130 **Extension:**

**FOR INFORMATION CONTACT THE BUYER**
John W Estep
304-558-2566
john.w.estep@wv.gov

**Vendor Signature X** Jay Colavita **FEIN#** 81-3911287 **DATE** 11.6.23

**All offers subject to all terms and conditions contained in this solicitation**

## ADDITIONAL INFORMATION

REQUEST FOR QUOTATION:

The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Department of Transportation (WVDOT) to establish an open-end contract for auditing cloud-hosted Saas to be utilized by the WV Transportation Division, per the attached documentation.

| INVOICE TO | SHIP TO |
|---|---|
| DEPT. OF TRANSPORTATION<br>1900 KANAWHA BLVD E,<br>BLD. 5 RM-720<br><br>CHARLESTON WV<br>US | DEPT. OF TRANSPORTATION<br>1900 KANAWHA BLVD E,<br>BLD. 5 RM-720<br><br>CHARLESTON WV<br>US |

| Line | Comm Ln Desc | Qty | Unit Issue | Unit Price | Total Price |
|---|---|---|---|---|---|
| 1 | Cloud-based software as a service | 0.00000 | EA | | |

| Comm Code | Manufacturer | Specification | Model # |
|---|---|---|---|
| 81162000 | | | |

**Extended Description:**
Auditing SaaS RFQ (81240046)

## SCHEDULE OF EVENTS

| Line | Event | Event Date |
|---|---|---|
| 1 | Technical questions due by 2:00 pm | 2023-10-25 |

## ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

## INSTRUCTIONS TO VENDORS SUBMITTING BIDS

**1. REVIEW DOCUMENTS THOROUGHLY:** The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

**2. MANDATORY TERMS:** The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

**3. PREBID MEETING:** The item identified below shall apply to this Solicitation.

☑ A pre-bid meeting will not be held prior to bid opening

☐ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

**4. VENDOR QUESTION DEADLINE:** Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: October 25, 2023 by 2:00 pm

Submit Questions to: John Estep, Senior Buyer
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Email: John.W.Estep@wv.gov

**5. VERBAL COMMUNICATION:** Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

**6. BID SUBMISSION:** All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in *wv*OASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

**For Request for Proposal ("RFP") Responses Only:** Submission of a response to a Request for Proposal is not permitted in *wv*OASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus _____convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

**Bid Delivery Address and Fax Number:**
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER:
SOLICITATION NO.:
BID OPENING DATE:
BID OPENING TIME:
FAX NUMBER:

**7. BID OPENING:** Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by *wv*OASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: November 2, 2023 at 1:30 pm

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

**8. ADDENDUM ACKNOWLEDGEMENT:** Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

**9. BID FORMATTING:** Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

**10. ALTERNATE MODEL OR BRAND:** Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

**11. EXCEPTIONS AND CLARIFICATIONS:** The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

**12. COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

**13. REGISTRATION:** Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

**14. UNIT PRICE:** Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

**15. PREFERENCE:** Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

**15A. RECIPROCAL PREFERENCE:** The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

**16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

**17. WAIVER OF MINOR IRREGULARITIES:** The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

**18. ELECTRONIC FILE ACCESS RESTRICTIONS:** Vendor must ensure that its submission in *wv*OASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

**19. NON-RESPONSIBLE:** The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

**20. ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b."

**21. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**22. WITH THE BID REQUIREMENTS:** In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

**23. EMAIL NOTIFICATION OF AWARD:** The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wv*OASIS or the Purchasing Division's website to determine when a contract has been awarded.

**24. ISRAEL BOYCOTT CERTIFICATION:** Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel. This certification is required by W. Va. Code § 5A-3-63.

