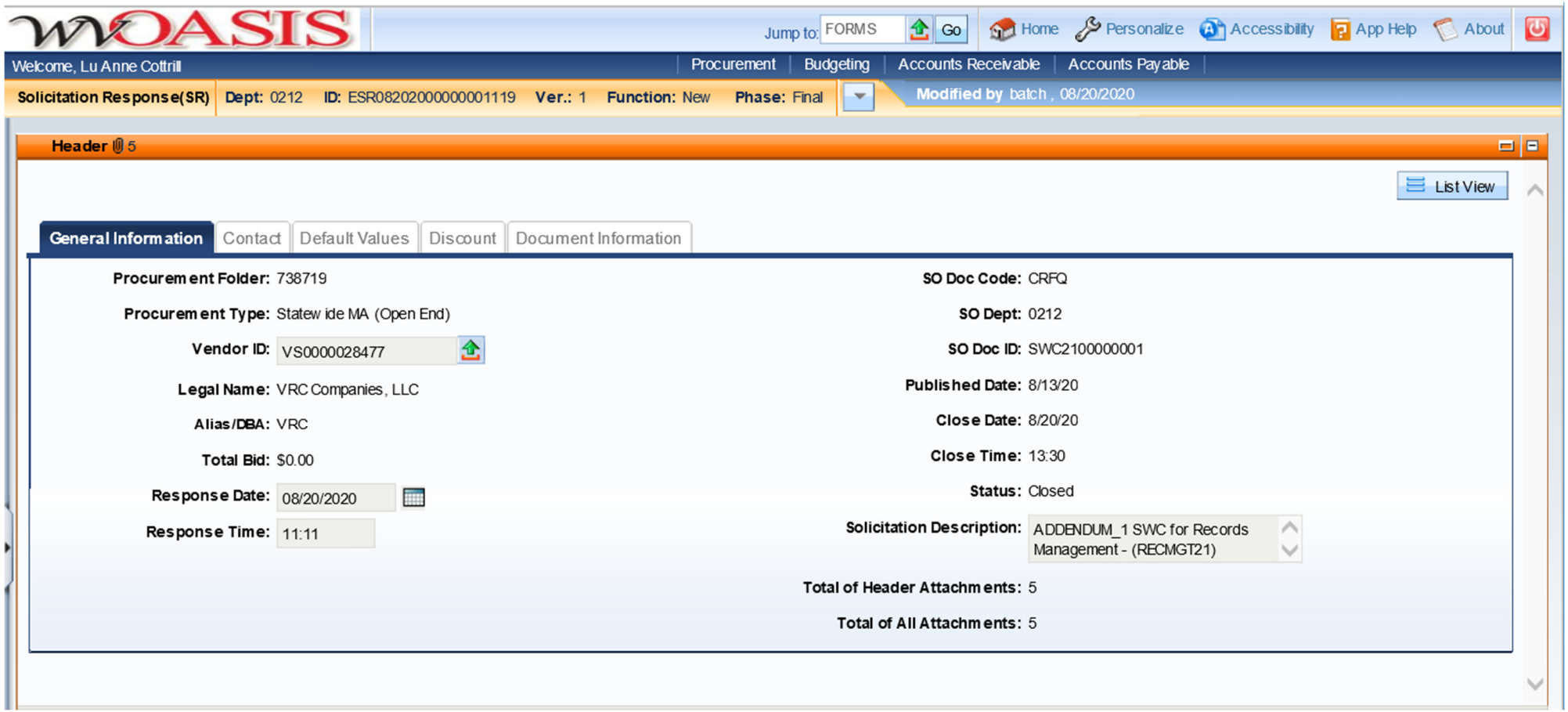
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0212 ID: ESR08202000000001119 Ver.: 1 Function: New Phase: Final
Modified by batch , 08/20/2020
Header 5
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 738719
Procurement Type: Statew ide MA (Open End)
Vendor ID: VS0000028477
Legal Name: VRC Companies, LLC
Alias/DBA: VRC
Total Bid: $0.00
Response Date: 08/20/2020
Response Time: 11:11
SO Doc Code: CRFQ
SO Dept: 0212
SO Doc ID: SWC2100000001
Published Date: 8/13/20
Close Date: 8/20/20
Close Time: 13:30
Status: Closed
Solicitation Description: ADDENDUM_1 SWC for Records Management - (RECMGT21)
Total of Header Attachments: 5
Total of All Attachments: 5

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

State of West Virginia
Solicitation Response

Proc Folder : 738719

Solicitation Description : ADDENDUM_1 SWC for Records Management - (RECMGT21)

Proc Type : Statewide MA (Open End)

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-08-20 13:30:00	SR 0212 ESR08202000000001119	1

VENDOR

VS0000028477

VRC Companies, LLC

VRC

Solicitation Number: CRFQ 0212 SWC2100000001

Total Bid : $0.00 **Response Date:** 2020-08-20 **Response Time:** 11:11:02

Comments:

FOR INFORMATION CONTACT THE BUYER

Mark A Atkins

(304) 558-2307
mark.a.atkins@wv.gov

Signature on File **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
2	Document Storage Services	0.00000	LS	$0.230000	$0.00

Comm Code	Manufacturer	Specification	Model #
78131804			

Extended Description :

Document Storage Services:

Note: Vendor shall use Exhibit_A Pricing Page for bid pricing.

If vendor is submitting a bid online, Vendor should enter $0.00 in the Oasis commodity line.

August 20th, 2020

Mr. Mark Atkins
State of West Virginia

RE: Executive Summary - Offer from Vital Records Control ("VRC") for Off-Site Records Storage

Dear Mr. Atkins:

Thank you for taking the time to consider a proposal from VRC regarding potentially consolidating offsite records storage and services for the State of West Virginia. VRC has a long and successful history of servicing agencies like yours. VRC has operated a facility in White Sulphur Springs for the last 5 years and we are honored to be part of this bid process.

Based on the information given, VRC can confidently state that by switching vendors, VRC can save the state a substantial amount of money annually. VRC is uniquely positioned to assist your agency in customizing a records and information management program to fit your needs. VRC has a specific recent history of doing exactly what we are proposing to the state.

VRC has established itself as a leader in the information management industry for over thirty years beginning in Memphis, with over twenty combined years in West Virginia (EveryChart). VRC has quietly assumed a place among the top three off-site records storage and destruction companies in the nation (over 65 nationwide facilities) while maintaining a strict focus on our customers. VRC has scored at least a 95% customer satisfaction scoring of excellent or superior at every VRC location for the last thirty plus years and is known for providing customized solutions at or below market pricing.

VRC is a great choice for the state and we are large enough to handle the complexities of this consolidation opportunity, but small enough to value your business, do it right the first time, and customize the solutions the state will need. VRC's proposal presents a 'depot' concept that we have used successfully for several enterprise accounts similar in size to the state, such as International Paper, HCA, Regions Bank, FedEx, and SunTrust Bank. VRC will relocate all inventory from Iron Mountain to our in-state facility in White Sulphur Springs or a possible new facility in Charleston. VRC will tag each box with a RFID barcode for easy processing and from there, the system will alert us if any inventory is "flagged" for review before shelving. VRC will then use the most current Iron Mountain inventory spreadsheet for data mapping purposes. VRC is prepared to move as fast as Iron Mountain will allow.

Based on our experience, we feel there are three major areas in which VRC can be of benefit to the state. These areas are in Compliance, Facilities, and Services and we have highlighted some areas below for your review:

Compliance

- **All** VRC facilities are SSAE 18 Certified (SOC2 TYPE2)
- VRC is a member of all the leading information management associations
- VRC is certified by multiple authorities and adheres to HIPAA, FACTA, NAID, NARA, Sarbanes-Oxley, and PCI among other standards
- VRC maintains an in-house Compliance Executive and team
- VRC has a comprehensive initial training and subsequent refresher training for all employees
- All employees must pass a ten-year background check including motor vehicle records, credit status, and criminal.
- All employees are bonded and insured

Facilities

- Controlled access to enter the facility and controlled access to secure storage areas
- Solid concrete construction
- ESFR (Early Suppression Fast Response) fire protection systems
- Customized storage racking with metal decking (no wood)
- VRC is a full-service records company that does not store any hazardous items
- Backup generators
- Seismic racking systems
- 24hr live security monitoring and recording of all cameras
- Bay doors are down and locked at all time unless loading or unloading
- All delivery vehicles are unmarked and equipped with GPS tracking
- Only employees and vendors (with a signed confidentiality agreement and escort) are allowed in the storage areas

Services

- VRC utilizes **VitalRF®** (RFID) technology to track all box and file movements
- Requests made to VRC by 10:00 am will be delivered the same day (local)
- Requests made to VRC by 3:00 pm will be delivered by noon the following business day (local)
- Free access to VRC's on-line inventory system **VitalWeb®**:
  - Search, review, sort inventory by department or in total
  - Create and print customized reports
  - Order boxes from storage
  - Add new boxes into inventory
  - Request, view, print or save documents instantly
- VRC will provide rapid time sensitive services including "**VitalScan®**" (scan on demand services) for immediate needs
- VRC can provide your inventory data in a variety of formats
- VRC provides no charge viewing rooms at VRC for customers to view records without having them delivered to your office

Highlights of VRC's Total Consolidation Proposal – Initial Transition to VRC:

- No up-front cost to the state whatsoever
  - VRC will reimburse the state for permanent removal fees from other vendors
  - VRC will provide all the needed transportation
  - VRC will waive all the inductions fees to add the inventory to VRC
  - VRC will lock in ALL rates for the entire initial term
  - The state is, effectively, receiving a free audit of all its boxes

The specifics of this proposal include:

Initial setup: $0.00

- VRC is willing to reimburse the state for reasonable removal fees to pull any boxes currently stored at other vendors and send to VRC
- VRC will pay for all transportation to get the records from the internally managed warehouses or existing vendor(s) to VRC
- No charge for the initial setup of all boxes into VRC's system
- No charge for the electronic data transfer from the state's internal systems or other vendor(s)
- The state may review the collections of transferred records at **no cost** prior to shelving of the boxes

Storage:

- **$0.23** per cubic foot per month for storage

Basic Services:

- Access in or out of boxes – First 250 Box Accesses are INCLUDED in the $0.23 per cubic foot storage rate. $2.00 per box (not cubic foot) after initial monthly 250
- Local Delivery – INCLUDED in the $0.23 per cubic foot storage rate
- Use of viewing rooms at VRC – No charge
- Induction - $1.00 per box (no charge for initial collections sent to VRC)
- Purchase of storage boxes - $2.00 per letter/legal box
- **VitalScan - Scan on Demand** – per page - $0.10 ($5.00 minimum)

Highlights of VRC's Proposal – On-Going with VRC:

- VRC charges for all services **by the box**, not the cubic foot. Most companies in the industry charge by the cubic foot for services resulting in 30% to 60% higher service rates
- VRC does not charge a handling, transportation or minimum order fee for each item delivered or picked-up from its customers.
- VRC does not charge department setup minimums or administration fees.
- VRC is including the first 250 Accesses and all Deliveries in the $0.23 cubic foot storage rate

Additional Services

The following is a list of additional service offerings within the VRC family of companies that are not specifically a part of the off-site records storage proposal prepared today for your review:

- **VitalShred®** - NAID compliant destruction services (onsite or offsite)
- Vital Vaulting Services – backup media vaulting for physical tapes
- Vital Vaulting Services - electronic vaulting for media backups
- VitalScan® Imaging – conversion services for turning paper records into digital images
- VRC provides project specific indexing services

VRC recognizes, envisions and is ready for the transition from paper to digital and other electronic document formats. VRC is one of the leading document conversion companies in the U.S. VRC itself has eliminated all paper forms other than chain of custody documents and assisted its clients in paper reduction strategies. VRC is an information governance partner rather than a simple storage-oriented company.

We hope this information provides you with an overview of the primary costs for using VRC and it hopefully demonstrates the sincere desire to partner with the State of West Virginia to manage your invaluable records and destruction. VRC is a turn-key management solution rather than just a storage solution.

Respectfully Submitted,

Chris Ferrell

Chris Ferrell
Chief Development Officer

EXHIBIT_A PRICING PAGE

CRFQ 0212 SWC2100000001
(RECMGT21)

Records Management - Offsite Storage and Document Destruction

Commodity Line Number	Description	Unit of Measure	Estimated Quantity	Unit Price	Extended Price
STORAGE:					
5.2.1.1 Contract Item #1	Transferring Existing Records to New Storage Facility	Per Cubic Foot	195,000	No Charge	$0.00
5.2.2.1 Contract Item #2	Indexing Existing Records at time of Transfer from existing Storage Facility	Per Box	195,000	No Charge	$0.00
5.2.3.1 Contract Item #3	Records Monthly Storage Fee	Per Cubic Foot	195,000	$ 0.23	$ 44,850.00
SUPPLIES:					
5.2.4.1 Contract Item #4	Storage Boxes (Aproximate Demensions 15"L x 12"W x 10"H)	Per Box	5,000	$ 2.00	$ 10,000.00
PICK UP:					
5.2.5.1 Contract Item #5	Records Pick Up (within 5 business days of request)	Per Box	2,500	$ -	$ -
5.2.6.1 Contract Item #6	Indexing New Records	Per Box	2,500	$ -	$ -
RETRIEVAL/DELIVERY:					
5.2.7.1 Contract Item #7	Retrieval/Delivery of Paper Records [Five (5) Business Day of Written Request]	Per Box	5,000		$ -
5.2.8.1 Contract Item #8	Emergency Retrieval/Delivery of Paper Records [Three (3) Calendar Days of Written Request]	Per Box	500	$ 2.00	$ 1,000.00
SECURE VIEWING AREA:					
5.2.9 Contract Item #9	Secure Area at Vendor's Facility for Records Viewing	Each (Per Visit)	100	No Charge	$0.00
DESTRUCTION:					
5.2.10.4 Contract Item #10	Destruction of Paper Records	Per Box	5,000	$ 3.00	$ 15,000.00
5.2.11.4 Contract Item #11	Destruction of Microfilm	Per Box	50	$ 18.00	$ 900.00

Total Cost	$ 71,750.00

Please type or print legibly

Vendor: _(VRC) Vital Records Control_____

Vendor Representative: __Chris Ferrell_____

Phone Number: __407-433-8732_____

Email: __cferrell@vrcnetwork.com_____

WV STATE GOVERNMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate") , and is effective as of the date of execution of the Addendum.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to discloses to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW, THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. Definitions. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

    a. Agency Procurement Officer shall mean the appropriate Agency individual listed at: http://www.state.wv.us/admin/purchase/vrc/agencyll.html.

    b. Agent shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of agency, as referenced in 45 CFR § 160.402(c).

c. Breach shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.

d. Business Associate shall have the meaning given to such term in 45 CFR § 160.103.

e. HITECH Act shall mean the Health Information, Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111th Congress (2009).

f. Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.

g. Protected Health Information or PHI shall have the meaning given to such term in 45 CFR § 160.103, limited to the information created or received by Associate from or on behalf of Agency.

h. Security incident means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

i. Security Rule means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.

j. Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

2. Permitted Uses and Disclosures.

a. PHI Described. This means PHI created, received, maintained or transmitted on behalf of the Agency by the Associate. This PHI is governed by this Addendum and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the original Agreement, and is described in Appendix A.

b. Purposes. Except as otherwise limited in this Addendum. Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, or as required by law, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency. The Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Agency.

c. Further Uses and Disclosures. Except as otherwise limited in this Addendum, the Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (I) the disclosure is required by law, or (II) the Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Associate; and, (III) an agreement to notify the Associate and Agency of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or take other measures as necessary to satisfy the Agency's obligations under 45 CFR § 164.502.

3. Obligations of Associate

a. Stated Purposes Only. The PHI may not be used by the Associate for any purpose other than as stated in this Addendum or as required or permitted by law.

b. Limited Disclosure. The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Agency gives written approval and the individual provides a valid authorization. Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Associate will report to Agency any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

c. Safeguards. The Associate will use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:

I. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;

II. Appropriate notification and training of its workforce and agents in order to protect the PHI from unauthorized use and disclosure;

III. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations, in compliance with the Security Rule;

IV. In accordance with 45 CFR § 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

d. Compliance With Law. The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.

e. Mitigation. Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum and report its mitigation activity back to the Agency.

f. Support of Individual Rights.

I. Access to PHI. Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying, and in electronic format, if requested, within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.

II. Amendment of PHI. Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526, subject to the applicable fees, including but not limited to those for retrieval and re-filing as demonstrated in the Agreement, pursuant to which Associate is to provide such services to Agency .

