



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

Header 2

List View

General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 738719


Procurement Type: Statewide MA (Open End)

Vendor ID: 

Legal Name: IRON MOUNTAIN INCORPORATED

Alias/DBA: IRON MOUNTAIN

Total Bid: \$0.00

Response Date: 

Response Time:

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: 

Total of Header Attachments: 2

Total of All Attachments: 2

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Document Storage Services	0.00000	LS	\$0.000000	\$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.



IRON MOUNTAIN®



**IRON MOUNTAIN PROPOSAL FOR
STATEWIDE CONTRACT FOR RECORDS MANAGEMENT**

SOLICITATION NUMBER: CRFQ 0212 SWC2100000001

SUBMITTED TO: WEST VIRGINIA OFFICE OF TECHNOLOGY (WVOT)

SUBMITTED BY: IRON MOUNTAIN INFORMATION MANAGEMENT, LLC

Iron Mountain Information Management, LLC
One Federal Street
Boston, MA 02110

DUNS: 621417633
CAGE CODE: 1F2Y7

Submission Date: 08/18/2020

CONFIDENTIALITY

This submission includes information that shall not be duplicated, used or disclosed — in whole or in part — for any purpose other than to evaluate this submission. Contains Iron Mountain confidential and proprietary information © 2020, Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated in the U.S. and other countries. All other trademarks are the property of their respective owners.



TABLE OF CONTENTS

1.0 Executive Summary 1
1.1 Avoiding the Operational Risk of Change 2
1.1.1 Transition Timescale 2
1.2.1 Risk of Loss or Damage 3
1.2.2 Program Savings 3
1.2.3 Our Ability to Deliver Much More 3
2.0 Records Management 4
2.1 Incoming Workflow 4
2.2 Retrieval Workflow 5
3.0 Records Management Chain of Custody 7
4.0 Transfer Process 9
5.0 SafeKeeperPLUS 10
6.0 IMConnect 12
6.1 Retention Management 13
6.2 Electronic Retrievals 14
6.3 Produce Reports 14
6.4 Control and Manage 15
6.5 Additional Features 15
7.0 Record Management Facilities 16
7.1 Facility Security 16
8.0 Vehicle Technology and Security 19
8.1 InControl Transportation System 19
8.2 Fleet Telematics 20
8.3 Driver Safety 20
9.0 Off-Site Shredding Workflow 21
9.1 Defined Workflow Process 22
9.2 In Control® Shred Usage Report 24
9.3 Shredding Specifications 24



9.3.1 Destruction Compliance 24

10.0 Appendix 25

10.1 Compliance With RFQ Specifications 25

 10.1.1 Section 4 Qualifications 25

 10.1.2 Section 5 General Requirements 27

 10.1.3 Permanent Withdrawal 30

10.2 Attachments 31

 10.2.1 BI Program Overview 31

 10.2.2 Visitor Safety and Security Welcome Policy 31

 10.2.3 Floodplain Certificate 31

10.3 Exceptions 32



1.0 EXECUTIVE SUMMARY

As the global leader in information management services, Iron Mountain provides record management, data management, information governance, and information destruction services for more than 225,000 organizations around the world. Iron Mountain offers Government agencies a comprehensive array of information management solutions that help government agencies secure their physical and digital assets to lower costs, mitigate risks, meet compliance and improve access to mission critical information.

West Virginia Presence

Iron Mountain currently provides Records Management and Storage services for the State of West Virginia at our two facilities in Charleston, located at MacCorkle Avenue, just seven miles from the State capital. For the life of this contract, Iron Mountain will keep all records stored within the State of West Virginia.

In addition to our two (2) primary facilities currently servicing the State, Iron Mountain has a sizeable business footprint in the State of West Virginia with a total of nine employees and Image on Demand services within the local market facility. We also provide Courier deliveries (we do not ship via third party). Iron Mountain also has the capacity to continue providing storage for the State’s existing records while accommodating the State’s increasing storage requirements.

Fac #	Address	City	Prov	L/O	Square Feet	Building Capacity	Racking Capacity	Volume
002911	5736 MacCorkle Ave Unit 3	Charleston	WV	L	67,847	609,669	608,669	565,630
003822	5736 MacCorkle Ave Unit 1	Charleston	WV	L	37,655	186,760	100,054	44,510
	Totals/Averages				105,502	796,429	708,723	610,140
							Racked Avail	98,583

We are happy to have a local presence to continue to do business within the state while also adding to the economy within West Virginia. We are committed to our neighborhoods through various volunteer events throughout the year, and are happy to make an impact in our local communities in more ways than through business. As your trusted business partner, and understanding the need for safeguarding public trust of taxpayer funds, we are pleased to present this offer which represents an immediate savings of \$97k in year one and nearly \$500k over the initial five year term of the contract. The savings will begin being realized as soon as the agreement is finalized; other options could take as many as five to ten years before the State and taxpayers of West Virginia gain any cost savings. Iron Mountain is committed to saving the taxpayers of the State of West Virginia more than half of a million dollars with the acceptance of this proposal.

A Trusted Partner

As a trusted provider for many states, cities, counties, universities, and hundreds of thousands of other companies around the globe, Iron Mountain is uniquely qualified to expand services to your organization. Our experience puts us in a unique position to capitalize on the experiences of being the industry leader for nearly 70 years. Iron Mountain is unmatched when it comes to stability, financial strength, and security.



We understand that our most valuable asset is trust. From the everyday to the extraordinary, our customer's rely on Iron Mountain to securely process their assets—with a chain of custody model that ensures that they are protected and accessible when needed.

Iron Mountain currently provides mission critical services to 29 State governments. We provide services to various agencies, including: Health and Human Services, Transportation, Courts and Public Safety. Within the state of West Virginia, Iron Mountain is a trusted partner with local government and educational institutions to secure and process informational assets with services such as storage, imaging, and secure destruction.

As the incumbent vendor, Iron Mountain is by far in the best position to deliver savings over the contract term specified in the RFQ. At the current industry standard and IRM inventory transition speed of 60 cubic feet per/market/per day, it would take almost 15 years to fully transition the State's program to another vendor. By maintaining Iron Mountain as their storage vendor, the State would see greater savings over the contract period and would avoid costly disruptions to their program associated with managing multiple vendors over an extended period of time.

1.1 AVOIDING THE OPERATIONAL RISK OF CHANGE

The burden and upheaval of transferring critical records from one supplier to another should not be underestimated. Below, we have outlined some of the operational risks associated with a transition of this scale and importance:

1.1.1 Transition Timescale

- The transition from Iron Mountain to a new vendor would take 177 months or almost 15 years (based on most vendors' mutually agreed exit/ingestion flow rates of 50 boxes per day).
- While we endeavor to limit any disruption to day-to-day business, clearly Boxes or Files will not be available for retrieval while they are in transit (and no guarantee from the new vendor that records will be inbound immediately). Additionally, the State of West Virginia will need to manage a dual vendor program for a considerable amount of time.
- Issues relating to moving to a dual vendor program for a significant period are:
 - Fragmented control of records and data potentially putting client and sensitive data at risk
 - User experience will be undeniably affected (SLAs, Customer Service etc.)
 - Invoicing – billing and accounts payable issues associated with operating the same service with two vendors
 - Management time – The State of West Virginia will need to have project resources to support the implementation and will have to spend additional time managing business with multiple suppliers – and operationally bringing the new vendor 'up-to-speed'
 - Storage to Iron Mountain will still be paid over a 14+ year exit – Concurrent invoicing from both suppliers, this will need to be managed closely and monitored over this period.



1.2.1 Risk of Loss or Damage

- While we (and other reputable vendors in our industry) take all precautions to ensure there is no loss or damage during transit, it remains a risk, given the high volume of records being moved.

1.2.2 Program Savings

- Immediate savings of \$97,000 in one year;
- \$485,000 in savings over the initial five-year term of the contract

1.2.3 Our Ability to Deliver Much More

By continuing to develop the partnership with Iron Mountain, the State of West Virginia has access to the broadest range, and most advanced solutions for both physical and digital information management. Iron Mountain is continually investing in new technology and offers solutions that can support The State of West Virginia as a whole and each of its lines of business. Innovation is an essential part of our strategy and value creation, and we are focused on investing in solutions and services to enable our customers to navigate the hybrid world of physical and digital. As an organization, we look to identify essential opportunities that will enhance customer experiences and generate savings for the State of West Virginia. An example of this is our partnership with Google to support Iron Mountain InSight, which is a content services platform that provides actionable business insights and predictive analytics through Machine-Learning-based classification of a company's physical and digital information.

Quality

Given the importance of the assets and intellectual property handled at our facilities, Iron Mountain utilizes institutionalized processes to actively monitor and manage program quality. Iron Mountain's Operational Excellence Program (OEP) enables continuous improvement by establishing targets, providing supporting tools and systems, and measuring three key areas: service, quality, and production.

Comprehensive Solutions

Iron Mountain offers a comprehensive array of information management solutions that help you know what information you have, where it is stored, and how to get to it quickly and confidently to reduce costs, risks, and inefficiencies unlocking its inherent value.

Our ability to service the State of West Virginia is further enhanced by a dedicated team of professionals with the experience necessary to provide a comprehensive solution.



2.0 RECORDS MANAGEMENT

With Iron Mountain's comprehensive solution, the State of West Virginia Office of Technology (WVOT/the State) will have the ability to locate, access, and delivery any records when required. We will provide the State with the confidence to entrust their records management with Iron Mountain's proven processes, practices, and thinking. As a trusted industry leader, we actively work with customers to tailor solutions to meet their information management needs of today and the future. The State can leverage this experience to understand a changing regulatory landscape and assist with the development of a compliance based and legally credible records management program.

WVOT will have the ability to document these guidelines and store them in a centralized online repository that is easily accessible by all members of the organization. Additionally, the State will be able to run a host of informative reports about retention and disposal practices, helping to evaluate performance and maintain compliance. In addition, the State will be able to develop a process for suspending the destruction of any records based on their internal or external needs.

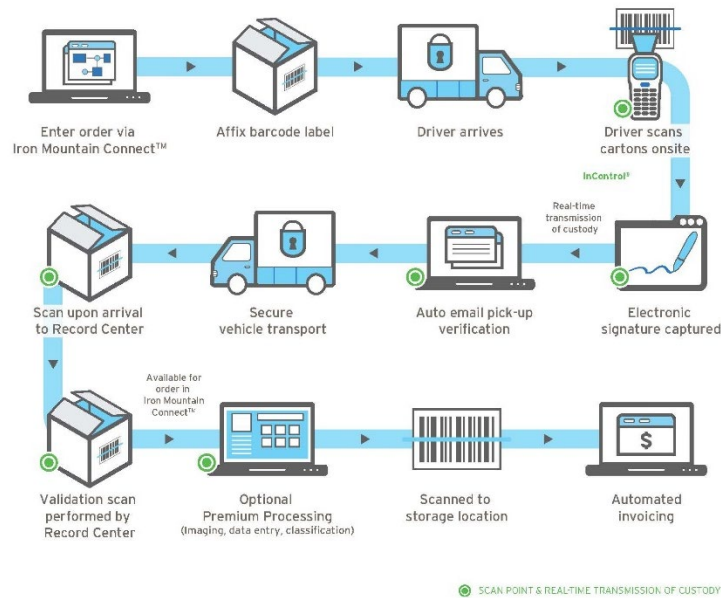
Iron Mountain's comprehensive records and information management services include standardized solutions for transportation, retrievals, refills, interfiling, rush/critical delivery, indexing, scanning, destruction, carton purchases, and specialized labor. Iron Mountain will provide the State with industry best practices, defined processes, and tested procedures to support the overall records program as well as provide effective support to the State records programs.

Once Iron Mountain assumes physical custody and responsibility for the State material, all records are tagged and classified using customer defined terminology, tracked with bar-coded labels, and made available on our intuitive IMConnect web portal, helping the State to quickly locate and retrieve the information required to address internal and external requests. Retention schedules, records storage policies and procedures, and other Iron Mountain services can also be requested through the portal.

