



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.



Jump to: FORMS

Home

Personalize

Accessibility

App Help

About



Welcome, Lu Anne Cottrill

Procurement

Budgeting

Accounts Receivable

Accounts Payable

Solicitation Response(SR)

Dept: 0212

ID: ESR05121600000005519

Ver.: 1

Function: New

Phase: Final

Modified by batch , 05/12/2016

## Header

List View

### General Information

Contact

Default Values

Discount

Document Information

Procurement Folder: 194707

Procurement Type: Central Master Agreement

Vendor ID: 000000126525



Legal Name: IRON MOUNTAIN INFORMATION MGMT

Alias/DBA:

Total Bid: \$64,996.08

Response Date: 05/12/2016



Response Time: 10:26

SO Doc Code: CRFQ

SO Dept: 0212

SO Doc ID: SWC1600000008

Published Date: 5/2/16

Close Date: 5/12/16

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum #2 Records Management and Off-Site storage

Total of Header Attachments: 0

Total of All Attachments: 0



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

State of West Virginia  
Solicitation Response

Proc Folder : 194707

Solicitation Description : Addendum #2 Records Management and Off-Site storage service

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation No	Version
	2016-05-12 13:30:00	SR        0212   ESR05121600000005519	1

VENDOR
000000126525  IRON MOUNTAIN INFORMATION MGMT

FOR INFORMATION CONTACT THE BUYER  Stephanie L Gale (304) 558-8801 stephanie.l.gale@wv.gov
--

Signature X	FEIN #	DATE
-------------	--------	------

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

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Contract Item #1 Transfer Existing Records to New Storage	230000.00000 CF			

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.11 The Vendor must transfer existing records to the new storage facility. Cost Per Cubic Feet

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Contract Item #2 Indexing of Existing Records	230000.00000 BOX			

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.12 Contract Item #2: The Vendor must index existing records. Cost Per Box.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Contract Item #3 Monthly Storage Fee	230000.00000 CF		\$0.264000	\$60,720.00

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.13 The Vendor must accommodate storage of a minimum of 230,000 cubic feet for the State's records. Monthly Cost Per Cubic Foot.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Contract Item #4: Storage Boxes	120.00000	EA	\$2.000000	\$240.00

Comm Code	Manufacturer	Specification	Model #
44111515			

**Extended Description :** 4.1.14 Contract Item #4: The Vendor must provide storage boxes; Dimensions: 10"Wx12"Lx15"H. Cost Per Box



Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
5	Contract Item #5: Records Pick Up	120.00000	BOX		

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	4.1.15 Contract Item #5: The Vendor must pick up the records within a maximum of five (5) business days after written notification by the Agency. Cost Per Box.
-------------------------------	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
6	Contract Item #6: Indexing New Records	120.00000	BOX		

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	4.1.16 Contract Item #6: The Vendor must index all new records. Cost Per Box.
-------------------------------	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
7	Contract Item #7: Documents Retrieval (3 Business Day)	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	4.1.17 Contract Item #7: The Vendor must retrieve any documents in storage and provide a digitalized version of the documents when requested by any Agency within a maximum of three (3) business days. The request must be completed during normal business hours.  4.1.17.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by
-------------------------------	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
8	Contract Item #7.1: Documents Retrieval 1-50 pages	36.00000	EA	\$12.000000	\$432.00

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	4.1.17.1 Contract Item #7.1: Cost Per Request for 1-50 pages  4.1.17.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.
-------------------------------	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
9	Contract Item #7.2: Documents Retrieval 51-200 pages	36.00000	EA	\$0.250000	\$9.00

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	<p>4.1.17.2 Contract Item #7.2: Cost Per Request for 51-200 pages</p> <p>4.1.17.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.</p>
-------------------------------	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
10	Contract Item #8: Emergency Documents Retrieval (1 Day)	36.00000	EA	\$8.240000	\$296.64

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	<p>4.1.18 Contract Item #8: The Vendor must retrieve any documents in storage and provide a digitalized version of the documents when requested by an Agency sending a written Emergency notification within a maximum of one (1) business day.</p> <p>4.1.18.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by</p>
-------------------------------	---

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
11	Contract Item #8.1: Emergency Documents Retrieval 1-50 pages	36.00000	EA	\$12.000000	\$432.00

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	<p>4.1.18.1 Contract Item #8.1: Cost Per Request for 1-50 pages</p> <p>4.1.18.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.</p>
-------------------------------	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
12	Contract Item #8.2: Emergency Documents Retrieval 51-200 pgs	36.00000	EA	\$0.250000	\$9.00

Comm Code	Manufacturer	Specification	Model #
78131804			

<b>Extended Description :</b>	<p>4.1.18.2 Contract Item #8.2: Cost Per Request for 51-200 pages</p> <p>4.1.18.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.</p>
-------------------------------	--

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
13	Contract Item #9: Documents Retrieval (3 Business Day)	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.19 Contract Item #9: The Vendor must retrieve any document in storage and deliver it to the requesting Agency within three (3) business days of written notification. Documents must be delivered during normal business hours.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
14	Contract Item #9.1: Documents Retrieval 1-50 pages	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.19.1 Contract Item #9.1: Cost Per Request for 1-50 pages

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
15	Contract Item #9.2: Documents Retrieval 51-200 pages	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.19.2 Contract Item #9.2: Cost Per Request for 51-200 pages

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
16	Contract Item #10: Emergency Documents Retrieval (1 Day)	36.00000	EA	\$8.240000	\$296.64

Comm Code	Manufacturer	Specification	Model #
78131804			

**Extended Description :** 4.1.20 Contract Item #10: The Vendor must retrieve any document in storage and deliver it to requesting Agency within one (1) business day if it is an Emergency.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
17	Contract Item #10.1: Emergency Documents Retrieval 1-50 pgs	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

Extended Description : 4.1.20.1 Contract Item #10.1: Cost Per Request for 1-50 pages

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
18	Contract Item #10.2: Emergency Documents Retrieval 51-200 pg	36.00000	EA		

Comm Code	Manufacturer	Specification	Model #
78131804			

Extended Description : 4.1.20.2 Contract Item #10.2: Cost per Request for 51-200 pages

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
19	Contract Item #11: Destruction of Paper Documents	120.00000	BOX	\$2.590000	\$310.80

Comm Code	Manufacturer	Specification	Model #
80161508			

Extended Description : 4.1.21 Contract Item #11: The Vendor must provide destruction of specified documents at the Agency's written request. Documents must be destroyed by a crosscut shredder for paper documents. Cost Per Box

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
20	Contract Item #12: Destruction of Microfilm	120.00000	BOX	\$18.750000	\$2,250.00

Comm Code	Manufacturer	Specification	Model #
80161508			

Extended Description : 4.1.22 Contract Item #12: The Vendor must provide destruction of Microfilm at the Agency's request. Microfilm must be shredded at a minimum of 1/35" strip or smaller. Cost Per Box

**EXHIBIT A – Pricing Page**  
**Records Management - Offsite Storage and Destruction**

Commodity Line Number	Description	Unit of Measure	Estimated Quantity	Unit Price	Extended Price
4.1.11 Contract Item #1	Transferring Existing Records to New Storage Facility	Per Cubic Foot	230,000.00	0.00	0.00
4.1.12 Contract Item #2	Indexing Existing Records	Per Cubic Foot	230,000.00	0.00	0.00
4.1.13 Contract Item #3	Monthly Storage Fee	Per Cubic Foot	230,000.00	0.264	60,720.00
4.1.14 Contract Item #4	Storage Boxes	Each	120.00	2.00	240.00
4.1.15 Contract Item #5	Records Pick Up	Box	120.00	0.00	0.00
4.1.16 Contract Item #6	Indexing New Records	Box	120.00	0.00	0.00
4.1.17 Contract Item #7	Documents Retrieval (3 Business Day Request)	Each	36.00	0.00	0.00
4.1.17.1 Contract Item #7.1	1-50 pages	Each	36.00	12.00	432.00
4.1.17.2 Contract Item #7.2	51-200 pages	Each	36.00	0.25	9.00
4.1.18 Contract Item #8	Emergency Documents Retrieval (1 Business Day Request)	Each	36.00	8.24	296.64
4.1.18.1 Contract Item #8.1	1-50 pages	Each	36.00	12.00	432.00
4.1.18.2 Contract Item #8.2	51-200 pages	Each	36.00	0.25	9.00
4.1.19 Contract Item #9	Documents Retrieval (3 Business Day Request for Delivery)	* Each	36.00	1.55	55.80
4.1.19.1 Contract Item #9.1	1-50 pages	Each	36.00	0.00	0.00
4.1.19.2 Contract Item #9.2	51-200 pages	Each	36.00	0.00	0.00
4.1.20 Contract Item #10	Emergency Documents Retrieval (1 Business Day Request For delivery)	* Each	36.00	8.24	296.64
4.1.20.1 Contract Item #10.1	1-50 pages	Each	36.00	0.00	0.00
4.1.20.2 Contract Item #10.2	51-200 pages	Each	36.00	0.00	0.00
4.1.21 Contract Item #11	Destruction of Paper Documents	Box	120.00	2.59	310.80
4.1.22 Contract Item #12	Destruction of Microfilm	Box	120.00	18.75	2,250.00
			<b>Total Cost</b>		<b>65,051.88</b>

\*  
\*\*

Retrieval per Cubic Foot per Box  
Administration Fee

Cubic Foot  
Per Month

\$1.55  
\$25.10

If Iron Mountain performs services not listed here, the Iron Mountain standard rate will apply; details available upon request.



MAY 12, 2016

**STEPHANIE GALE**

Buyer

**STATE OF WEST VIRGINIA**

2019 Washington Street East  
Charleston, WV 25305-0130

---

**DEAR STEPHANIE,**

It's been a pleasure speaking with you about your records and information management program. Based on your input, this proposal provides recommended solutions to successfully address your program goals and deliver business value.

You can be confident that Iron Mountain has the expertise, resources, and experience State of West Virginia needs. You will be working with a partner that has been helping companies with similar needs accelerate adoption and achievement of their records and information management goals for over 60 years. We look forward to doing the same for State of West Virginia, too.

With Iron Mountain, you get a focus on your customer experience and access to proven practices and new thinking from an industry leader. You will be able to drive policy adoption, provide information to people, and gain consistent records and information management performance across your business.

On behalf of the entire Iron Mountain team, we look forward to partnering with you. Please note that this proposal is effective for 90 days from May 10, 2016. You will hear from me shortly to answer any questions you may have. In the meantime, please do not hesitate to contact me at (724) 679-0672 or at [heather.sweesy@ironmountain.com](mailto:heather.sweesy@ironmountain.com).

Best regards,

**HEATHER SWEESY**

*Business Development Executive*



## RECORDS MANAGEMENT

PROPOSAL FOR

# STATE OF WEST VIRGINIA

BY IRON MOUNTAIN May 12, 2016

Re: Records Management  
Bid No.: CRFQ 0212 SWC1600000008

**HEATHER SWEESY**, Business Development Executive

1201 Freedom Road  
Cranberry Township, PA 16066  
(724) 679-0672  
heather.sweesy@ironmountain.com

MANAGE WITH CONFIDENCE.

# TABLE OF CONTENTS



Executive Summary ..... 1

RFP Cover Page ..... 4

Specifications, General Requirements..... 5

General Terms and Conditions ..... 25

Certification and Signature Page ..... 28

Vendor Preference Certificate..... 29

Purchasing Affidavit ..... 30

Iron Mountain Overview..... 31

Conclusion..... 35

Appendix ..... 36

---

## CONFIDENTIALITY

This proposal includes information that shall not be disclosed and shall not be duplicated, used or disclosed — in whole or in part — for any purpose other than to evaluate this proposal. If, however, a contract is awarded to Iron Mountain as a result of, or in connection with, the submission of this proposal, State of West Virginia shall have the right to duplicate, use, or disclose the information to the extent necessary to implement the resulting contract. This restriction does not limit State of West Virginia’s right to use information contained in this proposal if it is obtained without restriction from another source.

© 2015 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.

---



# EXECUTIVE SUMMARY



Iron Mountain is pleased to submit this proposal to State of West Virginia for records management services. We value our current relationship with the State of West Virginia and are committed to continuing to deliver superior service. We have enjoyed our partnership and aspire to continue as your chosen partner for all of your information management needs. The local West Virginia staff has the expertise and long standing relationship of servicing the state's record program for years and understands the needs of the departments.

Iron Mountain has developed a unique approach to helping our clients meet the challenges and complexities of Records and Information Management (RIM) from a 360 degree perspective. RIM 360° enables unified records management for the enterprise, allowing you to apply consistent practices to both physical and electronic records, building and auditing policies and enforcing retention guidelines. With RIM 360° you can find solutions that drive policy to adoption, provide information to people, unify your electronic and physical records, and build consistency across workflows, locations and departments. Your operations become more efficient, your program becomes more defensible, and your total program costs are lower.

Iron Mountain's Records and Information Management solution is the prudent choice for the State of West Virginia for the following reasons:

## Security and Chain of Custody

Companies entrust Iron Mountain to properly manage and secure their business records. It is vital, not only to our organization, but to those businesses that hand over their private records to us, that we maintain the highest level of ethical and security standards, derived from industry best practices. The continued success of Iron Mountain requires the commitment of all employees to the maintenance of appropriate standards of information security. Iron Mountain adheres to industry standard best practices in the management of all infrastructure hardware and software components, including daily operations, disaster recovery preparedness and business continuity. Our program is built upon the ISO27001/2 standard for the management of information security. Iron Mountain has unmatched resources to respond to your needs including more than 17,500 employees, a fleet of approximately 3,000 vehicles, and 1,000 facilities/offices worldwide. Furthermore, there is no other company in our industry that invests more money in the security and protection of our customer's information.

## Vehicle Security

Iron Mountain's patented vehicle security system is supplied by Babaco Alarm, Inc. of Moonachie, NJ, a specialist in high security and customized vehicle security applications. The objective is to focus protection around the cargo area, with features included in the base structure that mitigate cargo or vehicle theft. The patented Version 3.1 upgrade to the Babaco foundation system is available exclusively to Iron Mountain in the records management industry.

## InControl

Iron Mountain combines patent-pending security, real-time chain-of custody tracking, and standard operating procedures that deliver a higher standard of information protection specifically around the physical transportation of information.

- **Industry Leading Vehicle Security** — Patent-pending locks, RFID-enabled proximity alarms, compartmentalized cargo areas, and intrusion suppression interlocks eliminating virtually every threat while your information is in transit.
- **Wireless Scanning** — Through the use of wireless scanning technology, we deliver complete chain-of-custody and real-time tracking of the assets entrusted to Iron Mountain. Customer material is scanned at the point of pickup and scanned again at courier arrival to the Iron Mountain facility to verify transportation accuracy.
- **e-Sign Delivery Confirmation** — Improve accountability and keep a delivery audit trail with email confirmation and electronic signatures.

## Facility Security

Iron Mountain is committed to continuing the State of West Virginia's records program and has purchased a new storage facility within the city of Charleston so we can continue to provide a secure and convenient facility to protect and service the State of West Virginia's records.

Iron Mountain utilizes both electronic access controls and personal recognition as methodologies for controlling access to its facilities, and the majority of our larger operations are equipped with access card technology. We require that all facilities maintain a system of positive employee and visitor identification and logging, whether electronic or manual. All personnel are required to wear identification badges while on Iron Mountain premises. Badges are color coded to indicate access authorization levels. Unescorted access to our record centers is prohibited for all but Iron Mountain employees. 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.

## Fire Protection & Suppression

The company has been actively involved within the industry association PRISM to help set standards for fire protection and life safety. Iron Mountain participates and assists in directing the PRISM subcommittee charged with establishing standards in this area. Iron Mountain is also a member of the National Fire Protection Association's (NFPA) Technical Committee, which works with fire marshals and others in the establishment of applicable fire safety codes and procedures.

Iron Mountain's facilities (records centers, data vaults, and shred plants) are designed and constructed in accordance with all applicable local and national codes. Acquired facilities that don't meet or exceed local code are upgraded or vacated as promptly as is practical. Iron Mountain's specifications for new 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 include in-rack or in-aisle and ceiling sprinklers

- All detection, suppression and alarm systems are monitored around the clock and are routinely

## Iron Mountain Connect

The Iron Mountain Connect system facilitates multi-site records management programs, enabling centralized audit and management oversight while allowing individual sites, departments and authorized user's efficient access to records program information. The system helps you employees quickly and easily locate cartons or files, and manage inventory, utilizing its customized search engine. Basic searches are by keyword; advanced searches can filter by organization, record type, status, dates and descriptions. Employees can even search across the entire organization's records to get an enterprise-wide view of all relevant records and transactions. Because the search is fast and effective, it is more than just a transactional tool, it's a powerful research tool that enhances the value of archived information.

Reports are available to monitor and measure:

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

Retrieving records is as simple as a click of the mouse with the Iron Mountain Connect system. Once a customer has selected the cartons or files to be retrieved, Iron Mountain Connect 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

## Financial Strength

Iron Mountain combines the responsiveness of a local service provider with the unmatched resources of the world's largest information management company. Our commitments to security, contingency planning, and the development of cost-effective solutions, together with our national service capabilities, have made us the clear industry leader. Organizations in every major industry and of all sizes—including more than 94% of the Fortune 1000—rely on Iron Mountain to store and manage their information.

This proposal provides unmatched value to the State of West Virginia by addressing your information management needs and having a consistent workflow and a secure chain of custody throughout the following areas: transportation, inbound, storage, retrieval, data delivery and secure shredding. By partnering with Iron Mountain, you'll benefit from a single-vendor approach and customized solutions that accelerate your business processes, improve decision making organization-wide, and make compliance more achievable. Not only will your organization have a single vendor that will provide all vital services, you can rest comfortably knowing that your information is entrusted to the leader in the industry. The remainder of our response will cover all of the details related to our solution. Thank you for the opportunity to present the following information and we look forward to our continued discussions.



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

State of West Virginia  
Request for Quotation  
21 – Info Technology

Proc Folder: 194707

Doc Description: Records Management and Off-Site storage services

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2016-04-07	2016-05-03 13:30:00	CRFQ 0212 SWC1600000008	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

1537 Hansford Street

Charleston, WV 25311

Primary contact telephone: (724) 679-0672

**FOR INFORMATION CONTACT THE BUYER**

Stephanie L Gale

(304) 558-8801

stephanie.l.gale@wv.gov

Signature X

B.T. Menzies DM

FEIN # 23-2588479

DATE

May 10, 2016

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

# SPECIFICATIONS, GENERAL REQUIREMENTS



## 4. GENERAL REQUIREMENTS:

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

### *Facility Requirements:*

*4.1.1 The Vendor must provide a facility that will protect all documents from disaster as defined in West Virginia State Code 5A-8-3.*

You need to know that your records are stored safely. Iron Mountain dedicates considerable resources to ensure that our facilities are appropriate, safe and secure. Our corporate Real Estate and Facilities Engineering department includes a fully staffed engineering group led at the director level. All Iron Mountain record centers comply with standards established by this corporate function and with all appropriate building, fire & safety, electrical, mechanical and other regulatory codes. Before an Iron Mountain record center opens for storage deposits, we conduct a comprehensive quality control audit, including all relevant regulatory inspections and permits, as well as an internal audit of record center requirements. Most of the buildings coming on line are built-to-suit, and are constructed to the standards noted above. All Iron Mountain record centers meet or exceed National Fire Protection Association codes and PRISM (Professional Records & Information Services Management) standards for commercial record centers.

Our Principles of Global Facility Protection mandate some of the industry's most advanced systems to safeguard your information both inside and outside our buildings, including:

- Intrusion detection and alarm systems
- Alarm systems are tied to a local security company for monitoring and quick response
- Physical access control systems
- Fire detection systems
- Fire suppression systems
- In-rack sprinkler systems
- Central monitoring of protection systems

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.

*4.1.1.1 The Vendor must absorb cost related to recovery or restoration of damaged documents in the care of the Vendor.*

Iron Mountain's liability for damage and loss will be documented in the contract; please see our Legal response on page 25.

*4.1.2 The Vendor must provide a facility for existing and new records within the State of West Virginia.*

Iron Mountain complies with this requirement. We have existing storage facilities in Charleston as well as a new facility currently under construction, also in Charleston.

*4.1.3 The Vendor must provide a facility that meets the following requirements for archival storage of microfilm and paper-based records.*

*4.1.3.1 The Vendor must provide a storage area to accommodate a minimum of 230,000 cubic feet for the State's records.*

Iron Mountain complies with this requirement; we have sufficient capacity in the state to store a minimum of 230,000 cubic feet of the State's records.

*4.1.3.2 The Vendor must provide a facility that meets local building codes. Documentation from an applicable municipal or county office must be submitted upon award.*

Iron Mountain will comply with this requirement; the relevant documentation will be provided upon award.

*4.1.3.3 The Vendor's storage facility must provide the following security measures.*

*4.1.3.3.1 Facility must have security locks at each exterior entrance.*

*4.1.3.3.2 Facility must have a 24 hour-7 days a week- 365 days a year monitored anti-intrusion alarm system to protect against unauthorized entry.*

*4.1.3.3.3 Facility must have control procedures in place to ensure access security and must enforce said access policies and procedures. Vendor must provide documentation of such policies and procedures which ensure that only allow authorized individuals can access records. Documentation must be provided prior to award. Facility must enforce controls on access to records storage areas.*

Iron Mountain utilizes both electronic access controls and personal recognition as methodologies for controlling access to its facilities, and the majority of our larger operations are equipped with access card technology. We require that all facilities maintain a system of positive employee and visitor identification and logging, whether electronic or manual. All personnel are required to wear identification badges while on Iron Mountain premises. Badges are color-coded to indicate access authorization levels. Unescorted access to our record centers is prohibited for all but Iron Mountain employees. 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.

Our Security Assurance Reference Guide is included as an attachment.

*4.1.3.4 The storage room 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 has data storage facilities that meet this requirement; independent air circulation or filtration does not apply to standard storage environments for business records.