## GENERAL TERMS AND CONDITIONS:

**1. CONTRACTUAL AGREEMENT:** Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

**2. DEFINITIONS:** As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

**2.1. "Agency"** or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

**2.2. "Bid"** or **"Proposal"** means the vendors submitted response to this solicitation.

**2.3. "Contract"** means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

**2.4. "Director"** means the Director of the West Virginia Department of Administration, Purchasing Division.

**2.5. "Purchasing Division"** means the West Virginia Department of Administration, Purchasing Division.

**2.6. "Award Document"** means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

**2.7. "Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

**2.8. "State"** means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

**2.9. "Vendor"** or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

**3. CONTRACT TERM; RENEWAL; EXTENSION:** The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

**Initial Contract Term:** The Initial Contract Term will be for a period of one (1) year _____. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

**Renewal Term:** This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to four (4) _____ successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

**Delivery Order Limitations:** In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for _____ years;

☐ the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in _____

**4. AUTHORITY TO PROCEED:** Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

**5. QUANTITIES:** The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☑ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☑ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

**6. EMERGENCY PURCHASES:** The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

**7. REQUIRED DOCUMENTS:** All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☑ If applicable, please see specifications

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

**8. INSURANCE:** The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: 1,000,000.00 per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☑ **Cyber Liability Insurance** in an amount of: $1,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

**9. WORKERS' COMPENSATION INSURANCE:** Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

**10. VENUE:** All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

**11. LIQUIDATED DAMAGES:** This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ _____ for _____.

☐ Liquidated Damages Contained in the Specifications.

☑ Liquidated Damages Are Not Included in this Contract.

**12. ACCEPTANCE:** Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

**13. PRICING:** The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

**14. PAYMENT IN ARREARS:** Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

**15. PAYMENT METHODS:** Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

**16. TAXES:** The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

**17. ADDITIONAL FEES:** Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

**18. FUNDING:** This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

**19. CANCELLATION:** The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

**20. TIME:** Time is of the essence regarding all matters of time and performance in this Contract.

**21. APPLICABLE LAW:** This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

**22. COMPLIANCE WITH LAWS:** Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**23. ARBITRATION:** Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

**24. MODIFICATIONS:** This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

**25. WAIVER:** The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

**26. SUBSEQUENT FORMS:** The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

**27. ASSIGNMENT:** Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

**28. WARRANTY:** The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

**29. STATE EMPLOYEES:** State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

**30. PRIVACY, SECURITY, AND CONFIDENTIALITY:** The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

**31. YOUR SUBMISSION IS A PUBLIC DOCUMENT:** Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

**32. LICENSING:** In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

**SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

**33. ANTITRUST:** In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

**34. VENDOR NON-CONFLICT:** Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

**35. VENDOR RELATIONSHIP:** The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

**36. INDEMNIFICATION:** The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

**37. NO DEBT CERTIFICATION:** In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming 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, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

**38. CONFLICT OF INTEREST:** Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

**39. REPORTS:** Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☐ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

**40. BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

**41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS:** Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

    2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

**42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL:** In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

**43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE:** W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

**44. PROHIBITION AGAINST USED OR REFURBISHED:** Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

**45. VOID CONTRACT CLAUSES:** This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

**46. ISRAEL BOYCOTT:** Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

**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.

(Printed Name and Title) Jay Colavia - President

(Address) 1602 Village Market Blvd, Suite 320, Leesburg, VA 20175

(Phone Number) / (Fax Number) 571-707-4130

(email address) Jay@vertosoft.com

**CERTIFICATION AND SIGNATURE:** By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract 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/Contract 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; 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; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.*

Vertosoft, LLC
(Company)

Jay Colavita
(Signature of Authorized Representative)

Jay Colavita, President
(Printed Name and Title of Authorized Representative) (Date)

571-707-4130
(Phone Number) (Fax Number)

Jay@vertosoft.com
(Email Address)

REQUEST FOR QUOTATION
**Open-End Contract for Auditing Cloud-Hosted SaaS (81230134)**
**CRFQ DOT24*36**

## SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Department of Transportation (WVDOT) to establish an open-end contract for Auditing Cloud-hosted SaaS to be utilized by the West Virginia Transportation Auditing Division.