III. Accounting Rights. Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an individual for an accounting of disclosures of PHI in accordance

with 45 CRF § 164.528. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- a brief description of the PHI disclosed; and
- a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

IV. Request for Restriction. Under the direction of the Agency, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Agency determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

V. Immediate Discontinuance of Use or Disclosure. The Associate will immediately discontinue use or disclosure of Agency PHI pertaining to any individual when so requested by Agency. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

g. Retention of PHI. Notwithstanding Section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. Agent's, Subcontractor's Compliance. The Associate shall notify the Agency of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in Section 2.a. of this Addendum. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Agency Procurement Officer. The Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder. The Agency may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts, subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.

i. Federal and Agency Access. The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Associate shall also make these records available to Agency, or Agency's contractor, for periodic audit of Associate's compliance with the Privacy and Security Rules. Upon Agency's request, the Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Associate's subcontractors, if any.

j. Security. The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies that render PHI Unusable, Unreadable, or Indecipherable to Unauthorized individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required, to the extent practicable. If Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Addendum, it must submit such written rationale, including its Security Risk Analysis, to the Agency Procurement Officer for review prior to the execution of the Addendum. This review may take up to ten (10) days.

k. Notification of Breach. During the term of this Addendum, the Associate shall notify the Agency, Records Management Program Manager, and, unless otherwise directed by the Agency in writing, the WV Office of Technology immediately by email or web form upon the discovery of any Breach of unsecured PHI; or within ~~24 hours~~five (5) days by email or web form of any suspected Security Incident, Intrusion or Unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data effecting this Agreement. Notification shall be provided to the Agency Procurement Officer at www.state.wv.us/admin/purchase/vrc/agencyll.htm and, unless otherwise directed by the Agency in writing, the Office of Technology at incident@wv.gov or https://apps.wv.gov/ot/lr/Default.aspx. Notification to the Records Management Program Manager will be made via their supplied email address.

The Associate shall immediately investigate such Security Incident, Breach or unauthorized use or disclosure of PHI or confidential data. Within ~~72~~ five (5) days ~~hours~~ of the discovery, the Associate shall notify the Agency Procurement Officer and Record Management Program Manager, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved In the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure.~~; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.~~

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

Subject to the Liability Cap as set forth in Section 5. below, a~~A~~ll associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals which shall also be subject to the Liability Cap as set forth in Section 5.a., below.

If the Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in Section 2.a. of this Addendum, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Agency Procurement Officer. Failure to include such requirement in any subcontract or agreement may result in the Agency's termination of the Agreement.

l. Assistance in Litigation or Administrative Proceedings. The Associate shall make itself and any subcontractors, workforce or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, workforce or agent is a named as an adverse party.

4. Addendum Administration.

a. Term. This Addendum shall terminate on termination of the underlying Agreement or on the date the Agency terminates for cause as authorized in paragraph (c) of the Section, whichever is sooner.

b. Duties at Termination. Upon any termination of the underlying Agreement, the Associate shall return or destroy, at the Agency's option, all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement. Notwithstanding the forgoing, upon termination of this Addendum for any reason, any removal or destruction of PHI deposited with the Associate shall be subject to the respective removal or destruction fees applicable, as demonstrated in the underlying Agreement.

c. Termination for Cause. Associate authorizes termination of this Agreement by Agency, if Agency determines Associate has violated a material term of the Agreement. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material breach before termination.

d. Judicial or Administrative Proceedings. The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

e. Survival. The respective rights and obligations of Associate under this Addendum shall survive the termination of the underlying Agreement.

5. Liability: Indemnification.

a. Subject to the Liability Cap as established in Sec. 5.b. below, Associate shall indemnify and hold harmless Agency from and against any and all claims, damages, liabilities, losses, judgments, fines, assessments, penalties, awards, and expenses (including reasonable attorney's fees, expert witness fees, and costs of investigation, litigation or dispute resolution) (collectively "Damages") relating to or arising out of any breach of this Agreement, or any Breach, by Associate or its subcontractors or agents.

b. Associate's total liability, cumulatively, (i) to Covered Entity for claims, losses, or damages under this Agreement, (ii) for Indemnification obligations as set forth herein, (iii) for any other expenses that accrue as a result of Associate's Breach of this Addendum including but not limited to affected individuals notification obligations, shall be subject to a maximum liability limitation of five hundred thousand dollars ($500,000.) per occurrence and one million dollars ($1,000,000.) in the aggregate (the "Liability Cap")

c. The Associate's liability and indemnification obligations as defined in this Section 5., shall supersede and prevail over any liability or indemnification obligations as set forth in any underlying Agreement between the Agency and the Associate, as would pertain specifically to damages, claims, or losses that would accrue from the Associate's violation of this Agreement, HIPAA, HITECH, The Privacy Rules, The Security Rules or any other federal or state laws or regulations promulgated to protect PHI, or patient privacy

d. The foregoing indemnity obligation is expressly conditional on Agency granting Associate the right at Associate's option and expense, and with counsel of its own selection, to control or participate in the defense of any such Claim, provided however, that to the extent any such Claim is part of a larger proceeding or action, Associate's right to control or participate

shall be limited to the Claim, and not to the larger proceeding or action. In the event that Associate exercises its option to control the defense, then (i) Associate shall not settle any claim requiring any admission of fault on the part of the Agency without its prior written consent, (ii) the Agency shall have the right to participate, at its own expense, in the claim or suit and (iii) the Agency shall cooperate with the Associate as may be reasonably requested.

e. Notwithstanding any of the forgoing in this Section 5., Associate shall not be obligated to indemnify Agency for any portion of such fines or penalties to the extent resulting from (i) Agency 's violation of this Addendum, HIPAA, HITECH, The Privacy Rules, The Security Rules or any other federal or state laws or regulations promulgated to protect PHI, or patient privacy, or (ii) any negligent or intentional acts or omissions of Agency.

~~5.~~6. General Provisions/Ownership of PHI.

a. Retention of Ownership. Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option, at any time, and subject to the restrictions found within Section 4.b. above.

b. Secondary PHI. Any date or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Agency.

c. Electronic Transmission. Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.

d. No Sales. Reports or data containing the PHI may not be sold without the Agency's or the affected individual's written consent.

e. No Third-Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. Interpretation. The provisions of the Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.

g. Amendment. The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.

h. Additional Terms and Conditions. Additional discretionary terms may be included in the release order or change order process.

AGREED:

Name of Agency: _____ Name of Associate:_____

Signature: _____ Signature: _____

Title: _____ Title: _____

Date: _____ Date: _____

EXHIBIT A

Name of Associate: _____

Name of Covered Entity: **West Virginia Public Employees Insurance Agency, Department of Health and Human Resources, Department of Veterans Assistance, WV Office of Technology**

Describe the PHI:

Any individually identifiable health information held or maintained by the above covered entities, or information that could be combined with other information to identify an individual, including information related to an individual's health condition, the provision of care to the individual, payment information for the provision of healthcare. The PHI may be past, present or future protected health information of an individual in the context of this agreement. The PHI may contain individual identifiers including name, address, birthdate or Social Security numbers. This information includes but is not limited to medical records data, including account numbers, health insurance information, testing, lab results or diagnostic information, health status, medical history including past physical or mental health conditions, healthcare providers rendering services.

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
33 — Service - Misc

Proc Folder: 738719

Doc Description: ADDENDUM_1 SWC for Records Management - (RECMGT21)

Proc Type: Statewide MA (Open End)

Date Issued	Solicitation Closes	Solicitation No	Version
2020-08-12	2020-08-20 13:30:00	CRFQ 0212 SWC2100000001	2

BID RECEIVING LOCATION

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

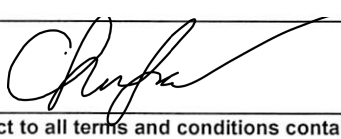
VENDOR

Vendor Name, Address and Telephone Number:

Vital Records Control (VRC)
362 MOUNTAIN AVENUE
WHITE SULPHUR SPRINGS, WV 24986
(304) 536-1290

FOR INFORMATION CONTACT THE BUYER

Mark A Atkins
(304) 558-2307
mark.a.atkins@wv.gov

Signature X  **FEIN #** 82-0796581 **DATE** 08/13/2020

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

ADDITIONAL INFORMATION:

ADDENDUM_1: Is issued for the following:
1. To extend the bid opening date from 08/18/2020 to 08/20/2020 at 1:30pm EDT.
2. To publish the Agency's response to the questions submitted by Vendors during the Technical Questioning period.

No other changes made.

The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a Statewide Open-End contract for records management and storage services per the attached documents.

This solicitation is intended to replace the current Statewide Contract for Records Management (RECMGT) expiring 11/30/2020. The RECMGT contract can be viewed on the Purchasing Division's Statewide Contracts page at:
http://www.state.wv.us/admin/purchase/swc/RECMGT.htm

Note: Please refer to Specification Section 5.2.1 Storage, for additional information.

INVOICE TO	SHIP TO
ALL STATE AGENCIES VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV99999 US	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Document Storage Services	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
78131804			

Extended Description :
Document Storage Services:

Note: Vendor shall use Exhibit_A Pricing Page for bid pricing.

If vendor is submitting a bid online, Vendor should enter $0.00 in the Oasis commodity line.

Vendor shall enter pricing into the Exhibit_A Pricing Page and must attach with bid.

See section 18 of Instructions to Bidders for additional information.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Technical Questions due by 10:00am EDT	2020-08-06

SOLICITATION NUMBER: CRFQ 0212 SWC2100000001
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as CRFQ 0212 SWC2100000001 ("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

[X] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1. **To extend the bid opening date from 08/18/2020 to 08/20/2020 at 1:30pm EDT.**
2. **To publish the Agency's response to the questions submitted by Vendors during the Technical Questioning period.**

No other changes made.

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.

Question #1: Due to the large value and significant scope of this solicitation, I would like to formally request the State's consideration in extending the current due date of 18 august 2020 until 2 September 2020. Such an extension will allow all potential vendors a sufficient amount of time to adequately address this substantial solicitation while ensuring that the State receives back durable and reliable responses from the greatest number of potential bidders.

Response #1: The State will extend the bid opening day and time to 08/20/2020 at 1:30pm EDT.

Question #2: The "Exhibit_A" Pricing Page indicates approximately 195,000 cubic feet of records to be transferred and stored. The RFQ has a provision requiring adequate storage for future increases in records stored. *Is there an estimate available, perhaps year-by-year, for the volumes that may be required?*

Response #2: We do not anticipate any significant increase. The volume of storage the past three years was 2017- 195,693 cartons, 2018- 189,791 cartons and 2019- 192,493 cartons.

Question #3: For Contract Items (5.2.5.1 #5, (5.2.7.1) #7, and (5.2.8.1) #8 there is a cost per box for pick-up and delivery to state agency offices, wherever located in West Virginia. *Is it intended that this cost, cover transportation and handling as well as pulling and refiling the box when returned?*

a. If there are no transportation cost in addition to the pick-up/delivery cost noted above, *is there an estimate or history of where boxes are generally delivered in the state (by city) and how often?*

Response #3: Yes, the cost per box must be all inclusive.

Response #3a: An estimate is not available. Historically, documents are mostly delivered in the Charleston metro area.

Question #4: Is there any assurance that a New Vendor, transferring the records from the Current Vendor, will have adequate cooperation from the Current Vendor to make an efficient and effective transfer?

Response #4: The state anticipates full cooperation from the current vendor.

Question #5: Will an accurate index of existing records be available to a New Vendor prior to the transfer of the records from the Current Vendor?

Response #5: The state will work with the current vendor and the State agencies utilizing record storage to provide an accurate and complete index.

Question #6: 5.2.6.1 – Indexing of all new Records – Please explain the indexing requirements.

a. Will the West Virginia approved user enter the carton/file information in a web-based application or complete a form of the metadata provided by the vendor?
b. Or is it the expectation that the vendor will open the carton and work to identify the contents of the carton?
c. Will there be a requirement that the vendor capture each file information in a carton – if so please provide an average number of files per carton and fields to be indexed.

Response #6a: The user will enter the carton/file information in the method requested by the vendor.

Response #6b: See Response #6a

Response #6c: No

Question #7: 5.2.7 The vendor must retrieve any record and hand deliver to the authorized agency personnel. Does this mean the expectation is that the vendor will have access to the facilities to make deliveries to an office?

Response #7: It is expected that the vendor will arrange delivery with the requesting agency and comply with an agency's access policies.

Question #8: 5.2.8.1 Emergency Retrieval and Delivery. You have asked for this as a per box price would you consider as a per trip price with a maximum number of cartons? Example – Emergency trip with a maximum of 10 cartons.

Response #8: No. Emergency retrieval and delivery will be charged by box as required in the solicitation.

Question #9: The proposal references microfilm but there is not a request for the storage of the material?

Response #9: The state considers microfilm a record and expects it will be stored and charged as per Cubic Foot of space required for storage.

Question #10: 5.2.9 Secure Area – There is a request to provide a secure area to review records, however there is not a price for the retrieval and refile of the requested cartons. Can pricing be added for the retrieval and refile from the vendor's site for records viewing?

Response #10: No, all costs will be included in the Per Box retrieval fee regardless of where files are viewed.

Question #11: Image of Demand – There isn't a place to provide pricing for **image on demand** – meaning can we offer to image information for West Virginia users and provide the file or carton back electronically – Pricing Minimum for first 50 pages and then per image?

Response #11: No imaging of records will be permitted under this contract.

Question #12: Can the vendor provide a complete price list of all record management services/supplies available to the State? As an example if the State would request a larger carton it would be nice to be able to support the request.

Response #12: No, only commodities/services specifically listed in the RFQ may be provided under this contract.

Question #13: What are the States payment terms?

Response #13: Per General Terms and Conditions:

#14 PAYMENT IN ARREARS: Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

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

Question #14: Will the State consider separating line items for retrieval and delivery?

Response #14: No, as the pricing will be the same for both services.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ 0212 SWC2100000001

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.

Vital Records Control (VRC)
Company

Authorized Signature

08/13/2020
Date

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

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

Pursuant to *W. Va. Code* § 6D-1-2, a state agency may not enter into a contract, or a series of related contracts, that has/have an actual or estimated value of $1 million or more until the business entity submits to the contracting state agency a Disclosure of Interested Parties to the applicable contract. In addition, the business entity awarded a contract is obligated to submit a supplemental Disclosure of Interested Parties reflecting any new or differing interested parties to the contract within 30 days following the completion or termination of the applicable contract.

For purposes of complying with these requirements, the following definitions apply:

"Business entity" means any entity recognized by law through which business is conducted, including a sole proprietorship, partnership or corporation, but does not include publicly traded companies listed on a national or international stock exchange.

"Interested party" or *"Interested parties"* means:

(1) A business entity performing work or service pursuant to, or in furtherance of, the applicable contract, including specifically sub-contractors;
(2) the person(s) who have an ownership interest equal to or greater than 25% in the business entity performing work or service pursuant to, or in furtherance of, the applicable contract. (This subdivision does not apply to a publicly traded company); and
(3) the person or business entity, if any, that served as a compensated broker or intermediary to actively facilitate the applicable contract or negotiated the terms of the applicable contract with the state agency. (This subdivision does not apply to persons or business entities performing legal services related to the negotiation or drafting of the applicable contract.)

"State agency" means a board, commission, office, department or other agency in the executive, judicial or legislative branch of state government, including publicly funded institutions of higher education: Provided, that for purposes of W. Va. Code § 6D-1-2, the West Virginia Investment Management Board shall not be deemed a state agency nor subject to the requirements of that provision.

The contracting business entity must complete this form and submit it to the contracting state agency prior to contract award and to complete another form within 30 days of contract completion or termination.

This form was created by the State of West Virginia Ethics Commission, 210 Brooks Street, Suite 300, Charleston, WV 25301-1804. Telephone: (304)558-0664; fax: (304)558-2169; e-mail: ethics@wv.gov; website: www.ethics.wv.gov.

Revised June 8, 2018

West Virginia Ethics Commission

Disclosure of Interested Parties to Contracts

(Required by *W. Va. Code* § 6D-1-2)

Name of Contracting Business Entity: VRC Companies, LLC **Address:** 362 MOUNTAIN AVENUE
WHITE SULPHUR SPRINGS, WV 24986

Name of Authorized Agent: Chris Ferrell **Address:** Same

Contract Number: CRFQ SWC21*01 **Contract Description:** RECORDS MANAGEMENT

Governmental agency awarding contract: WV Purchasing Division

☐ **Check here if this is a Supplemental Disclosure**

List the Names of Interested Parties to the contract which are known or reasonably anticipated by the contracting business entity for each category below *(attach additional pages if necessary)*:

1. **Subcontractors or other entities performing work or service under the Contract**
   ☑ Check here if none, otherwise list entity/individual names below.

2. **Any person or entity who owns 25% or more of contracting entity (not applicable to publicly traded entities)**
   ☑ Check here if none, otherwise list entity/individual names below.

3. **Any person or entity that facilitated, or negotiated the terms of, the applicable contract (excluding legal services related to the negotiation or drafting of the applicable contract)**
   ☑ Check here if none, otherwise list entity/individual names below.