*4.1.3.5 The Vendor must provide smoke detection. Smoke detection systems must meet the requirements of NFPA 72, National Fire Alarm Code, and must be maintained in accordance with NFPA 72, Part H.*

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's records centers are designed and constructed in accordance with all applicable local and national codes. Specifically, facilities meet all requirements of the local Authorities Having Jurisdiction (AHJ) and National Fire Protection Association (NFPA) standards 13, 25 and 72 at the time the facility was built. Iron Mountain monitors and routinely tests all detection, suppression and alarm systems. Iron Mountain is in compliance with all other relevant NFPA standards, as interpreted by the local AHJ at the time the facility was built, including 10 and 101 as required.

*4.1.3.6 The Vendor must provide a clean agent system that complies with the NFPA 2001 Standard on a pre-action sprinkler system. This system must be used in the records storage areas.*

Clean agent fire suppression is in place in our data centers. In our record centers, fire suppression systems include in-rack or in-aisle and ceiling sprinklers

*4.1.3.7 The Vendor must provide a storage area that is climate controlled with a maximum temperature of 65°F and relative humidity levels at 35-45% ± 5%. These temperatures must be maintained 24 hours a day, 7 days a week, 365 days a year.*

Iron Mountain currently stores about 200 cubic feet of vital records for the state in a climate-controlled environment, in addition to the business records in standard storage.

Setting the standard for reliable and secure offsite storage since 1951, Iron Mountain offers a variety of options to meet our customers' needs. These options include:

- **Standard Storage:** 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.
- **Temperature Controlled Storage:** For normal business records that require lower temperatures, Iron Mountain maintains temperature controlled storage in a variety of markets. Temperature Controlled Storage in our record centers are placed in enclosed, air conditioned rooms.
- **Vital Records Preservation:** For vital records, Iron Mountain maintains vaults in our underground facilities. Vital records vaults are designed and maintained for a specific media type since different media have different recommended archiving conditions. Our standard configurations include the following: temperature and relative humidity of 68°F/30-35%RH, 50°F/30-35% RH, and 35°F/30-35% RH.
- **Custom Vaults:** Iron Mountain hosts a variety of custom vaults in our underground facilities. These vaults can be designed to meet customer specific environmental conditions including temperature, relative humidity and lighting.
- **Magnetic Tape Vaults:** Iron Mountain maintains vaults in data protection centers designed specifically to house electronic media. These vaults hold temperature between 68°F and 72°F and relative humidity between 35% RH and 45% RH.
- **Entertainment Vaults:** Iron Mountain maintains vaults designed specifically to preserve audio and visual media. These include custom vaults, designed to meet customer specific environmental conditions, and open vaults. Our open vaults are configured for preservation of motion picture film (temperature and relative humidity 40°F/25% RH) and audio/video media (temperature and relative humidity 65°F/50% RH).

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

*4.1.3.8.1 Vendor must provide an elevation certificate from a land surveyor verifying the facility is out of the 100-year floodplain prior to award.*

Please see the "Elevation/Flood Zone Report" in the Appendix.



*4.1.3.9 The Vendor must keep records a minimum of one inch off the floor with the optimum of three inches. Records must be stored away from windows, steam, sewer or water pipes.*

Iron Mountain complies with this requirement.

*4.1.3.10 The Vendor must provide a moisture detection system throughout the storage facility.*

Moisture detection is in place in some of Iron Mountain's specialty storage environments and in our data centers.

*4.1.3.11 The Vendor must minimize light exposure by providing motion detectors and timers for the lighting system throughout the storage room.*

The lighting in our West Virginia storage facilities operates on timers.

*4.1.4 The State records can only be viewed by authorized parties. Authorized parties will be approved by Agency directors and department heads. The Vendor's facility must be secured to allow access to those approved to retrieve/view documents for their respective Agency. The Vendor must implement and document policies and procedures for accessing the records in the facility.*

Iron Mountain complies with this requirement. All record centers, including on-site reference rooms, are secure and protected from unauthorized access.

The following visitor procedures apply to every Iron Mountain record center:

- Requests to access records by parties other than customer personnel known to Iron Mountain employees must be written on company letterhead and signed by an authorized party.
- Iron Mountain maintains a list of individuals authorized to request retrievals, approve destruction and otherwise represent customers regarding their records program.
- Visitors must present identification upon entering an Iron Mountain record center; telephone verification may result if credentials are not in order.
- An Iron Mountain employee assists visitors during record center visits, a procedure that ensures both service quality and accountability.
- Visitors are escorted while in the record center and must display visitor badges at all times.
- Retrievals are brought to a conference room or audit area for review, photocopying or fax services.
- Visitors are not permitted unescorted access to storage areas; visitor access is restricted to conference areas only.

*4.1.4.1 Proof documenting the system must be submitted prior to award.*

Iron Mountain will comply with this requirement; the relevant documentation will be provided upon award.

*Indexing and Invoicing:*

*4.1.5 The Vendor must provide indexing for each box or file submitted. The Vendor must provide a minimum of 60 characters per box or per file.*

Iron Mountain complies with this requirement.

*4.1.5.1 The Vendor is required to index all received documents from State Agencies and furnish a report to the Department of Administration upon award that explain the indexing system and describes the location of all documents by Agency.*

At this time, most of the documents Iron Mountain stores for the state are indexed at the box level. Certain accounts are currently set up to use file-level indexing. We anticipate a continuation of the existing indexing practices but will be happy to review with you if the requirements change.

*4.1.6 The Vendor must invoice each state Agency storing records at the facility monthly in arrears.*

Iron Mountain invoices for services in arrears, and for storage in advance.

*4.1.7 The Vendor must invoice according to the prices and categories contained in this solicitation and the Vendor's response. When the Vendor must ship the materials to the Agency location, the costs for postage will be invoiced as a pass-through charge. The shipping invoice must be provided within 5 days of service being completed.*

Iron Mountain does not anticipate the need for third-party shipping; deliveries and pickups will be made with Iron Mountain personnel and vehicles. The State will be invoiced according to the contracted prices.

*4.1.8 The Vendor must provide a log of personnel or visitors that have accessed documents identified as regulated upon agency request.*

Iron Mountain complies with this requirement; inventory activity is captured in our system, and activity reports may be retrieved at any time through Iron Mountain Connect.

- 4.1.9 *The Vendor must provide the Department of Administration with monthly reports showing the Agencies storing documents in the facility during that month and listing the total amount of cubic feet of storage and extended cost for each Agency.*

Iron Mountain complies with these requirements; summary reports are included with each monthly invoice, and more detailed reporting is available online at any time through Iron Mountain Connect.

- 4.1.10 *The Vendor must include on their monthly invoice to the Agency all billing activity detail for the month.*

Iron Mountain complies with these requirements; summary reports are included with each monthly invoice, and more detailed reporting is available online at any time through Iron Mountain Connect.

#### *Requirements and Pricing for Storage, Retrieval, and Destruction*

- 4.1.11 *Contract Item #1: The Vendor must transfer existing records to the new storage facility. Cost Per Cubic Foot.*

Not applicable; since Iron Mountain is the incumbent supplier, the existing inventory will not need to be transferred.

- 4.1.12 *Contract Item #2: The Vendor must index existing records. Cost Per Cubic Foot.*

Not applicable; since Iron Mountain is the incumbent supplier, the existing inventory will not need to be indexed. Indexing services are available for new inventory as needed.

- 4.1.13 *Contract Item #3: The Vendor must accommodate storage of a minimum of 230,000 cubic feet for the State's records. Monthly Cost Per Cubic Foot.*

Iron Mountain complies with this requirement. We have provided the storage rate per cubic foot in our completed pricing sheet.

- 4.1.13.1 *The Vendor must invoice each state Agency storing records at the facility monthly in arrears.*

Iron Mountain invoices for services in arrears, and for storage in advance.

- 4.1.14 *Contract Item #4: The Vendor must provide storage boxes; Dimensions: 10"W x 12"L x 15"H. Cost Per Box.*

Iron Mountain complies with this requirement. We have provided the price per box in our completed pricing sheet.

4.1.15 *Contract Item #5: The Vendor must pick up the records within a maximum of five (5) business days after written notification by the Agency. Vendor to provide Cost Per Box.*

Iron Mountain complies with this requirement. We have provided pickup service pricing in our completed pricing sheet.

4.1.16 *Contract Item #6: The Vendor must index all new records. Vendor to provide Cost Per Box.*

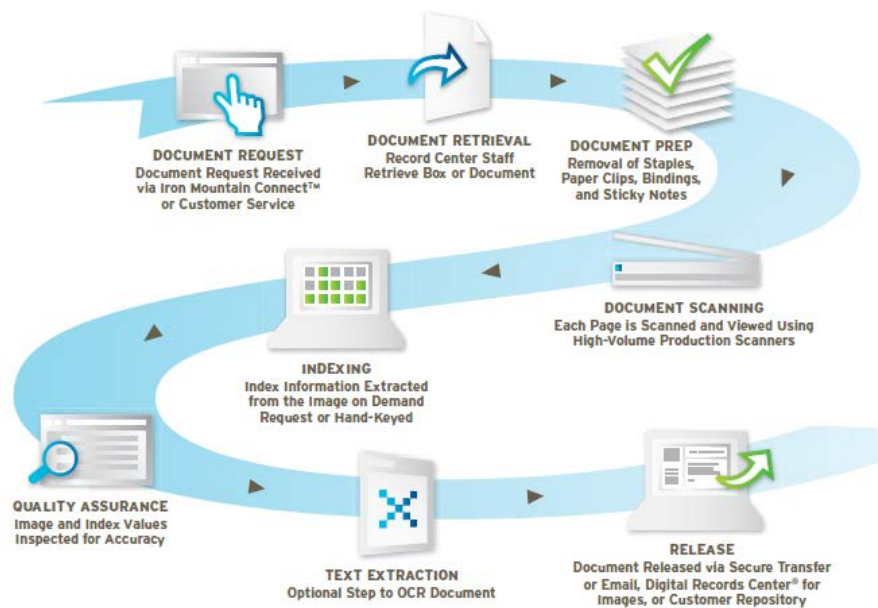
All new records will be indexed at the box level. We have provided the indexing labor rate in our completed pricing sheet. Alternatively, your authorized users may enter data about each new box into Iron Mountain Connect.

4.1.17 *Contract Item #7: The Vendor must retrieve any documents in storage and provide a digitalized version of the documents when requested by any Agency within a maximum of three (3) business days. The request must be completed during normal business hours.*

Iron Mountain can comply with this requirement utilizing our Image on Demand Service.

Image on Demand serves as an alternative document delivery service for current Iron Mountain box or open-shelf storage customers. This delivery service can be used in tandem with the more traditional delivery methods like box, file or fax.

With Image on Demand, you begin by using our web-based Iron Mountain Connect to select the document you want imaged. Our team at Iron Mountain then carefully retrieves, prepares and scans the document. Once the pages are scanned, each image is checked for clarity and readability. Any image that does not meet Iron Mountain's quality standards is rescanned. We then return the loose document to its original carrier and return it to its original storage location.



**Figure 1: Iron Mountain's Image on Demand program is delivered as a pay-as-you-go service model that requires no up-front investment from your organization.**

*4.1.17.1 Contract Item #7.1: Vendor to provide Flat Rate Cost Per Each Request for 1-50 pages*

Please see our completed pricing sheet.

*4.1.17.2 Contract Item #7.2: Vendor to provide Flat Rate Cost Per Each Request for 51 -200 pages*

Please see our completed pricing sheet.

*4.1.17.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.*

Once a document is scanned you can choose to access it via a secure FTP site, have it emailed as a securely encrypted hyperlink or email attachment, or securely hosted — with anytime access — via our Web-based hosted repository, the Digital Record Center® for Images. If you already have an electronic document management system in place, we can create and transmit the electronic document in a format that can be easily translated into your system. No matter how the document is transmitted, you can be sure it will be delivered quickly and safely without the original record ever leaving the security of the Iron Mountain facility.

*4.1.18 Contract Item #8: The Vendor must retrieve any documents in storage and provide a digitalized version of the documents when requested by an Agency sending a written Emergency notification within a maximum of one (1) business day.*

Iron Mountain will comply with this requirement.

*4.1.18.1 Contract Item #8.1: Vendor to provide Flat Rate Cost Per Each Request for 1-50 pages*

Please see our completed pricing sheet.

*4.1.18.2 Contract Item #8.2: Vendor to provide Flat Rate Cost Per Each Request for 51 -200 pages*

Please see our completed pricing sheet.

*4.1.18.3 The Vendor must upload the digitalized document to a secure server and provide a hyperlink to the customer by email so the document can be accessed.*

Iron Mountain complies with this requirement. Once a document is scanned you can choose to access it via a secure FTP site, have it emailed as a securely encrypted hyperlink or email attachment, or securely hosted — with anytime access — via our Web-based hosted repository, the Digital Record Center® for Images.

4.1.19 *Contract Item #9: The Vendor must retrieve any document in storage and hand deliver it to the requesting Agency within three (3) business days of written notification. Documents must be delivered during normal business hours. Documents containing confidential information must be signed for by authorized personnel.*

Iron Mountain complies with these requirements. Our standard service level agreements are:

- **Next Day** — Orders placed by 3 pm will be delivered by next business day (50 items or less)
- **Half Day** — Orders placed by 10 am will be delivered same day and orders placed by 3 pm will be delivered by 12 noon next business day (50 items or less)
- **Rush** — Orders will be delivered within 3 hours\* of receipt (40 items or less within 30 miles) \* *With consideration for any heavy traffic situations*
- **After Hours** — Orders will be delivered within 4 hours of receipt (40 items or less within 30 miles)

All deliveries must be signed for by authorized personnel.

4.1.19.1 *Contract Item #9.1: Vendor to Provide Flat Rate Cost Per Each Request for 1-50 pages*

Please see our completed pricing sheet.

4.1.19.2 *Contract Item #9.2: Vendor to Provide Flat Rate Cost per Each Request for 51 -200 pages*

Please see our completed pricing sheet.

4.1.20 *Contract Item #10: The Vendor must retrieve any document in storage and deliver it to requesting Agency within one (1) business day if it is an Emergency. The Agency's authorized point of contact will notify the vendor in writing when it is an Emergency.*

Iron Mountain complies with this requirement. Our SLA for "rush" delivery is three hours or less.

4.1.20.1 *Contract Item #10.1: Cost Per Each Request for 1-50 pages*

Please see our completed pricing sheet.

4.1.20.2 *Contract Item #10.2: Cost Per Each Request for 51 - 200 pages*

Please see our completed pricing sheet.

4.1.21 *Contract Item #11: The Vendor must provide destruction of specified documents at the Agency's written request. Documents must be destroyed by a crosscut shredder for paper documents. Vendor to provide Cost Per Box*

When you need to have stored records destroyed, the process must be accurate and secure. Iron Mountain takes exceptional care on both counts. First you determine the records you want

destroyed. Or, if you are using our advanced retention services, we can provide you with a *Destruction Eligibility Report* that lists the records due for destruction. Either way, you review and verify the records to be destroyed. Then, before proceeding, we send a destruction list to you for final approval. This step provides an additional layer of control to ensure that only approved items are authorized for destruction. We don't proceed until we have a confirmation and authorized signature.

Please see our completed pricing sheet for the pricing for this service.

Iron Mountain's destruction services facilitate the management of your storage program costs while helping your organization meet its legal and regulatory obligations.

- **Automated Destruction Eligibility Reporting:** Our services can help you systematically manage the lifecycle of your inventory based on your personalized retention schedule. You can easily identify which records can be safely destroyed in accordance with your organization's compliance obligations — as well as which records you need to keep for litigation, audit, or other reasons to ensure compliance.
- **Secure Destruction Checks and Balances:** We utilize multiple checks and balances to make sure that only the right items are ultimately destroyed. Destruction only proceeds after careful review and authorization by you and by Iron Mountain. As items are pulled from their shelves, we scan both the original carton label plus a specially colored destruction label to validate that the correct item has been pulled. Items staged for destruction are secured in black plastic wrap, and ultimately destroyed using Iron Mountain's Secure Shredding services.

The workflow sequence is as follows:

#### RECORDS MANAGEMENT WORKFLOW | ARCHIVAL DESTRUCTION

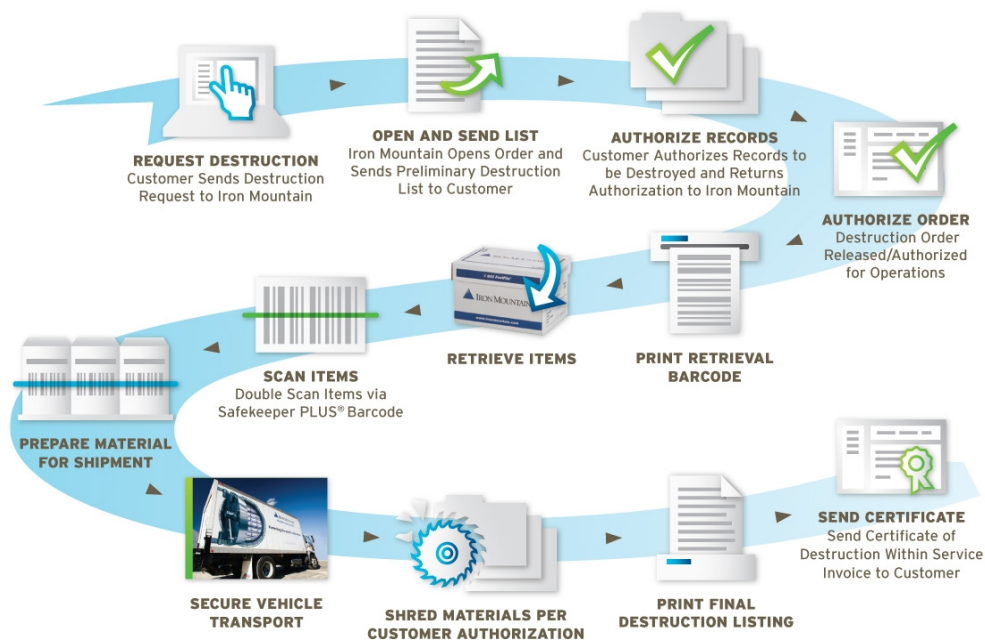


Figure 2: No records are destroyed without signed authorization from you.

- **Assign Destruction Review Dates:** The inventory tracking system calculates the Destruction Review Date for each container based on its classification code and base date information, or by utilizing dates provided by the customer.
- **Generate Destruction Eligibility Report:** The system generates a list of containers eligible for disposal and presents it for your review. The Destruction Eligibility Report provides a section in which you can indicate special instructions for each container: you may instruct us not to destroy the container, or you may make changes to Disposal Dates or Retention Codes (if applicable).
- **Modify/Authorize the Containers on the Report:** Iron Mountain receives the signed Destruction Eligibility report from you. Any changes you have made are entered and reviewed by a supervisor.
- **Print Destruction Labels:** The system generates container destruction labels. The labels identify containers that are part of the group to be destroyed according to the Destruction Order. The labels also visually distinguish containers to be destroyed from other containers.
- **Verify Picked Items on Dock:** We use barcode scanners to verify that the containers pulled are those authorized on the Destruction Order, using a double-scan confirmation process to guarantee accuracy. If a container is scanned that is not on the Destruction Order, an exception is generated and must be resolved.
- **Close Destruction Order:** In order to close the destruction order, Iron Mountain requires that all authorized containers have been picked and verified and that no unauthorized containers have been inadvertently picked and verified. The system cannot issue a Final Destruction Report to you for destruction services until the Destruction Order is closed.
- **Destruction Report:** We provide a Destruction Certificate report after the completion of each disposal.

4.1.22 *Contract Item #12: The Vendor must provide destruction of Microfilm at the Agency's request. Microfilm must be shredded at a minimum of 1/35" strip or smaller. Vendor to provide Cost Per Box*

Iron Mountain utilizes incineration rather than shredding for plastic media destruction. Please see our completed pricing sheet for the cost for this service.

*Qualifications:*

4.1.23 *Vendor must be Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) compliant. Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response.*

As a valued Business Associate to numerous HIPAA Covered Entities, Iron Mountain has long provided them with HIPAA Privacy and Security Rule compliant services, and fully expects to continue to do so as the HITECH Act changes to HIPAA come into effect over the next several years.



### ***Current HIPAA Privacy and Security Compliance Program***

Iron Mountain has long maintained a HIPAA compliance program to appropriately protect the privacy and security of individually identifiable health information in our possession. This program incorporates the physical, organizational, and technical security controls required of business associates by our customer contracts and the Security Rule. Iron Mountain's security program is comprehensive and includes dedicated security resources, mandatory safety and security policies, regular audits, and effective employee training and management oversight. Our facilities meet privacy regulation requirements and include physical access controls, intrusion detection systems and advanced fire suppression controls. We strictly enforce processes governing access to our buildings, and maintain a highly secure chain of custody for all patient information under our care.

In addition, to address the requirements of our customer contracts and the Privacy Rule, we carefully control and monitor all uses and disclosures of the protected health information (PHI) in our possession, and restrict access to that information to those necessary to deliver our services. These restrictions are reinforced through our policies, procedures, and training.

While Iron Mountain will work with each individual customer to determine their service levels, in general you may expect Iron Mountain's HIPAA-compliant services to follow these guidelines:

- Iron Mountain only uses and discloses customer PHI for the purpose of delivering its services.
- We physically restrict access to customer PHI during transit, storage, and disposal. Digitally stored patient information receives the additional benefit of strong technical controls over access.
- Iron Mountain maintains a regular dialogue with our customers regarding the privacy and security of their protected health information.

### ***A Sampling of our HIPAA Compliance Measures***

In response to the new regulations, Iron Mountain undertook and completed an extensive compliance assessment of each of our service lines regarding HIPAA's Privacy and Security Rule requirements. We also performed an enterprise-wide risk management analysis and have used this data to drive additional investments in our business operations.

These measures resulted in a number of new operating procedures as part of our HIPAA enforcement, including:

- HIPAA-compliant Business Associate Agreements with all of our third-party vendors who handle PHI
- Redesigned methods and procedures to reduce risk
- Documented procedures and workflows posted throughout our facilities
- Updated HIPAA training for all Iron Mountain employees and specific job functions that handle PHI to deliver our services

In addition, as new rules and guidelines are issued under the HITECH Act's requirements, and new provisions come into effect, Iron Mountain is committed to taking whatever steps are necessary to be in compliance with these requirements.

Iron Mountain does not obtain third party attestation of HIPAA compliance.