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

   **2.1.** **"Contract Item"** means the list of items identified in Section 3.1 below and on the Pricing Pages.

   **2.2.** **"Pricing Pages"** means the schedule of prices, estimated order quantity, and totals contained in wvOASIS or attached hereto as Exhibit A, and used to evaluate the Solicitation responses.

   **2.3.** **"SaaS"** means Software as a Service

   **2.4.** **"Solicitation"** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

   **2.5.** **"Working Papers"** means audit documentation is an essential element of audit quality. The process of preparing and reviewing audit documentation contributes to the quality of an audit. Audit documentation serves to (1) provide the principal support for the audit report, (2) aid auditors in conducting and supervising the audit, and (3) allow for the review of audit quality.

3. **QUALIFICATIONS:** Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

   **3.1.** Vendor must provide, upon request, documentation showing their experience with having successfully completed implementation of an existing Auditing Cloud-hosted SaaS with workflows within an organization of similar size and complexity or larger than WVDOT before contract award.

   **3.2.** Vendor must provide, upon request, proof as an authorized reseller of the proposed Auditing Cloud-hosted SaaS or a Sole Source letter if the Cloud-hosted SaaS is proprietary to the vendor before contract award.

   **3.3.** Vendor must provide, upon request, proof their proposed solution is ISO 27001 certified (SOC-2) before contract award.

## 4. GENERAL REQUIREMENTS:

**4.1. Mandatory Contract Item Requirements:** The Vendor shall provide Agency with the Contract Items listed below. Contract Items must meet or exceed the mandatory requirements listed below.

### 4.1.1. General Auditing Cloud-hosted SaaS Operating Requirements

**4.1.1.1.** Cloud-hosted SaaS must have the capability to store hundreds of audit files per fiscal year.

**4.1.1.2.** Cloud-hosted SaaS must have the capability to create and maintain a library of findings and create templates by individual client or engagement.

**4.1.1.3.** Cloud-hosted SaaS must include a subscription for up to a minimum of twenty-five (25) users in the audit work papers system concurrently from multiple locations, allow for at least one thousand five hundred (1500) audits annually, allow at least one hundred (100) automated integration workflows annually, allow at least fifty (50) automated integration monitors annually and must include unlimited stakeholders.

**4.1.1.3.1.** Cloud-Hosted SaaS must have the ability to add additional core user licenses as requested and purchased by the Agency.

**4.1.1.4.** Cloud-hosted SaaS must have the capability for the client to create work papers, audit programs, reports, and templates for use.

**4.1.1.5.** Cloud-hosted SaaS must filter work papers by client, engagement type, fiscal year, or by auditor.

**4.1.1.6.** Cloud-hosted SaaS must support and integrate with agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu (PDF) programs for searching, retrieval and saving of documents.

**4.1.1.7.** Cloud-hosted SaaS must be compatible with states Google email system.

**4.1.1.8.** Cloud-hosted SaaS must have the ability to assign hierarchy of roles for users.

**4.1.1.9.** Cloud-hosted SaaS must have the capability of add/alter client information, auditors, approvers, reviewers, and administrative personnel.

**4.1.1.10.** Cloud-hosted SaaS must be able to create assignments to specific users.

**4.1.1.11.** Cloud-hosted SaaS must have the capability to retrieve prior audit information from agency owned Teammate Software. This information would reference prior completed set of working papers for a particular entity.

**4.1.1.12.** Cloud-hosted SaaS must have the capability to convert past audit work papers from agency owned current TEAMMATE software.

**4.1.1.13.** Cloud-hosted SaaS must allow users have the capability to view, alter and create multiple workpapers at the same time.

**4.1.1.14.** Cloud-hosted SaaS must have evidence of workpaper completion and review by whom and the date completed.

**4.1.1.15.** Cloud-hosted SaaS must have controls over workpaper sharing and have the capability for different employees to alter same work paper.