2.1 INCOMING WORKFLOW

Iron Mountain's proven workflows ensure chain of custody and proper care for the State informational assets. Iron Mountain's workflows combine standard operating procedures with multiple barcode scan points to ensure records are accurately processed. Incoming workflow drives secure, reliable service, and augments the quality of records indexing for improved access and management. Highlights of our workflow elements that will greatly assist the State include:

- **Triple-Check Workflow.** Like all of our checks and balances, these process redundancies protect the security and chain of custody of your information.
- **Data Entry Validation.** We validate that all new items are received with descriptive information. Whether that information is keyed by us or by you via Iron Mountain Connect, it's another example of the checks and balances we use to ensure quality inventory control.



2-1. Incoming workflow.

Iron Mountain will provide pick-up service, within a 50 mile radius, using the following SLAs:

- **Regular pick-up:** Per the RFQ Contract Item #5, 5.2.5, Iron Mountain will pick up the records within a maximum of five (5) business days after written request by the agency.

2.2 RETRIEVAL WORKFLOW

Iron Mountain’s IMConnect provides WVOT with the ability to request records to be returned, as required, either by individual file, units of records, or entire containers of records. To simplify and accelerate the retrieval process, authorized State users will have access to Iron Mountain’s convenient, centralized portal, IMConnect, in order to submit service requests for all records stored in Iron Mountain facilities. WVOT can retrieve records by phone, fax or email 24/7/365. All record types are retrieved by records center staff and sent to the specified State location in accordance with their respective service level agreements. If WVOT determines the need for electronic delivery of a file, Iron Mountain can provide retrievals through our Image on Demand service provides a digitized/scanned retrieval solution for paper-based documentation with secure transfer of the output package to the destination system. Iron Mountain facilities contain private viewing areas that the State will have access to for file auditing or reviews if necessary.

Service Highlights:

- **Carton Banding.** To protect the contents while in transit, Iron Mountain double bands each carton scheduled for retrieval before it is placed in the Iron Mountain vehicle.
- **Retrieval Label Double Scan.** As a carton or package of files is pulled for retrieval, it is tagged with an additional retrieval label. This step prevents the wrong carton from being retrieved. The item is then brought to a staging area where all labels are scanned to verify that the correct item has been retrieved. This allows us to deliver greater order accuracy and improved performance.



- **Vehicle Validation.** We make sure every carton or package of files is loaded onto the right vehicle for optimum delivery efficiency. These are scanned as they are loaded, and the vehicle cannot leave until all requested cartons or packages have been accounted for.
- **Validation at Customer Site.** As part of the InControl process, drivers complete retrieval by scanning each carton at the customer’s location. This final check-and-balance step validates that the correct carton or package was delivered to the correct customer location.

Iron Mountain utilizes standard procedures, depicted in **Figure 2-2**, and trained personnel to accurately locate the records for retrieval with an auditable chain of custody.

Our retrieval workflow also employs a triple-check process. First, each carton or group of files pulled for retrieval is tagged with a label, which is scanned against the original to ensure order accuracy. We secure the contents of every carton with a security band, scan each carton again, and load it onto a designated vehicle. Finally, our driver scans the carton a third time at the State location and captures an electronic signature to verify chain of custody.

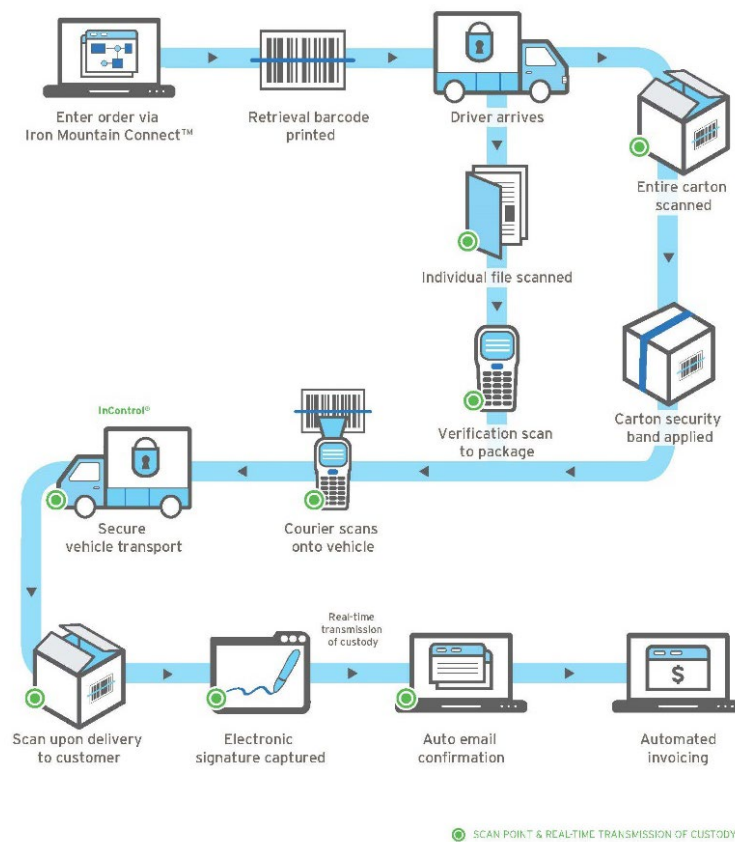


Figure 2-2. Record retrieval workflow.

In an instance when the State requires an additional pickup from a facility located within 50 miles of Iron Mountain’s facility, the following SLAs will be followed:



- **Regular Retrieval** Per the RFQ Contract Item #7, 5.2.7, Iron Mountain will retrieve any record in storage and hand deliver it to the authorized agency personnel within five (5) business days of written notification.
- **Rush Retrieval (Business Day):** Per the RFQ Contract Item #7, 5.2.7, Iron Mountain will 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.

3.0 RECORDS MANAGEMENT CHAIN OF CUSTODY

Iron Mountain will implement best in class chain-of-custody practices to mitigate any risk associated with the movement of State records to and from Iron Mountain's storage facilities. All State records requested and delivered need to follow a vigorous and secure chain-of-custody process to ensure information is protected and transitioned properly through the full lifecycle of the record. The WVOT program, and the importance of the records to be stored, demands an established and proven end-to-end model that provides full insight into records tracking and movement from initial receipt to retrieval / reference through final withdrawal.

The Iron Mountain Inventory Governance solution is built right into our normal chain of custody process. We keep chain of custody in mind at every step in our pickup, storage, and retrieval process. Our customers have options through the Iron Mountain Inventory Governance solution that can enhance chain of custody in order to take greater control over the inventory under our control. All State records will follow the same detailed process flow to ensure a complete chain-of-custody is instituted. This includes secure transportation, indexing, and tracking. These critical steps allow for controlled receiving and storing; and easy locating and re-filing of records upon the State's request, making access to information assured and reliable. **Figure 3-1** depicts Iron Mountain's standardized model for chain-of-custody best practices.

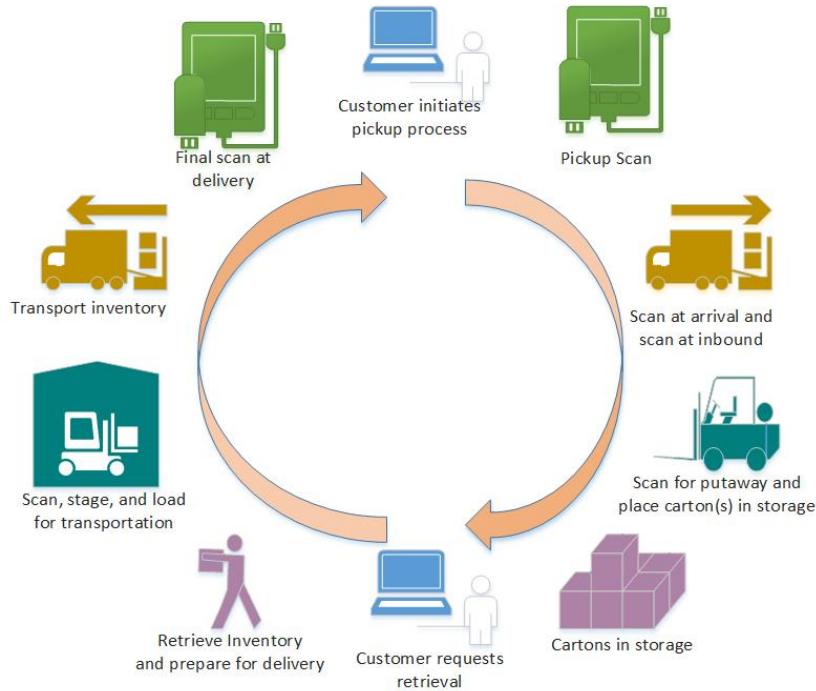


Figure 3-1. Records Management Chain of Custody.

Information security is dependent on a quality workflow process. Iron Mountain’s proven workflows combine standard operating procedures with multiple barcode scans to ensure that all records in our custody are accurately processed. We also regularly measure these quality control processes to drive continuous improvement.

Using Iron Mountain’s secure web portal, IMConnect, authorized users can easily schedule boxes for pickup. While entering order information and to facilitate future retrievals, our customers can enter descriptive information into IMConnect. From the moment Iron Mountain’s Transportation Specialist arrives at the State’s facility to pick up identified records and through their storage in our secure facilities, all records are protected. With our InControl system, our advanced transportation platform, all cartons and packages are scanned three times: at the State’s location, at Iron Mountain’s dock, and on their shelf location. Each scan is validated against the previous one to ensure accuracy and preserve a tight chain-of-custody. Once all records are safely stored, our customers receive email notification for orders placed via IMConnect.

To fully ensure chain-of-custody and protection in the records program, Iron Mountain utilizes industry best practices for the receipt and filing of records in storage locations.

- **Box Identifiers:** Assignment of a unique ID(s) that stay with a box for its lifecycle
- **Multiple Scanning Points:** Scanning of barcodes at multiple locations including pickup, facility loading dock, unique storage location, and for all further transactions that are performed, building an ongoing audit trail of activity
- **Temporary Holding Areas:** Holding of records in temporary space that is used prior to processing, filing, and retrieving



- Box Repair: Replacement of boxes that are damaged at the time of receipt
- Barcode Usage: Application of barcode labels to every box (and files when appropriate) to reduce data entry errors and validate accuracy as part of total quality processes

4.0 TRANSFER PROCESS

Iron Mountain is highly focused on the security of records and chain of custody while in transition, applying various protocols to protect State assets. **Figure 4-1** highlights the workflow necessary to transfer physical records from the State’s current locations to Iron Mountain and have the records available for retrieval five (5) business days after transfer from existing storage facilities. These critical steps will allow for easy receiving, storage, and locating of records; making access to information assured and reliable.



Figure 4-1. Box Transfer Workflow

To migrate materials, Iron Mountain will complete the following steps at the State’s facility:

- 1) Planning – Iron Mountain Project Manager (PM) works with the facility, and designated points of contact, to coordinate planning and provide training on transfer process.
- 2) Planning – Necessary supplies (e.g., labels, extra boxes) are delivered to the facility prior to the transfer commencement. Iron Mountain PM schedules pick-up and documents the order in our inventory tracking system.
- 3) Day 1 – On transfer day, asset-tracking labels are applied to each pallet that are part of the shipment and subsequently scanned by the Iron Mountain driver at the records center loading dock.
- 4) Day 1 – Pallets are placed onto an Iron Mountain vehicle. Once vehicle is fully loaded, materials are transported to the pre-determined Iron Mountain facility.
- 5) Day 2 – Upon receipt of materials at the Iron Mountain facility, a Records Specialist will scan the asset-tracking label at the receiving dock during the unloading process
- 6) Day 2 – Barcodes are added to each box and subsequently scanned to formally receive the box into the Iron Mountain facility. The SKP tracking system is immediately updated indicating that a box has been “scan-received.”
- 7) Day 3 – Metadata capture of information from boxes (on boxes with) is performed by Records Specialists, either manually or by scanning the legacy barcode.