Signature: _____ Date Signed: _____

Notary Verification

State of _____, County of _____:

I, _____, the authorized agent of the contracting business entity listed above, being duly sworn, acknowledge that the Disclosure herein is being made under oath and under the penalty of perjury.

Taken, sworn to and subscribed before me this _____ day of _____, _____.

_____
Notary Public's Signature

To be completed by State Agency:
Date Received by State Agency: _____
Date submitted to Ethics Commission: _____
Governmental agency submitting Disclosure: _____

Revised June 8, 2018

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a Statewide Open-End contract for records management and storage services per the attached documents.

   This solicitation is intended to replace the current Statewide Contract for Records Management (RECMGT) expiring 11/30/2020. The RECMGT contract can be viewed on the Purchasing Division's Statewide Contracts page at: http://www.state.wv.us/admin/purchase/swc/RECMGT.htm

   Note: Please refer to Specification Section 5.2.1 Storage, for additional information.

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"** or **"Contract Items"** means the list of items identified in Section 4.1 below and on the Pricing Pages.

   2.1 **"Box"** means a storage container used for temporary or permanent storage of files, record, or records. A standard box size is 15" L x 12" W x 10"H equal to approximately one (1) cubic foot in size.

   2.2 **"Business Hours"** means Monday – Friday 8:00 AM through 5:00 PM EST excluding weekends and Federal and State holidays. State Holidays are as follows:

   - New Year's Day (January 1)
   - Martin Luther King Day (Third Monday in January)
   - President's Day (Third Monday in February)
   - Memorial Day (Last Monday in May)
   - West Virginia Day (June 20)
   - Independence Day (July 4)
   - Labor Day (First Monday in September)
   - Columbus Day (Second Monday in October)
   - Veterans Day (November 11)
   - Thanksgiving (Fourth Thursday in November)
   - Day After Thanksgiving (Fourth Friday in November)
   - Christmas Day (December 25)

2.2 **"Disaster"** means any occurrence of fire, flood, storm, earthquake, explosion, epidemic, riot, sabotage or other condition of extreme peril resulting in substantial damage or injury to persons or property within this state, whether such occurrence is caused by an act of God, nature or man, including an enemy of the United States..

2.3 **"NFPA"** means National Fire Protection Association (www.nfpa.org).

2.4 **"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.

2.5 **"Record"** means a document, book, paper, photograph, sound recording or other material, regardless of physical form or characteristics, made or received pursuant to law or ordinance or in connection with the transaction of official business. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included within the definition of records as used in Chapter 5A Article 8 Public Records Management and Preservation Act for the Department of Administration. This can be used with the link: http://code.wvlegislature.gov/5a-8/

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

3. CURRENT ENVIRONMENT:

3.1 Pursuant to the West Virginia Code §5A-8-1 through §5A-8-22, and Legislative Rules 148-CSR-12, 148-CSR-13, and 148-CSR-14, the Department of Administration is responsible for the management of the State's day-to-day records management program.

3.2 Agencies are required to follow retention/destruction schedules that have been approved by the Department of Administration.

3.3 Currently records are stored in Charleston, West Virginia, and are picked-up at the state agency locations by the vendor. The agency locations are located throughout the state. Most records are received in boxes 1.2 cubic feet in size. However, some are delivered in other formats previously approved by the State Records Administrator or the records management vendor.

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

4.1 Vendor must be Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) compliant. An executed Business Associate Addendum (see attachment **Exhibit_B**) will be required prior to award.

4.2 Vendor must have established information security and privacy policies. Vendor must provide proof of a third-party audit of the security and privacy policies within the last 365 days upon request.

4.3 Vendor must have an established personnel security program designed to evaluate employee trustworthiness before being granted access to sensitive data. Vendor must provide documentation of security program upon request.

4.4 Vendor must have a documented plan for handling security and privacy incidents that complies with the West Virginia Notice of Confidentiality Policies and Information Security Accountability Requirements, made part of this contract through the General Terms and Conditions item #30.

4.4.1 The Vendor's incident management plan must define a security or privacy incident as an unauthorized access of an agency's records or any missing agency records from the vendor's custody.

4.4.2 The Vendor's incident management plan must describe what steps of the process are handled internally or externally; and

4.4.3 The Vendor's incident management plan must include timeframes or milestones.

4.4.4 The Vendor must provide the incident management plan within 30 calendar days of the contract start date to:

WV Office of Technology
Attention: Andrew Lore
Capitol Complex Bld. 5 10th Floor
Charleston, WV 25305
Andrew.C.Lore@wv.gov

5. GENERAL REQUIREMENTS:

5.1 Contract Items and Mandatory Requirements: Vendor shall provide Agency with the Contract Items listed below on an open-end and continuing basis. Contract Items must meet or exceed the mandatory requirements as shown below.

Facility Requirements:

5.1.1 The vendor must provide a facility that will protect all records from disaster as defined in West Virginia Code §5A-8-3. This may be viewed at http://code.wvlegislature.gov/5A-8-3/

5.1.1.1 The vendor must bear all costs related to recovery or restoration of damaged records in the care of the vendor.

5.1.2 The vendor must provide a facility that meets the following requirements for archival storage of records:

5.1.2.1 The vendor must provide storage to accommodate a minimum of 200,000 cubic feet for the State's existing records and must have the capacity to expand this storage as the State's storage requirements increase.

5.1.2.2 The Vendor's storage facility must provide the following physical security measures.

5.1.2.2.1 Facility must have security locks at each exterior entrance.

5.1.2.2.2 Facility must have 24-hour,7 days-per-week, 365-days-per-year monitored anti-intrusion alarm system to protect against unauthorized entry.

5.1.2.2.3 Facility must have a policy for providing access to the records storage area to ensure only duly authorized individuals have access.

5.1.2.2.3.1 Vendor should submit the policy with their bid and must provide documentation of such policy prior to award.

5.1.2.3 The records storage area must have an independent circulating system to keep the air as free as possible of pollutants and dust and to prevent the entry of unfiltered air from other parts of the building.

5.1.2.4 The vendor must provide smoke detection within the entire facility in accordance with NFPA code or standards.

5.1.2.5 The vendor must provide a fire suppression system in the records storage areas.

5.1.2.6 The vendor must provide a records storage area that is climate controlled (maximum temperature of 72 degrees Fahrenheit, and relative humidity between 45 and 60) 24-hours a day, 7 days-per-week, 365 days-per-year.

5.1.2.7 The vendor must limit its flooding risk by storing records in a facility that is located out of the 100-year floodplain.

5.1.2.7.1 Vendor should submit the elevation certificate with their bid and must provide the elevation certificate from a land surveyor verifying the facility is out of the 100-year floodplain prior to award.

5.1.2.8 The vendor must keep records a minimum of one inch (1") above the floor level with the optimum of three inches (3").

5.1.2.8.1 Records must be stored away from windows, steam, sewer, or water pipes.

5.1.2.9 The Vendor must provide a moisture detection system throughout the records storage area.

5.1.2.10 The Vendor must minimize light exposure to the records and must keep the lids on boxes at all times.

5.1.3 Records stored at the facility must only be viewed by authorized persons. The vendor must have security controls or policies to allow access only to those persons approved to retrieve/view records for their respective agency. Vendor must provide documentation of such policies and procedures prior to award.

Indexing and Invoicing:

5.1.4 The vendor must provide an indexing system for records inventory and must index each box or file submitted.

5.1.4.1 The indexing system must provide a minimum of sixty (60) characters per box or per file in the records description field.

5.1.5 The vendor must invoice each state agency storing records at the facility monthly in arrears.

5.1.6 The vendor must maintain a log of personnel or authorized individuals that have accessed records or boxes and must provide the log upon agency request.

5.1.7 The vendor must provide reporting on agency records, including inventory, storage costs, and activity, upon request to agency-authorized personnel, and to the Department of Administration-authorized personnel.

5.1.7.1 These reports shall include, but not be limited to, the following:

5.1.7.1.1 The agencies storing records in the facility and the total volume in number of boxes and cubic feet for each agency.

5.1.7.1.2 The account numbers, box numbers, date records were received by vendor, date of records, destruction dates, and full descriptions of the records.

5.1.7.1.3 The total amount of cubic feet of storage for the State.

5.1.7.1.4 The itemized cost for each for an agency.

5.1.7.1.5 The itemized cost for the State.

5.1.7.1.6 The authorized users for each account.

5.1.7.1.7 The requests for action made for each agency/account.

5.1.7.1.8 The destruction eligibility of records.

5.1.8 The vendor must include on its monthly invoice to the agency all billing activity detail for the month.

5.1.9 Vendor must only bill for storage of records that an agency has requested to be stored at the storage facility.

5.1.9.1 Once vendor is notified in writing by an agency that records have been permanently removed, or when records destruction is requested by an agency, no further storage fees shall be billed for any subsequent month for those records, regardless of the length of time it takes vendor to process said requests.

5.2 Requirements & Pricing for Storage, Supplies, Pick Up, Retrieval, and Destruction:

STORAGE:

5.2.1 **Contract Item #1: Transfer Existing Records to Vendor's Storage Facility:** The successful vendor should transfer existing records to their storage facility within eight (8) months of contract start date and must have all records transferred within (12) months of contract start date.

5.2.1.1 The successful vendor shall be responsible for all costs associated with the pick-up and organization of all records currently in storage at Iron Mountain, 5736 MacCorkle Avenue SE Charleston, WV 25304.

5.2.1.2 The successful vendor shall transfer currently stored records in their existing boxes, or furnish boxes and repackage records if needed, at no additional cost.

5.2.1.3 Vendor must have a secure tracking system in place to document the chain of custody of records from the time vendor takes possession of the records until their final disposition.

5.2.2 Contract Item #2: The vendor must index existing records at time of transfer from the current storage facility.

5.2.2.1 The vendor must provide indexing of boxes during transfer from current storage facility at no charge.

5.2.3 Contract Item #3: The vendor must accommodate storage of a minimum of 200,000 cubic feet for the State's records currently stored with the ability to expand.

5.2.3.1 The vendor must provide a monthly cost per cubic foot for storage at the facility.

5.2.3.2 The vendor must invoice each state agency storing records at the facility monthly in arrears.

SUPPLIES:

5.2.4 Contract Item #4: The vendor must provide storage boxes; Approximate dimensions: 15" L x 12" W x 10" H. (equal to approximately one (1) cubic foot of storage).

5.2.4.1 Vendor to provide cost per box.

5.2.4.2 Vendor shall provide replacement boxes for boxes damaged while in the vendor's possession at no cost to the agency.

PICK UP:

5.2.5 Contract Item #5: The vendor must pick up the records within a maximum of five (5) business days after written request by the agency. The vendor shall not take possession of records that do not include a description identifying the records and a date the records are eligible for destruction.

5.2.5.1 The vendor must provide a cost per box for pick-up.

5.2.6 **Contract Item #6: The vendor must index all new records received from an agency.**

5.2.6.1 The vendor must provide a cost per box for indexing of new records picked up from an agency.

RETRIEVAL/DELIVERY:

5.2.7 **Contract Item #7: The vendor must retrieve any record in storage and hand deliver it to the authorized agency personnel within five (5) business days of written notification.**

5.2.7.1 The vendor must provide a cost per box for retrieval and delivery of records from an agency.

5.2.7.2 Records must be delivered during normal business hours.

5.2.7.3 Records may only be signed for by authorized personnel as identified on the vendors Access Authorization Form and signed by the agency head.

5.2.7.4 Records must be delivered by the vendor and cannot be delivered by a third party.

5.2.8 **Contract Item #8: The vendor must retrieve any record in storage and hand deliver them to requesting agency within three (3) calendar days of written request, including weekends or holidays, if it is identified by the agency as an Emergency.**

5.2.8.1 The vendor must provide a cost per box for emergency retrieval and delivery of records from an agency.

5.2.8.2 Records may only be signed for by authorized personnel as identified on the vendors Access Authorization form and signed by the agency head.

5.2.9 **Contract Item #9: The vendor must provide a secure area for authorized agency personnel to view records at no cost at its facility.**

RECORD DESTRUCTION:

5.2.10 **Contract Item #10: The vendor must provide paper record destruction services at the authorized agency representative's written request.**

5.2.10.1 The request must include the written approval of the State Records Administrator to destroy the specified records.

5.2.10.1.1 No records shall be destroyed without State Records Administrator approval.

5.2.10.2 Records must be destroyed by a crosscut shredder for paper records using a cross-cut shredder to achieve 5/16-inch-wide or smaller strips. Alternatively, strips may be set at the industry standard of ½ inch, but when deviating from the 5/16-inch requirement, shredded paper must be safeguarded until it reaches the stage where it is rendered unreadable. Pulping of data should be accomplished only after material has been shredded.

5.2.10.3 Vendor shall provide proof of destruction to the owner of the record once they have been destroyed

5.2.10.4 The vendor must provide a cost per box for destruction of paper records.

5.2.11 **Contract Item #11: The vendor must provide destruction of microfilm at the authorized agency representative's request.**

5.2.11.1 The agency written request must include the written approval of the State Records Administrator to destroy the specified records.

5.2.11.1.1 No records shall be destroyed without State Records Administrator approval.

5.2.11.2 Vendor shall provide proof of destruction to the owner of the record once they have been destroyed.

5.2.11.3 Microfilm and microfiche must be shredded to achieve 1/35-inch by 3/8- inch strips.

5.2.11.4 The vendor must provide a cost per box for destruction of microfilm.

6. CONTRACT AWARD:

6.1 Contract Award: This Contract is intended to provide Agencies with a purchase price on all Contract Items. The Contract shall be awarded to the Vendor that provides all Contract Items meeting the required specification for the lowest overall total cost as shown on the Exhibit_A Pricing Pages.

6.1.1 The initial Contract will be for five (5) years with three (3) optional one-(1) year renewals for years six, seven, and eight. Renewal options will be initiated by the West Virginia Purchasing Division upon mutual agreement with the successful vendor and processed by the West Virginia Purchasing Division as Change Orders.

6.2 Pricing Pages: The vendor should complete the Pricing Pages by entering in the price for each contract item on wvOASIS and **Exhibit_A**. The vendor should complete the Pricing Pages in their entirety as failure to do so may result in the vendor's bid being disqualified.

The **Exhibit_A Pricing Page** has been provided in Excel and formatted to automatically calculate the **Total Cost** when the **Unit Price** is entered for each commodity line item. However, it is the Vendor's responsibility to ensure the pricing for their bid submission is correct. In the event of any errors, the **Unit Price** shall prevail.

The Pricing Page contains 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.

The Vendor should electronically upload The Exhibit_A Pricing Page in wvOASIS, as an electronic document or submit with their paper bid. In most cases, the Vendor can request an electronic copy of the Pricing Pages for bid purposes by sending an email request to:

Mark Atkins, Senior Buyer
West Virginia Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305
Phone: (304) 558-2307
Fax: (304) 558-4115
Email: mark.a.atkins@wv.gov

7. ORDERING AND PAYMENT:

7.1 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.

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

8. DELIVERY AND RETURN:

8.1 Delivery Time: The vendor shall pickup or deliver standard orders within five (5) business days after orders are received. The vendor shall deliver emergency orders within three (3) calendar days after orders are received. The vendor shall ship all orders in accordance with the above schedule and shall not hold orders until a minimum delivery quantity is met.

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

Any agency seeking to obtain items from a third party under this provision must first obtain the approval of the Purchasing Division.

8.3 Delivery Payment/Risk of Loss: Standard pickup/delivery shall be per the price established in the contract to the agency's location. The agency will pay delivery charges on all emergency orders per the price established in the contract.

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 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 The following remedies are available for damages associated with a breach of protected information:

9.2.3.1 If the breach is related to a direct result of the vendor's failure to meet its contract obligation to protect personally identifiable information (PII) or otherwise prevent its release, the vendor shall bear the costs associated with (a) the investigation and resolution of the breach; (b) notifications to individuals, regulators or others required by state or federal law; (c) a credit monitoring service (d) 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 PII 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 (e) complete all corrective actions as reasonably determined by the vendor based on root cause.

9.2.3.2 Any fines or penalties levied against the State by a regulatory body.

9.2.4 Any other remedies available in law or equity.

10. MISCELLANEOUS:

10.1 No Substitutions: The 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: The vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, the vendor certifies that it can supply the Contract Items contained in its bid response.

10.3 Reports: The vendor shall provide reports upon request as required in Section **5.1.7** above. Failure to supply such reports may be grounds for cancellation of this Contract.

10.4 Contract Manager and Customer Service Representative: During its performance of this Contract, the vendor must designate and maintain a primary contract manager responsible for overseeing the vendor's responsibilities under this Contract and must provide a dedicated customer service representative to process all requests for action by authorized agency personnel and authorized Department of Administration personnel. The Contract manager and the dedicated customer service representative must be available during normal business hours to address any customer service or other issues related to this Contract. The vendor should list its Contract manager and dedicated customer service representative and his or her contact information below.