**4.1.1.16.** Cloud-hosted SaaS must allow peer review team to view work papers.

**4.1.1.17.** Cloud-hosted SaaS must have the capability to leave reviewer comments notes for work paper corrections that can be removed by reviewer.

**4.1.1.18.** Cloud-hosted SaaS must have indicators that work papers have been altered and needs reviewed.

**4.1.1.19.** Cloud-hosted SaaS must have the capability to reference or link support documentation.

**4.1.1.20.** Cloud-hosted SaaS must automatically generate audit reports to agency owned Microsoft Office Suite, Google Workspace, Adobe Acrobat Professional and Bluebeam Revu with indicators of each engagement in progress.

**4.1.1.21.** Cloud-hosted SaaS must have the capability to run macros in agency owned Microsoft Office Suite software while in the audit Cloud-hosted SaaS system.

**4.1.1.22.** Cloud-hosted SaaS must have the capability to lock down work papers and have the capability of removing this lock if necessary.

**4.1.1.23.** Cloud-hosted SaaS must have the capability to access multiple clients working files at the same time.

**4.1.1.24.** Cloud-hosted SaaS must have the ability to spell and grammar-check text fields.

**4.1.1.25.** Cloud-hosted SaaS must have the capability to store client files on an external hard drive.

**4.1.1.26.** Cloud-hosted SaaS must have the capability to tick mark or reference agency owned Acrobat Adobe Professional or Bluebeam PDF software.

**4.1.1.27.** Cloud-hosted SaaS must have indicators that work paper has been changed after reviewer sign off.

**4.1.1.28.** Cloud-hosted SaaS must have the capability to run reports to compile data information such as number of audits completed, number of audits in progress, number of findings issued, audit hours per engagement, audit hours per auditor, audit hours per fiscal year for a section and for entire Division.

**4.1.1.29.** Cloud-hosted SaaS must have a dedicated audit workflow process and pages for each audit with configurable sections for planning, fieldwork, and reporting in a straightforward to navigate user interface.

**4.1.1.30.** Cloud-hosted SaaS must provide the ability for end-users to configure reporting dashboards straightforward without the need for vendor support or enchantment.

**4.1.1.31.** Cloud-hosted SaaS must provide the ability for WVDOT to update configuration of interface key field names, layout and attributes without requiring vendor assistance.

**4.1.1.32.** Cloud-hosted SaaS must accommodate any file size or file type with very small data load latency issues.

**4.1.1.33.** Cloud-hosted SaaS must integrate with agency-owned Microsoft Power BI report and visualization software.

**4.1.2. Auditing Cloud-hosted SaaS Security Requirements**

**4.1.2.1.** Cloud-hosted SaaS Servers must be replicated and load-balanced across data centers.

**4.1.2.2.** Cloud-hosted SaaS must take backups at a minimum every four to eight hours and ensure an RPO of four hours.

**4.1.2.3.** Cloud-hosted SaaS must save daily encrypted database backups that are also stored in encrypted, redundant, and versioned storage.

**4.1.2.4.** Cloud-hosted SaaS must have built in redundancies at the regional, datacenter, hardware, container, and data levels.

**4.1.2.5.** Cloud-hosted SaaS must be able to export all data and files to common formats such as CSV.

**4.1.2.6.** Cloud-hosted SaaS must be accessible and have full functionality from web browsers (eg: Chrome, Edge Firefox)

**4.1.2.7.** Cloud-hosted SaaS servers must have 24/7/365 physical security monitoring.

**4.1.2.8.** Cloud-hosted SaaS must have single sign-on ability and work with State owned Active Directory.

**4.1.2.9.** Cloud-hosted SaaS must have an out of the box role-based permission(s) or allow for custom roles to restrict what can be viewed or edited down to field level.

**4.1.2.10.** Cloud-hosted SaaS must have the ability for two-factor authentication.

**4.1.2.11.** Cloud-hosted SaaS must have data protection and at a minimum have end-to-end TLS 1.2 encryption or better.

**4.1.2.12.** Cloud-hosted SaaS must have storage encryption and protect all WVDOT auditing files, databases and backups with at least AES-256 bit encryption or better before being written to permanent disk storage.