*4.1.24 Vendor must follow the guidelines set forth by the National Institute of Standards and Technology Special Publication 800-53. Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response.*

While our security program does not specially align with these guidelines and we do not have a certification specific to this publication, Iron Mountain does have a very robust security program related to our business offerings and is also certified in PCI DSS and has a SOC2 certification. We have attached our PCI Attestation of Compliance in the Appendix. The SOC2 is a comprehensive report that lists the results of an audit by EY, our independent Big 4 accounting firm, over our Records Management, Data Management, and Shred Services system relevant to Security, Confidentiality, and Availability. This audit is conducted based on the criteria set forth by the AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy*. The audit lists all the details of operations from entity level controls to specific operations in the facility (e.g. scanning) and provides a significant level of assurance over operations. Please let us know if you would like a copy of this report, and we can provide once proper NDA/Confidentiality agreement is in place.

*4.1.25 Vendor must follow the Internal Revenue Service Publication 1075 Tax Information Security Guidelines. Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response.*

Based on the services provided, we do not believe that the Internal Revenue Service Publication 1075 Tax Information Security Guidelines is applicable, and we can confirm that we do not specifically align with these guidelines. While our security program does not specially align with these guidelines and we do not have a certification specific to this publication, Iron Mountain does have a very robust security program related to our business offerings and is also certified in PCI DSS and has a SOC2 certification. We have attached our PCI Attestation of Compliance in the Appendix.

*4.1.26 Vendor must follow Title 45, Public Welfare of the Code of Federal Regulations (CFR). Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response.*

Based on the services provided, we do not believe that this regulation is applicable.

Iron Mountain's security practices are guided by high corporate standards and driven by business-focused teams that are dedicated to safeguarding information and assets — now and in the years ahead.

The compliance experts within our Information Security team are dedicated to ensuring that Iron Mountain adheres to various governmental and regulatory requirements. In particular, proving Payment Card Industry (PCI) and Financial Institution Shared Assessment Program (FISAP) compliance here at Iron Mountain has been an important achievement, as it enables our customers to demonstrate compliance to their auditors. Iron Mountain is a participating member of the PCI Security Standards Council and one of the founding members of FISAP.

Our Security Assurance Reference Guide, included in the Appendix, provides details about our security programs.

*4.1.27 Vendor must follow the Payment Card Industry Data Security Standards (PCI DSS). Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response, upon request.*

Iron Mountain complies with this requirement. Our Attestation of Compliance is enclosed in the Appendix.

*4.1.28 All storage procedures must follow industry standard guidelines established by the Association of Records Managers and Administrators (ARMA). ARMA has published guidelines for records management- ANSI/ARMA 8-2005 Retention Management for Records and Information. Vendor must provide proof of compliance from a third party security assessment within the last 365 days with bid response.*

Iron Mountain subscribes to and supports the policies of ARMA International but does not seek third-party assessments related to our compliance with ARMA guidelines for records management.

*4.1.29 All Records Center employees must undergo an NCIC (national) background check as a condition of employment, as well as industry-standard privacy training. Proof of documentation must be submitted upon award.*

Iron Mountain's pre-employment hiring procedures in the United States 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, either on or off the job. The first step in the Iron Mountain background investigation process is the pre-employment drug test. This consists of a five-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:

- Marijuana metabolites
- Cocaine metabolites
- Opiate metabolites
- Phencyclidine (PCP)
- 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. Should a candidate fail the pre-employment test, no further employment consideration is given.

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 the applicant signs a written offer letter, a criminal background check is then conducted in all counties/states where the applicant has resided and 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.

Individuals with convictions pertaining to any drug/narcotics offense, any financial and abuse of trust crime, any crime of violence to include domestic assault and weapons crimes, and crimes involving theft within the review period are generally not eligible for employment. Further, applicants found to have been incarcerated for any of the aforementioned crimes at any time during the ten-year search period are also generally not be eligible for employment with Iron Mountain.

Individuals convicted of the crimes of arson, murder, rape, sexual assault, acts of terrorism, or identity theft are not eligible for employment.

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 is comprised of over 300 million records from, among others: the 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. Currently this search includes information from 49 states' Sex Offender Registries plus the District of Columbia, Puerto Rico and Guam; 39 states' Department of Corrections sources; 13 states' Administrative Office of the Courts sources; plus multiple online county records. In addition, this search contains a review of 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. This review is conducted annually.

#### **Employment Verifications**

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

#### **Education Verifications**

If an applicant claims education beyond high school (undergraduate, graduate, vocational), Iron Mountain will confirm the highest degree awarded.

#### **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 years are reviewed and adjudicated based upon seriousness of the offense and frequency of occurrence. For example, any conviction for Operating Under the Influence of Drugs or Alcohol is an automatic disqualification. All drivers are subject to an annual motor vehicle records check.

#### **Authorization to Work in the United States**

Iron Mountain subscribes to the Department of Homeland Security's E-Verify system in order to confirm that all employees are duly authorized to work in the United States. We also use this process where required to validate citizenship status for export control regulation (e.g. EAR, ITAR, etc.) compliance.

### **5. CONTRACT AWARD:**

Iron Mountain acknowledges and agrees to the requirements in section 5.

## 6. ORDERING AND PAYMENT:

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

Orders for pickup and delivery service may be made over the phone, via email or fax, or through the Iron Mountain Connect online system.

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

Iron Mountain agrees to this requirement.

## 7. DELIVERY AND RETURN:

7.1 *Delivery Time: Vendor shall deliver standard orders within fifteen (15) working days after orders are received. Vendor shall deliver emergency orders within three (3) working day(s) after orders are received. Vendor shall ship all orders in accordance with the above schedule and shall not hold orders until a minimum delivery quantity is met.*

Iron Mountain's standard service level agreements are:

- **Next Day** — Orders placed by 3 pm will be delivered by next business day (50 items or less)
- **Half Day** — Orders placed by 10 am will be delivered same day and orders placed by 3 pm will be delivered by 12 noon next business day (50 items or less)
- **Rush** — Orders will be delivered within 3 hours\* of receipt (40 items or less within 30 miles) \* *With consideration for any heavy traffic situations*
- **After Hours** — Orders will be delivered within 4 hours of receipt (40 items or less within 30 miles)

7.2 *Late Delivery: The Agency placing the order under this Contract must be notified in writing if orders will be delayed for any reason. Any delay in delivery that could cause harm to an Agency will be grounds for cancellation of the delayed order, and/or obtaining the items ordered from a third party. Any Agency seeking to obtain items from a third party under this provision must first obtain approval of the Purchasing Division.*

Ordering from a third party does not apply to the service model in place for this contract.

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

*pay delivery charges on all emergency orders provided that Vendor invoices those delivery costs as a separate charge with the original freight bill attached to the invoice.*

Iron Mountain will charge for retrievals and deliveries according to the contract rates for these services.

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

Not applicable; the only items being delivered under this contract are Agency records that are requested to be returned from storage and not items for purchase.

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

Not applicable; the only items being delivered under this contract are Agency records that are requested to be returned from storage and not items for purchase.

## 8. VENDOR DEFAULT:

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

- 8.1.1 Failure to provide Contract Items in accordance with the requirements contained herein.*
- 8.1.2 Failure to comply with other specifications and requirements contained herein.*
- 8.1.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.*
- 8.1.4 Failure to remedy deficient performance upon request.*

Iron Mountain accepts the terms in section 8.1.

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

- 8.2.1 Immediate cancellation of the Contract.*
- 8.2.2 Immediate cancellation of one or more release orders issued under this Contract.*
- 8.2.3 Any other remedies available in law or equity.*

Iron Mountain accepts the terms in section 8.1.

9. MISCELLANEOUS:

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

Not applicable; the only items being delivered under this contract are Agency records that are requested to be returned from storage and not items for purchase.

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

Not applicable; the only items being delivered under this contract are Agency records that are requested to be returned from storage and not items for purchase.

If Iron Mountain performs services not listed in the RFP price list, the Iron Mountain standard rate will apply; details available on request.



# GENERAL TERMS AND CONDITIONS



## AMENDMENT TO REQUEST FOR QUOTATION FOR RECORDS MANAGEMENT SERVICES STATE OF WEST VIRGINIA Bid No.: CRFQ 0212 SWC1600000008

In the event that the State of West Virginia (the “State” or “Customer”) awards a contract to Iron Mountain Information Management, LLC (“Iron Mountain” or “Vendor”) as a result of this Request for Quotation (“RFQ”), the terms and conditions of such resulting contract shall be mutually agreed, based upon good faith negotiations between the parties, notwithstanding anything to the contrary in the RFQ. Iron Mountain requests that the following key exceptions and additional industry standard terms and conditions form a part of that discussion.

### **A. Iron Mountain requests the following amendments and/or key exceptions to the General Terms and Conditions contained within the RFQ:**

1. Section 14, Payment. *Note: Storage charges are billed each month in advance. Other service charges are billed in arrears. Standard payment terms are net 30.*
2. Section 17, Time, is deleted in its entirety.
3. Section 36, Indemnification, is deleted in its entirety and replaced with the following:  
  
“Vendor agrees to indemnify the State with respect to any third party claim or demand for bodily injury (including death) or loss of or damage to tangible property (excluding stored materials or materials delivered to Vendor for services, the liability for which is limited elsewhere herein), to the extent based upon the negligent acts or omissions of Vendor, provided that the State provides Vendor prompt written notice of any such claim or demand. Vendor’s sole obligation hereunder shall be to pay any judgment rendered, or settlement made, as a result of any such claim or demand.”
4. Section 38, Additional Agency and Local Government Use. *Note: The requirements in this section require further review and discussion.*
5. Section 41, Background Check. *Note: Please see section 4.1.29 of RFQ response for details of Iron Mountain’s Background Check policies and procedures.*

### **B. Iron Mountain requests that the following customary industry terms and conditions be added to any resulting contract between the parties:**

1. **Limitation of Liability.** Notwithstanding anything to the contrary in this Agreement or any document referenced herein, this section entitled “Limitation of Liability” shall control with respect to Iron Mountain’s liability in connection with the Deposits and related data. For the purposes of this Agreement, Customer declares the following values for items stored under this Agreement (“Deposits”): (a) for hard-copy

records, \$1.00 per carton, linear foot of open-shelf files or other storage pricing unit, and (b) for media, the cost of replacing the physical item (each a "Declared Value"). Customer acknowledges that it has declined to declare an excess valuation, for which an excess valuation fee would have been charged. Iron Mountain shall not be liable under this Agreement, with respect to any claims related to the Deposits and data therein or with respect to any non-storage services or electronic storage services performed, unless Iron Mountain fails to exercise such care as a reasonably careful person would exercise under like circumstances. If liable, the amount of Iron Mountain's liability is limited as follows: (i) with respect to Deposits and related data, Iron Mountain's liability is limited to the Declared Value; and (ii) with respect to non-storage services and electronic storage services and data related to each, Iron Mountain's liability is limited to six (6) months of fees paid by Customer for the particular service that gave rise to the claim. Deposits and data are not insured by Iron Mountain against loss or damage, however caused. If Deposits and/or data are placed in the custody of a third-party carrier for transportation, the carrier shall be solely responsible for any claim related to the Deposits and/or data while in the custody of the carrier. In no event shall either party be liable for any consequential, incidental, special or punitive damages, or for loss of profits or loss or interruption of business, or the cost of recreating any data or information, regardless of whether an action is brought in tort, contract or under any other theory of liability.

2. **Operational Procedures.** Customer shall comply with Iron Mountain's reasonable operational requirements, as modified from time to time, regarding cartons, carton integrity, delivery/pickup volumes, preparation for pickup, security, secure shredding protocols, access and similar matters. Extraordinary volume requests may involve additional costs, such as overtime, which Customer will pay at Iron Mountain's overtime rates, provided Customer consents to such costs in advance.
3. **Governmental Orders.** Iron Mountain is authorized to comply with any subpoena or similar order related to the materials provided to it by Customer, at Customer's expense, provided that Iron Mountain notifies Customer promptly upon receipt thereof, unless such notice is prohibited by law. Iron Mountain will cooperate with Customer's efforts to quash or limit any subpoena, at Customer's expense.
4. **Ownership Warranty.** Customer warrants that it is the owner or legal custodian of the materials provided to Iron Mountain and has full authority to direct their disposition in accordance with the terms of this Agreement. Customer shall reimburse Iron Mountain for any expenses reasonably incurred by Iron Mountain (including reasonable legal fees) by reason of Iron Mountain's compliance with the instructions of Customer in the event of a dispute concerning the ownership, custody or disposition of Customer's materials provided by Customer to Iron Mountain.
5. **Safe Materials and Premises.** Customer shall not store with Iron Mountain nor deliver to Iron Mountain for shredding any material that is highly flammable, explosive, hazardous, toxic, radioactive, medical waste, organic material which may attract vermin or insects, or otherwise dangerous or unsafe to store or handle, or any material which is regulated under any federal or state law or regulation relating to the environment. Customer shall not store negotiable instruments, jewelry, check stock or other items that have intrinsic value. Any Customer premises where Iron Mountain employees perform services or make deliveries hereunder shall be free of hazardous substances and any other hazardous or dangerous conditions.

6. **Purchase Orders.** In the event that Customer issues a purchase order to Iron Mountain covering the services provided under this Agreement, any terms and conditions set forth in the purchase order which are in addition to or establish conflicting terms and conditions to those set forth in this Agreement are expressly rejected by Iron Mountain.
7. **Force Majeure.** In no event shall either party be liable for delay or inability to perform caused by acts of God, governmental actions, labor unrest, acts of terrorism, riots, unusual traffic delays or other causes beyond its reasonable control.

Approved as to Form and Legal  
Content:

Iron Mountain Legal Department




Name: Robert Liljedahl

### CERTIFICATION AND SIGNATURE PAGE

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

Iron Mountain

(Company)

 B. TC Menzies DM  
(Authorized Signature) (Representative Name, Title)

724-794-8474 10/14/2016  
(Phone Number) (Fax Number) (Date)

# VENDOR PREFERENCE CERTIFICATE



While Iron Mountain has operations in West Virginia and employs state residents, the location of our corporate headquarters and state of incorporation make us a “non-resident” vendor, and we employ less than 100 people in state. Therefore, we believe that none of the preference options on the Vendor Preference Certificate apply. We would be happy to provide more information about our in-state operations upon request.

STATE OF WEST VIRGINIA  
Purchasing Division

## PURCHASING AFFIDAVIT

**MANDATE:** 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 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  
Authorized Signature: [Signature] Date: 18 May 2016

State of PA

County of Butler, to-wit:

Taken, subscribed, and sworn to before me this 10 day of may, 2016

My Commission expires march 25, 2016

**AFFIX SEAL HERE**

**NOTARY PUBLIC**

[Signature]  
Purchasing Affidavit (Revised 07/01/2012)

COMMONWEALTH OF PENNSYLVANIA

NOTARIAL SEAL

Tyler Summerville, Notary Public

New Sewickley Twp., Beaver County

My Commission Expires March 25, 2020

MEMBER, PENNSYLVANIA ASSOCIATION OF NOTARIES

# IRON MOUNTAIN OVERVIEW

**Iron Mountain Incorporated (NYSE: IRM)** is the global leader in information management services.

## TRUST

Iron Mountain manages billions of information assets for organizations of all sizes in every major industry around the world. More than 92% of the Fortune 1000 rely on Iron Mountain's solutions for records and information management, data management, document imaging, and secure destruction to help them better use their information for business advantage. We're honored that our customers have put their trust in us, relying on us to protect a vast collection of critical and sometimes one-of-a-kind items, such as backup data, loan documents, employee files, pathology slides, geological rock samples, iconic songs, blockbuster films, and more.

## SECURITY

Regardless of the type of asset we're storing or destroying, our commitment is the same – to handle this material as if it were our own. At Iron Mountain, security is a never-ending process of setting safeguards, testing their effectiveness, and continually refining them to get stronger. We do this by:

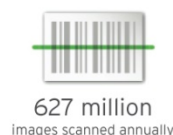
- Investing in and using proven security technology
- Implementing multi-step security checks at our facilities and in all our vehicles
- Screening all job candidates with strict hiring guidelines and intensive legal background checks
- Providing extensive and consistent employee training
- Employing third-party security audits to help detect weaknesses and further enhance our security culture

We abide by the strictest industry standards for safeguarding information and ensuring data privacy. We have received SysTrust® certification, are on the list of compliant service providers published by Visa and the Payment Card Industry, and our Secure Shredding service is "AAA" certified by the National Association for Information Destruction.

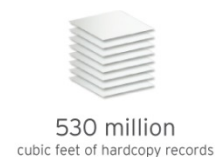
## TRUSTED AND TESTED

At Iron Mountain, trust is our greatest asset. Trust founded our company, globalized our offerings, and solidified our reputation. Our 155,000+ customers trust us to protect what matters most to them. We've invested in the resources to continue to earn that trust in everything we do. Here's a snapshot:

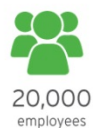
### SERVICES DELIVERED



### INFORMATION MANAGED



### RESOURCES AT THE READY



*"Our responsibility to protect your assets begins when you hand them over to us and doesn't end until we either return them to you or securely destroy them."*



## GLOBAL PRESENCE

Iron Mountain has a global network with local service. Promoting consistency across media and geographies, we service 36 countries on 5 continents:

- More than 1,000 facilities comprising 67.8 million square feet worldwide
- More than 530 million cubic feet of hardcopy records stored
- Over 10 million linear feet of medical records under management
- More than 89 million pieces of media stored in highly secure data protection vaults
- Over 155,000 customer accounts and growing daily plus 3,600+ vehicles making 15 million trips per year worldwide



## 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.

### Records & Information Management

- Records Storage Services
- Vault Storage Services
- Document Imaging & Management
- Inventory Audit with RFID-tagging
- Strategic Information Governance Consulting
- Information Management Services:
  - Healthcare
  - Government
  - Legal
  - Energy
  - Banking/Insurance

### Data Management

- Application and Cloud Services
- Data Center Services
- Restoration and Migration Services
- Disaster Recovery
- Secure Media Vaulting
- Managed Care
- Secure E-Waste and IT Asset Disposition
- Tape Identification / Audit Services
- Intellectual Property Escrow

### Information Destruction Services

- Onsite and Offsite Destruction Services
- Secure Paper, Media, and Film Destruction
- Secure Electronic Waste and IT Asset Disposition

*“At Iron Mountain we are committed to living by our core values and putting them into action every day and in everything we do – from safeguarding our customers’ information to empowering employees, serving our communities, protecting the environment, and delivering attractive stockholder returns.”*



## CORPORATE RESPONSIBILITY: IT'S THE WAY WE DO BUSINESS

At Iron Mountain we are committed to living by our core values and putting them into action every day and in everything we do – from safeguarding our customers' information to empowering employees, serving our communities, and protecting the environment. Please see our [2014 Corporate Responsibility Report](#) for a comprehensive look at our efforts.

### Our Planet

We have a great opportunity to impact the world in a positive way. To do this, we must continuously improve and find innovative solutions that raise the bar for good global citizenship.



**Greenhouse Gas Footprint** While we didn't achieve our goal to reduce company-wide greenhouse gas (GHG) emissions by 5% in 2014 compared to our 2012 baseline, due in part to higher-than-expected use of natural gas during an

exceptionally cold US winter, we've set three environmental goals for 2015: hold GHG emissions flat from 2014, reduce year-over-year facility energy use by 3%, and increase use of renewable energy six-fold to 2.4 million KWH.

**Energy Efficiency** In 2015, we received LEED Gold® certification for our U.S. headquarters in Boston and our newly constructed, highly secure data center just outside Boston. We have installed over 2MW of solar installations at our facilities.

**Fleet** Our routing optimization software allows us to use fewer vehicles and drive fewer miles, reducing our emissions and fuel usage. In 2014 in the US, we installed telematics technology in our vehicles, which collects and transmits real-time performance information on acceleration, idle time, mileage, and cruise control, giving insight into how to further improve fleet performance.

**Operations** In 2013, we established our first waste stream baseline and in 2014, after identifying shrink wrap as the largest component of our waste stream, we tested a reusable and 100% recyclable shrink wrap in four markets. Initial results are favorable.

**Supply Chain** In 2014, we used 8 million boxes made of 65% recycled content and 4.5 million boxes made of 71% recycled content for our customers in North America and Western Europe, respectively.

**Shredding** In 2014, we recycled 10,882 tons of cardboard and 456,059 tons of paper from our US customers through our Secure Shredding services.

**e-Waste** We are an e-Stewards® Enterprise, verifying our commitment to securely destroy, recycle, or dispose of our customers' electronic assets properly. In 2014, we helped our customers responsibly dispose of 1,067,115 pounds of electronics, 8,736,957 pounds of back-up tapes, and 8,398,825 pounds of x-ray film.

### Our Communities and Our People

We created the Living Legacy Initiative to help museums and other nonprofits protect and provide access to our shared cultural and heritage treasures. Some of our recent partners include The Papers of Abraham Lincoln, the City of Boston and the Boston

Marathon memorial, the JFK Presidential Library, The C.H. Booth Library in Newtown, Conn., and CyArk, a non-profit foundation that uses 3-D laser scanners to digitally preserve the world's most important cultural and heritage sites.

Our Moving Mountains volunteer program empowers our employees to support causes they care about by offering paid time off for volunteer work. In 2014, our employees in North

America volunteered over 56,000 hours during work hours or personal time.

We are a founding member of the 100,000 Jobs Mission Coalition, which set out to hire 100,000 US military veterans by 2012. These companies are now committed to hiring 300,000 veterans.

As a result, *GI Jobs* magazine has named us as a Military Friendly company.

We believe in creating an inclusive, supportive culture where all employees feel welcomed, accepted, and free to pursue their full potential both inside and outside the work-

place. Our employee resource groups allow employees to come together based on their shared life experiences and are open to all.



## AWARDS AND RECOGNITION

You can be confident that you're selecting an industry leader with the accolades and awards to back it up.

---

# FORTUNE

Iron Mountain ranks **730<sup>th</sup>** on Fortune Magazine's **Fortune 1000**.

---

# STANDARD & POOR'S

Iron Mountain is a member of the **S&P 500 Index**, the leading bellwether of the U.S. equities market.

---

# SECURITY

SOLUTIONS FOR ENTERPRISE SECURITY LEADERS

Security magazine named Iron Mountain to its 2013 **Security 500 Survey**, an annual ranking of the nation's most secure companies.