Contract Manager: Chris Ferrell
Telephone Number: 407-433-8732
Fax Number: _____
Email Address: cferrell@vrcnetwork.com

Customer Service Representative: David Cleland
Telephone Number: 615-967-0110
Fax Number: _____
Email Address: dcleland@vrcnetwork.com

CERTIFICATE OF LIABILITY INSURANCE

7/1/2021

DATE (MM/DD/YYYY) 6/29/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	LOCKTON COMPANIES 3657 BRIARPARK DRIVE, SUITE 700 HOUSTON TX 77042 866-260-3538
CONTACT NAME:	
PHONE (A/C, No, Ext):	**FAX (A/C, No):**
E-MAIL ADDRESS:	

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	National Fire Insurance Co of Hartford	20478
INSURER B :	The Continental Insurance Company	35289
INSURER C :	National Union Fire Ins Co Pitts. PA	19445
INSURER D :	American Casualty Company of Reading, PA	20427
INSURER E :	ACE American Insurance Company	22667
INSURER F :		

INSURED 1431956
VRC Companies, LLC.
868 Mt. Moriah
Memphis TN 38117

COVERAGES FLEET **CERTIFICATE NUMBER:** 14820862 **REVISION NUMBER:** XXXXXXX

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** CLAIMS-MADE [X] OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: [X] POLICY [ ] PRO-JECT [ ] LOC [ ] OTHER:	Y	Y	6046431608	7/1/2020	7/1/2021	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG $	$ 1,000,000 $ 1,000,000 $ 15,000 $ 1,000,000 $ 2,000,000 $ 2,000,000 $
B	**AUTOMOBILE LIABILITY** X ANY AUTO OWNED AUTOS ONLY [ ] SCHEDULED AUTOS X HIRED AUTOS ONLY [X] NON-OWNED AUTOS ONLY	Y	Y	6046431611	7/1/2020	7/1/2021	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident) $	$ 1,000,000 $ XXXXXXX $ XXXXXXX $ XXXXXXX $ XXXXXXX
B C	X **UMBRELLA LIAB** [X] OCCUR X **EXCESS LIAB** [ ] CLAIMS-MADE [ ] DED [ ] RETENTION $ 10,000	Y	Y	6046431639 026245681	7/1/2020 7/1/2020	7/1/2021 7/1/2021	EACH OCCURRENCE AGGREGATE $	$ 10,000,000 $ 10,000,000 $ XXXXXXX
D	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** Y / N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? N **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A	Y	6046431625	7/1/2020	7/1/2021	X PER STATUTE [ ] OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000
E C	Professional Liability/Cyber Excess Cyber	Y	Y	D95500948 01-450-14-45	7/1/2020 7/1/2020	7/1/2021 7/1/2021	$10,000,000 Limit $75,000 Retention $10,000,000 xs $10,000,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
The Umbrella Liability policy includes the General Liability, Automobile Liability and Employer's liability policies in the underlying schedule.

CERTIFICATE HOLDER

14820862

For Information Purposes Only

CANCELLATION See Attachments

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Professional Liability
Policy No.: D95500948
Insurer: ACE American Insurance Company
Policy Term: 7/1/2020-7/1/2021
Limits: $10,000,000 Limit

Crime (Clients Property)
Policy No.: BDY1051405-04
Insurer: The Hanover Insurance Company
Policy Term: 11/1/2019-11/1/2020
Limits: $5,000,000 Limit
$25,000 Retention

All policies (except Workers' Compensation/EL and Crime) include a blanket automatic additional insured [provision] that confers additional insured status to the certificate holder only if there is a written contract between the named insured and the certificate holder that requires the named insured to name the certificate holder as an additional insured. In the absence of such a contractual obligation on the part of the named insured, the certificate holder is not an additional insured under the policy.

All policies (except Crime) include a blanket automatic waiver of subrogation endorsement [provision] that provides this feature only when there is a written contract between the named insured and the certificate holder that requires it. In the absence of such a contractual obligation on the part of the named insured, the waiver of subrogation feature does not apply.

All policies include a blanket notice of cancellation to certificate holders endorsement, providing for 30 days' advance notice if the policy is cancelled by the company other than for nonpayment of premium, 10 days' notice if the policy is cancelled for nonpayment of premium. Notice is sent to certificate holders with mailing addresses on file with the agent or the company. The endorsement does not provide for notice of cancellation if the named insured requests cancellation.

Regulation Investigation or **Extortion Demand** in accordance with Section **VI. CONDITIONS**, paragraph **B. NOTICE OF CLAIM OR CIRCUMSTANCE/PRE-CLAIMS ASSISTANCE/DATE OF CLAIM**, and such amounts are consented to in writing by the Insurer, such consent not to be unreasonably withheld.

E. VICARIOUS LIABILITY

1. Third Party Vicarious Liability Coverage

Any entity or natural person the **Insured Entity** is required by written contract to include as an insured for liability of such entity or natural person for an **Insured's Wrongful Acts** shall be insured under this Policy but solely to the extent that a **Claim** is made against such entity or natural person for a **Wrongful Act** of an **Insured**, and only so long as the written contract is entered into before such **Claim** occurs, provided:

a. there shall be no coverage afforded to such entity or natural person for its **Wrongful Acts**; and,

b. nothing herein shall serve to confer any rights or duties to such person or entity under this Policy, other than as provided in this paragraph.

2. Assumed Liability of Insured

The **Insured Entity** is insured for liability it assumes in a written contract or agreement under which it assumes the tort liability (liability that would be imposed by law in the absence of any contract or agreement) of another party incurred by such third party as a result of an **Insured's Wrongful Act** provided the **Wrongful Act** gives rise to a **Claim** and occurs subsequent to the execution of such contract or agreement. Solely for the purposes of liability assumed by the **Insured Entity** in such contract or agreement reasonable attorney fees and necessary litigation expenses incurred by or for a party other than an **Insured** are deemed to be **Damages** provided:

a. liability to such party for, or for the cost of, that party's defense has also been assumed in such contract or agreement; and,

b. such attorney fees and litigation expenses are for defense of that party against a civil or alternative dispute resolution proceeding in which **Damages** to which this insurance applies are alleged.

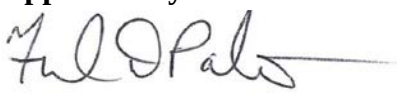
Any coverage afforded by this paragraph is subject always to all of the Policy's terms, conditions and exclusions.

II. DEFINITIONS

The following defined words shall have the same meaning throughout this Policy, whether expressed in the singular or the plural.

Application means all signed applications, any attachments to such applications, other materials submitted therewith or incorporated therein, and any other documents submitted in connection with the underwriting of this Policy by the Insurer, or any other policy underwritten by the Insurer or its affiliates of which this Policy is a direct or indirect renewal or replacement.

Assumed Under Contract means liability of others, for **Matter** furnished by the **Insured**, that the **Insured** agrees to assume under a hold harmless or indemnity agreement but only to the extent such liability arises out of any **Wrongful Act**.

VITAL RECORDS CONTROL COMPANIES Policies and Procedures	Supersedes: 08/29/2019	Date Effective: 01/31/2020	Number: 100.09.00
For Internal Use Only	Approved By: 		Page: 1 of 2
Section: VISION, MISSION, VALUES, AND QUALITY	Subject: SUSTAINABILITY STATEMENT		

VRC Companies, LLC (VRC) is committed to promoting sustainability. VRC believes that our business can only succeed where we meet the needs of the present generation without compromising the ability of future generations to meet their own needs. Concern for the environment and promoting a broader sustainability agenda are integral to VRC's professional activities and the management of the organization. We aim to follow and to promote good sustainability practice, to reduce the environmental impacts of all our activities and to help our clients to do the same.

Our Sustainability Policy is based upon the following principles:

- To comply with, and exceed where practicable, all applicable legislation, regulations and codes of practice.
- To integrate sustainability considerations into all our business decisions.
- To ensure that all staff are fully aware of our Sustainability Policy and are committed to implementing and improving it.
- To minimize the impact on sustainability of all office and transportation activities.
- To make clients and suppliers aware of our Sustainability Policy, and encourage them to adopt sound sustainable management practices.
- To review, annually report, and to continually strive to improve our sustainability performance.

In order to put these principles into practice we will:

- Avoid physically travelling to meetings etcetera where alternatives are available and practical, such as using teleconferencing, video conferencing or web cams, and efficient timing of meetings to avoid multiple trips. These options are also often more time efficient, while not sacrificing the benefits of regular contact with clients and partners.
- Reduce the need for our staff to travel by supporting alternative working arrangements.
- Minimize our use of paper and other office consumables, for example by double-siding all paper used, and identifying opportunities to reduce waste.
- Reduce the energy consumption of office equipment by purchasing energy efficient equipment and good housekeeping.
- Continue to work towards reducing our greenhouse gas emissions throughout our supply chain, including at our facilities, as part of our ultimate goal of becoming carbon neutral.

- Remain committed to ensuring that sourcing throughout our supply chain remains environmentally and socially responsible.

The reputation of VRC is built on trust and respect. Our employees and those who do business with us know we are committed to earning their trust with a set of values that represent the highest standards of quality, integrity, excellence, compliance with the law, and respect for sustainability in the communities where we operate.

- Total tons of paper recycled by VRC in 2019: 32,433
- Total number of trees recycled by VRC in 2019: 551,368
- Total gallons of water reserved due to VRC's recycling efforts: 227,033,870
- Total cubic yards of landfill space not utilized by VRC: 107,030
- Total metric tons of carbon reduced by VRC in 2019: 32,433

SOC 2 TYPE 2

Report on VRC Companies, LLC's Description of its Record Storage and Vaulting Systems and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality

Throughout the Period
June 1, 2018 to May 31, 2019

LBMC

Contents

SECTION 1 3

Independent Service Auditors' Report 4

SECTION II 7

Assertion of the Management of VRC Companies, LLC 8

SECTION III 9

Description of Vital Record Control's Record Storage and Vaulting System throughout the period June 1, 2018 to May 31, 2019 10

Introduction 10

Operations and Services provided by VRC Companies, LLC 10

Principal Service Commitments and System Requirements 11

Internal Control Framework 15

Control Environment 15

Control Activities 16

Risk Assessment Process 18

Monitoring 19

Information and Communication Systems 19

System Incident Information 20

Changes to the System During the Period 20

Complementary User Entity Controls 20

SECTION IV 21

Introduction 22

Description of Testing Procedures Performed 22

Results of Testing Performed 22

Complementary User Entity Controls 22

Description and Results of Testing 23

SECTION 1

Independent Service Auditors' Report

Independent Service Auditors' Report

VRC Companies, LLC
5400 Meltech Rd, Ste. 101
Memphis, TN 38118

To Management of VRC Companies, LLC:

Scope

We have examined the description in Section III titled "Description of VRC Companies, LLC's Record Storage and Vaulting System throughout the period June 1, 2018 to May 31, 2019" (description) based on the criteria for a description of a service organization's system set forth in DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2018 to May 31, 2019, to provide reasonable assurance that VRC Companies, LLC's (VRC) service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at VRC to achieve VRC's service commitments and system requirements based on the applicable trust services criteria. The description presents VRC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of VRC's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

VRC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that VRC's service commitments and system requirements were achieved. In Section II, VRC has provided the accompanying assertion titled "Assertion of the Management of VRC Companies, LLC" about the description and the suitability of design and operating effectiveness of controls stated therein. VRC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in section IV, "Trust Services Security, Availability, and Confidentiality Categories, Criteria, Related Controls, and Tests of Controls" of this report.

Opinion

In our opinion, in all material respects —

a. the description presents VRC's Record Storage and Vaulting system and related services that were designed and implemented throughout the period June 1, 2018 to May 31, 2019 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period period June 1, 2018 to May 31, 2019 to provide reasonable assurance that VRC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and user entities applied the complementary controls assumed in the design of VRC's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period period June 1, 2018 to May 31, 2019 to provide reasonable assurance that VRC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of VRC's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of VRC; user entities of VRC's Record Storage and Vaulting system and related services during some or all of the period June 1, 2018 to May 31, 2019; business partners of VRC subject to risks arising from interactions with the Record Storage and Vaulting system and related services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be and should not be used by anyone other than these specified parties.

LBMC, PC

Brentwood, Tennessee
September 19, 2019

SECTION II

VRC Companies, LLC's Assertion

Assertion of the Management of VRC Companies, LLC

We have prepared the accompanying description in Section III of VRC's Record Storage and Vaulting System titled "Description of VRC Companies, LLC's Record Storage and Vaulting System Throughout the Period June 1, 2018 to May 31, 2019" (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, Description Criteria), (description criteria). The description is intended to provide report users with information about the Record Storage and Vaulting system that may be useful when assessing the risks arising from interactions with VRC's system, particularly information about system controls that VRC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at VRC to achieve VRC's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

1. The description presents VRC's Record Storage and Vaulting system that was designed and implemented throughout the period June 1, 2018 to May 31, 2019 in accordance with the description criteria.

2. The controls stated in the description were suitably designed throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that VRC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

3. The controls stated in the description operated effectively throughout the period June 1, 2018 to May 31, 2019 to provide reasonable assurance that VRC's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of VRC's controls operated effectively throughout that period.

VRC Companies, LLC
September 19, 2019

SECTION III

Description of Controls Provided by VRC Companies, LLC

Description of Vital Record Control's Record Storage and Vaulting System throughout the period June 1, 2018 to May 31, 2019

Introduction

VRC Companies, LLC ("VRC") is a fast growing privately held company servicing the entire U.S. VRC was established in 1988 in Memphis, TN, and has grown to service accounts around the country.

VRC is known for its premium top-of-the-line customer service. Our willingness to customize an information and records management program allows us to fit into each customer's needs while providing first-rate facilities and security. With VRC's customized software, VitalTrac® and VaultTrac®, and their related web modules, VitalWeb® and VaultWeb®; VRC provides customized features to clients, including reporting, department/division hierarchy, retention scheduling, invoicing, data fields, etc. VRC's philosophy is to mold to the customer's needs and preferences rather than forcing the customer to accept one style of records management program.

VRC services scores of Fortune 500 companies and thousands of regional, state, and local companies throughout the country with a special concentration on the Southeastern United States. VRC is a full-service information management and storage company that works exclusively on information management for its customers.

Operations and Services provided by VRC Companies, LLC

VRC offers offsite records storage, open-file records storage, climate controlled storage, vaulting services for electronic media backups, online backup, destruction services, including plant based and mobile shredding, imaging services, including release of information, data integrity services, microfilm, records inventorying/indexing services, and on-site packing services at the customer's location.

VRC's organizational structure establishes a structure within that allows the activities necessary to achieve our stated trust principles, which are planned, controlled, monitored and executed throughout the year.

VRC has over 1000 employees, consisting of management, operations, and support personnel organized into the following areas.

- Executive Management
- Accounting
- Operational Management
- Customer Account Management
- Sales/Marketing
- Network Management
- Information Technology
- Human Resources
- Compliance
- Business Development

VRC Companies are located in:

- Memphis, Tennessee*
- Birmingham, Alabama*
- Florence, Alabama*
- Huntsville, Alabama
- Mobile, Alabama
- Montgomery, Alabama
- Fort Smith, Arkansas
- Little Rock, Arkansas
- Springdale, Arkansas
- Colorado Springs, Colorado
- Grand Junction, Colorado
- Fort Myers, Florida*
- Ft. Walton Beach, Florida
- Melbourne, Florida*
- Orlando, Florida*
- Palm City, Florida
- West Palm Beach, Florida
- Valdosta, Georgia
- Kansas City, Kansas
- Erlanger, Kentucky
- Lexington, Kentucky
- Baton Rouge, Louisiana
- New Orleans, Louisiana
- Lake Charles, Louisiana
- Lafayette, Louisiana
- Jackson, Mississippi
- Springfield, Missouri
- Newark, New Jersey
- Charlotte, North Carolina
- Greensboro, North Carolina
- Greenville, North Carolina
- Raleigh, North Carolina
- Winston-Salem, North Carolina*
- Tulsa, Oklahoma
- Reading, Pennsylvania
- Charleston, South Carolina*
- Columbia, South Carolina*
- Nashville, Tennessee*
- Chattanooga, Tennessee
- Knoxville, Tennessee
- Amarillo, Texas
- Dallas, Texas*
- El Paso, Texas
- Irving, Texas
- Houston, Texas
- Lubbock, Texas
- Low Moor, Virginia
- Newport News, Virginia
- Richmond, Virginia*
- White Sulphur Springs, West Virginia
- Casper, Wyoming

*Site(s) visited by the Service Auditor

Principal Service Commitments and System Requirements

VRC has designed processes and procedures to meet its objectives for its Record Storage and Vaulting System services. Those objectives are based on the service commitments that VRC makes to user entities, the laws and regulations that govern the provision of VRC's Record Storage and Vaulting System services.