**4.1.2.13.** Cloud-hosted SaaS must encrypt all wire transmissions and use hashing controls for sensitive data (passwords), have data loss capabilities at the firewalls and email and utilize TLS for encryption for data in transit and AES for encryption of data at rest.

**4.1.2.14.** Cloud-hosted SaaS must use NIST-compliant data sanitization procedures to securely delete data requested by WVDOT that has reached the end of use life.

**4.1.2.15.** Cloud-hosted SaaS audit trails must be strictly monitored to ensure performance, availability, and security.

**4.1.2.16.** Cloud-hosted SaaS audit trails must have audit logs that track every data change made in the system against an authenticated user.

**4.1.2.17.** Cloud-hosted SaaS audit trail must log every successful and failed attempt to access WVDOT SaaS Cloud-hosted instance. Vendor shall provide information concerning such successful or failed attempts to WVDOT/WVOT upon WVDOT/WVOT's request.

**4.1.3. Training & Implementation**

**4.1.3.1.** Vendor must implement, configure, build and setup proposed cloud-hosted SaaS for WVDOT.

**4.1.3.2.** Vendor shall provide the Agency with virtual training within five (5) working days of Cloud-hosted SaaS implementation.

**4.1.3.3.** Vendor shall provide on-going training rates for virtual instructor led training.

**4.1.3.4.** Vendor shall provide on-going training rates for virtual and on-site administrator training.

**4.1.4. Technical Support**

**4.1.4.1.** Vendor shall provide technical support for the Cloud-hosted SaaS utilizing a primary technical support phone number, ticket portal or primary technical support email address.

**4.1.4.2.** Vendor shall provide a minimum response time of two (2) hours call back for support requests during normal business hours of 8:00 a.m. through 5:00 p.m. Eastern Standard Time Monday through Friday excluding WV state holidays.

**4.1.5. Cloud-Hosted SaaS Professional Services Support**

**4.1.5.1.** Experienced Cloud-hosted SaaS consultants, analysts and software developers shall be available to assist WVDOT with software/workflow installation/configuration/ customizations.

**4.1.5.2.** Vendor shall provide both a virtual and on-site rate.

**4.1.5.3.** A Statement of Work (SOW) shall be developed that identifies the following:

**4.1.5.3.1.** Tasks to be performed.

**4.1.5.3.2.** Deliverables.

**4.1.5.3.3.** Staff assigned, resumes and experience level.

**4.1.5.3.4.** Cost breakdown based on the rates bid in this RFQ.

**4.1.5.3.5.** WVDOT shall review and approve the SOW before commencing of any services.

**4.1.6. Terms and Conditions**

**4.1.6.1.** Vendor should provide with their bid a copy of any software licensing and or support terms and conditions to which the State of West Virginia or the Agency must agree to or accept, either in writing or digitally, in order to receive the commodities or services offered as part of this contract. Written terms will be required prior to the award of any contract resulting from this solicitation. Failure to provide additional terms and conditions may result in disqualification or cancellation of the vendor's bid or contract.

**4.2. Acceptance of System and Test Period**

**4.2.1.** Once the open-end contract for Auditing Cloud-hosted SaaS has been awarded, the Agency will release a Central Delivery Order (CDO). Upon issuance of the CDO, the Agency will commence, in conjunction with the awarded vendor, a test period for up to thirty (30) days of the Auditing Cloud-hosted SaaS.

If the test period produces no issues at a minimum, the Agency will issue a Letter of Acceptance of the system. Prior to an Acceptance of the system, the following criteria must be met: (1) successful testing of all components and (2) validating full functionality.

Once the Acceptance of the system is agreed upon by both the Agency and Vendor, the contract subscription period will then begin. The Agency will issue a request for a Change Order to the CDO, stating the acceptance of the system and thereby beginning the first year of the subscription.