- 8) Day 3 to Day 4 – Records Specialist will print unique “put-away” barcode labels, apply them to each processed box, and move boxes to the storage area.
- 9) Day 4 – Boxes are placed in their final storage location in the racking system.
- 10) Day 4 – Final scan of box is performed to log the unique location identifier in the tracking system.
- 11) Day 4 to Day 5 – Metadata captured from boxes is entered into the SKP system and matched against the box registry that the State is responsible for submitting.

At the conclusion of the transfer process, records and historical State box/file level information is available for viewing in IMConnect. Iron Mountain takes pride in providing industry-leading protection for all customers’ assets while in transit and storage. Iron Mountain’s Program Manager will provide the State with the status of transfers on a regular basis, including milestones, metrics, and issues.

5.0 SAFEKEEPERPLUS

Iron Mountain’s key tool to successfully provide inventory management begins with our proprietary inventory tracking system, SafeKeeperPLUS (SKP). The SafeKeeperPLUS Inventory Control module manages the physical movement of every carton and file in our record centers by tracking records throughout their life cycle. Ultimately, SafeKeeperPLUS’ quality control workflow reduces human error to a minimum and provides our customers assurances that their records are maintained correctly and securely.

As cartons are received at Iron Mountain, they are barcode-scanned into our system and given a unique identifier that will stay with that carton for its complete life cycle. New cartons are scanned at the dock, and again at the unique storage location that corresponds to the carton barcode. Once a carton is scanned into SafeKeeperPLUS, all further transactions are consequently recorded, building an ongoing audit trail of activity. SafeKeeperPLUS' provides redundant processing and barcode tracking to location results in system-driven inventory accuracy.

Barcodes are scanned as each item is shelved. Iron Mountain is one of the few records management companies to scan each carton into a location. This extra step confirms not only that cartons have been received at our loading dock, but also that they have been accurately stored in the storage system. The “scan-to-shelf” process enables Iron Mountain to retrieve cartons promptly when our customers request them, while offering the relative anonymity of all records while in the facility.



Figure 5-1. Iron Mountain records management system ensures quality control to provide our customers with the assurance their records are stored safely.

Barcode technology is used to track records throughout their lifecycle.

Our record center operations leverage barcode technology to reduce data entry errors and to validate accuracy as part of our total quality processes.

Barcodes are used during each service transaction as follows:

Carton ID barcode — Each carton is identified with a unique SafeKeeperPLUS barcode number to allow Iron Mountain to track carton activity by scanning the ID barcode. Customers may also use SafeKeeperPLUS' carton ID barcode in conjunction with a second identifier, which we refer to as a customer box number, to accommodate internal numbering systems that users may wish to preserve.

Location ID barcode — All storage locations are barcoded with a unique number cross-referenced in SafeKeeperPLUS to a full address indicating capacity, carton size and client ownership. This extra step confirms that cartons have been received at our loading dock and accurately stored in the storage system which can guarantee that records are correctly located and available for efficient retrieval.

Retrieval label barcode — All items (cartons or files) retrieved from Iron Mountain are barcoded with retrieval labels. These labels distinguish returning items (refiles) from new storage items (receiving and entry); they also specify item requestor and mail codes to assist with delivery directly to the requestor. When items are refilled, Iron Mountain personnel scan the retrieval labels along with the refile labels and location IDs to ensure accurate refile. All retrievals are scanned prior to being retrieved to prevent incorrect cartons are retrieved and scanned again upon return to ensure they have been returned to the correct records center.

"File out" card barcode — Two barcode labels are printed for file retrievals. One label is affixed to the file and the other to a "file out" card. File out cards are placed inside home cartons when files are retrieved. When a file is refilled, the correct file out card must be removed and scanned to confirm accurate refile.

6.0 IMCONNECT

Iron Mountain Connect (IMConnect) allows our customers to view and track their records online. Iron Mountain developed an internal inventory tracking system, SafeKeeperPlus (SKP), which manages the physical movement of our customers records stored within an Iron Mountain facility. The Inventory Control module within SKP feeds directly in to the customer facing platform, IMConnect. This is accomplished through built-in quality control checks utilizing barcode technology and redundant processing at each step in the workflow. Highlights of IMConnect’s portal features are outlined in **Figure 6-1**.

Online Portal	Features and Capabilities	
IMConnect - Portal for paper records	<ul style="list-style-type: none"> • Query, search, locate <ul style="list-style-type: none"> ○ Easily locate individual records, set of records, or entire cartons ○ Enterprise-wide view or program-level view of records • Access to Iron Mountain services <ul style="list-style-type: none"> ○ Identify necessary records ○ Provide litigation support ○ Perform records analysis • Electronic retrievals • Report generation • View carton and file transaction history 	<ul style="list-style-type: none"> • Inventory control processes <ul style="list-style-type: none"> ○ Custom data entry fields ○ Custom required fields to capture critical information • Custom data validation for key fields Retention Management <ul style="list-style-type: none"> ○ Add detailed retention schedules, policies, and procedures for each Components ○ Manage and monitor Component and program level retention programs

Figure 6-1. Iron Mountain Online Portal Features

The State can use the online access capabilities of the IMConnect system to implement a compliant records management program. The IMConnect Record Center will facilitate the location of cartons or files quickly and easily, inventory management, and a customized search engine. Basic searches within the Record Center dashboard are by keyword; advanced searches can filter by record type, status, dates and descriptions. State personnel can search across the entire organization's records to get an enterprise-wide view of all relevant records and transactions. IMConnect will provide the State with a powerful research tool that enhances the value of archived information. Records can be identified by using structured searches based on: carton or barcode identifier; internal numbering system; keyword search to find groups of records with specified words or partial words in description fields; date range or alphanumeric range qualifiers; records classification codes.

The IMConnect system has a robust search engine built to provide our clients a research and analysis tool to manage record inventories. IMConnect will allow the State to

- Identify necessary records quickly
- Provide litigation support
- Perform record analysis



Iron Mountain Connect™ puts customers in total control of their records and information management program. Users can search through offsite inventory, locate what's required to satisfy an internal or external request, and arrange for it to be quickly delivered to a desired location – no matter where or when.

Iron Mountain Connect Benefits:

- ✓ **Quickly access** and manage records right from your desktop
- ✓ **Submit retrieval requests** no matter the day, time or delivery location
- ✓ **Streamline retention policy** to ensure compliance
- ✓ **Gain valuable insights** into the health of records management programs
- ✓ **Allow authorized users** to self serve

At-A-Glance

451K
active users

2.5M
online orders

Figure 6-2. IMConnect provides our customers the ability to maintain complete control and visibility of their records in our care.

The IMConnect Record Center data entry forms can be customized to help ensure the quality of the State data indexing. Customization options include data entry fields can be re-sequenced based on what is most important to your business; required fields can be set to make sure critical information is captured; data validation for key fields can be created based on your requirements. Other quality controls include industry-specific data entry screens and pre-populated data fields. The industry-specific screens tailored for the State include accounting file, medical file, legal file and two insurance file formats. Pre-populated fields with common values can reduce errors and streamline data entry.

IMConnect provides records managers and users serving multiple departments the ability to obtain a consolidated view of records information, while allowing departments to operate independently. Users may:

- View carton and file transaction history
- Check the status of cartons and files
- Browse retention information and retention hold codes
- Manage and monitor corporate retention programs
- Access summaries or recent legislation and regulatory resources affecting records management
- Request reports online

6.1 RETENTION MANAGEMENT

Our powerful web-based tool set can help our customers transform their records management programs into compliance programs. With IMConnect our customers can post company-wide retention schedules, policies, and procedures in a central location where they are easily referenced to help classify records consistently. Posting the organization's schedule within IMConnect puts it in a standard format with intuitive look-up capabilities which provides employees the ability to find record class codes by business function, record class, record type, or by keyword search.



Browsing and search results provide expedited access to official retention periods, legal group codes, retention events and record type examples. The powerful look-up capability makes it easier for employees to determine how to classify records properly. Inventory control processes ensure that users apply records codes to inventory in accordance with the organization's retention schedules.

The Record Center provides a systematic way to issue, review, and release litigation holds for records required for pending legal actions or administrative proceedings. Hold codes can be applied on individual boxes, departments, records series, or on whole accounts. This functionality provides an audit trail for records in contention and avoids indefensible anecdotal scenarios.

The IMConnect Retention Schedule supports a wide range of retention schedules and provides flexibility in schedule periods with support for schedules based on fixed date, event driven, calculated-date or alternative, ad hoc date. If the State does not have a corporate-wide retention schedule, Iron Mountain's Consulting Services will assist with the design of a retention schedule based on credible legal research.

6.2 ELECTRONIC RETRIEVALS

Retrieving records is now as simple as a click of the mouse with the IMConnect system. Once a customer has located the cartons or files to be retrieved, IMConnect sends the request directly to the records storage location. Retrieval labels are automatically generated, and records are sent to customers in accordance with their respective service level agreements. Iron Mountain automates the retrieval process by allowing users to specify items requested for retrieval by:

- Entering carton barcodes or internal reference numbers if the customer knows which cartons are needed
- Selecting the retrieval option after you have located a record through the user-friendly search engine

6.3 PRODUCE REPORTS

Accountability can be accomplished only with a corporate-wide commitment that starts at the top of the organization. However, our records management customer workspace can support management by providing the information necessary to effectively monitor performance and adherence to policy. In conjunction with the flexible sorting capabilities provided by IMConnect, customers can produce on demand financial, activity, retention and inventory reports. Reports are available to monitor and measure:

- Participation and usage.
- Inventory health and consistency.
- Retention management process.
- Records management costs.

Inventory Reports

RC INVENTORY Report Type

Carton Date Summary Displays total cartons for destruction review, event date, create date, to/from date, and year by customer ID.	Customer	Customer	Year	From Date	To Date	Create Date	Event Date	Receipt Date	Receipt Date	Destruction Review																											
	CUST1	CA001 INC	2000	16	12	3	3	30	18	6																											
	CUST1	CA001 INC	2001	32	19	6	7	101	93	5																											
Carton Descriptive Details Displays total percentage of cartons with a valid division/department, record code, destruction indicator, hold code, etc., for either a single or all customer IDs.	CUST1	CA001 INC	OWNERSHI	Cartons <thi< td=""> <td>1</td> <td>0.60%</td> <td>Cartons<thi< td=""> <td>1</td> <td>0.60%</td> <td>Cartons<thi< td=""> <td>90</td> <td>51.10%</td> <td>Cartons<thi< td=""> <td>90</td> <td>51.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>80</td> <td>45.50%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<></td></thi<>	1	0.60%	Cartons <thi< td=""> <td>1</td> <td>0.60%</td> <td>Cartons<thi< td=""> <td>90</td> <td>51.10%</td> <td>Cartons<thi< td=""> <td>90</td> <td>51.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>80</td> <td>45.50%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<>	1	0.60%	Cartons <thi< td=""> <td>90</td> <td>51.10%</td> <td>Cartons<thi< td=""> <td>90</td> <td>51.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>80</td> <td>45.50%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<>	90	51.10%	Cartons <thi< td=""> <td>90</td> <td>51.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>80</td> <td>45.50%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<>	90	51.10%	CONTENTS	Cartons <thi< td=""> <td>80</td> <td>45.50%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<>	80	45.50%	CONTENTS	Alpha Front																
	CUST2	CA002 INC	OWNERSHI	Cartons <thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<></td></thi<>	0	0.00%	Cartons <thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<>	0	0.00%	Cartons <thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<>	2	11.10%	Cartons <thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<>	2	11.10%	CONTENTS	Cartons <thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<>	1	5.60%	CONTENTS	Alpha Front																
	CUST3	CA003 INC	OWNERSHI	Cartons <thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<></td></thi<>	0	0.00%	Cartons <thi< td=""> <td>0</td> <td>0.00%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<>	0	0.00%	Cartons <thi< td=""> <td>2</td> <td>11.10%</td> <td>Cartons<thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<>	2	11.10%	Cartons <thi< td=""> <td>2</td> <td>11.10%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<>	2	11.10%	CONTENTS	Cartons <thi< td=""> <td>1</td> <td>5.60%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<>	1	5.60%	CONTENTS	Alpha Front																
All OWNERSHI Cartons <thi< td=""> <td>825</td> <td>37.30%</td> <td>Cartons<thi< td=""> <td>825</td> <td>37.30%</td> <td>Cartons<thi< td=""> <td>1,122</td> <td>50.70%</td> <td>Cartons<thi< td=""> <td>1,117</td> <td>50.50%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>893</td> <td>40.40%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<></td></thi<>																					825	37.30%	Cartons <thi< td=""> <td>825</td> <td>37.30%</td> <td>Cartons<thi< td=""> <td>1,122</td> <td>50.70%</td> <td>Cartons<thi< td=""> <td>1,117</td> <td>50.50%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>893</td> <td>40.40%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<></td></thi<>	825	37.30%	Cartons <thi< td=""> <td>1,122</td> <td>50.70%</td> <td>Cartons<thi< td=""> <td>1,117</td> <td>50.50%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>893</td> <td>40.40%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<></td></thi<>	1,122	50.70%	Cartons <thi< td=""> <td>1,117</td> <td>50.50%</td> <td>CONTENTS</td> <td>Cartons<thi< td=""> <td>893</td> <td>40.40%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<></td></thi<>	1,117	50.50%	CONTENTS	Cartons <thi< td=""> <td>893</td> <td>40.40%</td> <td>CONTENTS</td> <td>Alpha Front</td> </thi<>	893	40.40%	CONTENTS	Alpha Front