---



## FTSE4Good

Iron Mountain was added to the **FTSE4Good Index in 2013** for meeting globally recognized corporate social responsibility standards.

---

# InformationWeek

For the eleventh consecutive year, Iron Mountain made the **InformationWeek 500**, a listing of top technology companies. Iron Mountain **finished at #88** in the 2013 rankings.

---



The corporate research team at Selling Power magazine has ranked Iron Mountain **#5** of the 50 best companies to sell for in 2015.

---

# InfoWorld

InfoWorld magazine named Iron Mountain's Room 48 Data Center to its 2010 **Green 15 List** of the most environmentally friendly technology projects in the world.

---



In 2013, Iron Mountain's Sentinel training program was awarded the **Learning in Practice Gold Award** by Chief Learning Officer magazine. This program fully prepares front-line employees for their daily roles before they work independently and interact with customers and their information.

---

# CONCLUSION



Records and information management is complex. Knowing exactly where to focus to accelerate adoption and achievement of your program goals is overwhelming. Trust in Iron Mountain's solutions and expertise to solve State of West Virginia's evolving challenges now and in the future. No matter where your program is in maturity, you can be sure to have a partner that can provide you solutions to drive improvements that tighten defensibility and harness the power of your records and information for business use.

It will be our pleasure to partner with you to take your program to new heights of performance.

# APPENDIX



- ▶ Addenda Acknowledgement Form
- ▶ Elevation/Flood Zone Report
- ▶ PCI Attestation of Compliance
- ▶ Security Assurance Reference Guide

**ADDENDUM ACKNOWLEDGEMENT FORM**  
**SOLICITATION NO.:** \_\_\_\_\_

**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 checked="" 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 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

Company

\_\_\_\_\_  
 B.T. Menzies DM

Authorized Signature

\_\_\_\_\_  
May 10, 2016

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.  
Revised 6/8/2012



**Client Information:**

**Iron Mountain Incorporated**  
**5736 MacCorkle Avenue Southeast**  
**Charleston, West Virginia, 253041-2804**

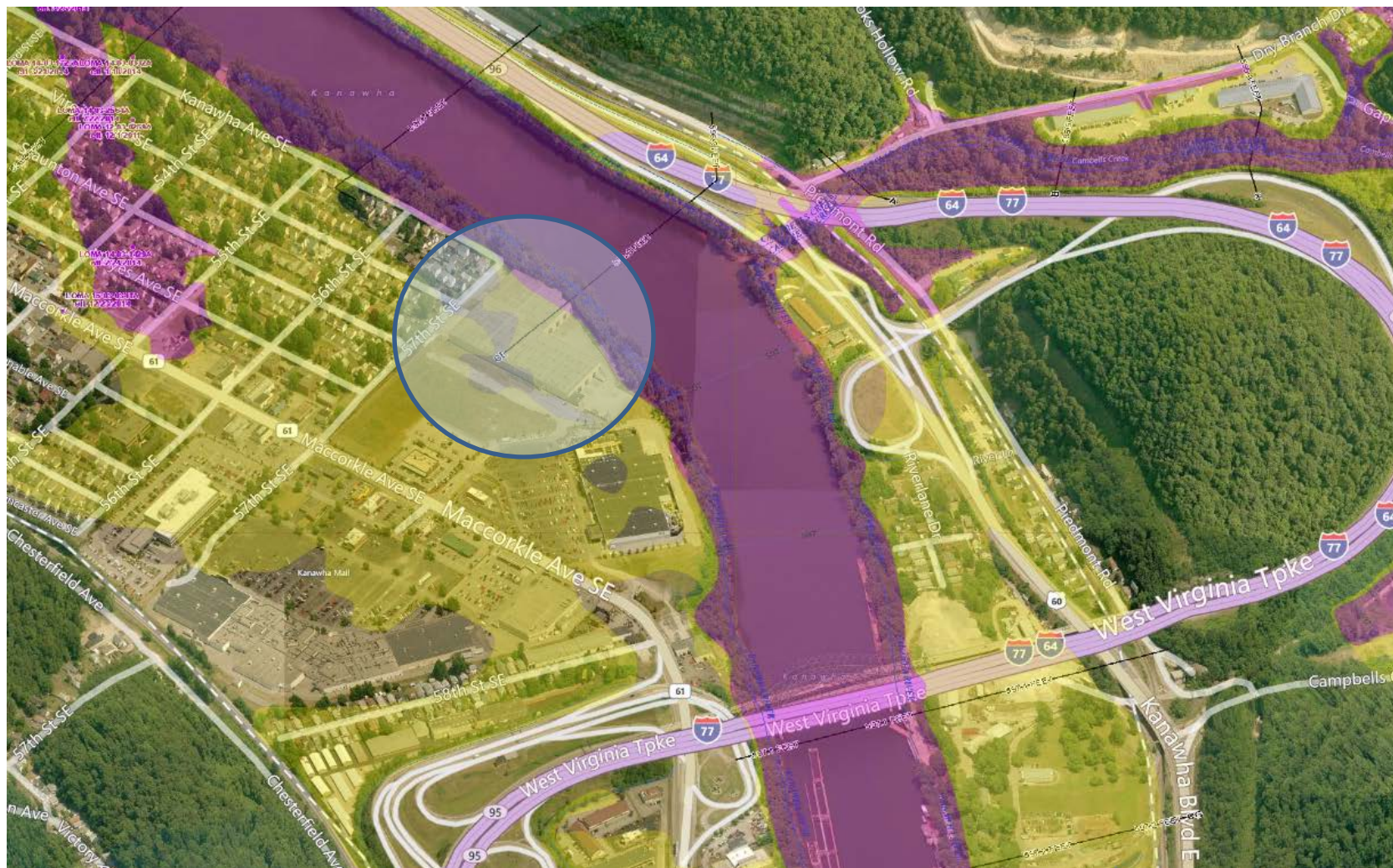
NGVD29 = NAVD 88 + 0.476-ft.

**FEMA Map Data:**

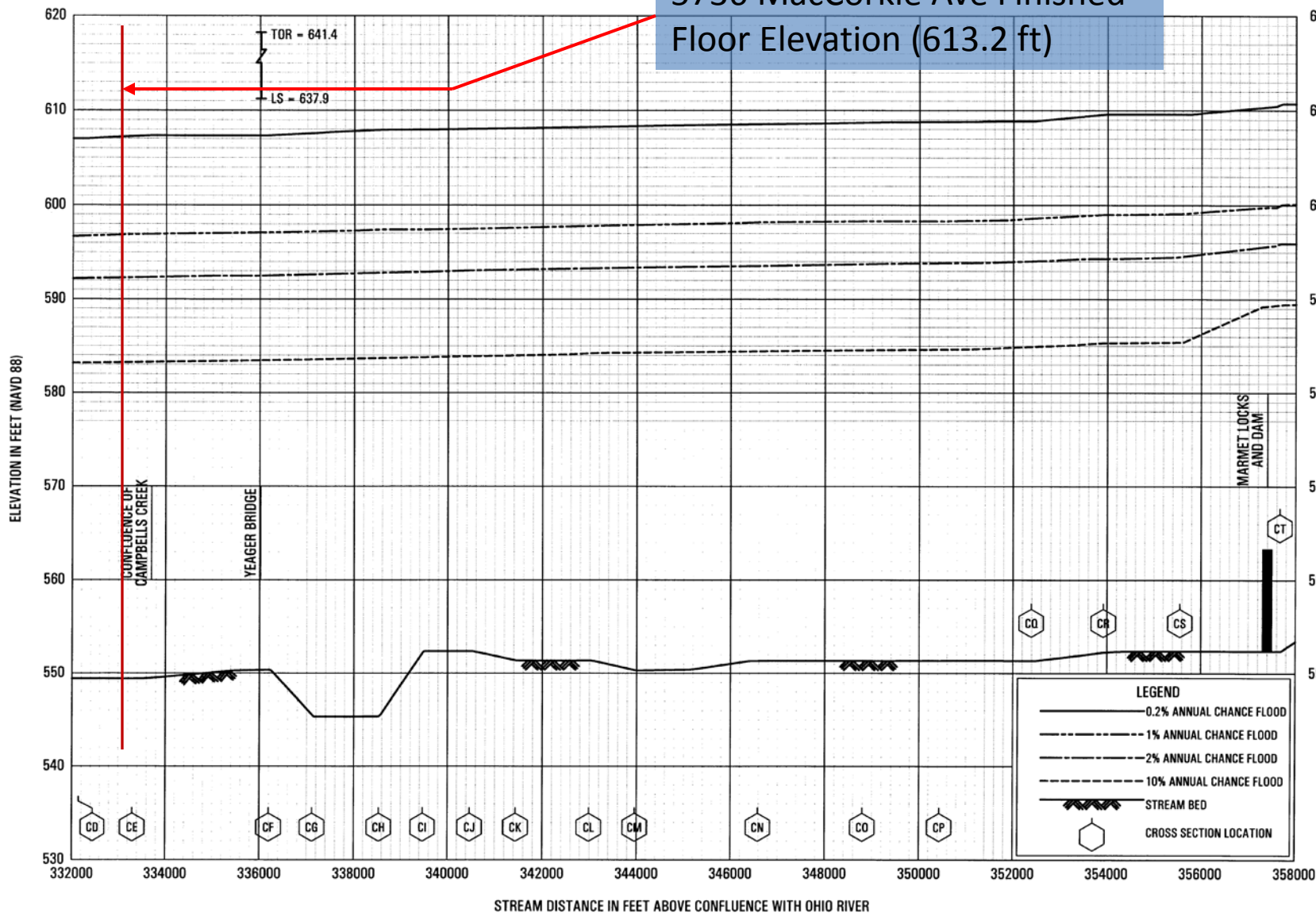
Depth Units	FEET
Vertical Datum	NAVD88
FIRM Map Effective Date	2008-02-08
FIRM Flood Zone Designation	AE
FIP 8 County Identifier	54039
FIRM Panel Identifier	0429E
Community Number	540073
FIRM Community Identifier	039C
BFE Static used for AH zones and coastal flooding scenarios	-9999
Depth used for AO zones	-9999
Floodway Designation	FW
Coastal Barrier Resources Act (COBRA) Zone Designation	COBRA_OUT



**Index: 47748.83-03**



5736 MacCorkle Ave Finished  
Floor Elevation (613.2 ft)





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 MaCcorkle 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.

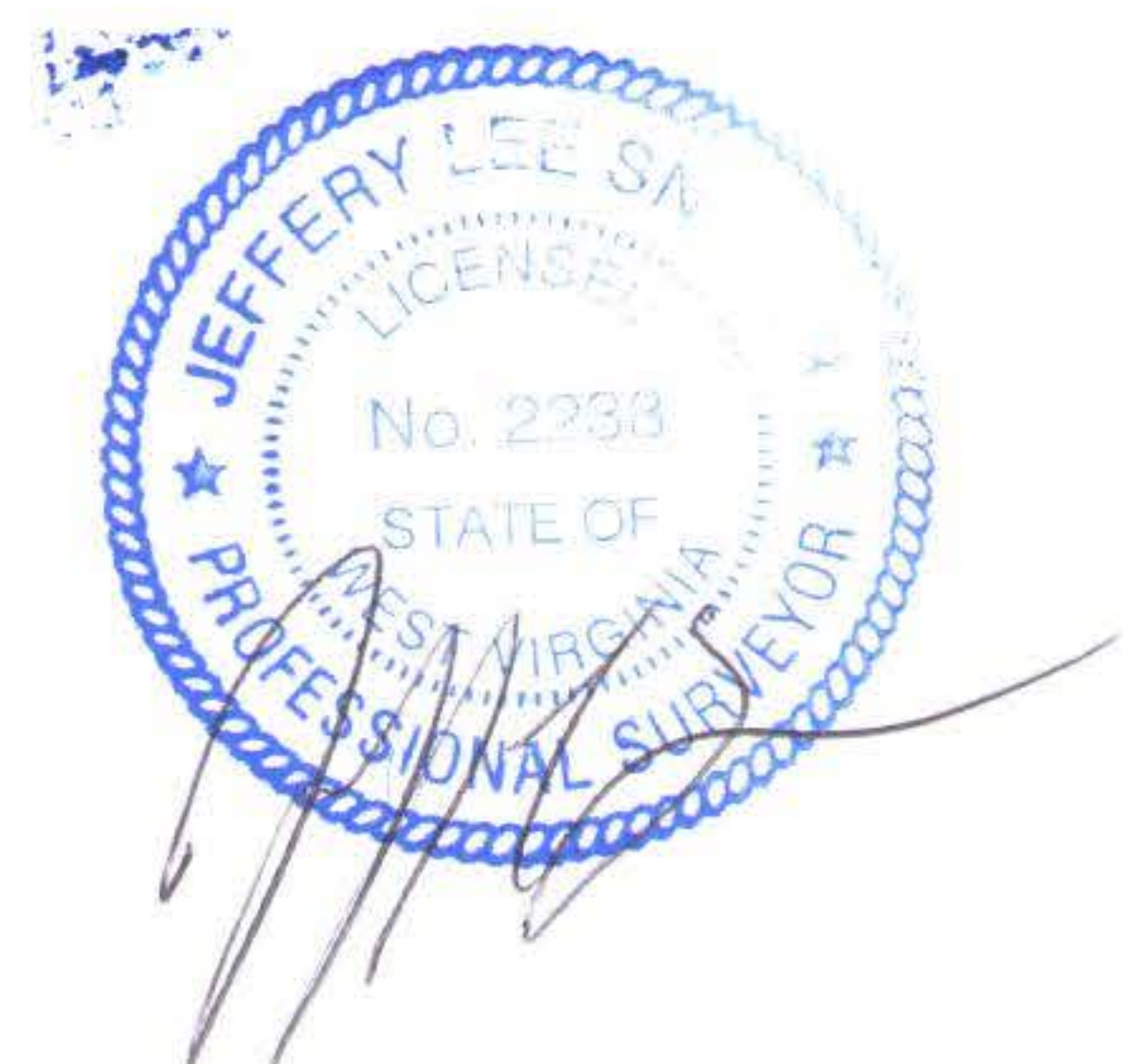
Certified by Jeffery Lee Snyder P.S. 2238

1<sup>st</sup>





2nd



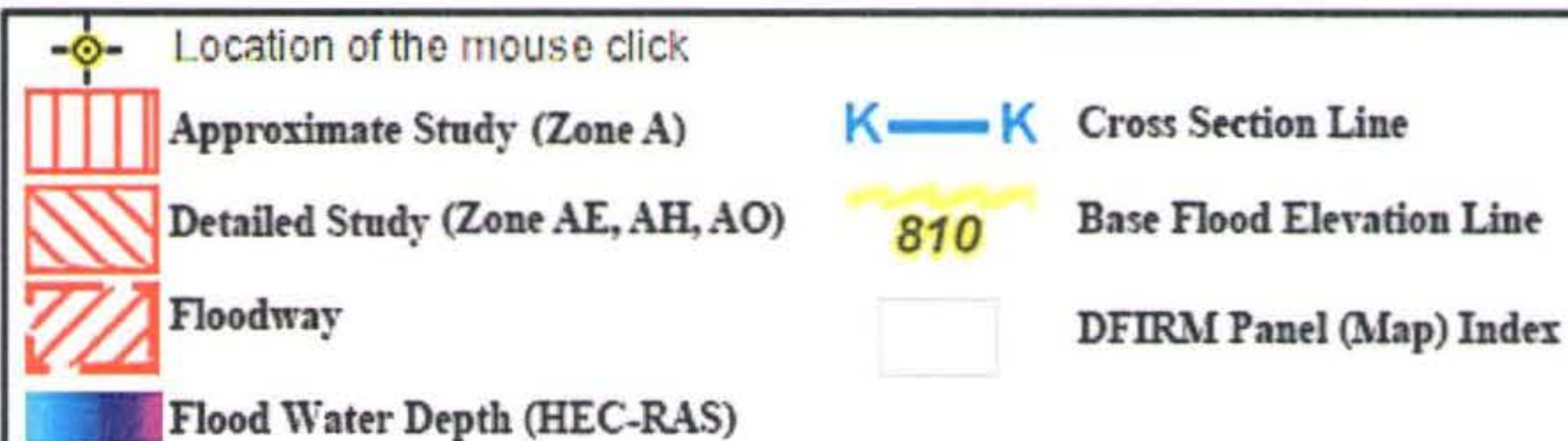


# WV Flood Map



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



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](http://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:





# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.1**

April 2015

## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

#### Part 1. Service Provider and Qualified Security Assessor Information

##### Part 1a. Service Provider Organization Information

Company Name:	Iron Mountain Information Management, Inc		DBA (doing business as):	Iron Mountain		
Contact Name:	Seth R. Bailey		Title:	Director, Information Security		
ISA Name(s) (if applicable):	Not Applicable		Title:	Not Applicable		
Telephone:	(617) 535-4935		E-mail:	seth.bailey@ironmountain.com		
Business Address:	One Federal Street		City:	Boston		
State/Province:	MA	Country:	USA		Zip:	02110
URL:	http:// www.ironmountain.com					

##### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Trustwave				
Lead QSA Contact Name:	Ted Meyer	Title:	Principal Security Consultant		
Telephone:	(312) 873-7500	E-mail:	tmeyer@trustwave.com		
Business Address:	70 W. Madison Street, Suite 1050	City:	Chicago		
State/Province:	IL	Country:	USA	Zip:	60602
URL:	http://www.trustwave.com				

## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment** (check all that apply):

Name of service(s) assessed: Media Vaulting, Records Management, Shredding Services

Type of service(s) assessed:

#### Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

#### Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

#### Payment Processing:

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

☐ Account Management

☐ Fraud and Chargeback

☐ Payment Gateway/Switch

☐ Back-Office Services

☐ Issuer Processing

☐ Prepaid Services

☐ Billing Management

☐ Loyalty Programs

☐ Records Management

☐ Clearing and Settlement

☐ Merchant Services

☐ Tax/Government Payments

☐ Network Provider

☒ Others (specify): Media Vaulting, Records Management, Shredding Services

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) not assessed: Not Applicable

Type of service(s) not assessed:

**Hosting Provider:**

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):

**Managed Services (specify):**

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):

**Payment Processing:**

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Account Management      | <input type="checkbox"/> Fraud and Chargeback | <input type="checkbox"/> Payment Gateway/Switch  |
| <input type="checkbox"/> Back-Office Services    | <input type="checkbox"/> Issuer Processing    | <input type="checkbox"/> Prepaid Services        |
| <input type="checkbox"/> Billing Management      | <input type="checkbox"/> Loyalty Programs     | <input type="checkbox"/> Records Management      |
| <input type="checkbox"/> Clearing and Settlement | <input type="checkbox"/> Merchant Services    | <input type="checkbox"/> Tax/Government Payments |
| <input type="checkbox"/> Network Provider        |   |  |
| <input type="checkbox"/> Others (specify):       |   |  |

Provide a brief explanation why any checked services were not included in the assessment:

**Part 2b. Description of Payment Card Business**

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12. Iron Mountain does not accept credit cards in their media storage and shredding facilities. Iron Mountain has no knowledge of what is being stored by their clients, either electronically or in hard copy.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12. Iron Mountain does not accept credit cards in their media storage and shredding facilities. Iron Mountain has no knowledge of what is being stored by their clients, either electronically or in hard copy.

## Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
Media Vault	6	<ul style="list-style-type: none"> <li>• [REDACTED] San Diego, CA, USA</li> <li>• [REDACTED] Boyers, PA, USA</li> <li>• [REDACTED] Colorado Springs, CO, USA</li> <li>• [REDACTED] Ashland, VA, USA</li> <li>• [REDACTED] Laval, Canada</li> <li>• [REDACTED] Norcross, GA, USA</li> </ul>
Records Management	9	<ul style="list-style-type: none"> <li>• [REDACTED] San Diego, CA, USA</li> <li>• [REDACTED] San Diego, CA, USA</li> <li>• [REDACTED] Cranberry Township, PA, USA</li> <li>• [REDACTED] Boyers, PA, USA</li> <li>• [REDACTED] Denver, CO, USA</li> <li>• [REDACTED] Denver, CO, USA</li> <li>• [REDACTED] Sandston, VA, USA</li> <li>• [REDACTED] Laval, Canada</li> <li>• [REDACTED] Laval, Canada</li> </ul>
Shredding Center	2	<ul style="list-style-type: none"> <li>• [REDACTED] PA, USA</li> <li>• [REDACTED] Montreal, Canada</li> </ul>

## Part 2d. Payment Applications

Does the organization use one or more Payment Applications? ☐ Yes ☒ No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Not Applicable	Not Applicable	Not Applicable	<input type="checkbox"/> Yes <input type="checkbox"/> No	Not Applicable

## Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

- Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12. There are no computer systems, processor connections, or networks in-scope for this Iron Mountain assessment.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

☐ Yes

☒ No

## Part 2f. Third-Party Service Providers

Does your company have a relationship with one or more third-party service providers (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

☒ Yes

☐ No

**If Yes:**

Type of service provider:	Description of services provided:
██████████	Transportation
████	Transportation
██████	Transportation
██████ ████████	Transportation
██████ █████ ██████	Transportation
████ █████	Transportation
██████ █████ ██████	Transportation
████ █████	Transportation
████ █████	Transportation
██████████████████	Transportation
██████████████████	Transportation
██████████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████████	Transportation
██████████	Transportation
██████████	Transportation



██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Transportation
██████████	Shredding
██████████	Shredding
██████████	Shredding
██████████	Shredding

**Note:** Requirement 12.8 applies to all entities in this list.

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed:		Media Vaulting, Records Management, Shredding Services		
PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
Requirement 1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	3.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 4:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	4.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 5:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	5.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 6:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	6.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 7:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	7.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 8:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	8.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.

Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9.1.3.x – No in-scope wireless 9.6.1 – No media classification 9.9.x – No payment devices
Requirement 10:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	10.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 11:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	11.x - Iron Mountain is a media storage and shredding service provider and was only assessed for PCI requirement sections 9 and 12.
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3 - No critical technologies
Appendix A:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Iron Mountain is not a shared hosting provider.