Security commitments to user entities are documented and communicated in Master Service Agreements (MSAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Record Storage and Vaulting System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of physical security controls to protect customer data both at rest and in transit

VRC establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in VRC's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been

documented on how to carry out specific manual and automated processes required in the operation and development of the VRC's Record Storage and Vaulting System services.

VitalStor: Box and File Storage

Delivery and Pickup of Records

VRC customizes its delivery procedures to fit each customer's needs. VRC provides a SAR (Service Activity Record) delivery form for customers to fill out ensuring an accurate description and chain of custody. Decisions on how deliveries are made is largely up to the customer, VRC will provide shipping services to out of town locations using the delivery service of your choice (e.g. FedEx).

VRC provides a variety of delivery or pickup options. If the request is made by 10:00 a.m., the boxes will be delivered or picked-up by 4:00 p.m. same day. If the request is made by 3:00 p.m., the service will be performed by noon of the next day. Additionally, VRC provides same-day additional deliveries for requests called in after the above-mentioned times. VRC also provides emergency delivery services, this service provides a two-hour turnaround promise, 24 hours a day, every day of the year.

On-site Viewing of Records

VRC has multiple on-site viewing rooms available at no cost, for reasonable use to customers for easier viewing and/or copying of records. This eliminates the delivery fee and the necessity of giving up your valuable office space for large audits, research projects, etc.

Destruction of Records

VRC is AAA certified with the National Association for Information Destruction (NAID). As part of VRC's destruction process, VRC provides customers a Destruction Report, which includes barcode numbers listing records eligible for destruction. By adding the barcodes to the report, VRC ensures 100% accuracy in the processing of records for destruction. VRC posts the Destruction Report monthly to on VitalWeb for the customer team to authorize.

Once authorization for destruction has been obtained, VRC updates the inventory system within 48 hours indicating the boxes are now status "D" for destroyed. This stops any additional storage charges after that month from being billed and legally updates the box as being destroyed. VRC then accesses the requested boxes and proceeds with the destruction process. The turnaround time for accessing the boxes is usually one to two weeks depending on the size of the list.

As part of the service line, VRC offers automatic customized retention scheduling to determine the dates for boxes to be reviewed for destruction. Customers need only to keep VRC informed of changes to the master retention schedule as opposed to updating each individual box.

VRC maintains NAID certification for destroying different types of media which include degaussing, punching the core of hard drives, and shredding/recycling. By default, VRC utilizes mobile shred units or in-house plant based shredding to destroy all paper media and completes the process for paper record destruction by recycling the shredded material. For all other types of media only NAID Certified methods of destruction are utilized. The practice of recycling is an important part of VRC's commitment to the environment. Upon request, VRC will provide a certificate of destruction to the customer after each destruction service.

VitalVault – Backup Tape Storage

VRC's media vault is a key component to its customer's comprehensive risk management program. To ensure the safety of customer data, as well as adhere to Business Continuity and Disaster Recovery compliance, secure offsite storage of customer backups is essential.

VRC's vault provides precise climate control which extends the life expectancy of customer media three fold from 5 to 15 years and is a highly recommended records management solution.

Security is maintained by a computer-controlled access system and is monitored 24 hours a day. The vault environment is protected by a FM200 Fire Suppression System, a waterless and odorless gas released in precise amounts to assure safety of customer media.

VaultTrac is VRC's proprietary inventory tracking software and incorporates barcode scanning technology into the critical task of accurately managing your offsite media library. VaultTrac allows online access for VRC clients to manage their offsite data. Special requests, tape movements and reporting can all be performed using this online system.

VRC's trained, bonded, and background checked courier's pickup vital data at the customer location at the specific time designated by the customer. VRC has flexible service programs to meet customer schedules for daily, weekly, or monthly offsite data rotation. Rush service is available with a guaranteed 2-hour turnaround time during normal business hours. Emergency access to customer data is provided 24 hours a day, every date of the year. For added security and protection, all service vehicles are climate controlled, unmarked, GPS tracked, and equipped with slam locks and fire extinguishers.

VitalWeb – Web Accessed Inventory Management

VitalWeb® is VRC's proprietary online box and file inventory management software. This state of the art, fully customizable software allows secure control and management of customer inventory online.

Key Features:

- No limits on files or descriptions
- Built in retention / compliance
- Customized reports
- Document searches
- Add boxes or change content
- Schedule destruction
- Department level management
- Multi-level security clearance capable

VitalScan – Scanning and Imaging Services

VRC's Imaging Service Bureaus are among the largest in the Southeast.

Imaging of active high volume or archival documents is rapidly becoming an integral part of many companies overall information management plans.

VRC's quality control processes are designed to meet or exceed industry standards. Documents are verified for quality and orientation as they are scanned. Scanner operators can rescan any document if it does not meet our strict standards for image quality.

VRC can scan documents on the customer's behalf using both "Back Log" and "Day Forward" methods. These document images can be stored into VRC's software or sent back for the customer to import into an imaging system of the customer's choice.

VRC's viewing software can be included on every CD-ROM produced for the customer. Technical support can be provided for customers after the original setup for a nominal fee.

VitalShred – Secure Document Destruction

Onsite Shredding

Onsite shredding is a service designed for organizations requiring the immediate and witnessed destruction of confidential materials on their premises. This service is typically required for destruction of copyrighted, royalty-based, or other highly sensitive materials. Strict best practices maintain security and privacy.

VRC's onsite document destruction service offers:

- Complete onsite destruction of paper-based media assets
- Service performed by background checked, safety and security screened destruction specialists and equipment operators
- Mobile shredding vehicles outfitted with precision destruction equipment and comprehensive security controls
- Documented, single chain-of-custody to establish accountability
- Secure and environmentally friendly disposition of shredded materials

Secure Mobile Shredding Units

VRC places secure containers in appropriate locations throughout the customer's premises. At regularly scheduled intervals, VRC's uniformed specialists transfer the contents of the containers to secure vehicles parked at the customer site. Materials are shredded beyond practical reconstruction in VRC's industrial-grade, mobile shredding units and then transferred to one of VRC's highly secure facilities.

From our facility, paper-based materials are sent to authorized plants for recycling, plastics are then delivered to a recycling facility or incinerated on premises. Upon request a certificate of destruction is provided at the conclusion of every shredding engagement ensuring a documented end to the chain-of-custody established by VRC.

VRC maintains National Association of Information Destruction (NAID) AAA Certification at all of its locations with the exception of Erlanger, KY, White Sulphur Springs, WV and the vault locations in Memphis, TN and Little Rock, AR.'

Plant Based or Off-Site Document Shredding or Media Destruction

For organizations which require ongoing, verified destruction of sensitive materials, VRC offers secure, offsite plant based destruction services. Strict best practices ensure a closed and consistent chain-of-custody, resulting in a tightly controlled, documented process that limits security breaches.

VRC's Plant Based Destruction offers:

- Complete destruction of paper, plastics and other media
- Trained, insured personnel and highly secure facilities and processes
- Documented chain-of-custody for accountability
- Secure, environmentally friendly disposition of destroyed materials
- Short-term holding service option to facilitate last-minute recovery
- Witnessed destruction, as required
- NAID AAA Certification

As required, representatives from your organization are allowed to witness VRC destruction activities first-hand. This may be desirable in the destruction of copyrighted, royalty-based, or highly sensitive materials – and is often legally required in the destruction of counterfeit or unlicensed materials.

VitalRF – Radio Frequency Tracking

VitalRF® is an exclusive customized Radio Frequency Identification (RFID) System offered only at VRC. VRC's proprietary software system, VitalWeb, utilizes this technology to better enhance the customer experience by providing maximum accountability. VRC is a pioneer in the use of RFID technology to manage inventory in its records

centers. Since 2011 every new box and file handled within the VRC system is tracked and managed utilizing our exclusive VitalRF® and VitalWeb products.

Radio-frequency Identification (RFID) is a technology that uses communication via radio waves to exchange data between a reader and an electronic tag which is attached to a custom passive VRC tag on every new box or file entering the VitalRF® system. This system is utilized for the purpose of identifying and tracking customer boxes and/or files throughout the VRC footprint. These RFID tags are integrated as a part of the barcode system that is associated with every box or file a customer may have stored at any of VRC's facilities.

Internal Control Framework

VRC consistently seeks to strengthen the ways in which it achieves expected results, accountability and stewardship of its resources. This section provides information about the five interrelated components of internal control at VRC and include VRC's:

- control environment,
- control activities,
- risk assessment process,
- monitoring activities, and
- information and communications systems.

Control Environment

The control environment sets the tone for VRC by providing fundamental discipline and structure. Key Elements of VRC's internal control systems include:

Integrity and Ethical Values

- Code of Conduct and Practice
  Senior Management sets the tone at the top for corporate behavior and corporate governance. All employees at VRC shall adhere to the policies and guidelines as set out in the Code of Conduct which sets out the principles to guide employees in carrying out their duties and responsibilities to the highest standards of personal and corporate integrity when dealing with internal and external parties. VRC's Code of Conduct covers areas such as compliance with respect to local laws and regulations, integrity, conduct in the workplace, business conduct, and protection of VRC's assets, confidentiality and conflicts of interest.

- Guidelines on Misconduct and Discipline
  Guidelines are in place for handling misconduct and disciplinary matters. These guidelines govern the actions to be taken in managing the misconduct of employees who breach the Code of Conduct or do not comply with the expressed and implied terms and conditions of employment.

Management's Philosophy and Operating Style

VRC's control environment reflects an overall attitude of awareness and actions of management, operations, systems, and sales concerning the importance of controls and their emphasis within the organization. The composition, activities, and attitudes of management combine to help verify that employees maintain the integrity of policies and controls and are knowledgeable of their responsibilities. Personnel policies concerning conduct standards, background checks, work hours, employment benefits, and general security have been developed to contribute to the overall control environment. Additionally, employee responsibilities are delineated to establish appropriate segregation of duties.

Organization Structure

VRC provides records and information management services through different locations and currently has 30 locations throughout the Southeast. VRC has a traditional organization structure led by senior leadership members who have clear roles of responsibility and lines of reporting. The proper segregation of duties promotes ownership and

accountability for risk taking and defines lines of accountability and delegated authority for planning, executing, controlling and monitoring business operations. Competent and professional individuals have been selected as part of the senior leadership to ensure we manage our business well and to deliver business results. Regular review of the organizational structure is held to address changes in the business environment as well as to keep up with current and future trending of new technologies, products and services.

Hiring Practices

The primary objective of personnel recruitment is to place qualified individuals in respective positions and to reduce operating costs by minimizing turnover. To meet these objectives, VRC implements strict hiring criteria for all employees. Each VRC employee must complete the following: (1) a pre-employment screen which includes a 7 year criminal (federal, state, county) background check, credit history check, motor vehicle record check, search of the sexual registry, 7 year employment verification, and a 10 panel drug screen; (2) employees are subject to random drug screens and criminal history checks bi-annually; (3) all employees must complete onboarding security awareness training and subsequent annual security awareness training; (4) employees are required to review and attest to their understanding of security related policies and procedures annually; (5) employees must participate in weekly staff meetings which include a refresher review of security measures used at VRC facilities; (6) all employees are required to review and sign the company Non-Disclosure Agreement prior to starting work at VRC.

Compliance

VRC monitors service levels through reporting generated out of its records management tracking applications as well as manual inspections of facilities and workflows. Internal audits are completed monthly at each VRC facility. The primary objective of the internal audits is to assist management with the effective execution of their responsibilities to customers and shareholders by providing management with assessments on internal control design and operating effectiveness, as well as recommendations to enhance internal controls. Additionally, the internal audits help VRC prepare for any third-party audits which are conducted by certifying bodies such as the Payment Card Industry Security Standards Council, National Association for Information Destruction, and PRISM. Audit reports are reviewed by executive management and remediation plans established as necessary.

Information Technology (IT)

IT modernization and digital enablement for superior customer experience is identified as one of VRC's key strategies. IT at VRC has been focusing on this strategy undertaking various initiatives which include the ground work for inducting changes and updates to the VitalWeb platform, improving application availability, modernizing Business Support Systems (BSS) and all around enhancements to system and data security in order to meet evolving business requirements and achieve competitive positioning. Cybersecurity is an essential and underlying part of our digital strategy and risk mitigation. In 2016, VRC worked to improve incident monitoring capability. In addition, focus continues on strengthening cybersecurity resilience through various initiatives. With business continuity being another critical area, continued focus and investments are being ensured in disaster recovery for key IT systems.

Sales

The Sales group is responsible for sales, sales support, and marketing of VRC's products and services. They coordinate service delivery to customers and manage customer relationships. This group serves as the interface between customer management and the other VRC departments. The Sales team represents customer interests within the organization and discusses issues with customers for assessment and resolution. After a prospective customer meets with Sales and selects VRC as their records and information management provider, they are set-up as a new customer and arrangements will be made to move their existing records to a designated VRC location. Once Sales has completed setup, the customer will begin interfacing with Customer Service and Customer Service will take over as the customer's point of contact and will assume responsibility for the input and loading of all relevant inventory data.

Control Activities

Control activities include appropriate processes and systems to ensure pickup, storage, retrieval, and destruction of customer records are done in accordance with best industry practices, customer contractual requirements, and

regulatory mandates. The control activities are comprised of general information system controls around the access to applications, physical security of facilities storing customer records as well as administrative areas, and maintaining appropriate environmental controls at storage facilities. Key activities within VRC are as follows:

Policies and Procedures.

VRC developed and maintains use of policies that establish what is expected or required, and procedures that put the policies into action. They are built into business processes and day-to-day activities. Policy documentation contains the principals that guide the conduct of employees and detail personnel policies. VRC has created and implemented policies that clearly define the expectations of their employees, including service standards, acceptable use of information systems as well as logical and physical security of systems and facilities. Compliance and the consequences of non-compliance are also contained within each policy and/or procedure. Procedures are readily available to employees and include, among others, customer implementation, incident and problem management, and emergency/disaster (e.g., HVAC, fire, water, and power). Periodic revisions and updates are released as needed to meet operational needs.

Environmental Controls and Physical Security

- Structure of Building

  All VRC locations are located within solid customized concrete facilities with no prefabricated metal walls. Additionally, where applicable facilities are hurricane or tornado wind rated. The facilities have a raised foundation of over three feet in the event of flooding. Additionally, each facility is equipped with emergency generators. The security systems are monitored 24 hours a day by a third-party, including live camera monitoring and recording of all cameras.

- Visitor Access

  All visitors to the VRC facility must be escorted upon arrival and register their presence. All facilities are equipped with access control points limiting the accessibility of visitors into the building and areas within VRC facilities. Only VRC employees or security cleared vendors with an escort are allowed into the secured storage areas. This virtually eliminates any opportunities for unauthorized viewing of records in storage at VRC. In addition to controlled access, all bay doors remain closed and locked at all times unless loading or unloading.

- Transport Vehicles

  VRC utilizes its own internal fleet of unmarked, slam lock equipped, GPS tracked and radio-dispatched vehicles to make 100% of customer deliveries and pick-ups. Only VRC employees are authorized to make deliveries to VRC customers.

- Fire Protection System

  VRC facilities utilize state of the art early suppression fast response (ESFR) fire suppression systems. ESFR systems are quick responding, high volume sprinkler systems that provide protection for high piled storage occupancies. Instead of merely controlling a fire until the original fuel source is depleted, ESFR systems are designed to suppress the fire by discharging a large volume of water directly to the fire to reduce the heat release rate. These systems, installed at the ceiling, use large volumes of water delivering large water droplets at a high velocity to knock down the fire plume and provide enhanced protection for High Piled Storage Occupancies, such as storage facilities. In addition to the ESFR systems, VRC has installed, throughout each facility, early warning detection equipment to provide a warning where there is a potential for fire.

- Temperature/climate conditions

  VRC recognizes the need for temperature maintenance in regard to successful long-term storage of records. The paper storage warehouses are air cooled and gas heated to maintain the facility temperature between 70 degrees and 80 degrees. The climate storage and vault storage areas, in which VRC stores more sensitive customer items, are specifically maintained at a temperature of 70 degrees with a constant humidity of 45%. The most important factor in maintaining long-term archival storage is consistency of the temperature to

reduce expanding and contracting of the items in storage, which can cause data loss. VRC monitors the facility's climatic condition every day to ensure consistency.