## 5. CONTRACT AWARD:

**5.1. Contract Award:** The Contract is intended to provide the Agency with a purchase price on all Contract Items. The Contract shall be awarded to the Vendor that provides the Contract Items meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

**5.2. Pricing Pages:** Vendor shall complete the Pricing Pages by completing the cost table included as Exhibit A. The Vendor shall complete the Pricing Pages in their entirety as failure to do so may result in Vendor's bids being disqualified.

The Pricing Pages contain a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

## 6. ORDERING AND PAYMENT:

**6.1. Ordering:** Vendor shall accept orders through wvOASIS, regular mail, facsimile, e-mail, or any other written form of communication. Vendor may, but is not required to, accept on-line orders through a secure internet ordering portal/website. If Vendor has the ability to accept on-line orders, it should include in its response a brief description of how Agencies may utilize the on-line ordering system. Vendor shall ensure that its on-line ordering system is properly secured prior to processing Agency orders on-line.

**6.2. Payment**: Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.

## 7. DELIVERY AND RETURN:

**7.1. Shipment and Delivery:** Vendor shall deliver the Contract Items within ten (10) working days after being awarded this Contract and receiving a purchase order or notice to proceed.

**7.2. Late Delivery:** The Agency placing the order under this Contract must be notified in writing if the shipment of the Contract Items will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the Contract, and/or obtaining the Contract Items from a third party.

Any Agency seeking to obtain the Contract Items from a third party under this provision must first obtain approval of the Purchasing Division.

**7.3. Delivery Payment/Risk of Loss:** Vendor shall deliver the Contract Items F.O.B. destination to the Agency's location. Vendor shall include the cost of order delivery charges in its bid pricing/discount and is not permitted to charge the Agency separately for such delivery.

**7.4. Return of Unacceptable Items:** If the Agency deems the Contract Items to be unacceptable, the Contract Items shall be returned to Vendor at Vendor's expense and with no restocking charge. Vendor shall either make arrangements for the return within five (5) days of being notified that item(s) are unacceptable or permit the Agency to arrange for the return and reimburse Agency for delivery expenses. If the original packaging cannot be utilized for the return, Vendor will supply the Agency with appropriate return packaging upon request. All returns of unacceptable items shall be F.O.B. the Agency's location. The returned product shall either be replaced, or the Agency shall receive a full credit or refund for the purchase price, at the Agency's discretion.

**7.5. Return Due to Agency Error:** Items ordered in error by the Agency will be returned for credit within 30 days of receipt, F.O.B. Vendor's location. Vendor shall not charge a restocking fee if returned products are in a resalable condition. Items shall be deemed to be in a resalable condition if they are unused and in the original packaging. Any restocking fee for items not in a resalable condition shall be the lower of the Vendor's customary restocking fee or 5% of the total invoiced value of the returned items.

8. **TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.