## Section 2: Report on Compliance

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	18 September 2015	
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No

## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

Based on the results noted in the ROC dated 18 September 2015, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of 18 September 2015: (**check one**):

- ☒ **Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby Iron Mountain Information Management, Inc has demonstrated full compliance with the PCI DSS.
- ☐ **Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall **NON-COMPLIANT** rating, thereby (*Service Provider Company Name*) has not demonstrated full compliance with the PCI DSS.
- Target Date** for Compliance:
- An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with the payment brand(s) before completing Part 4.*
- ☐ **Compliant but with Legal exception:** One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.
- If checked, complete the following:*
- | Affected Requirement | Details of how legal constraint prevents requirement being met |
|----------------------|--|
|                      |  |
|                      |  |

### Part 3a. Acknowledgement of Status

**Signatory(s) confirms:**

**(Check all that apply)**

- ☒ The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures*, Version 3.1, and was completed according to the instructions therein.
- ☒ All information within the above-referenced ROC and in this attestation fairly represents the results of my assessment in all material respects.
- ☐ I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- ☒ I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
- ☒ If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

**Part 3a. Acknowledgement of Status (continued)**

<input checked="" type="checkbox"/>	No evidence of full track data <sup>1</sup> , CAV2, CVC2, CID, or CVV2 data <sup>2</sup> , or PIN data <sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
<input type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

### Part 3b. Service Provider Attestation

*John Tomovcsik*

Signature of Service Provider Executive Officer ↑	Date: 22 September 2015
Service Provider Executive Officer Name: John Tomovcsik	Title: EVP and General Manager Records and Information Mgt.

### Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	Primary Assessor
--	------------------

*Ted Meyer*

Signature of Duly Authorized Officer of QSA Company ↑	Date: 18 September 2015
Duly Authorized Officer Name: Ted Meyer	QSA Company: Trustwave

### Part 3d. ISA Acknowledgement (if applicable)

If an ISA was involved or assisted with this assessment, describe the role performed:	Not Applicable
---	----------------

Signature of ISA ↑	Date:
ISA Name:	Title:

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	





# Security Assurance Reference (SAR) Guide

Version 2016.2 | Effective as of April 1, 2016

PREPARED BY:

Global Safety Risk and Security Services

Proprietary and Confidential

The information referenced in this document is Iron Mountain Confidential and not for public distribution. Only customers or prospective customers who have signed non-disclosure agreements are permitted access to this information.

## DOCUMENT HISTORY

This document is reviewed annually and updated on a quarterly basis. The following table lists the previous and current revisions to this document in chronological order. For each revision one or more contributors is listed and the changes to the document briefly described.

The most recent revision is given in the last entry of the table below and that version is printed in the footer of each page of the document.

Version	Date	Author	Description of Changes
2016.1	01/01/2016	Jazmin Minaya	<b>Updated</b> <ul style="list-style-type: none"> <li>– Access Control Policy</li> <li>– Authorized Devices Policy</li> <li>– Breach Notification</li> <li>– Business Continuity Policy</li> <li>– Information Classification and Handling Policy</li> <li>– Iron Mountain Acceptable Use Policy</li> <li>– Third Party Risk Management</li> </ul>
2016.2	4/1/2016	Melony Isaac Jazmin Minaya Rory O'Connor	<b>Updated</b> <ul style="list-style-type: none"> <li>– Iron Mountain Visitor Safety &amp; Security Welcome</li> <li>– Global Internal Audit Overview</li> <li>– Certificate of Liability Insurance – Cyber Security</li> <li>– SysTrust Report</li> </ul> <b>Added</b> <ul style="list-style-type: none"> <li>– Certificate of Liability Insurance – Cyber Security</li> <li>– Enterprise Event Reporting Policy</li> <li>– Vehicle Incident Management Policy</li> </ul> <b>Removed</b> <ul style="list-style-type: none"> <li>– Iron Mountain Computer Incident Response Team</li> <li>– Security Monitoring and Response Policy</li> <li>– Safe Harbor Declaration</li> <li>– CWISP</li> </ul>

**DOCUMENT SIGNOFF**

Approver	Name	Date
Director, Information Security	Seth Bailey	04/08/2016

Table of Contents	
Document History	i
Document Signoff	ii
<b>Foreword</b>	<b>5</b>
Introduction	5
Communications	6
Scope	6
Summary	6
<b>Information Security Policies</b>	<b>7</b>
Introduction	7
<b>Organization of Information Security</b>	<b>14</b>
Information Security Organization Policy	14
<b>Human Resource Security</b>	<b>16</b>
Personnel Security Policy	16
Iron Mountain Acceptable Use Policy (Global)	18
Background Investigations Policy	19
Background Investigation Program – U.S.	20
Background Investigation Program – Canada	23
<b>Asset Management</b>	<b>25</b>
Information Classification and Handling Policy	25
Records Management Policy	26
Authorized Devices Policy	27
<b>Access Control</b>	<b>28</b>
Access Control Policy	28
<b>Physical and Environmental Security</b>	<b>30</b>
Global Facility Policy	30
Iron Mountain Visitor Safety & Security Welcome	31
<b>Cryptography, Communications and Operations Security</b>	<b>32</b>
Communications and Operations Management Policy	32
IT System Logging and Log Monitoring Policy	33
Intrusion Detection and prevention policy	34
Network Architecture Diagrams	35
<b>System Acquisition, Development, and Maintenance</b>	<b>37</b>
Application Development Policy	37
Information Security Assessment Program	39
Software Development LifeCycle (SDLC) Summary	45
<b>Supplier Relationships</b>	<b>50</b>
Third-Party Risk Management Policy	50
Overview of Third-Party Risk Assessment Program – North America	51
<b>Risk Management</b>	<b>53</b>
Operational Risk Policy	53

Global Internal Audit	54
Certificate of Liability Insurance – General	56
Certificate of Liability Insurance – Warehouse	57
FM Global Certificate of Property Insurance	58
Certificate of Insurance - Crime	59
Certificate of Liability Insurance - Cyber Security	60
Canada General Liability Insurance	61
<b>Information Security Incident Management</b>	<b>62</b>
Breach Notification Policy	62
Incident Management Program	63
Enterprise Event Reporting Policy Global	64
Vehicle Incident Management Policy	65
<b>Information Security Aspects of Business Continuity Management</b>	<b>66</b>
Business Continuity Policy	66
Abstract of Business Continuity Management (BCM) Program	67
Business Continuity Plan, Pandemic Plan, and Executive Summary	77
<b>Compliance</b>	<b>80</b>
Legal, Compliance and Regulatory Policy	80
Health Insurance Portability and Accountability Act (HIPPA) Policy	82
Global Privacy Policy	83
Employee Confidentiality and Non-Competition Agreement	84
Privacy, Data Protection, & Compliance Policies and Procedures Summary	86
Privacy Protection in Canada	91
Global Anti-corruption & Anti-bribery Program Overview	93
Iron Mountain Code of Ethics and Business Conduct Overview	94
SOC 3 Report	95
Iron Mountain PCI Attestation of Compliance	96
FACTA Red Flags Summary	97
Massachusetts Data Privacy Statement	98
Global Fraud, Waste, & Abuse Program Summary	99

# Foreword

---

## INTRODUCTION

The information contained in this document addresses the safeguards Iron Mountain has implemented to protect information assets and ensure its Security program objectives are achieved.

Information Security policies and standards have been derived from the Company's information security risk management process, legal/regulatory requirements, industry standards, and the nature of the Company's activities. The Board of Directors recognizes that the information security landscape is constantly changing and that management must implement, interpret and, at times, modify the control documents to reflect the changing landscape.

The Chief Security Officer (CSO) is responsible for overall enterprise security and provides centralized oversight for security policy, administration, and operations; including security monitoring and compliance, physical security design and engineering, information security projects and service delivery, and technology risk management.

Security is Iron Mountain's #1 core value and information one of the most critical assets. The information security policies and standards provided in this document are the basis for ensuring the security and the protection of information and related technologies.

This document is organized by ISO 27001:2013 domains:

- Information Security Policies
- Organization of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Physical and Environment Security
- Cryptography, Communications and Operation Security
- System Acquisition, Development and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity
- Compliance

The policies summarized in this document set forth the organizational standards and provide direction to management and employees for achieving the following security program objectives:

- **Confidentiality.** Ensure customer and company data is not used for unauthorized purposes.
- **Integrity.** Protect the accuracy, completeness, and reliability of information.
- **Availability.** Provide authorized users with prompt access to information.
- **Accountability.** Ensure actions can be definitively attributed to individuals.

## COMMUNICATIONS

Global Safety, Risk and Security (GSRS) is responsible for defining the requirements for protecting information and communicating these requirements to management through steering committees, executive presentations, intranet, training, and new employee orientation.

This document should be requested through Iron Mountain's account management or customer service organizations. Questions and/or comments concerning this document should be directed to the appropriate Iron Mountain business relationship manager who will then contact the Iron Mountain GSRS department.

Requests to review the Security Standards must be communicated to Iron Mountain and will be considered on a case by case basis.

## SCOPE

The Security policies and standards apply to Iron Mountain and its affiliates, subsidiaries, personnel, third party consultants, contractors, vendors and any individual or entity provided access to Iron Mountain's information resources.

The policies apply to all forms of information created, used or maintained by or on behalf of Iron Mountain, including that pertaining to consumers, commercial and corporate customers and proprietary information about the Company's products, services, processes, strategies and performance.

The SAR Guide is used to address customer Security/Risk/Compliance inquiries, Questionnaires, and Audits.

## SUMMARY

The Iron Mountain Security Assurance Reference (SAR) Guide is a collection of frequently requested customer-facing documentation that outlines the Iron Mountain Security, Risk and Compliance controls.

The SAR Guide, along with the Iron Mountain Standardized Information Gathering (SIG) Questionnaire, Global Security Services Presentation, and Security Whitepaper make up the Iron Mountain Security Assurance Package (SAP). The SAR Guide is frequently referenced within the SIG Questionnaire to provide supporting information regarding Iron Mountain security processes.

The Iron Mountain SAR Guide is updated quarterly by internal stakeholders. As a result, it is recommended new SAR Guide copies be obtained that reflect the changes to Iron Mountain's Security, Risk and Compliance postures.

# Information Security Policies

## INTRODUCTION

<b>Policy Name</b>	0.00 Introduction
<b>Policy Purpose</b>	The Iron Mountain Information Security Policy defines the rules and processes that protect the information resources of Iron Mountain.
<b>Policy Statement</b>	The Iron Mountain Information Security Policy defines the fundamental principles for the protection of Iron Mountain information resources, the proper controls needed to ensure compliance with internal and external regulations, and to uphold Iron Mountain's reputation with its clients. All personnel are responsible for ensuring compliance with the Iron Mountain Information Security Policy.
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Information security is the responsibility of everyone at Iron Mountain, including service providers and contractors who have been hired by Iron Mountain.</li> <li>– Information resources play a vital role in the conduct and success of Iron Mountain's business worldwide. Information resources must be protected throughout their life cycle to ensure the confidentiality, integrity and availability of the information processed or stored on these resources. The Iron Mountain Information Security Policy defines the fundamental principles for the protection of Iron Mountain information resources, the proper controls needed to ensure compliance with internal and external regulations, and to uphold Iron Mountain's reputation with its clients. All personnel are responsible for ensuring compliance with the Iron Mountain Information Security Policy. The safeguards defined in this policy must be continuously and vigorously applied. The Board of Directors, management and employees all have different roles in developing and implementing an effective security process. The Iron Mountain Information Security Policy demonstrates the commitment of Executive Management to information security. Executive Management acknowledges their responsibility for securing the information resources of Iron Mountain, and they have delegated this responsibility to information security, under the control of the Chief Security Officer. Failure to comply with the Iron Mountain Information Security Policy may compromise Iron Mountain information resources, thereby exposing Iron Mountain and its clients to unnecessary risk. Violations of the Information Security Policy will result in legal and/or disciplinary action, up to and including dismissal.</li> <li>– Dispensation from Iron Mountain policy requires the express written consent of management in accordance with approved procedures. All personnel must adhere to the Information Security Policy in conjunction with all other policies of Iron Mountain.</li> <li>– Personnel who have questions regarding the Information Security Policy should consult with their management or Information Security.</li> </ul>



Functional Area Name	A. Industry Standards / Regulations
Functional Area Purpose	<p>The Iron Mountain Information Security Policy has been developed and updated after reviewing leading information security industry standards and relevant regulatory acts, and after seeking the advice of third party information security policy experts.</p> <p>The following reference materials have served as guidance for the Iron Mountain Information Security Policy framework:</p> <p><b>ISO/IEC 17799.</b> ISO 17799 is an internationally recognized security standard that is being followed by most financial service organizations in the United States and Europe. This standard is based on and supersedes the British standard BS7799 Code of Practice for Information Security Management, which was last published in May 1999, an edition which itself included many enhancements and improvements on previous versions. The first version of ISO 17799 was published in December 2000.</p> <p><b>Information Security Forum.</b> The Information Security Forum (ISF) is an internationally recognized information security organization whose standards have mainly been adopted within the European community. The ISF standard is based on BS7799 and COBIT, and attempts to restructure the policies outlined in BS7799 and COBIT into a "Business Objective" point of view. The ISF standards were last updated in November of 2000. The ISF standard is known for refining proven practices and addressing 'hot topics,' such as electronic commerce, Public-key Infrastructure (PKI) and malicious 'mobile' code (including viruses and Web-based threats).</p> <p><b>Control Objectives for Information and related Technologies.</b> Control Objectives for Information and Related Technologies (COBIT) is an authoritative, up-to-date, international set of generally accepted IT Control Objectives for day-to-day use by business managers as well as security, control and audit practitioners. COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners. The IT Governance Institute provides the objectives.</p> <p><b>EU Privacy Directive.</b> The EU Privacy directive adopted in February 1995 was designed to bridge the gap between national data protection laws in the European Union. This normalizing of data protection laws is primarily aimed at solving issues of transporting private personal data between EU member states. The EU privacy directive forbids any transfer of personal data outside the EU countries that do not guarantee or do not have in place adequate safeguards for such data.</p> <p><b>Health Insurance Portability &amp; Accountability Act.</b> The Health Insurance Portability &amp; Accountability Act (HIPAA) of 1996 (August 21, 1996), Public Law 104-191, amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, this act authorized the Secretary of Health and Human Services to develop security and privacy standards to protect electronic healthcare information. The security and privacy standards were to cover the processing, storing and transmission of data to prevent inadvertent or unauthorized use or disclosure of an individual's health information.</p>

---

**Children's Online Privacy & Protection Act.** The Children's Online Privacy Protection Act (COPPA), effective April 21, 2000, applies to the online collection of personal information from children under the age of 13. The rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online.

**Bill C-6.** Passed by the House of Commons of Canada in October 1999, Bill C-6 is an Act to support and promote electronic commerce in Canada by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

**ETS 185 Conventions on Cyber Crime.** Established November 2001 by the member states of the Council of Europe, ETS 185 is a by-product of the Committee of Experts on Crime in Cyber-space (PC-CY) by decision n CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers Deputies (held on 4 February 1997). The revised and finalized draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature. The Convention aims principally at (1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international cooperation.

**Gramm-Leach-Bliley.** The Gramm-Leach-Bliley Act (GLB) regulates the sharing of personal information about individuals who obtain financial products or services from financial institutions. It attempts to inform individuals about the privacy policies and practices of financial institutions, so that consumers can use that information to make choices about financial institutions with whom they wish to do business. The Privacy Rights Clearinghouse provides information about how to read privacy notices and exercise rights under the Gramm-Leach-Bliley Act.

**Monetary Authority of Singapore.** The Monetary Authority of Singapore (MAS) was passed by the Singapore Parliament in 1970, and acts as the authority to regulate all elements of monetary, banking and financial aspects of Singapore.

**The Bank for International Settlement.** The Bank for International Settlement (BIS) was established in Basel Switzerland in 1930 and is the oldest international banking organization in the world. The BIS fosters cooperation among central banks and other agencies in pursuit of monetary and financial stability and functions as a center for monetary and economic research. The Basel Committee on Banking Supervision published the Risk Management Principles for Electronic Banking in May of 2001. This document was created as a reference guide for best practice security principles. The document is not intended to provide absolute requirements.

**Payment Card Industry (PCI) Data Security Requirements.** The Payment Card Industry (PCI) Data Security Requirements were first published in January of 2005. These requirements apply to all members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security

---

requirements apply to all *system components* which is defined as any *network component, server, or application* included in, or connected to, the cardholder data environment.

## Functional Area Name

### B. Overview of Security Policies

## Functional Area Purpose

The Iron Mountain Information Security Policy has been organized in a three-tier structure, so readers may quickly find the specific guidance they are seeking. Each tier contains a numerical reference to allow users to quickly navigate through the policies. This three-tier structure is referred to as the Policy Framework, which defines the elements and structure for the delivery of information security policies. Each tier of the Policy Framework is described below:

1. **Policy.** A policy is a broad statement of principles that presents management's position for a defined subject. Policies are long-lasting, strategic guides that provide overall direction to Iron Mountain in regards to information security. All Iron Mountain information security policies are supported and have been approved by Executive Management.
2. **Functional Area.** Functional Area is the second highest level in the Policy Framework. Functional Areas describe the purpose and scope of the underlying standards and act as a categorical stepping-stone to help readers navigate to specific standards and find the guidance they are seeking for a specific topic.
3. **Category.** Category is a grouping of related standards that support a given area of a policy.
  - **Standard.** A standard provides specific guidance on management expectations for a specific area of a policy. Standards are technology independent, and outline specific actions that must be taken in order to ensure compliance with a policy.

A brief overview of each of Iron Mountain's information security policies is provided below:

**Global Acceptable Use Policy** and **Global Authorized Devices Policy.** Provides guidance related to access privileges to Iron Mountain Computing Assets and Data.

**Information Security Organization Global.** Outlines Executive Management's responsibility for securing the information resources of Iron Mountain, and the organization of Iron Mountain's Global Safety Risk and Security team.

**Operational Risk Policy.** Formalizes the structure and requirements of Iron Mountain's operational risk program. This program is tasked with determining the appropriate controls which must be implemented to secure information resources, based on the information classification of those resources.

**27.0 Personnel Security.** This policy provides guidance on governing Iron Mountain personnel and third party consultants or vendors who have access to or custody of Iron Mountain information resources.

**Global Facility Policy.** Iron Mountain's Global Facility Policy outlines the high level physical and environmental security controls required for all storage, datacenter, and corporate facilities. The policy is supported by several standards documents which address specific controls in greater detail.

**Global Communications and Operations Management Policy.** Specifies required controls for Iron Mountain IT systems' communications and operations. Control requirements include items such as securing internet connections, encryption of transmissions, change control, and secure system administration.

**IT System Logging and Log Monitoring Policy.** Establishes capture, retention, and monitoring requirements for computer generated logs. System, application, network device, and other logs are addressed. Baseline requirements for Iron Mountain's Security Information and Event Management (SIEM) system are also outlined by this policy.

**Intrusion Detection and Prevention Policy.** Details requirements for the purchasing, deployment, configuration, and maintenance of Intrusion Detection and Intrusion Prevention systems on Iron Mountain's network.

**Global Access Control.** Iron Mountain's Global Access control policy addresses requirements for authorizing and authenticating personnel prior to granting them access to information resources.

**34.0 Application Development.** This policy provides guidance on the information security issues surrounding the development or acquisition of new systems and the maintenance of existing systems.

**Global Business Continuity Policy.** Provides guidance to ensure that critical information resources are promptly recovered and available to authorized users in the event of a disruption of service. Iron Mountain's business continuity and disaster recovery programs comprehensively address issues such as IT system failure, environmental hazards to our storage facilities, and measures to mitigate significant reductions in workforce.

**36.0 Legal, Compliance and Regulatory.** Iron Mountain's guiding document for compliance with legislative, regulatory and contractual requirements affecting information resources.

**Third Party Risk Management.** Addresses third party risk by outlining assessment and ongoing monitoring controls for third parties.

**Breach Notification Policy.** Creates a structured process to inform customers of security breaches affecting their assets, in accordance with applicable law and/or their contracts.

---

**Functional Area  
Name**

**C. Management Commitment**

---

**Functional Area  
Purpose**

The Iron Mountain Executive Management is committed to protecting Iron Mountain information resources from internal and external threats to their confidentiality, integrity and availability. It is the Executive Management who is responsible for overseeing the development, implementation and maintenance of the Iron Mountain Information Security program. Executive Management should approve written information security policies and the information security program at least annually. Executive Management should provide management with its expectations and requirements for:

- Central oversight and coordination
  - Area of responsibility
  - Risk Measurement
-

- Monitoring and testing
- Reporting
- Acceptable residual risk

It is management's responsibility to ensure that:

- A proactive and consistent approach is taken to implementing the Iron Mountain Information Security Policy
- Formal procedures are established to react effectively to information security incidents
- Clients and partners are confident that their information assets are adequately protected
- Auditors, regulators and Iron Mountain management are satisfied with the security controls that are in place
- Information security requirements are built into technology solutions implemented to meet business requirements
- Information security concepts and controls are understood by personnel responsible for securing and maintaining Iron Mountain information resources
- Vulnerabilities of Iron Mountain's information resources are clearly understood and minimized through the performance of risk assessments

---

**Functional Area  
Name**

**D. Review and Evaluation**

---

**Functional Area  
Purpose:**

Iron Mountain's information security policies should be assigned owners who are responsible for their development and maintenance. The Information Security Steering Committee is responsible for assigning policy and standard ownership, and for reviewing and approving the Iron Mountain Information Security Policy at least annually and when updates are made.

---

**Functional Area  
Name**

**E. Compliance with Security Policies**

---

**Functional Area  
Purpose**

Failure to comply with the Iron Mountain Information Security Policy may expose Iron Mountain and its clients to unnecessary risk and may compromise information resources. Violations of the Iron Mountain Information Security Policy will result in disciplinary action, up to and including dismissal.

Internal Audit and Information Security are responsible for conducting periodic reviews to ensure compliance with the Iron Mountain Information Security Policy.

---

**Functional Area  
Name**

**F. Policy Acknowledgement**

---

**Functional Area  
Purpose**

All Iron Mountain personnel must acknowledge receiving and understanding of the Information Security Policy by signing an agreement (i.e., online or hardcopy).