RC INVENTORY Report Type continued >

Activity Reports

RC ACTIVITY Report Type

Account List Displays list of accounts, contact name, phone number, whether the department ID is validated, record code parameter, type of pickup validation, total files, total cartons, and total cubic footage.	Customer ID	Customer	Contact Name	Phone	Validate De	Record Coc	Pickup Vali	File Quanti	Carton Qua	Cub Foot						
	CUST1	CA001 INC	John Smith	(800) 000-0000	YES		1	IM FACILITY	0	123	147.6					
	CUST2	CA002 INC	Mary Smith	(866) 000-0000	NO		0	NO VALIDA	0	3	3.6					
	CUST3	CA003 INC	Pat Smith	(877) 000-0000	YES		2	IM FACILITY	0	1,963	3,053.07					
	CUST4	CA004 INC	Brian Scott	(888) 000-0000	YES		1	IM FACILITY	0	123	147.6					
	CUST5	CA005 INC	Dan Mahor	(899) 000-0000	NO		0	NO VALIDA	0	3	3.6					
Activity by Location Displays activity type (retrieval, pickup, products, permanent withdrawals, onsite shredding, offsite shredding, XOD, IPD, and other orders) by address for a customer ID.	Customer ID	Address 1	Address 2	Address 3	City, State,	Address Co	Retrieval C	Pickup Orc	Product Or	Permanent	Onsite Shr	Offsite Shr	XOD Order	IOD Orders	Other Ord	Total Orde
	CUST1	1000 Camp Building 1	Suite 400		COLLEGEVI	123456	3	1	1	1	1	1	1	1	1	11
	CUST1	2000 Camp Building 2	Suite 100		COLLEGEVI	123457	45	5	5	5	5	5	5	5	5	85
	CUST1	3000 Camp Building 3	Suite 500		COLLEGEVI	123458	0	1	1	1	1	1	1	1	1	8
	CUST1	10 Campus Building 4	Suite 500		COLLEGEVI	123459	0	0	0	0	0	0	0	0	0	0
	CUST1	1001 Camp Building 5	Suite 40		COLLEGEVI	123410	1	0	0	0	0	0	0	0	0	1
	CUST1	1000 Colle Building 6	Suite 321		BOSTON, M	123411	4	0	0	0	0	0	0	0	0	4

Financial Reports

RC FINANCIAL Report Type

Cost and Activity Report Displays extended amount, billing code with description, and quantity by cost and activity.	Product	Quantity	Billing Cod	Billing Desc	Extended Am																	
	PRODUCT	1,548	4255	#2000 STA	1,935.00																	
	PRODUCT	150	4256	#2000 STA	402																	
	PRODUCT	320	4257	#2000 STA	475.2																	
Invoice Download Report Displays order, service, charge code, quantity/unit, amount, taxes, storage date, and invoice number for a customer, including by division and department.	Customer ID	Division ID	Division No	Department	Department Invoice No	Invoice Date	Order No	Order Date	Charge Code	Unit/Quant	Charge per	Amount	Requested	Contact No	PO Number	Service Desc	City	State	Zip			
	CUST1	1111	Headquar	ADMN	ADMNSTR	BH48604	8/31/10	1,376-08	8/30/10	890	32.4	3	32.4	Brian@Iron	John Smith	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1111	Headquar	SALES	SALES	BH48604	8/31/10	1,376-08	8/30/10	890	4.8	1	4.8	Brian@Iron	Mary Smith	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1111	Headquar	CSPRVCE	CUSTOMER	BH48605	8/31/10	1,376-08	8/30/10	890	1.2	1	1.2	Brian@Iron	Pat Smith	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1111	Headquar	SALES	SALES	BH48606	8/31/10	1,851-08	8/30/10	890	1.2	1	1.2	Brian@Iron	Brian Scott	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1112	Boston	ADMN	ADMNSTR	BH48607	8/31/10	1,851-08	8/30/10	890	13.2	1	13.2	Brian@Iron	Dan Mahor	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1112	Boston	CSPRVCE	CUSTOMER	BH48608	8/31/10	1,851-08	8/30/10	890	20.8	1	20.8	Brian@Iron	Tommy King	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1112	Boston	HR	HUMAN RE	BH48608	8/31/10	1,851-08	8/30/10	890	1.2	1	1.2	Brian@Iron	Alphonso V	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1112	Boston	FIELD	FIELD SUPP	BH48609	8/31/10	1,761-08	8/30/10	890	1.2	1	1.2	Brian@Iron	Richard W	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1113	Warehouse	CSPRVCE	CUSTOMER	BH48610	8/31/10	2,748-08	8/30/10	890	1	1	1	Brian@Iron	Randy Mac	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942
	CUST1	1113	Warehouse	FIELD	FIELD SUPP	BH48610	8/31/10	2,748-08	8/30/10	890	10.8	1	10.8	Brian@Iron	Mat Scott	8103	STORAGE	1.5	6.33	1/3/10	1000 CAMP COLLEGEVI PA	1942

6.4 CONTROL AND MANAGE

Because IMConnect resides on a centralized dedicated server, users can navigate their databases without fear of data corruption that can occur with location-specific databases. IMConnect consolidates inventory data from multiple locations to provide customers with a complete database of records stored. This approach provides users with robust query and reporting capabilities, while enabling them to manage records at several locations as if they were in a single location. IMConnect also features security driven by individual logins and passwords. These checks and balances ensure confidentiality and database integrity.

6.5 ADDITIONAL FEATURES

IMConnect provides records managers and users serving multiple departments to obtain a consolidated view of records information, while allowing departments to operate independently. Users may:



- View carton and file transaction history
- Check the status of cartons and files
- Browse retention information and retention hold codes
- Manage and monitor corporate retention programs
- Access summaries or recent legislation and regulatory resources affecting records management
- Request reports online

7.0 RECORD MANAGEMENT FACILITIES

Creating and maintaining safe, secure facilities for the storage of customer records forms the cornerstone of our records management philosophy. Accordingly, Iron Mountain sets and maintains state-of-the-art industry standards for our record centers. We have dedicated considerable resources to ensure our facilities are appropriate, safe, and secure for the storage of our customers informational records. All Iron Mountain record centers comply with established company standards and with all appropriate building, fire and safety, electrical, mechanical, and other regulatory codes.

Iron Mountain's specifications for record storage buildings include:

- Utilization of smoke and/or heat detection systems designed in accordance with NFPA72, "Standards for Fire Alarm System," and NFPA 101, "System Smoke Detection," to provide an early warning during the incipient stage of fire development
- Fire Suppression systems, including in-rack or in-aisle and ceiling sprinklers
- All detection, suppression, and alarm systems are monitored around the clock, and are routinely tested

7.1 FACILITY SECURITY

Iron Mountain employs a professional Global Security Services organization which is responsible for information security and incident management. Our security measures include:

- A comprehensive personnel screening process that includes a thorough background investigation and pre-employment drug screening
- Stringent physical security measures tailored to the needs of specific location and environment. These measures include: positive access control and intrusion detection systems, alarms, and CCTV
- Industry-leading asset protection policy and procedures with continuous employee training to ensure strict adherence to requirements
- On-going security integrity audits to monitor compliance and ensure our security plans are current, viable, and reflect industry best practices

Iron Mountain utilizes both electronic access controls and personal recognition as methodologies for controlling access to and ensuring the security of our facilities. We require that all facilities maintain a



system of positive employee and visitor identification and logging. All personnel are required to wear identification badges while on premises, and all badges are color coded to indicate access authorization levels.

All of our facilities are equipped with intrusion detection systems that are monitored by a central station for after-hours control. Alarm technology may include passive infrared motion detectors, dual technology glass break detection, photo-beam detectors, sound-activated microphones, and magnetic door contacts. Alarm systems are designed to accommodate specific site requirements.

Finally, Iron Mountain utilizes education and awareness-training tools to ensure that all employees are aware of the criticality of controlling access to our buildings.

A secure, tailored record storage environment is the foundation of our commitment to our customers; it is the basis upon which our customers entrust their records to Iron Mountain. Iron Mountain leads the industry in quality record center construction, safety, and security.

Fire Suppression

All Iron Mountain storage systems are designed in accordance with the National Fire Protection Association (NFPA) standards. The largest and most reputable storage systems manufacturers in the US manufacture and install our storage systems. Although systems may vary to accommodate building configurations, most build-to-suit record centers feature high-bay storage with catwalk access systems. A ten-foot-wide main aisle runs the length of each building with intersecting service aisles of 30 to 36 inches. Most sections are 48 inches deep to accommodate standard letter/legal 1.2 cubic foot cartons three deep. This same shelving depth holds letter and legal transfile cartons and 24-inch deep check size cartons in a two carton deep fashion, thus providing maximum flexibility for customer storage. All record cartons/boxes are stored at least four (4) inches from the floor for protection from moisture.

Adherence to NFPA applicable state and local codes is a prerequisite when we open a record center and when we inspect each new section of a storage system. Iron Mountain's Corporate Facilities Engineering department prepares full site drawings in conjunction with the storage system supplier and Global Fire Protection Consulting (Fire Protection Engineers and consultants). All drawings are submitted to local officials when permits are required.

Iron Mountain meets the qualifications and the standards for NFPA 2513 for our facilities and those records are on file with the authority having jurisdiction over those facilities and upon award, Iron Mountain can provide the information requested.

Confidentiality of Records Stored

Iron Mountain takes extensive precautions to protect the confidentiality of our customers' records and ensure that unauthorized parties cannot access records. Access to confidential information is governed by a set of procedures, some of which are Iron Mountain's standard operating procedures, and others that may be determined by regulatory agencies or the customer.

- Levels of password protection deemed appropriate for stored material.
- Deliveries limited to addresses registered in Iron Mountain's computerized customer master file.
- Unauthorized facility access is prevented by electronic security systems monitored by a central station, physical barriers, and administrative controls.



- Retrievals may be shrink-wrapped or sealed to protect against tampering while en route.
- Employees are trained and sign an acknowledgement of confidentiality requirements.
- Iron Mountain maintains the highest level of customer confidentiality in the industry.

Centralized Station Monitoring Alarm System

- Glass break sensors for all windows
- Motion detectors are used throughout the facility
- Third-party integrity auditors to monitor standard compliance

Employee Background Checks & Training

- Background Investigations are conducted for all employees prior to beginning work; drug testing is also required for U.S. employees
- Privacy and Security training is required for all employees prior to beginning work and annually thereafter
- In response to RFQ Section, “Qualifications,” number 4.3, please find included in our response a copy of Iron Mountain’s Background Investigation Policy (titled “Iron Mountain BI Program Overview US”).

Keycard Entry

- Access to all keycard entryways is strictly controlled; logs are maintained and reviewed.
- Iron Mountain conducts regular user audits within the card access system.