9. **VENDOR DEFAULT:**

**9.1.** The following shall be considered a vendor default under this Contract.

**9.1.1.** Failure to provide Contract Items in accordance with the requirements contained herein.

**9.1.2.** Failure to comply with other specifications and requirements contained herein.

**9.1.3.** Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

**9.1.4.** Failure to remedy deficient performance upon request.

**9.2.** The following remedies shall be available to the Agency upon default.

**9.2.1.** Immediate cancellation of the Contract.

**9.2.2.** Immediate cancellation of one or more release orders issued under this Contract.

**9.2.3.** Any other remedies available in law or equity.

10. **MISCELLANEOUS:**

**10.1.** **No Substitutions**: Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

**10.2.** **Vendor Supply:** Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

**10.3.** **Contract Manager:** During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

**Contract Manager:** _____

**Telephone Number:** _____

**Fax Number:** _____

**Email Address:** _____

# EXHIBIT A - PRICING PAGE - CRFQ DOT24*36

| Auditing Cloud-Hosted SaaS RFQ (81240046) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| LOCATION: BUILDING 5, ROOM A-720, CHARLESTON, WV 25305 | | | | | | | | | |
| **Contract Item Number** | **Description*** | **Unit of Measure** | **Estimated Quantity*** | **Year One Unit Cost** | **Optional - Year Two Unit Cost** | **Optional - Year Three Unit Cost** | **Optional - Year Four Unit Cost** | **Optional - Year Five Unit Cost** | **Extended Cost** |
| **Auditing Cloud-Hosted SaaS Subscription / License** | | | | | | | | | |
| 4.1.1, 4.1.2, 4.1.1.2. | Enterprise SaaS Subscription - Must at a minimum include 25 core user licenses, 1500 audits anually, 100 integration workflows (automation) annually, 50 integration monitors (automation) anually and unlimited stakeholders | LS | 1 | | | | | | $0.00 |
| 4.1.1, 4.1.2, 4.1.1.2.1 | Enterprise SaaS Subscription Per Additional Core User (per license) | EA | 1 | | | | | | $0.00 |
| **Auditing Cloud-Hosted SaaS Services**** | | | | | | | | | |
| 4.1.3.1 | Initial Cloud-Hosted SaaS Implementation Fee (lump sum) | LS | 1 | | | | | | $0.00 |
| 4.1.3.2 | Initial Cloud-Hosted SaaS Virtual Instructor Led Training (hourly rate) | EA | 4 | | | | | | $0.00 |
| 4.1.3.3 | Virtual Instructor Led-Training (hourly rate) | EA | 25 | | | | | | $0.00 |
| 4.1.3.4 | Virtual Adminstrator Training (hourly rate) | EA | 25 | | | | | | $0.00 |
| 4.1.3.4 | On-Site System Adminstrator Training (hourly rate) | EA | 25 | | | | | | $0.00 |
| 4.1.5 | Cloud-Hosted SaaS Professional Services Support On-Site Rate (hourly rate) | EA | 25 | | | | | | $0.00 |
| 4.1.5 | Cloud-Hosted SaaS Professional Services Support Virtual Rate (hourly rate) | EA | 25 | | | | | | $0.00 |
| | | | | | | **OVERALL TOTAL COST:** | | | **$0.00** |

*** The estimated purchase volume for new licenses represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.**
****TRAVEL: Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately. Location: 1900 Kanawha Boulevard E. Building 5, Charleston, WV 25305**
*****Optional Renewals- Year Two through Year Five may be renewed by Change Order upon mutual agreement between the Vendor and Agency.**

_____

Vendor Signature

# Software as a Service Addendum

## 1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

**2. Data Ownership:** The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

**3. Data Protection and Privacy:** Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

**4. Security Incident or Data Breach Notification:** The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

**5. Breach Responsibilities:** This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

**6. Notification of Legal Requests:** The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

**7. Termination and Suspension of Service:**

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

**8. Background Checks:** The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

**9. Oversight of Authorized Persons:** During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

**10. Access to Security Logs and Reports:** The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

**11. Data Protection Self-Assessment:** The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**12. Data Center Audit:** The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

**13. Change Control and Advance Notice:** The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

**14. Security:**

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

**15. Non-disclosure and Separation of Duties:** The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

**16. Import and Export of Data:** The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

**17. Responsibilities:** The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

**18. Subcontractor Compliance:** The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

**19. Right to Remove Individuals:** The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

**20. Business Continuity and Disaster Recovery:** The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

**21. Compliance with Accessibility Standards:** The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

**22. Web Services:** The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

**23. Encryption of Data at Rest:** The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

**24. Subscription Terms:** Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

**25. Equitable Relief:** Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

| | |
|---|---|
| Name of Agency: _____ | Name of Vendor: Vertosoft, LLC |
| Signature: _____ | Signature: Jay Colavita |
| Title: _____ | Title: President |
| Date: _____ | Date: 11.6.2023 |

# Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐
2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐
3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐
5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: _____

   Email address: _____

   Phone Number: _____ _____