Third party consultants, contractors and vendors must sign a Service Confidentiality Agreement (i.e., online or hardcopy), which requires them to comply with the Iron Mountain Information Security Policy.

---

Functional Area Name	G. Policy Exceptions
Functional Area Purpose	<p>Technical or business requirements may indicate the need for dispensation from the Iron Mountain Information Security Policy for specific matters. Following an appropriate risk assessment, the Chief Security Officer or their appointed designee, can authorize such exceptions. Requests for such waivers must be presented to the appropriate security officer, who must assist in preparing the request. Prior to submitting such a request, the requestor must:</p> <ul style="list-style-type: none"> <li>– Document the control for which the exception is required, the reason for the exception, and the risk introduced</li> <li>– Attempt to identify alternative controls that mitigate the risk due to the exception</li> <li>– Obtain management approval from the department requesting the exception</li> </ul> <p><b>Note:</b> Unless alternative controls eliminate all risk introduced by the exception, dispensation is granted for a limited lifespan, as determined by the Chief Security Officer or their designee. New control techniques, new threats or a re-evaluation of the risk may eliminate Iron Mountain's continued support of the exception.</p>
Functional Area Name	H. Roles and Responsibilities
Functional Area Purpose	<p>Information security is not just an ongoing managerial task; it is the responsibility of all Iron Mountain personnel, as well as Iron Mountain's service providers and contractors. The Board of Directors, management and employees all have different roles in developing and implementing an effective security process. The following provides an overview of the responsibilities or various roles within Iron Mountain:</p> <ul style="list-style-type: none"> <li>– Board of Directors</li> <li>– Executive Boards of Business Units</li> <li>– Information Security Steering Committee</li> <li>– Business Managers (Line Management)</li> <li>– Information Owners</li> <li>– Resource Administrators</li> <li>– Help Desk</li> <li>– Application Developers</li> <li>– Legal, Compliance and Audit Personnel</li> <li>– Human Resources</li> <li>– All Iron Mountain Personnel</li> </ul>
Functional Area Name	I. Contacts
Functional Area Purpose	<p>To request additional information or to comment on Iron Mountain's Information Security Policy, please contact Information Security at <a href="mailto:GlobalSecurity@IronMountain.com">GlobalSecurity@IronMountain.com</a>.</p>



# Organization of Information Security

## INFORMATION SECURITY ORGANIZATION POLICY

<b>Policy Name</b>	Information Security Organization (Global)
<b>Policy Purpose and Scope</b>	<p>Iron Mountain's Executive Management has charged Global Security Services with the responsibility for developing, maintaining and communicating a comprehensive information security program ("the Program") to protect the confidentiality, integrity and availability of Iron Mountain information resources and customer information assets ("Information Assets").</p> <p>The establishment, implementation and management of the Program involves creating, administering, and overseeing policies to ensure the prevention, detection, containment and correction of security breaches, through standardized risk management principles.</p> <p>The Program is a summary description of the principal aspects of a multi-faceted and detailed set of activities more fully described in policies, procedures, guidelines and practices adopted and observed by Iron Mountain, its employees and third parties with access to Information Assets. Policies, procedures, guidelines and practices will change from time to time to respond to new threats to security, changes in applicable laws and/or regulations, changes in contractual requirements or to adopt (or adapt) to changes in technology.</p> <p>The objectives of the Program include:</p> <ul style="list-style-type: none"> <li>• Reducing the number of information security incidents;</li> <li>• Identifying and managing the company's information risks;</li> <li>• Establishing responsibility and accountability for information security in the organization;</li> <li>• Ensuring that the organization is able to continue its commercial activities in the event of a significant information security related incident;</li> </ul> <p>This policy applies to all employees, contractors, customers, vendors, guests or other parties of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain or who otherwise have access to Information Assets, regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions, except to the extent they maintain, follow and enforce a similar policy.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Information Security Background Investigation and Training</li> <li>– Information Security Coordinators</li> <li>– Information Security Coordinators Responsibilities</li> <li>– Information Security ERMS Incident Managers</li> <li>– Information Security Event Reporting Management System (ERMS)</li> <li>– Information Security Global Security Services</li> <li>– Information Security Hardware and Software</li> <li>– Information Security Internal Audit</li> </ul>

- 
- Information Security Policies and Procedures
  - Information Security Policy Alignment
  - Information Security Incident Reporting
  - Information Security Technical and Security Purchases
  - Information Security Vulnerability Assessment
-



# Human Resource Security

## PERSONNEL SECURITY POLICY

<b>Policy Name</b>	27.0 Personnel Security Policy
<b>Policy Purpose</b>	This policy provides guidance on managing personnel, consultants, contractors and vendors who have access to, or custody of Iron Mountain information resources. This policy is intended to reduce risks of human error, theft, fraud or misuse of information resources and facilities.
<b>Policy Statement</b>	Information security controls should be implemented to ensure that individuals hired by Iron Mountain are appropriately screened and made aware of the Iron Mountain Information Security Policy.
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– All potential personnel, consultants, contractors and vendors should be subjected to a formal background screening that will be used by managers to make informed hiring decisions. The terms and conditions of employment should state the candidate's responsibility for information security.</li> <li>– All personnel and third parties should sign non-disclosure agreements as part of their initial condition of employment.</li> <li>– All personnel must receive initial security compliance training at hire time, and periodically receive updates regarding the Iron Mountain Information Security Policy.</li> <li>– Where appropriate, separation of duties for personnel assigned to critical tasks should be employed to minimize the risk of negligent or deliberate information system misuse and conflicts of interest.</li> <li>– Personnel assigned positions with significant information security duties should be provided specialized information security training.</li> <li>– Information security considerations should be included in the termination or transfer of personnel.</li> <li>– Managers should take appropriate disciplinary action against personnel who violate the Information Security Policy.</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>– Iron Mountain Computing Policy (Acceptable Access and Use of Company Computer Resources)</li> <li>– Evaluation of Security Activities During Performance Reviews</li> <li>– Formal Disciplinary Process for Security Violations</li> <li>– Including Security Responsibilities in the Terms and Conditions of Employment</li> <li>– Information Security Training</li> <li>– List of Duties to be Separated</li> <li>– Monitoring Employee Compliance to the Iron Mountain Information Security Policy</li> <li>– Non-Disclosure Agreements (NDAs)</li> <li>– Potential Disciplinary Actions</li> <li>– Pre-Employment Background Checks</li> <li>– Process of Escorting Terminated Employees and Contractors</li> <li>– Revoking System Access</li> </ul>

- 
- Separation of Sensitive Duties
  - Situations When Non-Disclosure Agreements Must be Revisited
  - Specialized Training for Security Personnel
  - Third Party Accountability to Security Policy
-

## IRON MOUNTAIN ACCEPTABLE USE POLICY (GLOBAL)

<b>Policy Name</b>	Acceptable Use (Global)
<b>Policy Purpose</b>	<p>It is the policy of Iron Mountain to provide fit-for-purpose, efficient, cost-effective, secure and reliable Information Technology systems, services and resources to all Users for the purpose of conducting Iron Mountain business activities, supporting business operations, and successfully achieving Iron Mountain's business goals.</p> <p>The company has made an investment in establishing IT systems, services and information assets, and the company incurs significant cost to operate, maintain and improve IT resources on an ongoing basis.</p> <p>The purpose of this policy is to:</p> <ul style="list-style-type: none"><li>• Protect Iron Mountain, its employees, customers, and business partners, by providing rules and guidance on acceptable use of Company Computer Resources.</li><li>• Provide notice to Users on their expectation of privacy when accessing and using Company Computer Resources.</li><li>• Satisfy compliance requirements for various laws, rules, regulations, and other binding Company commitments, including contracts and standards certifications.</li></ul> <p>This policy applies to all employees, contractors, vendors, guests or other parties of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– AUP Company Computer Resources</li><li>– AUP Violations</li><li>– AUP Special Precautions</li><li>– AUP Internet Activity</li><li>– AUP Privacy and Ownership Expectation of Privacy</li><li>– AUP Unacceptable Use</li></ul>

## BACKGROUND INVESTIGATIONS POLICY

<b>Policy Name</b>	Background Investigations Policy (Global)
<b>Policy Purpose</b>	<p>To describe and document Iron Mountain's policy related to background investigations. The inquiry into a candidate's background is a fundamental element of the screening process designed to maintain integrity and reduce risk. This policy provides guidance on managing personnel, consultants, contractors and vendors who have access to, or custody of Company information resources. This policy is intended to reduce risks of human error, theft, fraud or misuse of company or customer information, resources and facilities.</p> <p>This policy applies to all employees, contractors, vendor partner staff or other parties of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Background Investigation Conditional Offer of Employment</li><li>– Background Investigation Frequency</li><li>– Background Investigation Policy Compliance</li><li>– Background Investigation Policy Right to Modify</li><li>– Background Investigation Self Reporting</li><li>– Background Investigation Validity Period</li></ul>

## BACKGROUND INVESTIGATION PROGRAM – U.S.



---

### 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, either on or off the job.

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:

- Marijuana metabolites
- Cocaine metabolites
- Opiate Metabolites
- Phencyclidine (PCP)
- 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. Should a candidate fail the pre-employment test, no further employment consideration is given.

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 the applicant signs a written offer letter, 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.

Individuals with convictions pertaining to any drug/narcotics offense, any financial and abuse of trust crime, any crime of violence to include domestic assault and weapons crimes, and crimes involving theft within the review period are generally not eligible for employment. Further, applicants found to have been incarcerated for any of the aforementioned crimes at any time during the ten-year search period are also generally not be eligible for employment with Iron Mountain.

Individuals convicted of the crimes of arson, murder, rape, sexual assault, acts of terrorism, or identity theft are not eligible for employment.

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 is comprised of over 300 million records from, among others: the 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. Currently this search includes information from 49 states' Sex Offender Registries plus the District of Columbia, Puerto Rico and Guam; 39 states' Department of Corrections sources; 13 states' Administrative Office of the Courts sources; plus multiple online county records. In addition, this search contains a review of 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.

This review is conducted annually.

**Employment Verifications**

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

**Education Verifications**

If an applicant claims education beyond high school (undergraduate, graduate, vocational), Iron Mountain will confirm the highest degree awarded.

**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. For example, any conviction for Operating Under the Influence of Drugs or Alcohol is an automatic disqualification. All drivers are subject to an annual motor vehicle records check.

**Authorization to Work in the United States**

Iron Mountain subscribes to the Department of Homeland Security's E-Verify system in order to confirm that all employees are duly authorized to work in the United States. We also use this process where required to validate citizenship status for export control regulation (e.g. EAR, ITAR, etc.) compliance.

## BACKGROUND INVESTIGATION PROGRAM – CANADA



---

### Overview of Background Investigation Program – Canada

---

Canadian human rights legislation places a distinct emphasis on the protection of the individual from certain intrusions on their person – and alcohol and drug testing has been previously circumscribed by the courts interpreting such human rights legislation. IMCC maintains a background check policy (which is permitted) and such policy may provide useful information regarding a substance abuse history (the standard, representation is set forth below), but IMCC has determined that this is the full extent of its permitted inquiry into such behavior.

Iron Mountain implemented a background investigation program for employees in Canada hired on or after December 1, 2005. Under this program, candidates (including casual employees, temporary employees and employees acquired through acquisitions) must successfully pass a background investigation as a condition of employment. The background investigation covers a period of ten years back from the date of the candidate's signed authorization and release form or the candidate's employment application.

All background investigations are conducted by an independent, national service provider (currently Sterling Backcheck) and reported to a central corporate point of contact at Iron Mountain to preserve the integrity of the process and the results.

Iron Mountain recognizes that the law is evolving in this area – and that some courts have revised the balance between human rights legislation and an employer's (and the public's) considerable interest in safety issues. At this time, Iron Mountain policy continues to reflect the traditional Canadian emphasis on the human rights and the protection of the individual from discrimination.

#### **Criminal Records Check**

A criminal records check is performed for evidence of criminal convictions, including offenses relating to theft, violence, fraud or drug trafficking for which a pardon has not been granted.

#### **Terrorist Watch List (Canadian National Terrorism Advisory)**

A name check is performed against the listing maintained under the United Nations Suppression of Terrorism Regulations, which was developed by the Department of Foreign Affairs and International Trade and modified by the Department of Public Safety and Emergency Preparedness and is currently maintained by the Office of the Superintendent of Financial Institutions.

#### **Motor Vehicle Review**

A review of the candidate's driver record abstract is performed, if applicable. Driver candidates are screened for appropriate license class and any motor vehicle violation history. Violation and accident history for the past three years are reviewed and adjudicated based upon seriousness of the offense and frequency of occurrence. For example, any conviction for operating under the influence of drugs or alcohol is an automatic disqualification. In addition, all drivers (whether hired before or after December 1, 2005) are subject to an annual motor vehicle records check.

#### **Education and Employment Verifications**



Education and employment verifications are performed, if required; this may vary according to the level of the position to be filled.

**Substance Abuse Policy**

Although IMCC does not perform mandatory Drug Screening of its employees, IMCC does have the following Substance Abuse Policy:

While abuse of alcohol and drugs among our employees is the exception rather than the rule, the Company shares the concern expressed by many over the growth of substance abuse in society.

In order to meet our responsibilities to our employees and customers, we must maintain a healthy and productive work environment, unimpaired by drug or alcohol abuse. Our customers have put their confidence in us to handle material that is sensitive in nature and requiring a quick turnaround.

Iron Mountain's policy is to employ a workforce free from abuse of drugs and alcohol, either on or off the job. This program includes post-accident, drug and alcohol testing managed in accordance with provincial and federal regulations. Any employee determined to be in violation of this policy is subject to disciplinary action, up to and including termination.

Prohibited activities include, but may not be limited to:

- Any employee in possession of any illegal drug(s);
- Any employee under the influence of alcohol during working hours;
- Sale, attempted sale, or distribution of illegal drugs or prescription medication;
- Possession in the employee's body, blood, or urine any prohibited level of alcohol; and
- The ingestion, sale, or distribution of any illegal drug(s) whether on duty or not, whether on Iron Mountain property or not, is guilty of misconduct and is subject to disciplinary action up to and including termination.

This policy covers both legal and illegal drugs and alcohol. Legal drugs are defined as prescribed and over the counter drugs, which have been legally obtained and are being used solely for the purpose for which they were prescribed or manufactured. Alcohol is considered a legal drug. Illegal drugs are defined as any drug, which is not legally obtainable, which may be legally obtainable but has not been legally obtained, or which is being used in a manner for a purpose other than prescribed.

If prior to detection and discovery, an employee seeks assistance from Iron Mountain for drug and/or alcohol abuse problems, Iron Mountain will provide the employee assistance in locating treatment and rehabilitative services.

The ultimate goal of this policy is to balance our respect for individual privacy with our need to keep a safe, productive, drug-free workplace. We encourage anyone who abuses drugs, non-prescription inhalants and/or alcohol to seek help in overcoming their problem.

# Asset Management

## INFORMATION CLASSIFICATION AND HANDLING POLICY

<b>Policy Name</b>	Information Classification and Handling Policy
<b>Policy Purpose</b>	<p>Classification is central to information management. By understanding, and classifying, information according to its value, legal requirements, sensitivity, and importance to Iron Mountain and our clients, we can ensure that appropriate protection is provided.</p> <p>This Policy sets out the requirements for the classification and handling of Information Assets for Iron Mountain globally.</p> <p>These requirements are applicable to all forms of information produced, stored or transmitted within Iron Mountain regardless of media or format (includes electronic, e-mail, paper, image, etc.).</p> <p>This policy applies to all employees and contractors of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Clear Desk and Screen Computers Not in Use</li> <li>– Clear Desk and Screen Confidential</li> <li>– Clear Desk and Screen End of Work Day</li> <li>– Clear Desk and Screen Saver</li> <li>– Clear Desk and Screen Workspace</li> <li>– External Requirements Client Information</li> <li>– External Requirements Contractual</li> <li>– External Requirements Customer Information Assets</li> <li>– External Requirements Government Protectively Marked Information</li> <li>– Information Classification Asset Ownership</li> <li>– Information Classification Customer Data</li> <li>– Information Classification Default</li> <li>– Information Classification Defined</li> <li>– Information Classification Determination</li> <li>– Information Classification Highest Classification Marking</li> <li>– Information Classification Level Assignment Alteration</li> <li>– Information Classification Periodic Review</li> <li>– Information Classification Policy Violations</li> </ul>

## RECORDS MANAGEMENT POLICY

---

**Policy Name** Records Management Policy

---

**Policy Purpose** This Iron Mountain Records Management Policy (Policy) establishes the framework of rules and guidelines for handling all of Iron Mountain's records throughout their lifecycle, including creation, access, use, storage, retention, preservation for legal holds and disposition. This Policy addresses how to satisfy legal obligations, regulatory requirements, and operational needs for records and their retention by establishing consistent and accountable recordkeeping practices throughout the organization. Failure to keep records in good order can result in serious consequences for Iron Mountain including regulatory enforcement action, reputational damage, or an inability to defend or pursue litigation.

The Policy and Procedures adopted under the Records Management Program apply to:

- All records created or received in the transaction of Iron Mountain business or in the fulfillment of legal obligation, regardless of media or format (e.g., electronic, e-mail, imaged, paper, etc.).
- All physical locations where records are maintained globally, including firms and individuals acting as agents of Iron Mountain
- All employees, contractors, agents, third parties, and vendors globally who create, receive, manage, store, or use Iron Mountain records.

This Policy is established and maintained by the Legal department and supersedes all previous records management policies, procedures, or standards intended to apply to the subject matter of this Policy.

---

**Key Points**

- Records Management Best Practices
- Records Management Electronic Records
- Records Management Litigation and Compliance Risks
- Records Management Official Records
- Records Management Program

---

## AUTHORIZED DEVICES POLICY

<b>Policy Name</b>	Authorized Devices (Global)
<b>Policy Purpose</b>	<p>To describe and document Iron Mountain's policy related to authorized devices. Specifically, this Policy provides guidance in the administration and use of handhelds, laptops, tablets and desktops to maximize employee productivity and effectiveness while conducting business, and to ensure the confidentiality, availability and integrity of the systems on our networks and the data stored therein.</p> <p>This Policy applies to all employees, contractors, customers, vendors, guests or other parties performing services for or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates") in all geographies, business lines and functions, including Joint Ventures.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Authorized Devices Administration Antimalware</li> <li>– Authorized Devices Administration Encryption</li> <li>– Authorized Devices Administration Handheld and Tablet Current Settings</li> <li>– Authorized Devices Administration Handheld and Tablet Management</li> <li>– Authorized Devices Administration Inactive Account</li> <li>– Authorized Devices Administration Laptop Desktop Current Settings</li> <li>– Authorized Devices Administration Laptop Desktop Management</li> <li>– Authorized Devices Administration Multi-Function Printers Management</li> <li>– Authorized Devices Administration Policy Exceptions</li> <li>– Authorized Devices Administration Policy Violations</li> <li>– Authorized Devices Administration Repair Replacement Procedure</li> <li>– Authorized Devices Administration Standard Build Documents</li> <li>– Authorized Devices Administration Wipe Command</li> <li>– Authorized Devices Business Use</li> <li>– Authorized Devices Company Issued</li> <li>– Authorized Devices Defined</li> <li>– Authorized Devices General</li> <li>– Authorized Devices Handheld and Tablet Approval</li> <li>– Authorized Devices Laptop and Desktop</li> <li>– Authorized Devices Multi Function Printers</li> <li>– Authorized Devices Network Connection</li> <li>– Authorized Devices Personal Devices</li> <li>– Authorized Devices Unmanaged Personal</li> </ul>

# Access Control

## ACCESS CONTROL POLICY

<b>Policy Name</b>	Access Control Policy (Global)
<b>Policy Purpose and Scope</b>	<p>This policy provides requirements for authorizing and authenticating personnel and systems prior to granting them access to information resources, and for the ongoing management of those access rights.</p> <p>This policy applies to all employees, contractors, vendors, guests or other parties of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– AC Business Requirements Authentication and Authorization</li> <li>– AC Business Requirements Least Required Privilege</li> <li>– AC Business Requirements Managed Process</li> <li>– AC Business Requirements Authentication Information</li> <li>– AC Business Requirements Security Devices and Network Connections</li> <li>– AC Business Requirements User Account Access</li> <li>– AC System and Application Advanced Operating System Utilities</li> <li>– AC System and Application Display and Printing</li> <li>– AC System and Application Legacy Application or System</li> <li>– AC System and Application Logging Events</li> <li>– AC System and Application Resource Administrator Access</li> <li>– AC System and Application Sensitive Configuration Files</li> <li>– AC System and Application Service Account Password Specifications</li> <li>– AC System and Application Service Account Passwords</li> <li>– AC System and Application Service Accounts</li> <li>– AC System and Application Shared Secrets and Passwords</li> <li>– AC System and Application Storing Password</li> <li>– AC System and Application System Development Tools</li> <li>– AC System and Application System Error</li> <li>– AC System and Application Vendor Supplied Defaults</li> <li>– AC System and Application Wireless Network Devices</li> <li>– AC User Access Management Access Control Requests</li> <li>– AC User Access Management Access Review</li> <li>– AC User Access Management Account Reviews</li> <li>– AC User Access Management Audit Trails</li> <li>– AC User Access Management Authentication Methods</li> <li>– AC User Access Management Cross Reference</li> <li>– AC User Access Management Disabled Passwords</li> <li>– AC User Access Management Encrypted Administrative Access</li> </ul>

- 
- AC User Access Management Extended Absence
  - AC User Access Management Failed Login Attempt
  - AC User Access Management Handheld Password Length
  - AC User Access Management New or Change Requests
  - AC User Access Management New Password Requirements
  - AC User Access Management Password
  - AC User Access Management Password Change Process
  - AC User Access Management Password Contents
  - AC User Access Management Password Expiration
  - AC User Access Management Password Expiration Warning
  - AC User Access Management Remote Access
  - AC User Access Management Role Based Access
  - AC User Access Management Segregation of Duties
  - AC User Access Management Temporary Password
  - AC User Access Management Temporary Password Requirements
  - AC User Access Management Third Party
  - AC User Access Management Third Party Access Request
  - AC User Access Management Transfers and Leave
  - AC User Access Management Two Factor Authentication
-

# Physical and Environmental Security

## GLOBAL FACILITY POLICY

<b>Policy Name</b>	Facility Policy (Global)
<b>Policy Purpose</b>	<p>The purpose of this policy is to define physical security requirements and fire protection system requirements for Iron Mountain facilities anywhere in the world that store or process customer assets or carry out corporate functions. This policy applies to all facilities whether purchased, leased, constructed, or retrofitted including facilities that were purchased, leased, constructed or retrofitted by an Iron Mountain majority-owned joint venture.</p> <p>Iron Mountain is committed to:</p> <ol style="list-style-type: none"><li>1. Protecting the lives of our employees, customers and visitors when in an Iron Mountain location.</li><li>2. Monitoring both human and physical threats and applying appropriate combinations of systems and procedures to secure our facilities and protect the customer assets under our control.</li></ol>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Global Facility CFR Buildings</li><li>– Global Facility Changes to Duration</li><li>– Global Facility New Construction Requirements</li><li>– Global Facility Requirements Approach for Physical Security and Fire Protection</li><li>– Global Facility Specification Methodology</li><li>– Global Facility Specification Methodology Application</li></ul>



## IRON MOUNTAIN VISITOR SAFETY &amp; 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, 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.