Facility Maintenance

We have a 24x7, robust facility maintenance program that meets all local and national legislative and statutory requirements, and ensures that we appropriately maintain all critical building systems to reduce the risk of failure and downtime.

Additionally, we have outsourced partners who ensure our buildings are clean, free of pests and safe to operate. We track the performance of these partners using key performance indicators, and our over 100 technicians ensure that our systems are well maintained. We also have an energy efficiency program goal to reduce our greenhouse gas emissions by 25% by 2025 and increase our usage of renewable energy sources.

Records storage, by and large, is a clean industry that generates no toxic wastes and virtually no noise, odor, bacterial or other pollution. We clean our record centers daily as part of our standard operating procedures. We contract with various local companies to prevent pests. Record center maintenance, including cleanliness, is managed at the district level following strict procedures. In addition, managers at the regional, area, divisional, and corporate level who travel to our field locations routinely check cleanliness as part of a field audit program.

Material Handling

Iron Mountain mitigates the risk of exposure and damage to all records in our storage facilities by applying strict standards regarding structural integrity in the design of our records centers and storage



systems, and through employee training and strict adherence to procedures governing the transportation, handling, and storage of customer materials. At Iron Mountain we believe training is the single most important protective measure against material handling equipment damage. We require employees who operate equipment within a record center to be trained and certified in its operation. Our storage system design has built-in protections against carton damage and are interconnected throughout the record center, providing extra structural integrity.

8.0 VEHICLE TECHNOLOGY AND SECURITY

The requirements to provide our customers with a reliable, secure transportation solution to transfer existing storage holdings, accommodate regular pick-ups, and support retrieval requests has driven Iron Mountain to develop a fleet of vehicles outfitted with capable operational controls. Iron Mountain maintains one of the largest commercial fleets in the world, performing 15 million trips per year, capable of providing more than 3,600 transportation vehicles equipped to handle all aspects of its information management program. Iron Mountain's Transportation System provides industry leading security, chain of custody visibility, and consistent operational controls to protect State records in transit.

8.1 INCONTROL TRANSPORTATION SYSTEM

In order to meet our stringent security needs, Iron Mountain has all vehicles specifically customized to meet our customer's security and usage requirements. Our vehicle specifications were carefully developed and selected to support our material handling mission while putting an emphasis on equipment reliability, operator route efficiency, employee safety, and cargo security. To ensure the safety and security of our customer's material in transit we created Iron Mountain's patented InControl Transportation System.

InControl will provide the State with industry leading security, real time tracking, chain-of-custody visibility, and standardized operational controls to protect all State material while in transit from the State site to our facility in Charleston, WV. The InControl transportation process utilizes real-time wireless scanning technology to validate pickup and delivery transactions which provides our customers the assurance that their records have arrived to the storage facility within the designated timeframe.

Patented Vehicle Process Controls

Iron Mountain's patented security controls are designed to mitigate sources of transportation workflow errors. This combination of security controls is exclusive to the Iron Mountain transportation platform includes:

- *Compartmentalized cargo areas* are protected by patented locking mechanisms on all vehicles. In all of our vehicles, only one (1) door can be opened at a time which ensures the driver cannot inadvertently leave doors open without receiving a warning.
- *Driver proximity controls* utilize RF key fobs which trigger an audible vehicle alarm should the driver and/or fob leave the proximity of the vehicle with an unsecured cargo area.
- *Dual key ignition immobilizer* requires two (2) keys to be inserted into the ignition to start the vehicle. Both keys are designed to prevent vehicle theft while one (1) of the keys is also



designed to prevent breaches or errors in the vehicle cargo area by securing, locking, and activating the cargo alarming system prior to vehicle ignition.

- *In Motion Security Detection System* prevents information loss while the vehicle is in motion. The operator warning alarm is triggered if any cargo-area locking or security system is improperly opened or fails while the vehicle is in motion.
- *Six-Sided Interior Cargo Padding* offers additional protection for media, tapes and records if an unexpected vehicle disturbance occurs.

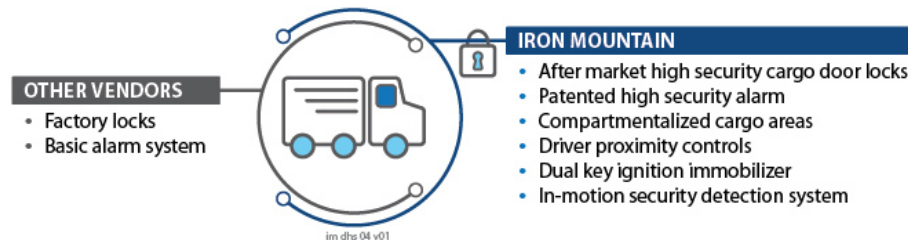


Figure 8-1: Iron Mountain Transportation Security Controls

Standard operating procedures are created by our delivery teams in order to support clearly defined processes that are designed to meet the need for consistent and secure information transport through error reduction and process integrity. Our drivers are trained to follow careful procedures during the loading and transport of all customer material to prevent exposure to risk at any Iron Mountain location. We have instituted a strict loading and unloading process that is supervised by an Iron Mountain employee and ensures vehicle and facility doors are only unlocked and opened during the loading and unloading process.

8.2 FLEET TELEMATICS

Every Iron Mountain vehicle is marked and branded, installed with GPS systems and Advanced Fleet Telematics for vehicle whereabouts and driver’s safety tracking. Advanced Fleet Telematics is used to project accurate estimated time-of-arrival information. This technology delivers a variety of benefits to our customers, our drivers, and our company. Our critical event messaging system enhances driver awareness by notifying them of unsafe driving behavior. Through this system, Iron Mountain also has visibility into these behaviors which allows us coaching opportunities to reduce the risk of accidents and the potential cost associated with them. This system creates a historical record of all vehicle activity during a transport which provides an improved chain of custody for our customers. Our dispatchers and customer care representatives have visibility into the location of drivers which enables them the ability to provide our customers with an accurate estimate of time of arrival or, if necessary, the ability to send a driver any help they may need. The turn-by-turn navigation system ensures our drivers don’t get lost looking for a stop or inadvertently travel on roads not designed for commercial use.

8.3 DRIVER SAFETY

Employees hired by Iron Mountain to operate a motor vehicle must have the basic skills and credentials necessary to perform this function. Our Management team is responsible for ensuring that our couriers



demonstrate the knowledge and skill for operating the vehicle safely in a normal business environment. For any driver in our fleet, a Safe Driving Evaluation is completed prior to putting new couriers on the road; in the event of a route or equipment change; annually to evaluate a courier's performance; and as refresher training for any courier involved in a collision. The safety of our employees, our vehicles, and our customer's material is extremely important to Iron Mountain and we have specific processes and procedures in place to ensure safety remains a priority. All Iron Mountain drivers and carriers wear Iron Mountain branded uniforms and display company issued badges at all times.

9.0 OFF-SITE SHREDDING WORKFLOW

Iron Mountain understands the State has a requirement to protect against privacy information theft and breaches, which provides the State assurance that all documents and media are destroyed safely and securely. We have designed our operating procedures based upon many years of experience, enabling us to provide our customers with the most reliable, consistent, and secure service. Fifty-six percent of individuals surveyed believe that more than half of their organizations' sensitive or confidential information is contained within paper documents. With Iron Mountain's Secure Shredding services, the State will be able to safely, and cost-effectively, destroy unnecessary paper-based documents while overcoming information privacy challenges.

Though most customers understand how important information security is to promoting the well-being of its employees and customers, all too often there is one critical point where security is an afterthought: information destruction. If the State lacks the proper information destruction controls, the State may run the risk of compromising the security of sensitive information, adding to the administrative burden and potentially increasing budgetary responsibility. Without proper insight into the current state of an information destruction program, it can be impossible to effectively manage a secure, information destruction program. Additionally, if the State is unable to provide accurate documentation to identify when specific information was destroyed, there could be penalties associated with failed audits and compliance reviews.

Iron Mountain's Secure Shredding will provide the State with the necessary resources and proven expertise to create, implement, and monitor a comprehensive, compliant, cost-effective, and sustainable information destruction program. Leveraging Iron Mountain's destruction best practices the State will be able to:

- Maintain a consistent, auditable chain of custody from pickup to destruction
- Stay current and compliant in an ever-changing regulatory climate
- Retain complete visibility via reporting and online monitoring tools that help you keep control over your program, services, and costs

Benefits of Iron Mountain's Offsite shredding program include:

- **Secure Chain of Custody:** Offsite shredding offers a rigorous chain of custody, secure transport supported by Babaco lock systems, and certificate of destruction for your records. The volume of paper in your shred bin is captured at the time of service, and scan points throughout the journey ensure we know where your sensitive information is at all times



- Safety: Offsite customers benefit from a reduced risk of equipment failure as well as reduced exposure to the possibility of fire or other weather related issues
- Cost-Efficiency: Offsite service is a more cost effective destruction methodology and Iron Mountain can often save new customers up to 30% from their previous vendor’s on-site program
- Broad Service Coverage: With more trucks equipped to handle transport to a variety of locations, Iron Mountain’s offsite service provides a more extended coverage model than a typical onsite service would cover
- Affordable Pricing and Container Options: Iron Mountain offers low-cost, per-container pricing and, with offsite service, customers with nonstandard needs can benefit from additional container options.

9.1 DEFINED WORKFLOW PROCESS

From the moment our driver arrives to pick up the materials at the identified the State locations to final destruction at a secure shredding plant, the State information will be protected. With InControl, the State shredding containers are scanned at the designated location, where key service information, such as barcode ID and container volume are captured. This information will become part of the State verifiable audit trail.

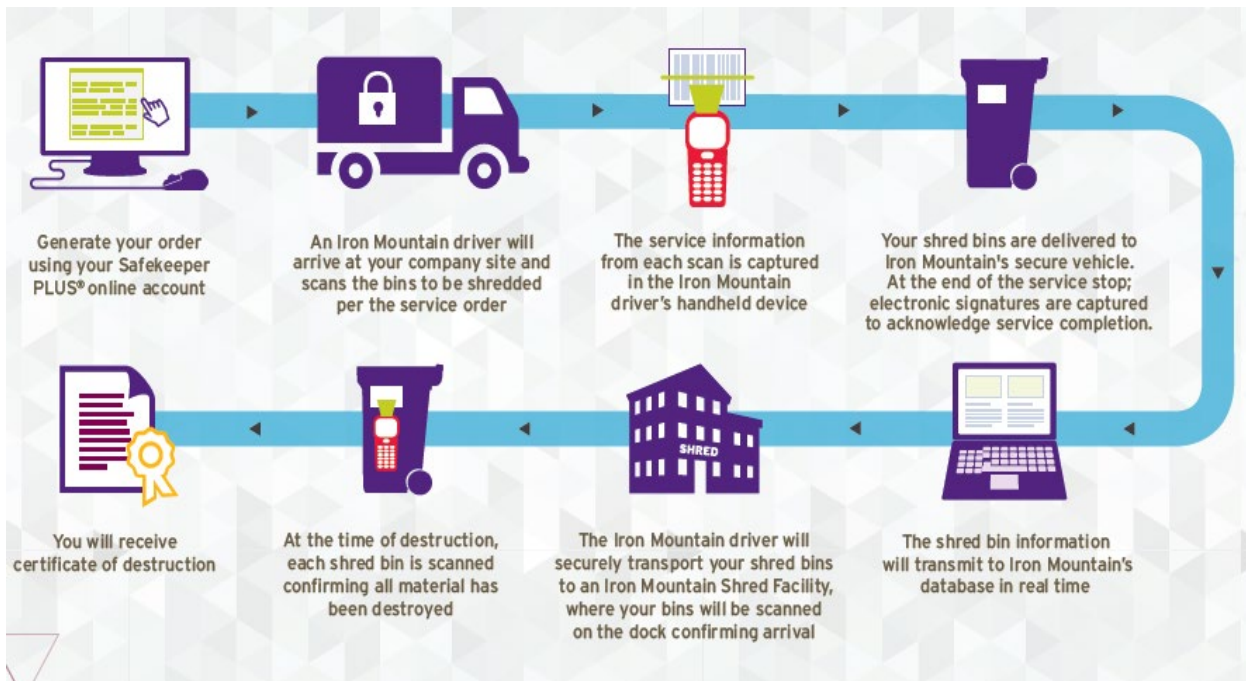


Figure 9-1. Offsite Document Destruction Process.