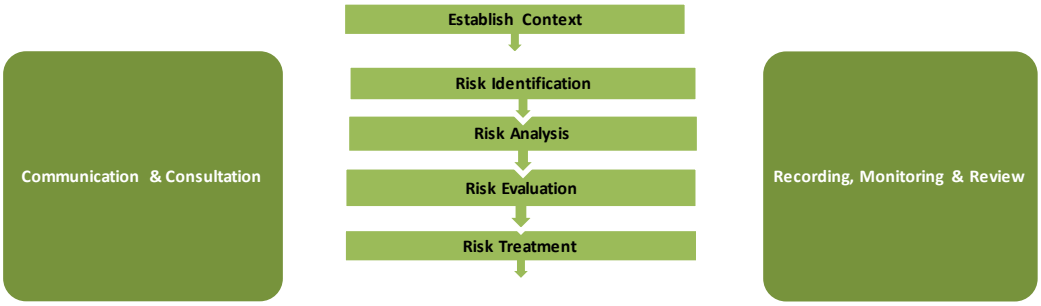
- Storage System Systematic Method
  VRC manages all of its client's records in a manner that is unique to the offsite storage industry. VRC does not inter-mix multiple customers' boxes, files, or tapes within their storage facilities. Most off-site storage companies use a LIFO or FIFO inventory system that will mix a customer's media with media from other customers on a daily basis. In the event a human error occurs, finding a box is nearly impossible using the LIFO or FIFO method.
  VRC assigns a unique location identifier to all of the media types stored with VRC, thus ensuring a negligible loss ratio. When a customer returns a box, file, tape, or other type of media to VRC, it is put back into the exact same slot from which it was pulled. Once again, there is no "revolving" system to increase the chances for a misplaced records.

- Racking/shelving systems
  VRC box facilities utilize a custom built racking system specifically designed for records storage. This system features corrugated flow through steel decking for boxes to be stored upon as opposed to wood decking, which can rot, sag, or become fuel for a fire. Where applicable, seismic racking systems are installed.

Risk Assessment Process

VRC's risk management process is guided and principally aligned with NIST guidelines where risk is managed to ensure the achievement and implementation of strategic objectives. VRC's risk management process typically involves identifying particular events or circumstances relevant to our objectives and risk appetite, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, evaluation of adequacy of existing controls, and monitoring the implementation of the response. The objective is to protect and create value for our key stakeholders.

Process for Managing Risk



The risk identification process, which is done on an ongoing basis entails scanning all key factors within VRC's business context from an 'outside-in" perspective. Risks are generally classified into distinct categories, i.e. strategic, financial, operational, and compliance representing the challenges to VRC's business operations. Risk information and treatment plans are captured and updated into a risk log which is maintained by Compliance. The information is then consolidated to provide an enterprise overview of material risks faced by VRC and the associated risk mitigation plans, which are tracked and reviewed from time to time.

Insurance and Physical Safeguard

VRC maintains an insurance program to ensure that its assets and businesses are sufficiently covered against damage that will result in material losses. At the same time, we also ensure that our major assets are physically safeguarded

and review the adequacy of the type of insurance coverage at regular intervals to ensure alignment against VRC's risk exposure.

Business Continuity Management

VRC is committed to safeguarding the interest of our customers by ensuring the ability of business operations to continue during a crisis and to have speedier recovery from a crisis through the implementation of Business Continuity Management (BCM) across the VRC enterprise. The BCM program provides a framework for VRC in building organizational resilience in the face of a crisis. The program created is sufficiently robust in catering to enhancements due to technological evolution and organizational changes.

VRC's BCM framework, aligned against industry standards and recommended guidelines have been formalized and standardized across VRC's corporate and operational footprint. At the same time, our versatile framework allows for customization in each location's requirements and operating environment. Business recovery plans have been documented for mission critical processes, tested and rehearsed regularly to ensure effective coordination, familiarity and awareness among employees. VRC's Compliance group, which is led by the Vice President of Compliance is responsible for ensuring effective implementation and coordination of business continuity efforts across VRC.

Monitoring

Monitoring covers the oversight of internal control by management or other parties outside the process or the application of independent methodologies, such as customized procedures or standard checklists, by employees within the process. Key monitoring activities within VRC are as follows:

- *Senior Leadership Team Meetings*
  The Senior Leadership Team meets bi-monthly and as when required, to deliberate on business performance, financial and operating risks and issues which include reviewing, resolving and approving all key business strategic measures and policies. Progress, exceptions and variations are also fully discussed and appropriate action taken.

- *Internal Audit (IA)*
  VRC monitors service levels through reporting generated out of its records management tracking applications as well as manual inspections of facilities and workflows. Internal audits are completed monthly at each VRC location. The primary objective of the internal audits is to assist management with the effective execution of their responsibilities to customers by providing management with assessments on internal control design and operating effectiveness, as well as recommendations to enhance internal controls.

Information and Communication Systems

VRC has various methods of communication to verify all employees understand their individual roles and responsibilities regarding protecting sensitive information, client service, and promoting timely communication of significant events. VRC has implemented Information Security procedures to enforce physical and logical protection of company and customer assets. All employees are informed of acceptable use of company assets via the VRC Employee Handbook. All employees are required to sign an acknowledgement that they have read the VRC Employee Handbook, which includes details of protecting sensitive information, prior to any access being granted.

In addition, the below communication methods are in place regarding client service and timely communication:

- Relaying notifications of significant policy and organizational events and changes
- Periodic departmental, general staff, and management meetings as appropriate
- Written position descriptions and other policies and procedures, including the responsibility to appropriately communicate significant issues and exceptions in a timely manner.

System Incident Information

There were no incidents that are likely to affect report users' understanding of how VRC met its security commitments in relation to Record Storage and Vaulting Systems during the period from June 1, 2018 to May 31, 2019.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of how Record Storage and Vaulting Systems is used to provide the service during the period from June 1, 2018, through May 31, 2019.

Complementary User Entity Controls

The Company's processes were designed with the assumption that certain controls would be implemented at the client organizations. In certain situations, the application of specified controls at client organizations is necessary to achieve certain applicable trust services criteria included in this report.

This section describes controls that should be in operation at the client organizations to complement the controls at VRC. Client auditors should consider whether the following controls have been placed in operation at the client organizations:

1. User organizations must ensure that only authorized individuals are registered as valid representatives to order pickup, retrieval, and or destruction requests to VRC.
2. User organizations must ensure that VRC is notified promptly when an authorized customer representative is terminated or is no longer authorized for system or facility access.
3. User organizations must notify VRC with users with administrative access to VitalWeb/VaultTrac/EvriChart or other VRC systems should have their access removed or modified.
4. User organizations must have a process in place to grant and revoke access privileges for their non-administrator users to VitalWeb/VaultTrac/EvriChart.
5. User organizations should identify an administrator commensurate with job responsibilities to control security access rights for individuals within their company.
6. User organizations should have controls in place to review all reports and documents provided or made available by VRC and inform VRC of any inaccuracies.

SECTION IV

Trust Services Security, Availability, and Confidentiality Categories, Criteria, Related Controls, and Tests of Controls

Introduction

This report is intended to provide user organizations of VRC Companies, LLC's (VRC) Record Storage and Vaulting system information about the controls that may affect the processing of user organizations transactions and provide users with information about the operating effectiveness of the controls that were tested. This report, when combined with an understanding and assessment of the controls at user organizations, is intended to assist user auditors in planning the audit of user organization's controls and in assessing control risk for assertions in user organization's environments that may be affected by controls at VRC.

Description of Testing Procedures Performed

As a part of the examination, we performed a variety of tests, each of which provided the basis for understanding the framework for controls. From this work, we determined whether the controls were actually in place and operating effectively during the reporting period.

Our tests of effectiveness of controls included such tests as we considered necessary in the circumstances to evaluate whether those controls, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specified control criteria were achieved during the reporting period. Our tests of the operational effectiveness of controls were designed to cover a representative number of transactions throughout the period.

In selecting particular tests of the operational effectiveness of controls, we considered (a) the nature of the items being tested, (b) the types of available evidential matter, (c) the nature of the audit objectives to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test in performing our testing procedures. In performing our work, we visited the VRC Companies, LLC's offices in Memphis, Tennessee, Nashville, Tennessee, Birmingham, Alabama, Florence, Alabama, Fort Myers, Florida, Melbourne, Florida, Orlando, Florida, Winston-Salem, North Carolina, Charleston, South Carolina, Columbia, South Carolina, and Richmond, Virginia.

Results of Testing Performed

The controls that were tested, as described in Section IV, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in Section IV were achieved during the period from June 1, 2018 to May 31, 2019.

It is each interested party's responsibility to evaluate this information in relation to internal controls in place at each user organization in order to assess the total system of internal controls if it is concluded that the user organization does not have effective internal controls in place, VRC Companes, LLC's internal controls may not compensate for such weaknesses.

The following tests, applied to specific controls that are referenced in the matrix below, were designed to obtain evidence about each control's effectiveness in meeting the stated control criteria.

In addition, as required by paragraph .35 of AT-C section 205, *Examination Engagements* (AICPA, Professional Standards, when using information produced (or provided) by the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

Complementary User Entity Controls

VRC's processes and underlying applications were designed/set-up with the assumption that certain controls would be implemented by user organizations (i.e., clients). In certain situations, the application of specific controls at user organizations is advisable and/or necessary, in conjunction with VRC's controls, to ensure user control objectives are accomplished.

The complementary user entity controls presented in Section III do not represent a comprehensive list of all controls that should be employed by user organizations. Other controls will likely be required at each user organization to mitigate risks affecting internal control to an acceptable level.