# Cryptography, Communications and Operations Security

## COMMUNICATIONS AND OPERATIONS MANAGEMENT POLICY

<b>Policy Name</b>	Communications and Operations Management (Global)
<b>Policy Purpose</b>	<p>Iron Mountain's Global Communications and Operations Management Policy outlines the framework for governance of information system operation and intercommunication. Requirements outlined in this policy represent a baseline for the development of standards and procedures documents targeted at specific types of information systems.</p> <p>This policy applies to all employees, contractors, vendors, guests or other parties of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates"), in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Communications Security – Cryptography</li><li>– Communications Security – Information Transfer</li><li>– Communications Security – Network Security Management</li><li>– Operations Security – Backup</li><li>– Operations Security – Control of Operational Software</li><li>– Operations Security – Information Resource Availability</li><li>– Operations Security – Information Systems Audit Considerations</li><li>– Operations Security – Logging and Monitoring</li><li>– Operations Security – Operational Procedures and Responsibilities</li><li>– Operations Security – Protection From Malware</li><li>– Operations Security – Technical Vulnerability Management</li></ul>

## IT SYSTEM LOGGING AND LOG MONITORING POLICY

---

**Policy Name** IT System Logging and Log Monitoring Policy

---

**Policy Purpose** This security policy establishes the criteria for near real-time monitoring of all activities across the Iron Mountain enterprise network, and the creation, maintenance, and protection of system and security logs. This document is intended to provide general policy statements for the collection, content, storage, and review of operating system and application activity logs and security audit logs generated by critical and essential information assets throughout the Iron Mountain enterprise. Auditing the activities of information assets is necessary to detect anomalies, irregularities, and unauthorized activities that violate security policies, while monitoring information assets verifies regulatory compliance. Adherence to the policies specified herein will provide Iron Mountain the ability to maintain compliance with regulatory and customer requirements.

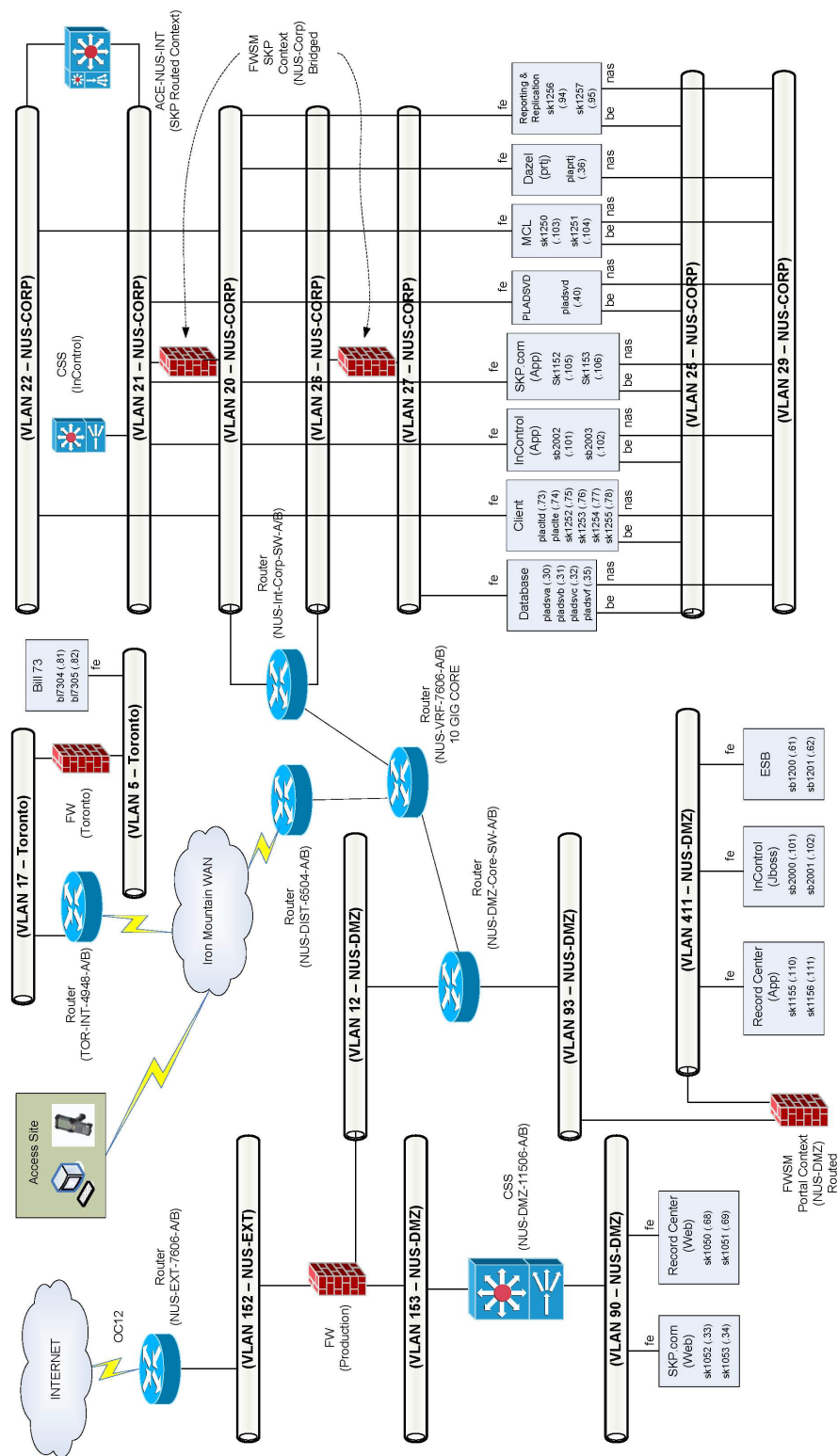
---

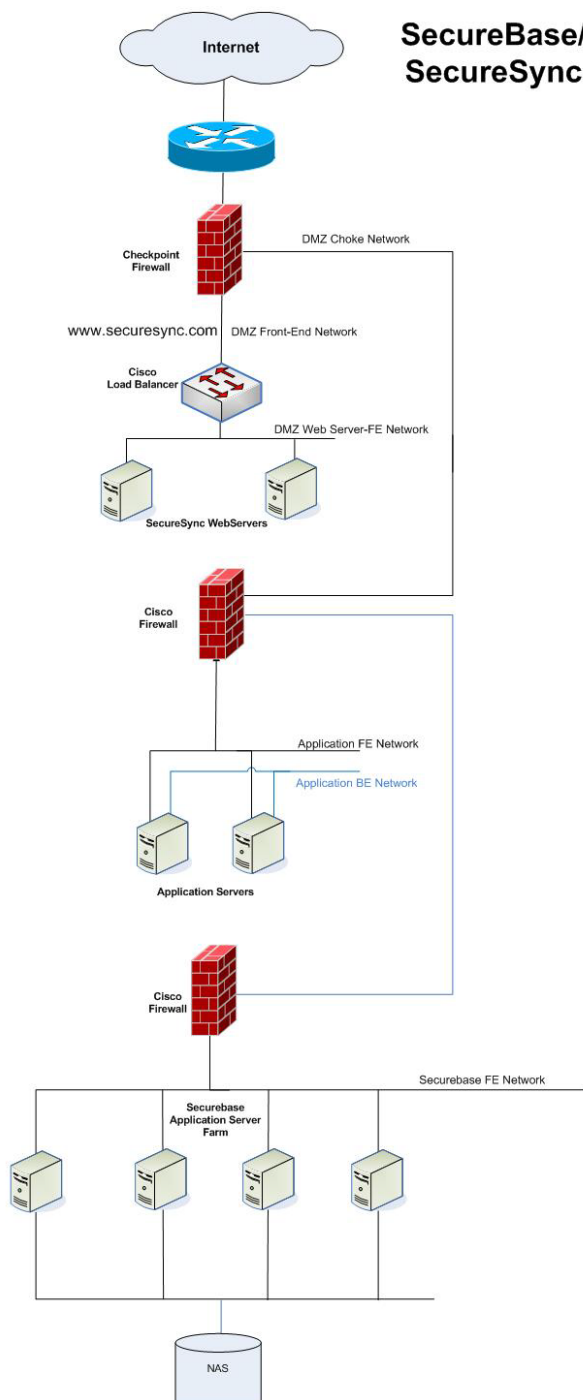
- Key Points**
- Access to Logs
  - Application Logs
  - Clock Synchronization
  - Log Creation
  - Log File Retention
  - Logging Enablement
  - Operating System Logs
  - Security Device and Security Software Logs
  - SIEM (Security Information and Event Management) Logging Requirements
  - System and Security Audit Logs
  - Unauthorized Modifications
-

## INTRUSION DETECTION AND PREVENTION POLICY

<b>Policy Name</b>	Intrusion Detection and Prevention Policy
<b>Policy Purpose</b>	<p>This security policy establishes the criteria for real-time intrusion monitoring of all ingress and egress activities across the Iron Mountain enterprise network. This document is intended to provide general policy statements for sensor hardware, maintenance, network placement, and signature use on network intrusion sensors throughout the Iron Mountain enterprise.</p> <p>Intrusion detection and prevention sensors are necessary to detect network based attacks that put Iron Mountain enterprise infrastructure, assets, data and customer data at availability, integrity, or confidentiality risk.</p> <p>The intent of this policy is to ensure network intrusion detection and prevention sensor signatures correspond to network, application, and system risks inherent to the Iron Mountain enterprise.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Blacklists</li> <li>– Blacklists and Whitelists Filters and Filter Tuning</li> <li>– Blacklists and Whitelists Logging</li> <li>– Blocking Mode Approval Process and Workflows</li> <li>– Blocking Mode Implementation</li> <li>– Blocking Mode Temporary Blocking Enablement</li> <li>– Blocking Mode Testing</li> <li>– Controls Access Restrictions</li> <li>– Controls Change Control Procedures</li> <li>– Controls Legal Compliance</li> <li>– Controls Log Preservation</li> <li>– Controls Logging Systems</li> <li>– Controls Unauthorized Modifications</li> <li>– Enabled Signature Categories</li> <li>– Hardware and Performance Clock Synchronization</li> <li>– Hardware and Performance Decryption</li> <li>– Hardware and Performance Detection and Protection</li> <li>– Hardware and Performance Sensor Construction and Implementation</li> <li>– Maintenance Management Console</li> <li>– Maintenance Sensor and Backup Sensor</li> <li>– Maintenance Vendor Specific Signatures</li> <li>– Network Placement Ingress and Egress Points</li> <li>– Networks Placement Internal Network Sensor</li> <li>– Network Placement Sensor</li> </ul>

## NETWORK ARCHITECTURE DIAGRAMS





# System Acquisition, Development, and Maintenance

## APPLICATION DEVELOPMENT POLICY

<b>Policy Name</b>	34.0 Application Development Policy
<b>Policy Purpose</b>	This policy provides guidance on designing, building and purchasing applications.
<b>Policy Statement</b>	Application development activities should comply with a development methodology that incorporates information security controls into each stage.
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Development environments should be physically, or at a minimum logically, isolated from production environments</li> <li>– Any application developed for Iron Mountain use should be subject to the same information classification and protection requirements as all other information resources</li> <li>– Production data should not be used for testing purposes unless the data has been declassified or all personnel involved in testing are pre-authorized to access the data</li> <li>– Outsourced application development efforts should be subject to the same risk assessments and security controls as internal development efforts</li> <li>– Requests for dispensation from the Iron Mountain Information Security Policy should be reviewed and approved by the Chief Security Officer or an appointed designee</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>– Access to Program Source Libraries</li> <li>– Adherence to a System Development Life Cycle (SDLC)</li> <li>– Adhering to Copyright Laws and License Agreements</li> <li>– Application Controls</li> <li>– Application Development Documentation</li> <li>– Approval for Using Production Data for Testing</li> <li>– Approval of User Training Programs</li> <li>– Approving Production Software</li> <li>– Assessment of New Hardware and Software</li> <li>– Checks Prior to Promoting Applications to Production</li> <li>– Data Conversion</li> <li>– Data Processing Controls</li> <li>– Data Processing Validation and Editing</li> <li>– Default Settings</li> <li>– Definition of Interfaces</li> <li>– Developer Access During Testing</li> <li>– Escrow of Source Code</li> <li>– Evaluating Software for Security Safeguards</li> <li>– File Requirements Definition and Documentation</li> </ul>



- 
- Formulation of Acquisition Strategy
  - Implementation Plan
  - Information Security Review of Business Requirements
  - Input Requirements Definition and Documentation
  - Integrating Security Requirements in System Design
  - Integrating Security Tasks into a Systems Development Life Cycle (SDLC)
  - Isolation of Application Development Activities
  - Modeling Tools
  - Post Implementation Evaluation
  - Processing Requirements Definition and Documentation
  - Production Installs Must Follow a Formal Process
  - Program Specifications
  - Protecting Source Code
  - Protection of Resources Under Development
  - Quality Assurance Process
  - Requesting Exclusion from Security Controls
  - Review of Application Security Features
  - Revising Design Documents to Reflect Changes in Security Requirements
  - Security Features Must be Included in Application Design
  - Security Verification Tests
  - Selection of System Software
  - Software Product Acquisition
  - Source Data Collection Design
  - System Conversion
  - Third-Party Service Requirements
  - Training Users Prior to Production Rollout
  - Use of Output Controls
  - Use of Production Data for Testing Purposes
  - Use of Validation Controls
-

## INFORMATION SECURITY ASSESSMENT PROGRAM



---

### Information Security Assessment Program

---

March 25, 2016 | Version 2016.1

#### Security Assessment Program Introduction

The purpose of the Security Assessment Program is to provide visibility into the risks associated with vulnerabilities in Iron Mountain's infrastructure and electronic business applications. This program demonstrates the importance of reviewing the report and the associated steps needed for remediation by the business and application owners.

This document is divided into the following sections:

- **Services.** Description of the services to be performed
- **Security Program Development.** Involvement with IT, Service Delivery and Engineering groups.
- **Deliverables.** Identifiable work product resulting from the Services

---

#### APPLICATION ARCHITECTURE ASSESSMENT PROCESS

---

An application architecture assessment is designed to provide insight into the constituent elements, and identify typical application use cases and risks which the product or application will encounter through published interfaces. The process also identifies the definition of application roles, and deployment scenarios.

An application architecture assessment is intended to review these components, potential exposures and use case scenarios and rate typical security controls with respect to industry best practices. An application architecture assessment is not intended to identify all vulnerabilities or to enumerate each instance of vulnerability; rather, the assessment process is intended to ensure representational coverage of security control elements throughout the observed functionality within the product.

## GOALS AND OBJECTIVES

---

- Review relevant documentation, including technical design documents, process flows, and security architecture to identify potential vulnerabilities
- Review the product's core functionality, technical requirements including technical specifications, high-level design documents, and technologies in use
- Assess detailed design documentation and conduct interviews with key stakeholders (product architects and developers) to identify the security architecture and areas with potential security exposure
- Identify security vulnerabilities and the impact associated with the most-likely and worst-case exploitation scenarios
- Identify and make recommendations to address security issues of immediate concern
- Develop long-term recommendations to enhance security
- Perform Product Architecture Assessment for each of the following criteria:
  - Administration
  - Authentication
  - Authorization
  - Business Logic
  - Cryptography
  - Data Validation
  - Deployment Configuration
  - Error Handling
  - Network Level Access Controls
  - Secure Communications
  - 3rd party components/dependencies
  - Development of Product Threat Model
  - Rank assessment areas with respect to security industry best practices
  - Identify and make recommendations to address security issues of immediate consequence
  - Develop long-term recommendations and strategic initiatives to enhance security by leveraging industry best practices and Virtual Security Research, LLC's expertise
  - Deliver reports which include findings, analysis, and recommendations
  - Transfer knowledge

## SECURITY CODE REVIEW

---

Once coding has completed its lifecycle and is ready for QA, the security team conducts a security code review in addition to the standard functional code review. This review consists of a focused (time-boxed) evaluation of critical components defined via a high-level threat modeling exercise. The service deliverable is a full remediation plan and customized training module to proactively address identified vulnerabilities and raise the level of knowledge and create a security conscious development organization, using real examples, rather than traditional off the shelf security training. The goal of this service is to identify as many coding vulnerabilities prior to production release.

## APPLICATION ASSESSMENT PROCESS

---

An application code review assessment is designed to highlight potential security vulnerabilities within the application based upon a defined application threat model.

It is intended to identify unsafe coding practices, including but not limited to: authentication, authorization, session management, use of data validation, cryptography, error handling, information leakage, and language specific coding issues.

The following techniques are used to assess a system:

- Interview business and technical staff
- Develop threat model and prioritization
- Perform focused application code review
- Perform limited application verification testing to validate findings uncovered during focused application code review and to identify additional areas of risk
- Document all potential risk areas discovered during focused application code review, including suggested fixes
- Leverage vendor knowledge base
- Prioritize vulnerabilities based on:
  - Ease of exploitation
  - Potential impact to Iron Mountain's business
  - And if exploited, the required effort to remediate the identified vulnerability

---

## GOALS AND OBJECTIVES

Code reviews identify instances of insecure coding practices and other language specific security vulnerabilities. Security source code reviews audit applications for specific security critical components and for implementation level security vulnerabilities. The output of a security code review provides product architects and developers with a detailed list of implementation level security concerns and general remediation guidance to adjust the development process in order to reduce the occurrence of oft repeated coding mistakes.

The code review begins with a review of the software documentation or architecture to understand the software design criteria and interactions. Coding standards, guidelines and policies are reviewed as well as design and architecture documents. After review of the documentation, Development team interviews are planned to learn more about the application's purpose, functionality and the application's high-level architecture. The vendor subject matter experts (SME) discuss the approach to important security issues such as authentication, session management and data validation in order to focus the code review on likely problem areas. The actual code review employs both manual and automated means to inspect the code. As necessary, the vendor will engage developers to address any further questions raised during the code inspection. Each code review focuses on likely problem areas in the application. The following areas are commonly assessed:

- Implementation of authentication, authorization and session management
- User input validation, including the handling of user input data intended to execute additional functions or spawn external programs
- Proper use of cryptography
- Existence of hard coded information
- Proper handling of security-critical data, including authentication credentials and cryptographic keys
- Proper use of security-critical APIs
- Secure interaction with the operating system, web server, file system, etc.
- Appropriate error handling
- Existence of test or debug code not intended for production deployment
- Logging of errors and informational messages
- Information leakage (e.g. unnecessary messages displayed back to the user)
- Adherence to any additional secure code standards required by the Client
- Code maintenance and code complexity

The code assessment is not intended to provide a comprehensive security evaluation of the product; rather, it concentrates on highlighting areas of increased risk exposure, and validating exploitation possibilities when practical. Only when all three-assessment services are combined (architecture, code, and application penetration) is a comprehensive security evaluation able to be determined.

#### APPLICATION PENETRATION TEST

---

An application penetration assessment is designed to highlight potential security vulnerabilities within the application based upon a defined application threat-model. It is intended to identify unsafe coding practices, including but not limited to: authentication, authorization, session management, data validation, use of cryptography, error handling, information leakage, and language specific coding issues.

#### GOALS AND OBJECTIVES

---

The purpose of the assessment is to evaluate an application, its security architecture, enumerating potential threats, and validating those threats during the application penetration assessment component of the engagement.

The assessment is designed to achieve the following key objectives:

- Review relevant documentation, including technical design documents, process flows, and security architecture to identify potential vulnerabilities
- Review the application's core functionality, technical requirements including technical specifications, high level design documents, and technologies in use
- Assess detailed design documentation and conduct interviews with key stakeholders (application architects and developers) to identify the security architecture and areas with critical security exposures
- Analyze the interaction between the application and integrated components or products
- Identify security vulnerabilities and the impact associated with the most-likely and worst-case exploitation scenarios
- Develop long-term recommendations to enhance security
- Analyze applications in a production similar environment as per the agreed upon Iron Mountain deployment specifications
- Perform informed vulnerability tests attempting to:
  - Circumvent authentication and authorization mechanisms
  - Circumvent application session management
  - Break or analyze use of cryptography within user accessible components
  - Escalate application user privileges
  - Alter data or data presentation
  - Corrupt application and data integrity, functionality, and performance
- Determine possible extent access or impact to the system by attempting to exploit vulnerabilities
- Prioritize vulnerabilities based on difficulty of exploit, remediation effort required, and impact of exploit on business
- Conduct additional research to support analysis and proof of vulnerabilities
- Identify and make recommendations to address security issues of immediate consequence
- Develop long-term recommendations and strategic initiatives to enhance security by leveraging industry best practices
- Deliver report which includes findings, analysis, and recommendations
- Transfer knowledge

The application penetration assessment is not intended to provide a comprehensive security evaluation, outlining every instance of a given vulnerability; rather, it concentrates on highlighting areas of increased risk exposure, and validating exploitation possibilities when feasible.

#### INFRASTRUCTURE ASSESSMENT

---

An overall risk profile of the infrastructure is determined as a baseline for the program going forward. A penetration test of the infrastructure provides the results necessary for the baseline. A penetration test models specific threat scenarios against a network and its supported services. The testing imitates a malicious attacker with an intended goal, for example: “compromise a host in our DMZ,” “access the corporate database,” or “break in to a custom application.” The penetration test provides insight into methods of attack against a network. This is a point-in-time reference.