Once all materials have been securely destroyed, Iron Mountain is proud to safely and securely recycle all pulverized shredding output. This destruction process provides benefits to both the security of your business and to the global environment by reducing pollution, preserving landfill space and likewise saving trees, water, and energy resources. Recycling results are calculated based on the shredding orders serviced on customer account(s) using average container weight calculations.

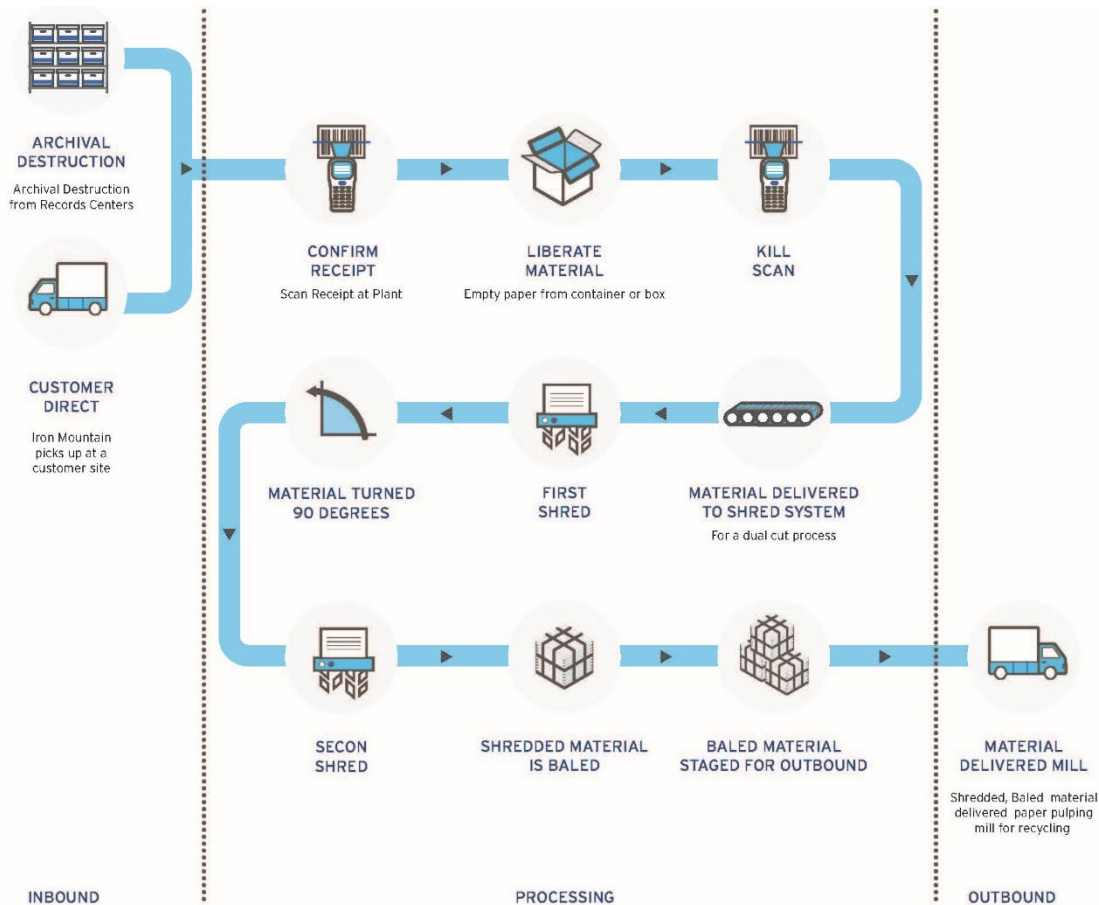


Figure 9-2. Secure Shred Paper Processing.

The State can also expect a Certificate of Destruction available through our secure web-portal, Iron Mountain Connect™, and included on the State’s monthly invoice. IMConnect is Iron Mountain’s online customer hub that helps manage information. As an Iron Mountain customer, IMConnect can be used to place orders, run activity reports, and access inventory data — anytime from anywhere.

Through our secure online hub, the State can easily link to the features you need to manage your offsite records and shred programs as well as your assets in escrow. You can also access value-added tools and resources like the Global Risk and Compliance Service to assess risks within your records program, access Records Management education, and information on the latest trends in information management and assist in setting up legally compliant automated retention schedules.



9.2 IN CONTROL® SHRED USAGE REPORT

While establishing a secure shredding program is a crucial step toward achieving compliance, simply implementing the program is not enough. Regular program monitoring is critical to minimizing business risk, ensuring ongoing compliance and managing program costs.

The InControl Shred Usage Report gives the State the visibility you need to evaluate the many variables that can impact your program: container volume, number of containers, service frequency, awareness and compliance of employees, and much more.

Iron Mountain is committed to helping the State manage secure shredding program from initial program design and implementation through ongoing management and audit. Our InControl® Shred Usage Report is a valuable tool that will provide the insight and analysis needed to better manage and monitor all aspects of secure shredding program.

9.3 SHREDDING SPECIFICATIONS

Iron Mountain's NAID-certified paper destruction process utilizes equipment designed to meet currently established industry standards. These standards require equipment with cutting blades calibrated to the following OEM specifications for paper destruction:

- Dual-cut shred system with the first blades set at 2-inches and the second blades set at 5/8-inch

Iron Mountain's shredding equipment has the capability to destroy the following types of material, which can be deposited in to the provided Iron Mountain shredding containers:

- Clean paper, any color and any size
- Blueprints
- Newspapers
- Magazines
- Brochures
- Mail (including window envelopes)
- Photographs
- File folders, any color
- No need to remove staples, paper clips, rubber bands or small binders

9.3.1 Destruction Compliance

Iron Mountain's offsite shredding capabilities perform cross cut or pierce and tear with a width (max) of 3/4 inch and length (max) of 2.5 inches. The typical average cut is 1 ½ x 5/8 which meet/exceeds the State's requirement.

Our Secure Shredding service is AAA Certified by the National Association for Information Destruction, Inc. (NAID). Iron Mountain is the largest shredding vendor to achieve NAID certification, and we are proud to have taken a leadership role in the development of NAID's standards, which focus on operational workflows and security.

10.0 APPENDIX

10.1 COMPLIANCE WITH RFQ SPECIFICATIONS

10.1.1 Section 4 Qualifications

Requirement	Iron Mountain Compliance
<p>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.</p>	<p>Iron Mountain is in compliance.</p> <p>Iron Mountain’s workflows and facilities incorporate the latest in technology, best practices, and regulatory compliance. We protect all of your data as if it were our own, meeting and often exceeding HIPAA standards. That’s why Iron Mountain is the Public Sector partner of choice for data protection and compliant media management.</p> <p>With more than 60 years of information management experience, over 90 dedicated facilities, and 3400 highly secure vehicles, Iron Mountain has the resources and expertise necessary to support your compliant media management program. We have invested years in developing a proven, comprehensive approach to compliant media backup and archiving. And, we continue to invest in keeping our systems fully up to date with the latest HIPAA regulations.</p>
<p>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.</p>	<p>Iron Mountain is in compliance.</p> <p>Iron Mountain employs a professional Global Security Services organization. This team is also responsible for information security and incident management. Our security measures include:</p> <ul style="list-style-type: none"> • A comprehensive personnel screening process that includes a thorough background investigation and pre-employment drug screening • Stringent physical security measures tailored to the needs of specific location and environment. These measures include: positive access control and intrusion detection systems, alarms, and CCTV • Industry-leading asset protection policy and procedures with continuous employee training to ensure strict adherence to requirements • On-going security integrity audits to monitor compliance and ensure our security plans are current, viable, and reflect industry best practices
<p>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.</p>	<p>Iron Mountain is in compliance. We understand information is an agency’s most valuable asset. Iron Mountain strives to hire and retain the best candidates for all positions. Iron Mountain has significant experience obtaining and maintaining security clearances for a variety of Federal agencies. Iron Mountain will work with the State’s designated point-of-contact as necessary to coordinate, track and process additional background investigations for employees required for this contract.</p>



	<p>By using stringent pre-employment screening and hiring procedures and ongoing training and development programs, we attract and retain qualified, motivated employees who demonstrate strong customer service skills. Some of Iron Mountain’s thorough pre-employment hiring procedures include:</p> <ul style="list-style-type: none"> • Drug Screening • Identity Verification • Employment Verifications • Education Verifications • Motor Vehicle Reviews for Drivers/Couriers • Criminal Conviction Searches <p>In addition, all applicants are screened to confirm authorization to work in the United States. Furthermore, Iron Mountain employees undergo recurring background investigations every three years. Iron Mountain employees sign confidentiality agreements as part of their employment with Iron Mountain, so our customers can be assured that any sensitive information will be treated as such.</p>
<p>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.</p>	<p>Iron Mountain is in compliance. Iron Mountain developed its Incident Management Program with a tactical and business strategy, including governance, industry standard and best practices. The program provides a framework to support successful incident response, including:</p> <ul style="list-style-type: none"> • Triage, investigate, and escalate the event to internal support resources; • Mitigate the event and its impact; • Coordinate notifications in compliance with legal, regulatory and contractual requirements; • Notify appropriate insurance partners; • Develop trending and reporting; and • Develop processes and procedures to help prevent recurring events. <p>If an event threatens the security, availability and confidentiality of personal data or customer information, Iron Mountain reports the incident through established escalation protocols, which are designed to help streamline the incident reporting process and enable Iron Mountain personnel to register vital incident information quickly, thoroughly, and efficiently about events that occur. Once an incident is reported, the appropriate Iron Mountain team is alerted to begin researching the matter. We track the incident until a resolution is reached and appropriately documented. As necessary, Iron Mountain response team members coordinate customer notifications in accordance with laws, regulations and customer agreements. Additionally, Iron Mountain personnel perform analysis to identify trends and develop</p>

	<p>processes and procedures to proactively prevent reoccurring events.</p> <p>Iron Mountain also utilizes automated tools to monitor the production IT environment and detect events that impact the security, availability or confidentiality of data. When such events are identified, a ticket is generated and routed to the appropriate response team for triage and resolution.</p> <p>On at least a quarterly basis, Iron Mountain management meets to monitor the IT infrastructure and application hosting environment and review information related to incident volume, response time, and incident breakdowns by service.</p>
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.	Iron Mountain is in compliance.
4.4.2 The Vendor’s incident management plan must describe what steps of the process are handled internally or externally; and	Iron Mountain is in compliance.
4.4.3 The Vendor’s incident management plan must include timeframes or milestones.	Iron Mountain is in compliance.
4.4.4 The Vendor must provide the incident management plan within 30 calendar days of the contract start date	Iron Mountain is in compliance.

10.1.2 Section 5 General Requirements

Requirement	Iron Mountain Compliance
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/	Iron Mountain is in compliance.
5.1.1.1 The vendor must bear all costs related to recovery or restoration of damaged records in the care of the vendor.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
5.1.2.2.1 Facility must have security locks at each exterior entrance.	Iron Mountain is in compliance.



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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
5.1.2.2.3.1 Vendor should submit the policy with their bid and must provide documentation of such policy prior to award.	Iron Mountain is in compliance (please see policy included as an attachment in proposal section 10.3 below).
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.	Iron Mountain is in compliance.
5.1.2.4 The vendor must provide smoke detection within the entire facility in accordance with NFPA code or standards.	Iron Mountain is in compliance.
5.1.2.5 The vendor must provide a fire suppression system in the records storage areas.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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").	Iron Mountain is in compliance.
5.1.2.8.1 Records must be stored away from windows, steam, sewer, or water pipes.	Iron Mountain is in compliance.
5.1.2.9 The Vendor must provide a moisture detection system throughout the records storage area.	For normal hard-copy business records, Iron Mountain offers standard storage in our record centers. Since paper records will not suffer significant deterioration within periods of time far exceeding most retention schedules, Iron Mountain does not regulate the temperature or humidity in Standard Storage space except for a basic level of heating in northern climates.