Description and Results of Testing

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CONTROL ENVIRONMENT			
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The organization has formal, written job descriptions. Job descriptions are provided to employees at the time of hire.	Verified the organization has formal job descriptions and ensured they are provided to employees at the time of hire.	No exceptions noted.
CC1.1.2	The organization maintains an updated organizational chart.	Obtained and inspected the current organizational chart.	No exceptions noted.
CC1.1.3	The organization has a formal employee handbook which defines the integrity and ethical values of VRC. Employees receive the handbook at the time of hire and are required to read and acknowledge.	Obtained and inspected the employee handbook. For a sample of new hires, confirmed that employees are required to sign the employee handbook.	No exceptions noted.
CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The organization has formal, written job descriptions. Job descriptions are provided to employees at the time of hire.	Verified the organization has formal job descriptions and ensured they are provided to employees at the time of hire.	No exceptions noted.
CC1.2.2	The organization has identified and established oversight responsibilities for senior management in relation to established requirements and expectations and has established an independent audit function.	Obtained the organizational chart and verified the organization has established an independent audit function.	No exceptions noted.
CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The organization maintains an updated organizational chart.	Obtained and inspected the current organizational chart.	No exceptions noted.
CC1.3.2	The organization has formal, written job descriptions. Job descriptions are provided to employees at the time of hire.	Verified the organization has formal job descriptions and ensured they are provided to employees at the time of hire.	No exceptions noted.
CC1.3.3	The organization performs background checks on potential employees, including criminal, credit, pre-employment, and reference checks.	Selected a sample of employees and obtained evidence a background check was performed.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The organization has formal, written job descriptions and are provided to employees at the time of hire. These job descriptions define expectations and competencies necessary to perform job duties.	Verified the organization has formal job descriptions and ensured they are provided to employees at the time of hire.	No exceptions noted.
CC1.4.2	The organization provides annual training to employees to attract, develop, and retain competent personnel to support and achieve organizational objectives.	For a sample of employees confirmed that the information security training is conducted at least annually.	No exceptions noted.
CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The organization has formal, written job descriptions. Job descriptions are provided to employees at the time of hire.	Verified the organization has formal job descriptions and ensured they are provided to employees at the time of hire.	No exceptions noted.
CC1.5.2	VRC compliance performs quarterly facility scorecard assessments which include security controls to ensure organizational guidelines are met.	Obtained and examined a sample of quarterly self-audits.	No exceptions noted.
CC1.5.3	The organization has a formal employee handbook. Employees receive the handbook at the time of hire and are required to read and acknowledge. VRC employee handbook outlines responsibilities of VRC employees.	Obtained and reviewed sanction policy within the employee handbook.	No exceptions noted.
CC1.5.4	The organization has documented hiring and termination procedures to provide or remove access to customer information.	Obtained and inspected the hiring and termination procedures to provide or remove access to customer information.	No exceptions noted.
COMMUNICATION AND INFORMATION			
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The information security policy specifies the methods for employee training to be conducted at least annually.	For a sample of employees confirmed that the information security training is conducted at least annually.	No exceptions noted.
CC2.1.2	The organization has a formal employee handbook. Employees receive the handbook at the time of hire and are required to read and acknowledge.	Obtained and inspected the employee handbook. For a sample of new hires, confirmed that employees are required to sign the employee handbook.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC2.1.3	VRC compliance performs quarterly facility scorecard assessments which includes security controls.	Obtained and examined a sample of quarterly self-audits.	No exceptions noted.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The organization has a formal, written information security policy.	Obtained and inspected the information security policy.	No exceptions noted.
CC2.2.2	The information security policy specifies the methods for employee training to be conducted at least annually.	For a sample of employees confirmed that the information security training is conducted at least annually.	No exceptions noted.
CC2.2.3	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10.	No exceptions noted.
CC2.2.4	The organization contractually communicates security responsibilities to each vendor.	Obtained and inspected a listing of contracts and confirmed that security responsibilities are communicated.	No exceptions noted.
CC2.2.5	Policies and procedure documents for significant processes are available VRC's network.	Examine evidence that confirms policies and procedures are stored in a readily accessible location for all employees.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The organization has a formal, written information security policy.	Obtained and inspected the information security policy.	No exceptions noted.
CC2.3.2	The organization contractually communicates security responsibilities to each vendor.	Obtained and inspected a listing of contracts and confirmed that security responsibilities are communicated.	No exceptions noted.
CC2.3.3	Organization maintains a current network diagram which is updated as necessary.	Obtained and inspected the network diagram and confirmed it is current and updated.	No exceptions noted.
CC2.3.4	Organization has formal written policies outlining a user's boundaries within a system.	Obtained and inspected the policies and procedures that define user boundaries within the VRC applications and environment.	No exceptions noted.
CC2.3.5	Organization utilizes user agreements to deliver expectations and/or limitations of access and use to users both external and internal. (Exhibit A or B)	For a sample of user agreements, confirm that expectation and limitation of use have been defined for internal and external users.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC2.3.6	The information security policy specifies the methods for employee training to be conducted at least annually.	Obtained and inspected the Privacy and Training policy. For a sample of employees confirmed that the information security training is conducted at least annually.	No exceptions noted.
CC2.3.7	Each employee and contractor signs a confidentiality agreement.	For a sample of employees and contractors confirmed that a confidentiality agreement is signed.	No exceptions noted.
CC2.3.8	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10.	No exceptions noted.
RISK ASSESSMENT			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The organization conducts a risk assessment at least annually, resulting in documented threats and mitigation plans.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established.	No exceptions noted.
CC3.1.2	VRC management performs a risk assessment annually. The risk assessment is based on the objectives established by management under the oversight of the board of directors. The objectives incorporate the service commitments and system requirements for vaulting services. Assessed risks are reviewed quarterly with the facility scorecard to identify changes in underlying threats or in the environment that would require an update to assessed risks.	Inspected the annual risk assessment documentation to determine whether the risk assessment process included consideration vaulting services. Obtained and examined a sample of facility scorecard assessments.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The organization conducts a risk assessment at least annually, resulting in documented threats and mitigation plans.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The organization has a formal, written risk-assessment plan.	Obtained and inspected the formal, written risk-assessment plan.	No exceptions noted.
CC3.3.2	The organization conducts a risk assessment at least annually, resulting in documented threats and mitigation plans.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established.	No exceptions noted.
CC3.3.3	As a part of risk assessment activities, VRC management has determined that relevant fraud risk would relate to control over client assets. In order to address this risk, VRC management has established controls to address physical security. VRC has established physical security controls (as documented in criteria 6.4) and conducts a risk assessment annually to address physical risk to assets.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established and physical risks are assessed.	No exceptions noted.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The organization has a formal, written risk-assessment plan.	Obtained and inspected the formal, written risk-assessment plan.	No exceptions noted.
CC3.4.2	The organization conducts a risk assessment at least annually, resulting in documented threats and mitigation plans.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established.	No exceptions noted.
CC3.4.3	Organization has a formal written information technology security policy which outlines authorization process.	Obtained and inspected the information security policy.	No exceptions noted.
CC3.4.4	Organization has a formal written change management policy.	Obtained and inspected the change management policy.	No exceptions noted.
CC3.4.5	Changes are managed and tracked and communicated to external users as necessary.	Obtained and inspected the change management logs for VitalTrac and VaultTrac applications and infrastructure changes. Examined examples of change communications to external users, if any.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC3.4.6	The organization utilizes automated tools to monitor for system changes and security threats.	Obtained and reviewed vulnerability scan utilities and scan results. Obtained and reviewed IT systems management and monitoring tool configurations.	No exceptions noted.
CC3.4.7	As part of the change management process, changes are approved, tested, and tracked through the ticketing system.	For a sample of changes, obtained evidence to confirm changes were approved, tested, and tracked through the ticketing system.	No exceptions noted.
MONITORING ACTIVITIES			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	VRC compliance performs quarterly facility scorecard assessments which includes security controls.	Obtained and examined a sample of quarterly self-audits.	No exceptions noted.
CC4.1.2	The organization monitors systems for security threats.	Obtained and reviewed vulnerability scan utilities and scan results. Obtained and reviewed IT systems management and monitoring tool configurations.	No exceptions noted.
CC4.1.3	External vulnerability scans are performed at least annually or after any significant change in the network to validate and identify vulnerabilities in the configuration.	Obtained evidence of external vulnerability scans to ensure they are performed annually or after any significant changes in the network.	No exceptions noted.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	VRC management performs quarterly facility scorecard assessments which includes security controls. Scorecard results are communicated to the VRC compliance department and VP of Compliance.	Obtained and examined a sample of quarterly self-audits.	No exceptions noted.
CC4.2.2	VRC IT monitors system infrastructure and applications for security threats and vulnerabilities. Security alerts and deficiencies are communicated to the VP of Information Technology.	Obtained and reviewed vulnerability scan utilities and scan results. Obtained and reviewed IT systems management and monitoring tool configurations.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CONTROL ACTIVITIES			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	External vulnerability scans are performed at least annually or after any significant change in the network to validate and identify vulnerabilities in the configuration.	Obtained evidence of external vulnerability scans to ensure they are performed annually or after any significant changes in the network.	No exceptions noted.
CC5.1.2	Strict control over the internal or external distribution of any kind of media is maintained, including the following: – Classify the media so the sensitivity of the data can be determined – Send the media by secured courier or other delivery method that can be accurately tracked.	Obtained VRC's Media Handling Procedures and verified that all media is classified. Obtained media tracking evidence and confirmed that it is secured and tracked.	No exceptions noted.
CC5.1.3	All access points to the facility are locked or have an electronic access mechanism.	Observed all access points at each location to ensure they are secured with lock or electronic access mechanism.	No exceptions noted.
CC5.1.4	The facility is equipped with a burglar alarm and monitored 24/7.	Obtained and inspected the facility's alarm monitoring service agreement or recent invoice.	No exceptions noted.
CC5.1.5	All entry points are monitored at all times.	Observed all access points at each location to ensure they are were being monitored by camera at all times.	No exceptions noted.
CC5.1.6	All visitors provide valid identification and sign a written log to gain entry.	Observed the visitor check-in process and validated visitors are required to provide valid identification and sign a log.	No exceptions noted.
CC5.1.7	GPS tracking software is installed on VRC vehicles and alerts are configured to email management based on defined settings, such as speeding, unexpected stops, and route changes.	Examine evidence to confirm GPS tracking software is installed and is configured to sent alerts.	No exceptions noted.
CC5.1.8	The facility is equipped with a fire suppression system.	Observed the fire suppression system.	No exceptions noted.
CC5.1.9	The facility is equipped with a fire detection system and monitored 24/7.	Obtained and examined recent invoices from fire detection system and monitoring service to verify facility is being monitored 24/7.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	External vulnerability scans are performed at least annually or after any significant change in the network to validate and identify vulnerabilities in the configuration.	Obtained evidence of external vulnerability scans to ensure they are performed annually or after any significant changes in the network.	No exceptions noted.
CC5.2.2	VRC, Inc has implemented a centrally managed antivirus solution. All windows servers have an antivirus agent installed and are configured to report to a centralized antivirus service.	Examine Antivirus installation and configuration documentation.	No exceptions noted.
CC5.2.3	VRC monitors all system components through an automated management interface to log, track, and maintain all inventory components.	Inspected the automated inventory management tool to determine that the tool is in place to monitor the system components. Inspected information system inventory records from the inventory management tool to determine that the tool was providing necessary information to manage assets.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC5.2.4	Each user account is appropriate according to business needs. All privileges are assigned based on job classification and function.	Selected a sample of user accounts to ensure appropriateness given roles, responsibilities, and business need.	Exceptions noted. LBMC identified 13 terminated associates and 6 test accounts with active access to the VitalWeb application. LBMC reviewed last login dates and confirmed the 6 test accounts were never logged in and 12 of the 13 terminated associate accounts were not accessed after the termination date. For the 1 account with activity after termination, LBMC obtained and reviewed VitalWeb access logs and confirmed no customer data was viewed or updated. Because no activity occurred from any of the accounts, LBMC determined the overall criteria was not impacted.
CC5.2.5	Systems are configured to enforce strong password construction (minimum character requirements, alpha and numeric characters, requiring at least one special character), if the current software supports this function.	Obtained evidence systems are configured to enforce minimum character requirements, require alpha and numeric characters, and require at least one special character, where the software allows.	No exceptions noted.
CC5.2.6	Management performs a monthly user review for the VitalTrack and VaulltTrack applications to ensure that users are terminated.	Inspected user review documentation for a sample of months to determine that user reviews were performed for the Vitaltrack and VaultTrac applications and that users are appropriate.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	VRC compliance performs quarterly facility scorecard assessments which includes security controls.	Obtained and examined a sample of quarterly self-audits.	No exceptions noted.
CC5.3.2	The organization has documented hiring and termination procedures to provide or remove access to customer information.	Obtained and inspected the hiring and termination procedures to provide or remove access to customer information.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC5.3.3	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10. For a recent incident, obtained evidence the documented process was followed.	No exceptions noted.
CC5.3.4	Organization has a formal written information technology security policy which outlines authorization process.	Obtained and inspected the information security policy.	No exceptions noted.
CC5.3.5	Organization has a formal written change management policy.	Obtained and inspected the change management policy.	No exceptions noted.
CC5.3.6	Organization has formal written policies and procedures addressing the handling, transmitting, or changing the environment in which confidential information is stored.	Obtained policies and inspected to determine the process for handling, transmitting, or changing the environment in which confidential information is stored.	No exceptions noted.
LOGICAL AND PHYSICAL ACCESS CONTROLS			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	VRC monitors all system components through an automated management interface to log, track, and maintain all inventory components.	Inspected the automated inventory management tool to determine that the tool is in place to monitor the system components. Inspected information system inventory records from the inventory management tool to determine that the tool was providing necessary information to manage assets.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.1.2	Each user account is appropriate according to business needs. All privileges are assigned based on job classification and function.	Selected a sample of user accounts to ensure appropriateness given roles, responsibilities, and business need.	Exceptions noted. LBMC identified 13 terminated associates and 6 test accounts with active access to the VitalWeb application. LBMC reviewed last login dates and confirmed the 6 test accounts were never logged in and 12 of the 13 terminated associate accounts were not accessed after the termination date. For the 1 account with activity after termination, LBMC obtained and reviewed VitalWeb access logs and confirmed no customer data was viewed or updated. Because no activity occurred from any of the accounts, LBMC determined the overall criteria was not impacted.
CC6.1.3	Systems are configured to enforce strong password construction (minimum character requirements, alpha and numeric characters, requiring at least one special character), if the current software supports this function.	Obtained evidence systems are configured to enforce minimum character requirements, require alpha and numeric characters, and require at least one special character, where the software allows.	No exceptions noted.
CC6.1.4	Clients complete a predetermined authorization process prior to receiving credentials to records management tools.	Obtained access policies and inspected to determine the process for authorizing clients to access record management tools. For a sample of clients, example evidence of the authorization process.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.1.5	Strict control over the internal or external distribution of any kind of media is maintained, including the following: – Classify the media so the sensitivity of the data can be determined – Send the media by secured courier or other delivery method that can be accurately tracked.	Obtained VRC's Media Handling Procedures and verified that all media is classified. Obtained media tracking evidence and confirmed that it is secured and tracked.	No exceptions noted.
CC6.1.6	A firewall is installed at each Internet connection and between any wireless networks.	Obtained and inspected network diagram to ensure a firewall is installed at each internet connection and between any wireless networks.	No exceptions noted.
CC6.1.7	Management performs a monthly user review for the Vitaltrack and VaultTrac applications to ensure terminated users are removed.	Inspected user review documentation for sample of months to determine that user reviews were performed for the Vitaltrack and VaultTrac applications to ensure access for terminated associates was removed.	No exceptions noted.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	There is a formal user registration and de-registration procedure in place for granting and revoking logical access to all information systems and services.	Selected a sample of new users to ensure new users are properly approved and terminated users are removed from information systems and services.	Exceptions noted. LBMC identified 13 terminated users with access to the VitalWeb application. LBMC reviewed last login dates and confirmed 12 of the 13 accounts were not accessed after the termination date. For the 1 account with activity after termination, LBMC obtained and reviewed VitalWeb access logs and confirmed no customer data was viewed or updated. Because no activity occurred from any of the accounts, LBMC determined the overall criteria was not impacted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.2.2	Employee passwords must be changed during designated intervals, not to exceed 90 days.	Obtained password policies and inspected to determine passwords must be changed every 90 days or more frequently.	No exceptions noted.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Each user account is appropriate according to business needs. All privileges are assigned based on job classification and function.	Selected a sample of user accounts to ensure appropriateness given roles, responsibilities, and business need.	Exceptions noted. LBMC identified 13 terminated associates and 6 test accounts with active access to the VitalWeb application. LBMC reviewed last login dates and confirmed the 6 test accounts were never logged in and 12 of the 13 terminated associate accounts were not accessed after the termination date. For the 1 account with activity after termination, LBMC obtained and reviewed VitalWeb access logs and confirmed no customer data was viewed or updated. Because no activity occurred from any of the accounts, LBMC determined the overall criteria was not impacted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.3.2	There is a formal user registration and de-registration procedure in place for granting and revoking logical access to all information systems and services.	Selected a sample of new users to ensure new users are properly approved and terminated users are removed from information systems and services.	Exceptions noted. LBMC identified 13 terminated users with access to the VitalWeb application. LBMC reviewed last login dates and confirmed 12 of the 13 accounts were not accessed after the termination date. For the 1 account with activity after termination, LBMC obtained and reviewed VitalWeb access logs and confirmed no customer data was viewed or updated. Because no activity occurred from any of the accounts, LBMC determined the overall criteria was not impacted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	The organization performs background checks on potential employees, including criminal, credit, pre-employment, and reference checks.	Selected a sample of employees and obtained evidence a background check was performed.	No exceptions noted.
CC6.4.2	All access points to the facility are locked or have an electronic access mechanism.	Observed all access points at each location to ensure they are secured with lock or electronic access mechanism.	No exceptions noted.
CC6.4.3	The facility is equipped with a burglar alarm and monitored 24/7.	Obtained and inspected the facility's alarm monitoring service agreement or recent invoice.	No exceptions noted.
CC6.4.4	All entry points are monitored at all times.	Observed all access points at each location to ensure they are were being monitored by camera at all times.	No exceptions noted.
CC6.4.5	All visitors provide valid identification and sign a written log to gain entry.	Observed the visitor check-in process and validated visitors are required to provide valid identification and sign a log.	No exceptions noted.
CC6.4.6	All visitors wear a badge that clearly designates them as a visitor.	Observed the visitor process and validated that visitors are required to wear a badge that clearly designates them as a visitor.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.4.7	All visitors are escorted at all times by an authorized employee unless preauthorized as a known visitor, such as common vendors.	Observed the visitor process and validated visitors are required to be escorted by an authorized employee at all times.	No exceptions noted.
CC6.4.8	Entry to client records are logged, either manually or electronically.	Observed that accessing client records is logged in the card history report.	No exceptions noted.
CC6.4.9	Keys are secured and restricted to appropriate employees.	Observed that an electronic key box or security cabinet is used to secure keys.	No exceptions noted.
CC6.4.10	There is a formal user registration and de-registration procedure in place for granting and revoking physical access to all information systems and services.	Selected a sample of new users to ensure new users are properly approved and terminated users are removed from information systems and services.	No exceptions noted.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	Formal data protection and disposal policies are in place to guide the secure disposal of the company's and customers' data.	Obtained and reviewed the data protection and disposal policies. Examine evidence to confirm processes are implemented in accordance with policy.	No exceptions noted.
CC6.5.2	VRC maintains strict physical control over all assets, including those identified for destruction, and has established controls to address physical security of all assets. VRC has established physical security controls (as documented in criteria 6.4) to protect all assets.	Observed physical asset protection controls for a sample of VRC locations.	No exceptions noted.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	A firewall is installed at each Internet connection and between any wireless networks.	Obtained and inspected network diagram to ensure a firewall is installed at each internet connection and between any wireless networks.	No exceptions noted.
CC6.6.2	Websites or browser-based utilities use secure sockets layer encryption when accessing client information.	Obtained and inspected the SSL certificates for websites.	No exceptions noted.
CC6.6.3	The organization monitors systems for security threats.	Obtained third-party contract to confirm that security threats are monitored.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Strict control over the internal or external distribution of any kind of media is maintained, including the following: – Classify the media so the sensitivity of the data can be determined – Send the media by secured courier or other delivery method that can be accurately tracked.	Obtained VRC's Media Handling Procedures and verified that all media is classified. Obtained media tracking evidence and confirmed that it is secured and tracked.	No exceptions noted.
CC6.7.2	Websites or browser-based utilities use secure sockets layer encryption when accessing client information.	Obtained and inspected the SSL certificates for websites.	No exceptions noted.
CC6.7.3	GPS tracking software is installed on VRC vehicles and alerts are configured to email management based on defined settings, such as speeding, unexpected stops, and route changes.	Examine evidence to confirm GPS tracking software is installed and is configured to sent alerts.	No exceptions noted.
CC6.7.4	A Service Activity Record (SAR) is created to manage the custody of media using item bar codes and RFID. The movement of media is tracked using the SAR and is reflected in the online tools.	For a sample of SARs, obtained and examined documentation and traced the movement of the media to the online tracking tool.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Antivirus and antimalware utilities are installed on every system commonly affected by malicious code, with automatic updates configured.	Obtained evidence that antivirus and antimalware utilities are centrally installed with automatic updates configured.	No exceptions noted.
SYSTEM OPERATIONS			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	The organization monitors systems for security threats.	Obtained third-party contract to confirm that security threats are monitored.	No exceptions noted.
CC7.1.2	VRC monitors and evaluates current processing capacity for critical information systems and notifies IT personnel when capacity thresholds are exceeded.	Obtained and reviewed the disk capacity monitoring tool evidence.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	External vulnerability scans are performed at least annually or after any significant change in the network to validate and identify vulnerabilities in the configuration.	Obtained evidence of external vulnerability scans to ensure they are performed annually or after any significant changes in the network.	No exceptions noted.
CC7.2.2	All entry points are monitored at all times.	Observed all access points at each location to ensure they are were being monitored by camera at all times.	No exceptions noted.
CC7.2.3	All visitors are escorted at all times by an authorized employee unless preauthorized as a known visitor, such as common vendors.	Observed the visitor process and validated visitors are required to be escorted by an authorized employee at all times.	No exceptions noted.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10. For a recent incident, obtained evidence the documented process was followed.	No exceptions noted.
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10. For a recent incident, obtained evidence the documented process was followed.	No exceptions noted.
CC7.4.2	Internal network vulnerability scans are performed weekly to identify critical and high vulnerabilities at a minimum.	Inspected internal vulnerability scan configuration and a sample scan report to confirm internal vulnerability scans were performed weekly.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The information security policy specifies the process for incident response that complies with Payment Card Industry Data Security Standard (PCI DSS) requirement 12.10.	Inspected the information security policy to ensure it specifies the process for incident response in compliance with PCI DSS 12.10. For a recent incident, obtained evidence the documented process was followed.	No exceptions noted.
CHANGE MANAGEMENT			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Organization has a formal written information technology security policy which outlines authorization process.	Obtained and inspected the information security policy.	No exceptions noted.
CC8.1.2	Organization has a formal written change management policy.	Obtained and inspected the change management policy.	No exceptions noted.
CC8.1.3	Organization can provide change management log and examples of change management communications to external users.	Obtained and inspected the change management logs for VitalTrac and VaultTrac applications and infrastructure changes.	No exceptions noted.
CC8.1.4	Organization utilizes help desk ticket system to track and post changes to the system.	Obtained and inspected evidence of help desk tickets tracked in the system.	No exceptions noted.
CC8.1.5	Patch management is performed at least quarterly and within 30 days for critical releases.	Observed critical application servers and a sample of workstations at each facility to ensure they are configured for automatic updates and have recent versions installed.	No exceptions noted.
CC8.1.6	Organization has formal written policies and procedures addressing the handling, transmitting, or changing the environment in which confidential information is stored.	Obtained policies and inspected to determine the process for handling, transmitting, or changing the environment in which confidential information is stored.	No exceptions noted.
CC8.1.7	Entry to client records are logged, either manually or electronically.	Observed that accessing client records is logged in the card history report.	No exceptions noted.
CC8.1.8	As part of the change management process, changes are approved, tested, and tracked through the ticketing system.	For a sample of changes, obtained evidence to confirm changes were approved, tested, and tracked through the ticketing system.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
RISK MITIGATION			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The organization conducts a risk assessment at least annually, resulting in documented threats and mitigation plans.	Obtained the most recent risk assessment to validate it has been performed annually. Inspected the risk assessment to ensure threats were identified and a mitigation plan was established.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Each vendor signs a confidentiality agreement.	Obtained and inspected a listing of vendors and confirm that all vendors have signed a confidentiality agreement.	No exceptions noted.
CC9.2.2	The organization contractually communicates security responsibilities to each vendor.	Obtained and inspected a listing of contracts and confirmed that security responsibilities are communicated.	No exceptions noted.
CC9.2.3	The organization has a formal selection process to evaluate third-party capabilities and service delivery.	Obtained and reviewed the Vendor Management Policy. For a vendor added during the audit period, obtained evidence the vendor went through the vetting process.	No exceptions noted.
ADDITIONAL CRITERIA FOR AVAILABILITY			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	VRC monitors and evaluates current processing capacity for critical information systems and notifies IT personnel when capacity thresholds are exceeded.	Obtained and reviewed the disk capacity monitoring tool evidence.	No exceptions noted.
A1.1.2	Organization monitors the VRC system usage and system analytics for the patterns of usage or instability within the VRC environment.	Observed Kaseya application. Obtained and reviewed Kaseya reports.	No exceptions noted.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	The facility is equipped with a fire suppression system.	Observed the fire suppression system.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
A1.2.2	The facility is equipped with a fire detection system and monitored 24/7.	Obtained and examined recent invoices from fire detection system and monitoring service to verify facility is being monitored 24/7.	No exceptions noted.
A1.2.3	Critical operation servers, including those containing client-owned information, are equipped with battery backup systems.	Observed battery backup systems supporting critical operation servers in server rooms for sampled locations.	No exceptions noted.
A1.2.4	Critical operation servers are properly cooled if contained within an enclosed computer room.	Observed server room to ensure critical operations servers are properly cooled.	No exceptions noted.
A1.2.5	Critical operation servers are backed up from Memphis to Dallas using BackupChain.	Obtained and inspected evidence critical servers are backed up to Dallas using BackupChain.	No exceptions noted.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Critical VRC servers are backed up and tested.	Obtained and inspected backup results from the backup software and confirm that servers are backed up and tested.	No exceptions noted.
A1.3.2	Organization can provide verification of successful backups.	Obtained and inspected backup results from the backup software and confirm that servers are backed up and successful.	No exceptions noted.
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	Each vendor signs a confidentiality agreement.	Obtained and inspected a listing of vendors and confirm that all vendors have signed a confidentiality agreement.	No exceptions noted.
C1.1.2	The organization contractually communicates security responsibilities to each vendor.	Obtained and inspected a listing of contracts and confirmed that security responsibilities are communicated.	No exceptions noted.
C1.1.3	The organization has a formal employee handbook. Employees receive the handbook at the time of hire and are required to read and acknowledge.	Obtained and inspected the employee handbook. For a sample of new hires, confirmed that employees are required to sign the employee handbook.	No exceptions noted.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	The organization contractually communicates security responsibilities to each vendor.	Obtained and inspected a listing of contracts and confirmed that security responsibilities are communicated.	No exceptions noted.