5.1.2.10 The Vendor must minimize light exposure to the records and must keep the lids on boxes at all times.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
5.1.4 The vendor must provide an indexing system for records inventory and must index each box or file submitted.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
5.1.5 The vendor must invoice each state agency storing records at the facility monthly in arrears.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.
5.1.7.1.3 The total amount of cubic feet of storage for the State.	Iron Mountain is in compliance.
5.1.7.1.4 The itemized cost for each for an agency.	Iron Mountain is in compliance.



5.1.7.1.5 The itemized cost for the State.	Iron Mountain is in compliance.
5.1.7.1.6 The authorized users for each account.	Iron Mountain is in compliance.
5.1.7.1.7 The requests for action made for each agency/account.	Iron Mountain is in compliance.
5.1.7.1.8 The destruction eligibility of records.	Iron Mountain is in compliance.
5.1.8 The vendor must include on its monthly invoice to the agency all billing activity detail for the month.	Iron Mountain is in compliance.
5.1.9 Vendor must only bill for storage of records that an agency has requested to be stored at the storage facility.	Iron Mountain is in compliance.
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.	Iron Mountain is in compliance.

10.1.3 Permanent Withdrawal

The act of processing a Permanent Withdrawal order to prepare and confirm Items retrieved at Iron Mountain's dock for transportation and to update the status of the Item in the inventory system. Permanent Withdrawal applies to Items that will not be returned to Iron Mountain for storage, but are not to be destroyed by Iron Mountain. Permanent Withdrawal charges will apply when Items are removed from Iron Mountain and will not be returned, regardless of whether the removal occurs during the contract term, at the end of the contact term, upon expiration of the contract, or as a result of a customer terminating the contract, by non-renewing or otherwise. Deposits processed for Permanent Withdrawal are deducted from the storage billing at the end of the month this process occurs. The Permanent Withdrawal process includes both the Permanent Withdrawal charge plus a Retrieval charge for each item to be withdrawn. Permanent Withdrawal processing includes: scanning to confirm each Deposit is being changed to permanently withdrawn status, preparation for shipment, loading on a secure vehicle for transportation, and closing the order within the system (up to the standard destruction volume of 1,200 cubic feet per Iron Mountain Market per month). In the context of a customer ending its relationship with Iron Mountain and closing its account, whether by way of contract expiration, contract non-renewal, contract termination or otherwise, then the maximum cubic feet of cartons that Iron Mountain will transfer back to the customer (or the customer’s new vendor) is 1,200 cubic feet per month, per Iron Mountain market. Items that are not picked up by a customer within 30 days may be subject to additional charges, including but not limited to charges for refileing and retrieval.



10.2 ATTACHMENTS

10.2.1 BI Program Overview

Please find included in our response a copy of Iron Mountain's Background Investigation Program Overview (immediately following this page).

10.2.2 Visitor Safety and Security Welcome Policy

In response to requirement 5.1.2.2.3.1, please find included in our response a copy of Iron Mountain's Visitor Safety and Security Welcome Policy (immediately following this page).

10.2.3 Floodplain Certificate

Please find included in our response a copy of Iron Mountain's Elevation Report (immediately following this page).



Overview of Background Investigation Program – U.S.

Iron Mountain's pre-employment hiring procedures include drug screening, identity verification, criminal conviction searches, government/terrorist watch list reviews, employment verifications, education verifications (where applicable), as well as annual motor vehicle reviews for drivers and couriers. In addition, all applicants are screened to confirm authorization to work in the United States.

All drug testing, background investigations and driver checks are conducted by reputable national services and reported to the Iron Mountain corporate office to preserve the integrity of the process and the results. Employment decisions are reviewed on an individualized basis with consideration given to the recency, severity and relevance of any derogatory information in an employee or applicant's background check. To validate their continued eligibility for employment, Iron Mountain employees undergo recurring background investigations every three years.

This program has been in place for many years, and the Company is continually reviewing and implementing improved processes to ensure that the highest standards are applied to our employment decisions.

Drug Screening

Iron Mountain maintains a “zero tolerance” policy to employ a workforce free from abuse of drugs and alcohol.

The first step in the Iron Mountain background investigation process is the pre-employment drug test. This consists of a 5-panel screening test administered in accordance with the Substance Abuse and Mental Health Services Administration (SAMHSA) guidelines. Substances covered by the 5-panel test are:

- (1) Marijuana metabolites
- (2) Cocaine metabolites
- (3) Opiate Metabolites
- (4) Phencyclidine (PCP)
- (5) Amphetamines / Methamphetamines

Negative test results are reported via a secure web site to authorized users. Positive results are reported to a single corporate contact to maintain privacy and confidentiality.

Once employed, individuals may be subject to additional testing under the following conditions:

- Reasonable Suspicion
- Post Collision/Post Accident
- CDL Random
- Return to Duty
- Follow up from Return to Duty

Criminal Conviction Searches

Once a written offer letter is signed by the applicant, a criminal background check is then conducted in all counties/states where the applicant has resided/been employed for the past ten years (effective for new employees hired after July 1, 2011) . Appropriate jurisdictions are identified via disclosure by the applicant as well as a Social Security Number trace, to the extent permitted by law. In addition, a search of Federal Criminal courts is also conducted.

Iron Mountain maintains a team of skilled background investigation professionals who review any derogatory criminal history before making recommendations on employment decisions. Iron Mountain takes into consideration the date of any conviction, the nature of the offense, the position being applied for, and other factors, when determining whether to allow an individual to work for the company.

Iron Mountain reserves the right to review and adjudicate personnel decisions with regard to hiring, terminating and suspending individuals based on the nature of the offense, timing of the offense, recidivism and relationship of the offense to the job being considered.

Government/Terrorist Watch Lists

Iron Mountain conducts a comprehensive review of government and terrorist watch lists via its preferred background investigations provider. The search includes, among others: Department of Public Safety, Department of Corrections, Administrative Office of the Courts, Bureau of Criminal Apprehension, and/or the Department of Criminal Justice and other applicable government agencies, where available; Information from 49 states' Sex Offender Registries plus the District of Columbia, Puerto Rico and Guam; the Office of Foreign Assets and Control's (OFAC) Specially Designated Nationals and Blocked Individuals (SDN) List, a review of the Interpol Most Wanted list, as well as numerous other domestic and international government terrorist and sanctions watch lists.

The search also includes a review of excluded parties in databases maintained by the Office of Inspector General (U.S. Department of Health and Human Services) and complies with OIG and U.S. General Services Administration guidelines.

Employment Verifications

Employment verifications consist of a review of an applicant's employment history going back seven years.

Education Verifications

Iron Mountain will confirm the highest degree awarded post high school if required for the role.

Motor Vehicle Review

Driver candidates are screened for appropriate license class and any motor vehicle violation history. Violation and accident history for the past three (3) years are reviewed and adjudicated based upon seriousness of the offense and frequency of occurrence. All drivers are subject to an annual motor vehicle records check.

IRON MOUNTAIN VISITOR SAFETY & SECURITY WELCOME



Iron Mountain Visitor Safety & Security Welcome

Dear Iron Mountain Visitor: Safety & Security is of paramount concern to Iron Mountain. Procedures have been established to ensure protection of our customer's records as well as your safety. Failure to follow these procedures may result in the loss of visiting privileges.

Logs. Visitors must sign in and out of the facility on the logs provided using legible handwriting or printing. Sign in / sign out is recorded through visitor registration software at all corporate sites.

Badges: All Visitors must show a valid government issued ID (ID card, Passport, and Driver's License) upon entering the facility before being issued a numbered visitor badge. All Iron Mountain employees and visitors are required to wear Iron Mountain issued identification badges while on site at any Iron Mountain location. The badges are to be color-coded to indicate the nature of the individual's business at Iron Mountain. Anyone without a visible badge will be politely requested to produce it and wear it. Lost badges are to be reported immediately to your host. Badges are to be turned in at the conclusion of the visit and at least on a daily basis.

Access Control. Visitors are not authorized to admit any person (including persons with Iron Mountain photo identification badges) into any facility. Visitors are to use only authorized entrances and exits.

Key Control. Visitors will not be given keys to any facility at any time.

Internal Security. Visitor participating in tours or conducting audits will be limited to defined areas, audit or viewing rooms and are not allowed to be in areas where other customer materials are located or could be viewed unless accompanied and monitored by an authorized escort. Visitors found unattended in any storage areas will be requested to leave the premises.

Information Access. Visitors are not permitted to access (to include reading, copying, removing or otherwise possessing) information Iron Mountain deems as private and/or proprietary, unless such access is required by contract, law or regulation. Exceptions to this rule must be coordinated with the Iron Mountain department who owns the requested information.

Photography/Video Recording. Use of any recording equipment (photographic, video, cellular telephones with photographic or video function, imaging, audio or other recording activities; collectively "recording equipment") for recording purposes is strictly forbidden at all Iron Mountain facilities without prior permission of the District Manager (NA) Vice President (corporate locations) or Country Managers (International).

Security or Safety Concerns. Any Visitor who observes a situation or practice they believe is unsafe or insecure is encouraged to report the matter to the local manager.

Smoking. Smoking, including electronic alternatives is not permitted in any Iron Mountain facility. Visitors may only smoke in designated areas external to the facility that are at a minimum of 10 feet / 3 meters away from the perimeter of the building and from combustible or flammable material such as propane, dumpsters or landscaping mulch. Smoking anywhere within the building will result in your permanent loss of privilege to visit the facility.

To whom it may concern, on 5-29-15 White Brothers Consulting LLC. Shot to two finished floor elevations on the property located at 5730 MaCorkle Ave. SE, Charleston WV 25304. The first shot elevation was in the doorway shown on the first picture attached here to and was 613.30'. The second shot was on the dock shown in the second picture attached hereto and was 613.18'. The base flood elevation in this area according to the firm map 54039C0429E is 597.00' and shown on a map attached hereto.

Certified by Jeffery Lee Snyder P.S. 2238

1st



2nd



JEFFERY LEE SMITH
LICENSED
No. 2233
STATE OF WEST VIRGINIA
PROFESSIONAL SURVEYOR

WV Flood Map



This map is not the official regulatory FIRM or DFIRM. Its purpose is to assist with determining potential flood risk for the selected location.

Map Created on 6/1/2015

	Location of the mouse click		Cross Section Line
	Approximate Study (Zone A)		Base Flood Elevation Line
	Detailed Study (Zone AE, AH, AO)		DFIRM Panel (Map) Index
	Floodway		
	Flood Water Depth (HEC-RAS)		

User Notes:

Disclaimer:
 The online map is for use in administering the National Flood Insurance Program. It does not necessarily identify all areas subject to flooding, particularly from local drainage sources of small size. To obtain more detailed information in areas where Base Flood Elevations have been determined, users are encouraged to consult the latest Flood Profile data contained in the official flood insurance study. These studies are available online at www.msc.fema.gov.

WV Flood Tool is supported by FEMA, WV NFIP Office, and WV GIS Technical Center (<http://www.MapWV.gov/flood>)

Flood Hazard Area:
 Advisory Flood Height: N/A
 Water Depth: N/A
 Elevation: N/A
 Location (long, lat):
 Location (UTM 17N):
 FEMA Issued Flood Map:
 Contacts:
 CRS Information:
 Flood Profile: **No Profile**
 HEC-RAS Model: **No Model**
 Parcel Number:



10.3 EXCEPTIONS

Please find attached Iron Mountain's Exceptions to CRFQ 0212 SWC210000001 immediately following this page.

EXCEPTIONS TO THE REQUEST FOR QUOTE (the “CRFQ”)

No. SWSC210000001

BY AND BETWEEN

IRON MOUNTAIN INFORMATION MANAGEMENT, LLC (“Iron Mountain”)

and

STATE OF WEST VIRGINIA (“CUSTOMER”)

The contract terms shall be defined by a written agreement that is not binding until fully executed by both parties. In the event Iron Mountain is selected by Customer as the winning bidder to the above-referenced CRFQ, Iron Mountain is requesting the following exceptions to the General Terms and Conditions, including the Exhibit B HIPAA Business Associate Addendum:

Section, Sub Paragraph, Line	Contract Text	Proposed Text
Section 8. Insurance, Sentence 1	The apparent successful Vendor shall furnish proof of insurance identified by a checkmark below and must include the State as additional insured on each policy prior to Contract award.	The apparent successful Vendor shall furnish proof of insurance identified by a checkmark below and must include the State as additional insured on the Commercial General Liability Insurance Policy and Automobile Liability Insurance Policy, to the extent of Vendor’s liability under this Agreement.
Section 8. Insurance, Sentence 3 and 4.	Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued.	In the event of cancelation of Vendor’s insurance policies, Vendor will provide notice to the agency in accordance with the terms of such policy.
Section 8, sentence 6: Commercial General Liability Insurance	Commercial General Liability Insurance in at least the amount of 1,000,000 per occurrence.	Commercial General Liability Insurance in the amount of 1,000,000 per occurrence.
Section 8, sentence 6: Automobile Liability Insurance	Automobile Liability Insurance in at least the amount of 1,000,000 per occurrence.	Automobile Liability Insurance in the amount of 1,000,000 per occurrence.
Section 11, sentence 2	Vendor shall pay liquidated damages in the amount specific	Sentence removed in its entirety.

	<p>below or as described in the specifications:</p> <p>Liquidated Damages Contained in the Specifications</p>	
Section 27. Assignment	Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.	Neither this Contract nor any monies due, or to become due hereunder, may be assigned (except to an Affiliate of Vendor) by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.
Section 30. Privacy Security, and Confidentiality, Sentence 1	The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures and rules.	The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, excluding disclosures to personnel and subcontractors who require such personally identifiable information for the performance of the Services and are bound to substantially similar terms regarding the protection of such information as is set out in this Agreement, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures and rules.
Section 30. Privacy Security, and Confidentiality, Sentence 2	Vendor further agrees to comply with the Confidentiality Policies and Information Security and Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy.html	Vendor further agrees to comply with the HIPAA Business Addendum attached hereto as Exhibit B. *Note to WV, any additional confidentiality and information security agreements will need to be attached the agreement and negotiated between the parties.
Section 41. Background Check, Sentence 1.	In accordance with W. Va. Code Section 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the	Vendor has drug screening and background investigation policies in effect for its employees in the United States. Vendor will continue to maintain such drug screening and background investigation policies for

	<p>buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the finger print-based state and federal background inquiry.</p>	<p>the term of this Agreement. Background Investigations include, but are not limited to, criminal record searches, employment verifications, government/terrorist watch list and sanction list searches, education verification (if required for the role), and motor vehicle report reviews for driver candidates. Pre-employment drug screens are conducted on all candidates who have been extended an offer, prior to employment, in accordance with local law. All drug testing, background investigations and driver checks are conducted by reputable national services and reported to the Vendor corporate office to preserve the integrity of the process and the results. Employment decisions are reviewed on an individualized basis with consideration given to the recency, severity and relevance of any derogatory information in an employee or applicant's background check.</p>
<p>Exhibit B, Section 3, f, I</p>	<p>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.</p>	<p>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., subject to any applicable fees as set out in the Pricing Schedule.</p>
<p>Exhibit B, Section 3, f., III., Sentence 1</p>	<p>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.</p>	<p>Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents 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.</p>

<p>Exhibit B, Section 3., f., III., Sentence 3</p>	<p>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.</p>	<p>This should include a process that allows for an accounting to be collected and maintained by Associate for at least one year after the termination of the Agreement or longer if required by state law.</p>
<p>Exhibit B, Section 3., g.</p>	<p>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.</p>	<p>Notwithstanding Section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law.</p> <p>*Please note, PHI would likely be included in the Agency’s deposits, which Iron Mountain will not retain after the termination of the Agreement.</p>
<p>Exhibit B, Section 3., g.</p>	<p>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.</p>	<p>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 substantially similar restrictions and conditions to those which apply to the Associate hereunder.</p>
<p>Exhibit B, Section 3., i.</p>	<p>The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the</p>	<p>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</p>

	<p>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.</p>	<p>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 audit of Associate’s compliance with the Privacy and Security Rules, upon ten (10) days notice and no more than once per year. 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.</p>
<p>Exhibit B, Section 3., k., Sentences 1 and 2.</p>	<p>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 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.</p>	<p>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 promptly by email or web form upon the discovery of any Breach of unsecured PHI or 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.</p>
<p>Exhibit B, Section 3., k., Sentence 5.</p>	<p>Within 72 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</p>	<p>Within 72 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, to the extent known by the Associate: (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</p>

	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.	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.
Exhibit B, Section 3., k., Sentence 6.	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.	Agency will coordinate with Associate to mutually determine additional and reasonable actions that will be required for mitigation of the Breach.
Exhibit B, Section 3., k., Sentence 7.	All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.	Associate shall reimburse Agency for the direct, verifiable third-party costs incurred by Agency in (a) preparation and mailing of notices to such individuals to whom such notification is required by statute or regulation and (b) the provision of credit monitoring services to such individuals as required by statute or regulation, for a period not exceeding twelve (12) months, provided that Agency gives Associate reasonable prior written notice of its intent to deliver such notice and services.
Exhibit B, Section 3., k., Sentence 8.	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.	All subcontracts relating to the Agreement will contain substantially similar notification requirements as contained herein.
Exhibit B, Section 3., l.	The Associate shall make itself and any subcontractors, workforce or	This subsection l is removed in its entirety.

	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.	
Exhibit B, Section 4., b.	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.	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, subject to any applicable fees set out in the Pricing Schedule 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 of Associate. The duty of the Associate and its agents to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.
Exhibit B, Section 4., d. Sentence 3	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.	Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH, as permitted by law, and shall be responsible for any and all costs associated with prosecution.
Exhibit B, Section 4., e.	The respective rights and obligations of Associate under this Addendum shall survive the	The respective rights and obligations of Associate under this Addendum shall survive the termination of the

	termination of the underlying Agreement.	underlying Agreement so long as Associate continues to hold PHI.
--	--	--

The Customer will assume agreement on all other terms unless otherwise noted by Iron Mountain.



10.4 ADDENDA AND REQUIRED FORMS

Please find attached immediately following this page Iron Mountain's signed Addendum Acknowledgement Form and the following required forms:

- West Virginia CRFQ Form
- West Virginia Ethics Disclosure Form
- General Terms and Conditions Certification and Signature
- West Virginia State Government HIPA Business Associate Addendum (BAA)
- State of West Virginia Purchasing Affidavit

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Iron Mountain Information Management, LLC

Company



Digitally signed by Randy D. Mayer
DN: cn=Randy D. Mayer, o=Iron Mountain Information Management, Inc.,
ou=Sr. Director, Business Support, email=randy.mayer@ironmountain.com,
c=US
Date: 2020.08.14 09:43:30 -04'00'

Authorized Signature

August 14, 2020

Date

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



Purchasing Division
 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: Statewide Contract for Records Management - (RECMGT21)

Proc Type: Statewide MA (Open End)

Date Issued	Solicitation Closes	Solicitation No	Version
2020-07-31	2020-08-18 13:30:00	CRFQ 0212 SWC210000001	1

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:
 Iron Mountain Information Management, LLC
 One Federal Street
 Boston, MA 02110
 1-800-899-4766

FOR INFORMATION CONTACT THE BUYER

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

Signature X  FEIN # 23-2588479 DATE 08-18-2020

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



Purchasing Division
 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:

Iron Mountain Information Management, LLC
 One Federal Street
 Boston, MA 02110
 1-800-899-4766

FOR INFORMATION CONTACT THE BUYER

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

Signature X

Digitally signed by Randy D. Mayer
 DN: cn=Randy D. Mayer, o=Iron Mountain
 Information Management, Inc., ou=SR,
 Director, Business Support,
 email=randy.mayers@ironmountain.com, c=US
 Date: 2020.08.18 10:28:43 -0400

FEIN # 23-2588479

DATE 8-18-2020

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		STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER	
No City	WV99999	No City	WV 99999
US		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

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.

West Virginia Ethics Commission
Disclosure of Interested Parties to Contracts

(Required by W. Va. Code § 6D-1-2)

Name of Contracting Business Entity: Iron Mountain Information Management, LLC Address: One Federal Street
Boston, MA 02110

Name of Authorized Agent: Randy Mayer Address: _____

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)

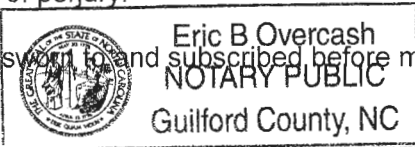
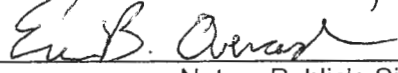
Check here if none, otherwise list entity/individual names below.

Signature:  Date Signed: August 18, 2020

Notary Verification

State of North Carolina, County of Guilford:

I, Eric B. Overcash, 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 10 day of August, 2020
 
Notary Public's Signature

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

My Commission Expires: 6/7/2021

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 disclose 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.
 - 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 CFR § 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 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 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.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

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.
- 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. 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.

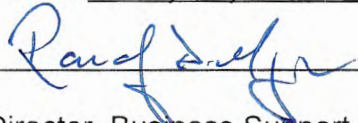
- c. Electronic Transmission. Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Addendum 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: West Virginia Office of Technology

Name of Associate: Randy Mayer

Signature: _____

Signature:  _____

Title: _____

Title: Sr. Director, Business Support

Date: _____

Date: August 18, 2020

EXHIBIT A

Name of Associate: Iron Mountain Information Management, LLC

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.

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

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

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

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

DEFINITIONS:

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

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

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

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

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Iron Mountain Information Management, LLC

Authorized Signature:  Date: 08/18/2020

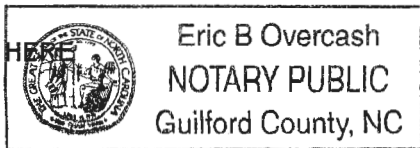
State of North Carolina

County of Guilford, to-wit:

Taken, subscribed, and sworn to before me this 10 day of August, 2020.

My Commission expires 6/7, 2021.

AFFIX SEAL HERE



NOTARY PUBLIC



**CRFQ 0212 SWC210000001
(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	\$ 44,655.00
SUPPLIES:					
5.2.4.1 Contract Item #4	Storage Boxes (Aproximate Demensions 15"L x 12"W x 10"H)	Per Box	5,000	\$ 1.89	\$ 9,450.00
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	\$ 1.84	\$ 4,600.00
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	\$ 1.84	\$ 9,200.00
5.2.8.1 Contract Item #8	Emergency Retrieval/Delivery of Paper Records [Three (3) Calendar Days of Written Request]	Per Box	500	\$ 9.79	\$ 4,895.00
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	\$ 3.06	\$ 15,300.00
5.2.11.4 Contract Item #11	Destruction of Microfilm	Per Box	50	\$ 22.50	\$ 1,125.00

Total Cost	\$ 89,225.00
-------------------	---------------------

Please type or print legibly	
Vendor:	Iron Mountain Information Management, LLC
Vendor Representative:	Tom Burt
Phone Number:	610.731.7944
Email:	Tom.Burt@ironmountain.com



NOTE ON EXHIBIT A – PRICING PAGE

Regarding Iron Mountain's proposed pricing in Exhibit A – Pricing Page, please note the following:

1. Regarding Exhibit A, 5.2.3.1, Contract Item #3 Records Monthly Storage Fee: the extended price shown in our response is a monthly rate and not the full extended price for the duration of the full year (12 months).
2. Regarding Exhibit A, 5.2.6.1, Contract Item #6 Indexing of New Records, Iron Mountain will bill this under Receiving and Entry. Iron Mountain considers the process of indexing new records to be synonymous with Receiving and Entry, which will be actioned and billed accordingly.