Control Number	Controls Specified by VRC	Testing Procedures Performed by LBMC	Testing Results
C1.2.2	Formal data Protection and disposal policies are in place to guide the secure disposal of the company's and customers' data.	Obtained and reviewed the data protection and disposal policies.	No exceptions noted.
C1.2.3	VRC maintains strict physical control over all assets, including those identified for destruction, and has established controls to address physical security of all assets. VRC has established physical security controls (as documented in criteria 6.4) to protect all assets.	Observed physical asset protection controls (see CC6.4) for a sample of VRC locations.	No exceptions noted.

VITAL RECORDS CONTROL COMPANIES Policies and Procedures	Supersedes: 03/28/2017	Date Effective: 08/07/2018	Number: 300.18.04
For Internal Use Only	Approved By:		Page: 1 of 3
Section: SECURITY	Subject: PRIVACY POLICY		

Purpose: This document is intended to establish the policy for VRC Companies, LLC ("Company") to maintain a secure environment ensuring the privacy of client information. The Company has always safeguarded the confidentiality of information provided to us by our clients and are bound by our professional standards to continue to maintain this vital aspect of our professional relationship.

Responsibility: All employees, Service Providers and Company vendors.

1. Acquisition of Client Information

The Company stores and maintains on our clients behalf nonpublic personal information about our clients from the following sources:

- Information You Provide: Our client engagements routinely require us to obtain private information about our clients so that we can proceed with the various services we perform for our clients as part of the professional relationship.

- Other Sources: Depending upon the particular service a client engages the firm to complete, we may request nonpublic information concerning the matter at hand. However, this information is certainly not obtained without our client's specific authorization for the type of information and the source(s) from which it may be obtained.

2. Disclosure of Nonpublic Information

Our Company policy is to on no occasion disclose nonpublic information about our clients. Nonpublic personal information is defined in the regulations as any publicly available information that we acquire by using information you have provided us in connection with any professional services we perform for you, which is not public information. An example would be a bank account number that is somehow used to acquire information regarding a court trial or other public record that would not have been found by us without using the bank account number acquired from you. In a generic sense, any information that a client

provides us that involves financial product or service is likely considered nonpublic personal information and receives the same protection from disclosure as all other information about our clients. For purposes of our business relationships with our clients, all information acquired is disclosed only under the following conditions:

- Employees of the Company: Authorized employees who need such information to conclude a transaction for which the client has engaged the firm.

- Service Providers: As with any business, we have our own accounting, insurance and other service firms that we may need to provide information that the regulations consider nonpublic personal information. An example might be your account activity for our accounting firm to prepare financial statements for our internal or external purposes. Another example would be computer consultants that must have access to certain client records so as to be able to increase the efficiency of our computer processing systems. We have always insisted that any such information that needed to be disclosed for a business purpose be considered confidential and not used for any purpose other than the specific business need. That well-understood business policy of confidentiality will be reinforced as needed by contractual agreements between such service providers to the Company.

- Others: Other than as stated above, we do not disclose nonpublic personal information, or any other information, to any outside party without specific client authorization.

3. Security Arrangements

The Company maintains physical, electronic and procedural safeguards that comply with federal regulations to guard our clients' nonpublic personal information and any other information, to ensure our clients that their privacy is a major part of the Company's commitment to provide the finest service possible.

4. Opt Out Provision

The Federal Trade Commission regulations provide that this notice must include a provision for you to request that the firm not release your nonpublic personal information.

While such request is unnecessary, because the Company does not disclose your nonpublic personal information in a manner that would allow you to opt out, in the interests of satisfying regulations, we include this Opt-Out Provision.

Please contact the Vice President of Compliance at (901) 685-1177 if you have any questions. Our privacy, our professional standard, and the ability to provide you with quality professional services are very important to us.

VITAL RECORDS CONTROL COMPANIES Policies and Procedures	Supersedes: 01/02/2015	Date Effective: 08/07/2018	Number: 400.04.00
For Internal Use Only	Approved By:		Page: 1 of 3
Section: WAREHOUSE/DRIVER	Subject: MATERIAL HANDLING OF BOXES STORAGE, PICKUP AND STAGING		

PURPOSE: To establish the procedures for customers and VRC Companies, LLC ("VRC") employees to follow when handling records before storage, while packaging records for storage, pickup by VRC employees and staging of boxes on pallets within VRC facilities.

RESPONSIBILITY: Customers and VRC employees.

Preparing to Store Hard Copies

To facilitate process improvement controls over records in storage at VRC Companies, the following standard procedures for preparing records for storage have been established:

I. Unless otherwise approved, all records must be packed in a standard records center storage box (1.3 cubic feet) with attached lid.

II. In estimating the number of boxes needed, figure two boxes per letter size file drawer and two and one-half boxes per legal size file drawer. Contact the manager of your VRC facility to purchase these boxes.

III. Correct assembly of records storage boxes is necessary to ensure the structural integrity of the box and to protect the contents. For example, all flaps are designed to be tucked inside to strengthen the bottom and sides of the box. Use of double-walled boxes is preferred for better structural integrity.

IV. Boxes must be new and free of markings except for the clients' box, series or other numbers etc. or at least be free of all other markings on one end where the bar code label will be placed

V. Determine how the records will be divided for placement in the boxes. The series can be divided monthly, quarterly, annually by fiscal or calendar year, or any other logical sub-division, such as by closure date. All the records in a box must be the same records series and eligible for final disposition at the same time.

VI. When packing records, keep the records in the original filing arrangement provided it is a logical and systematic order, whether alphabetical, numerical or chronological. For files in numerical order, place the lowest number first to the front of the box. For files in

alphabetical order, begin with "A" in the front of the box. For files in chronological order, place them in the box by consecutive dates.

VII. Place files upright in the box and leave at least one inch space at each end to make handling the box easier. Place legal size files in the box sideways, facing the left-hand side of the front end of the box.

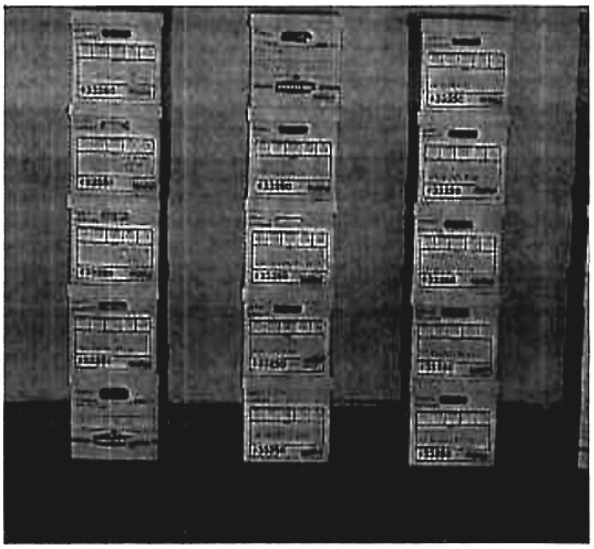
VIII. Stack computer printouts and ledgers on the bottom of the box facing the lid. Do not stack paper above the handles. You may purchase special sized boxes if needed.

IX. Stacked Boxes for Pickup

X. Stack boxes six high or less to prevent crashing of bottom boxes and have your transmittal sheet ready for the customer service representative. (Figure 2)

Stacking Boxes for Pickup

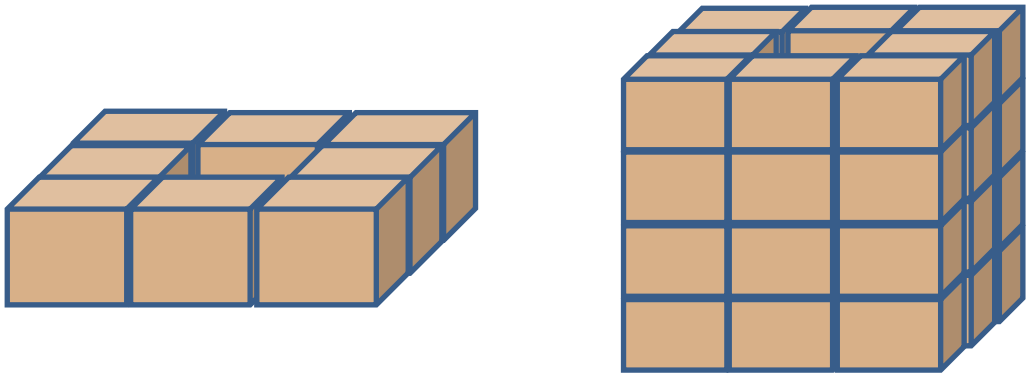
When preparing/stacking boxes for pickup which are not on a pallet, stack them five high per the photo below.



Stacking Boxes on Pallets

I. Begin in one corner, placing boxes with barcodes facing out.

II. Place one on another corner with barcode facing out. Continue around and finish the bottom row. Then start another row and follow the illustrated example below.



III. Make sure the stack is tight. There will be a hole down the middle of the stack. This is alright as we will shrink wrap the pallet of boxes. This design facilitates your customer service representative's ability to scan the barcodes without additional labor and cost to you.

IV. Barcode labels will be placed in the top right corner of each box. They should not be placed along an edge of the box or on top of any paperwork stuck to the outside of the box. Make sure they are at least one inch from any edge.

VITAL RECORDS CONTROL COMPANIES Policies and Procedures	Supersedes: 04/14/2017	Date Effective: 07/16/2018	Number: 300.01.00
For Internal Use Only	Approved by:		Page: 1 of 4
Section: SECURITY	Subject: ACCESS CONTROL AND PHYSICAL SECURITY POLICY		

Purpose: The purpose of the VRC Companies ("VRC") Access Control and Physical Security Policy is to establish the guidelines for enhancing and preserving the personal safety of employees and facility visitors; secure the physical property and tangible assets of VRC and its' customers, and protect VRC buildings from unauthorized intrusion.

Responsibility: All employees.

Frequency: Daily

This policy will institute the standards for limiting, controlling, and monitoring access to sensitive, restricted and controlled areas of VRC to authorized personnel only. Additionally, this policy will serve as a guide for the adherence to the Identification Badge System and the Access Control system used in the identification of persons who have legitimate access to and use of VRC resources.

Identification Badge System - Employee

- All employee identification badges will be issued exclusively by Human Resources and will remain the property of VRC.
- The cardholder must report the loss/theft of an identification badge immediately to their supervisor.
- All employees are to display their employee identification badge anytime an employee is on VRC property or while providing service to VRC customers.
- When a person no longer needs the identification badge, i.e. termination, voluntary separation, etc., the badge must be returned to the Hiring Manager.

Identification Badge System – Visitor

- All visitors must present government issued identification.
- All visitors will be issued identification badges by the attendant in the reception area prior to entry into the facility.
- As part of the registration process all visitors will be required to sign a Visitor Non-Disclosure Agreement.

- Identification badges are not coded to grant access to restricted areas, however, the badge is equipped with RFID tracking.
- All badges must be returned at the close of business and accounted for each day as part of the daily Closing Log responsibilities.

Identification Badge System – Vendor

- All vendors must present government issued identification.
- All vendors will be issued identification badges by the attendant in the reception area prior to entry into the facility.
- As part of the registration process all vendors will be required to sign a Vendor Confidentiality Agreement.
- Identification badges are not coded to grant access to restricted areas, however, the badge is equipped with RFID tracking.
- All badges must be returned at the close of business and accounted for each month as part of the daily Closing Log responsibilities.

Secure Perimeters

- All exterior doors (including bay doors) to all facilities will be alarmed to ensure a secure perimeter of each building after the close of business.
- All exterior doors (including bay doors) are to remain closed and locked, except to load and unload trucks.
- VRC installs access control devices at each building's primary entrances and restricted areas where the contents of the area present a high risk.
- Visitors/Vendors must remain in public areas unless unique circumstances require entrance into the restricted areas, i.e. landlord, building/equipment maintenance, etc. If the vendor is allowed in a restricted area they must be accompanied by a VRC employee at all times.

Closed Circuit Television (CCTV) and Phones

- VRC uses CCTV systems as an integral part of its physical security system. The integration of cameras adds efficiency and effectiveness to guard functions.

- VRC's CCTV footage is monitored 24/7/365 by personnel in the Nerve Center located at corporate headquarters (formerly NS&T).
- All camera issues (i.e., outage, obstructed view, etc.) are reported to facility management (Director of Operations and/or Area Vice President), Information Technology (if hardware related) and Vice President, Compliance.
- Cameras are positioned on building roofs, all points of ingress and egress to the building, central interior junctions, and in areas of high risk.
- All VRC facilities provide 24 hour phone access. If needed, customers have the option of calling the VRC answering service after hours to request emergency services.
- No customer names can be used over the intercom or phone systems, customers will only be referenced to by account number.
- All drivers are in constant contact with the facility.

Alarms

- All exterior perimeter doors are alarmed and motion sensors activated at the close of business each day and monitored by an external security company 24 hours a day.
- All buildings are equipped with facility intrusion silent alarms, extra sensitive early warning smoke detectors, and flood detectors.
- All buildings are equipped with ceiling mounted Early Suppression Fast Response density specific sprinkler systems or gaseous fire extinguisher systems, i.e. Halon or FM2000.

Keys

- All keys are locked in a controlled access key lockbox or locked secure desk each day. Employees are only allowed to use keys that are available at their access level.
- Each day the closing supervisor verifies all keys have been returned to the lockbox/desk and signs the Closing Log signifying they have performed the verification check.

Security Enforcement

The integrity and value of VRC rests with the individual commitment of each employee to support the objectives of this policy and all supporting security related policies and procedures. It is imperative employees self-police all protected areas. This means that everyone notes doors

that have been propped open, have tape across the door's strike, unescorted visitors, the wrong people in the wrong areas, intruders in offices, missing files, equipment, etc. and takes reasonable steps to remedy observations. This would further include notification to your immediate supervisor, and said supervisor must in turn notify the facility Area Vice President and Vice President, Compliance. Any employee not complying with this policy is subject to disciplinary action up to and including termination.