Specific services include:

- Reviewing technical architecture including technical specifications and high-level design documentation
- Performing reconnaissance to develop an overall representation of the network, including topology, devices and hosts, and services
- Testing identified components to gain access to network:
  - Network devices such as firewalls, routers, and switches
  - Hosts such as web, FTP, database, application, and mail servers
- Play the role of an Iron Mountain customer to determine the ability to exploit customer data as well as Iron Mountain internal networks
- Identifying and validating vulnerabilities
- Ranking vulnerabilities based on ease of exploit, effort required for remediation, and impact to business if exploited
- Identifying and suggesting recommendations to address security issues of immediate consequence
- Developing long-term recommendations to enhance security
- Transfer of knowledge to system administrators, developers, engineering, and infrastructure personnel

The goal of this service is to provide a final opportunity to discover and remediate application and infrastructure vulnerabilities prior to production release.

#### QUARTERLY RE-TEST

---

- Re-test identified vulnerabilities and validate.
- Comprised of an application test separate from the baseline scan.
- Targeted test with knowledge gained from baseline.
- Emulate a signed customer with login information to the application in an attempt to cause the application to do something it was not designed to do.
- This test also focuses on detailed exploration into the vulnerabilities of the code or the infrastructure the application is installed on.

#### CUSTOMIZED TRAINING

---

At all points in this service offering there are opportunities for knowledge transfer. These opportunities are used to create customized training using real examples of exploited conditions to solidify security concepts and best practices around development and infrastructure configuration. The goal of this service is to increase knowledge and ultimately reduce our assessment costs by building, deploying and maintaining secure application environments.

Application Developers are the intended audience for this level of training. The course is conducted in a way that does not exemplify an individual's coding expertise and is designed to show examples of flaws and then provide real solutions.

**Security Program Development**

- Provide subject matter expertise regarding program development, regulatory requirements, and information security staff development
- Tool identification and analysis
- Policy framework and Standards
- Task prioritization for remediation
- Risk analytics

**Deliverables**

At the completion of this effort, our vendor will deliver a document containing the following components:

- Executive summary
- Objectives and process
- Analysis and details of security issues
- Recommendations to reduce risk, enhance operation, and improve scalability, including:
  - Architectural alternatives
  - Industry best practices and design principles
  - Recommendations to address security issues of immediate consequence
- Recommended next steps that support business initiatives
- Customer Facing Deliverable outlining Iron Mountain's Security posture as it relates to industry best practices.

**Summary**

The goals will be achieved annually through a series of checks and balances outlined above at key points in the lifecycle of a production application. This coupled with a customized training approach using the findings during each analysis point creates a security conscious IT culture that will build skill sets, reduce cost, increase efficiency and build consumer trust.



## SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SUMMARY

### Overview

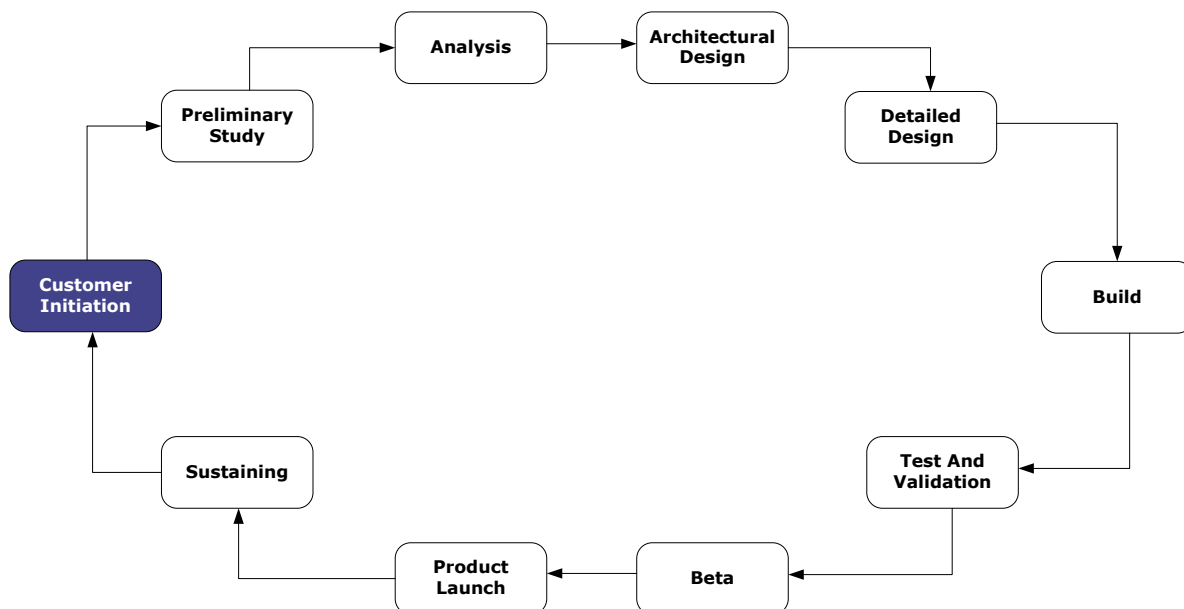
Iron Mountain's SDLC is an approved methodology which IT organizations and independent business units are encouraged to adopt.

Although prescriptive in nature, the SDLC's applicability and implementation by the various development groups across Iron Mountain's enterprise may be different.

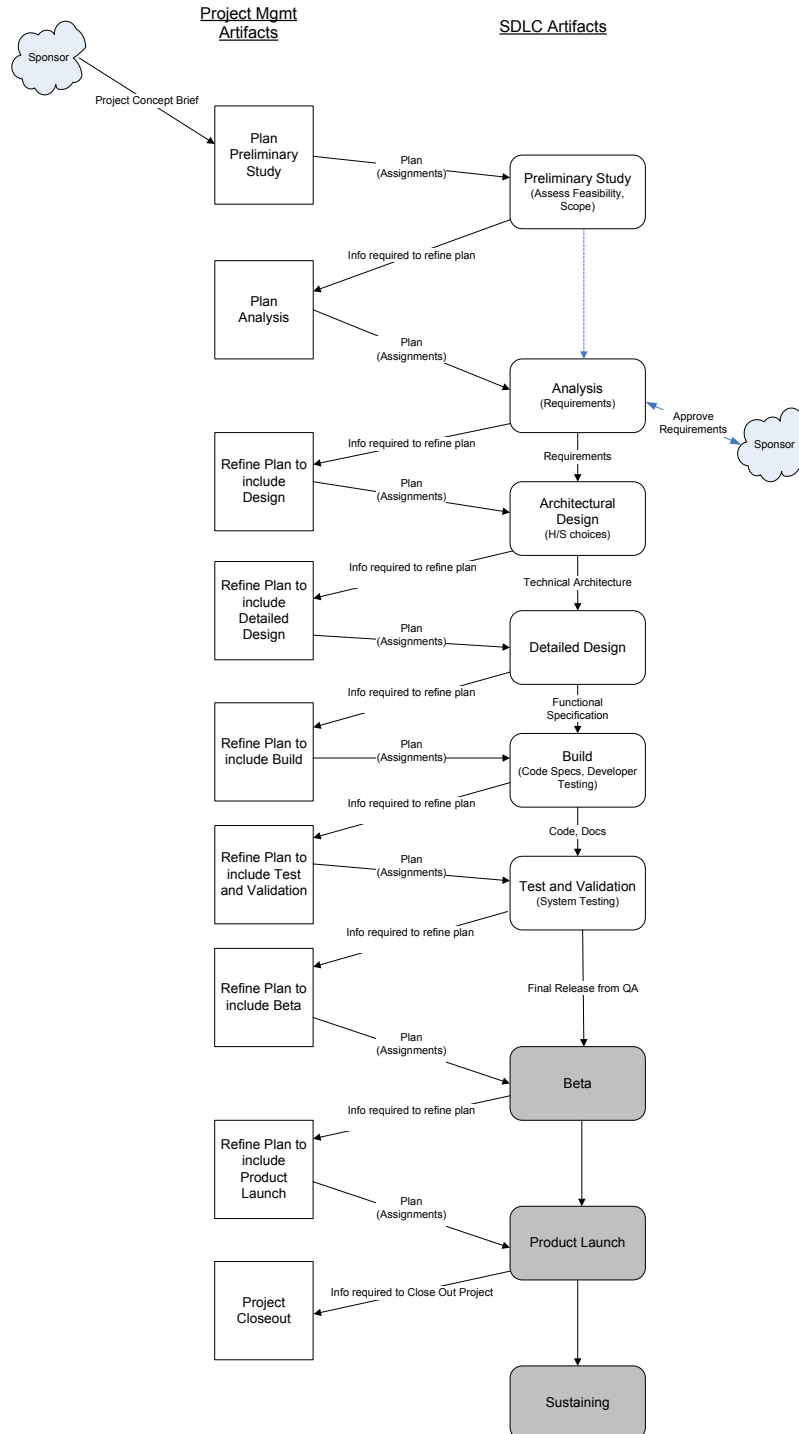
Iron Mountain's SDLC contains the following 10 phases:

- **Customer Initiation**
- **Preliminary Study**
- **Analysis**
- **Architectural Design**
- **Detailed Design**
- **Build**
- **Test and Validation**
- **Beta**
- **Product Launch**
- **Sustaining**

The relationships of the phases are shown in the process model:



## SDLC and Project Management Flow



## THE PHASES:

### Customer Initiation

The first phase, Customer Initiation, acts as a placeholder for the various ways a customer may initiate a project with engineering.

### Preliminary Study

The first engineering phase of the SDLC is the Preliminary Study. This study serves two purposes: first it allows the project manager and the project team to evaluate the amount and quality of work that was done by the customer prior to requesting a project. The project manager can determine if the proper information is available to begin the project or what needs to be done to get started. Secondly, the Preliminary Study provides the team the opportunity to determine if a solution is feasible without spending a great deal of money and time.

It is appropriate to think of the Preliminary Study as a small-scale systems study-containing aspects of the Analysis and Architectural Design phases. The central artifact, Preliminary Findings, has sections to capture requirements at a cursory level and architectural design choices based on those requirements. Each of the primary sections is a precursor to an artifact in a later phase where the analysis and design work is done completely.

At the end of a preliminary study, the project team will have a good understanding of the request and the customer will have an estimate of the resources necessary to accomplish the project.

An objective of the preliminary study is to present information on a requested project to customers and management so that they can make decisions whether it is worthwhile to do further analysis and design.

Possible decisions are:

- Proceed immediately with the project as currently proposed
- Place the project into the project portfolio, prioritized to begin at a later date
- Modify the recommended solution and then continue
- Reevaluate the preliminary study
- Cancel any further investigation

### Analysis

The Analysis phase continues the work completed in the Preliminary Study. The goal of the Analysis phase is to understand the customer's requirements and create the information necessary to communicate the requirements to the developers, technical writers, user experience analysts and quality assurance analysts so that a correct solution can be designed, built and tested.

At times, in order to understand new requirements it is necessary to recapture information about the Current State. This recapture is designed to create an understanding of what is currently being done, how it is being done, what nonfunctional requirements are currently being met, and what areas are not performing as required.

The primary emphasis in Analysis is to fully define the functional requirements for a new product or application and the new non-functional requirements.

### Architectural Design

The purpose of the Architectural Design phase is to create a system's architecture for products being developed. The architecture consists essentially of hardware components and software components. Software can be subdivided into a tier structure with different components for each item: UI, database, middleware, operating system, etc.

Also, choices of outside services or components, COTS, off-site data storage, etc. are to be considered.

The key to this process is to generate alternatives and evaluate them against:

- Project constraints
- The ability to meet functional and nonfunctional requirements
- The long term strategy and product set defined by the Enterprise Architecture organization

The goal is to create a systems architecture that meets requirements, fits within the constraints of the project, and is in line with Enterprise Architecture strategies and product sets. This means it must be acceptable to both business and IT management.

Once a specific architecture has been selected it can be elaborated further in the detailed design phase.

### Detailed Design

The purpose of this phase is for engineering to expand the system's architecture agreed upon in the previous phase and create detailed specifications that can be used to create and test the product. Also, as requirements can be viewed in a more concrete form the testing strategy begun in the analysis phase can be expanded as well. Also it may be practical and desirable to begin usability testing so that customers can experience the product early before the build phase begins.

### Build

The purpose of the build phase is to create the product. Primarily this involves specifying, creating, and testing the source code. The complete product however may consist of other items including manuals, user guides, and online help. Each of these items is also subject to testing as well.

Also, during this phase any work done to create or update the hardware necessary to support the product begins here.

### Test and Validation

The purpose of this phase is for QA to test the product prior to use by:

- A sub-set of the user community, prior to release of the product/application to Beta testing (if applicable) *and/or*
- Normal customer use by the business community or Iron Mountain customers.

The types of testing conducted depend on the scope of the project. Appropriate testing types consist of: Build Verification Testing, Functional Testing, Non-Functional Testing, Acceptance Testing/User Acceptance Testing, Regression testing, Installation Testing and Rollback Testing. Each test, Functional, Regression, etc. provides for a feedback loop. Results of test are summarized and a Pass/Fail Grade is applied. If the test fails the results are used to plan another cycle of the test; if the test passes, the product or portion of the product is released to the next process.

An Installation Checklist is created in this phase that is subsequently used to guide the work of the installation team.

Pre-defined entry and exit criteria specify all initial deliverables are available and no critical issues are open at the end of test execution.

**Beta**

Beta testing refers to testing of a new product, system or service under controlled conditions, to a sub-set of the user community prior to release of the product/application for normal customer use. Beta Testing can be done prior to the release to production or after installation. Beta testing done prior to installation is designed to ultimately obtain the user's acceptance of the new product and provide engineering with the confidence that the product can be released into production. Beta testing done after installation is designed to capture any undiagnosed defects and to correct them prior to rolling out the application to a wider audience.

In either case production activity is monitored and validated throughout the Beta period. As with all tests, its purpose is to validate that the product will work properly, is usable, and meet customer requirements along with ensuring that proper support infrastructure and processes are in place.

The Beta Test Strategy is a composite of tests, each having its own objective, test cases, and procedures.

**Product Launch**

The purpose of this phase is for engineering to install the product for use by the business community or Iron Mountain customers. The Installation Checklist created in the test and validation phase is used to guide the work of the installation team. Installation activities must be coordinated with activities being done by the business community in preparation for the new application or product. Also, installation must be coordinated with IT services to ensure that the product or application can be deployed into the correct environment, on the correct hardware and that all concerned, including support personnel, will be aware that the product has been launched.

**Sustaining**

This is the operational phase of a product's life. Initially this is the phase where the engineering team evaluates the completed project. This evaluation referred to as a post implementation review consists of three separate reviews or at least has three separate goals:

1. Assess the quality of the work done to create the product
2. Assess the quality of the product
3. Evaluate if the resulting product is achieving business objectives

It is also in the Sustaining phase that information regarding the performance characteristics of the project or product is captured. These can be used to provide the information to both IT and customer management regarding the costs to operate the system over its lifespan. This information can contribute to an end-of-life decision for the product.

# Supplier Relationships

## THIRD-PARTY RISK MANAGEMENT POLICY

<b>Policy Name</b>	Third Party Risk Management Policy Global
<b>Policy Purpose</b>	This policy provides guidance to control the use of third-party services.
<b>Policy Statement</b>	Third parties must adhere to all Iron Mountain Policies related to the provision of services, equipment and material ("Services" include resellers of IRM product) to Iron Mountain and shall acknowledge their obligations as a third party through formal written documents.
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Contracts</li><li>– Due Diligence</li><li>– Exceptions to this Policy</li><li>– Ongoing Third Party Relationship Management</li><li>– Third Party Risk Management Program</li><li>– Treatment of Confidential Information</li></ul>

## OVERVIEW OF THIRD-PARTY RISK ASSESSMENT PROGRAM – NORTH AMERICA

Iron Mountain conducts reviews of its third-party business partners. These reviews include an initial survey completed by the business unit sponsor responsible for the relationship.

The business unit sponsor answers qualifying questions based on the services the third-party provides. These answers generate a risk score and based on the risk score and the analyst review the third-party is classified as Critical, High, Medium or Low Risk. The profile contains several data points used to determine the risk level based on interaction with Iron Mountain or Iron Mountain customers:

- Physical or logical access to assets and information
- Storage and transportation of hard copy or electronic information
- Utilization of contractors
- Single points of failure

Following this initial assessment, the third-party will be asked to answer up to 269 questions pertaining to the below subject areas, as it pertains to the services the third-party will be providing.

- Physical or logical access
- Risk Assessment and Treatment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Physical and Environmental Security (Digital)
- Communications/Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Business Continuity Management (Digital)
- Compliance
- Third-Party Management
- Third-Party Management (Digital)
- Insurance (low)
- Insurance (medium)
- Insurance (high)
- Cloud
- EU PII
- HIPAA
- ITAR
- Transportation



Answers to questions are reviewed by the Iron Mountain Global Safety, Risk and Security (GSRS) team to determine that proper information and general security controls are in place. If necessary, the GSRS team will consult with subject matter experts such as Legal, InfoSec, Privacy & Compliance, Procurement, and other teams to evaluate and mitigate risks. Any acceptable unresolved issues are entered into a Risk Register and tracked to resolution.

In addition, the GSRS team may conduct reputational due diligence reviews of the third-party's operations to identify any other matters that may cause undue risk to Iron Mountain or its customers.

# Risk Management

## OPERATIONAL RISK POLICY

<b>Policy Name</b>	Operational Risk Policy
<b>Policy Purpose</b>	<p>Iron Mountain operates an Operational Risk Framework (“Framework”) that provides a structured approach to identification, assessment, management and reporting of risks associated with our processes, people and systems that may impact Iron Mountain’s strategic business objectives and the information it processes. The purpose of the Framework is to improve our resilience to risk by reducing the likelihood that objectives are jeopardized by events and the impact on the business if they do occur.</p> <p>The Framework is directed by the Senior Executive Team who act in the interests of the Company’s shareholders, employees, customers and the community at all times. This policy applies to all wholly owned entities and majority-owned joint ventures performing services for, or on behalf of Iron Mountain, in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Operational Risk Communications</li><li>– Operational Risk Methodology</li><li>– Operational Risk Reporting</li><li>– Operational Risk Responsibilities and Accountabilities</li><li>– Operational Risk Training Strategy</li><li>– Operational Risk Trends and Root Causes</li></ul>

## GLOBAL INTERNAL AUDIT



---

## Global Internal Audit Overview

---

Internal Audit at Iron Mountain is an independent appraisal activity chartered to examine and evaluate the Company's activities as a service to the organization. The objective of the Iron Mountain Internal Audit Department is to assist Iron Mountain management in the effective discharge of their responsibilities by providing independent, objective assurance and consulting services designed to add value and improve the operations of our Company globally. Internal Audit accomplishes this by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of the business risk management, internal control, and governance processes.

The scope of internal audit work performed within the Iron Mountain Companies is risk-based and includes operational, information security, anti-bribery anti-corruption and financial reviews across the global enterprise. Operational reviews focus on key operational risks, such as chain of custody, physical security and employee safety. Information Security audits focus on General Computer Controls and Applications Security and general vulnerability risks. Financial reviews focus on financial process integrity and accounting basics while Anti-Bribery Anti-Corruption reviews measure the Organization's compliance to legislature such as the US Foreign Corrupt Practices Act and the UK Anti-Bribery Act.

Entities are selected for review based on the results of the comprehensive risk assessment performed by the Internal Audit Department. A key input into this process is the Enterprise Risk Assessment, which identifies relevant business risks to the enterprise.

In addition to the work performed by Global Internal Audit Services, our External Auditors also perform analysis and testing of selected market operations as part of their year-end and interim audit work. The results of these reviews are communicated to Senior Management upon completion.

### Operational Reviews

Operational reviews are conducted by market in North America and by country or subsidiary level outside of North America. These reviews include but are not limited to the following functions, as appropriate:

- Administrative Processes
- Account Initiation and Retention
- Record Center, Vault Library, and Fulfillment Center Workflow
- Customer Billing and Revenue Management
- Procurement and Disbursement Procedures
- Safety and Security Processes
- Information System Procedures
- Business Resumption and Disaster Recovery
- Fleet Management
- Inventory and Revenue System Testing

### Internal Audit Department Background

The Internal Audit Department is an independent function which reports to the Audit Committee of the Iron Mountain Board of Directors. The Internal Audit function at Iron Mountain is authorized through its Charter to have unrestricted access to all functions, records, property, and personnel of Iron Mountain Inc., worldwide, and full and free access to the Audit Committee.

The Iron Mountain Internal Audit Department is also empowered to allocate resources, set audit frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives. Internal Audit can obtain, as required, the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized services from within or outside the organization, as required. The Internal Audit team includes individuals with diverse skill sets and work experience.

**Field Audit Process: Management Self-Assessment**

The Field Audit program is designed to bring awareness to various operational, workflow, safety and security risks across our Global Iron Mountain Operations. Global Internal Audit's role includes strategic involvement meant to assess any changes to the Field Audit structure in the current year. Global Internal Audit also performs an independent validation highlighting compliance to high risk operational criteria while ensuring key issues across Global operations are reported and appropriately remediated.

Global Internal Audit participates in various training and business stakeholder forums resulting in guidance rendered to Field Audit resources, functional expertise and Management leadership. Any significant observations are reported to the Iron Mountain Board of Directors to ensure informed decision and appropriate coverage are in place to protect our Company's brand, employees and services offered to our customers.

**Compliance Reviews: Foreign Corrupt Practices Act (FCPA)**

The Board and Iron Mountain Global Audit have recognized the importance of having an effective Anti-Bribery and Anti-Corruption framework and adopted a "zero tolerance" policy to ensure appropriate monitoring and compliance reporting over the bribery and corruption of foreign official in order to gain or retain business. The coverage within the ABAC framework is driven by an annual risk assessment process designed to evaluate the degree of corruption and compliance risk across our Global operations. In partnership with the Corporate Compliance and the Global Safety, Risk and Security functions, a number of periodic reviews are performed designed to improve compliance as well as continuous monitoring, policy awareness and training.

**Sarbanes Oxley (SOX) Program**

The overall objective of the SOX Program is to ensure that Iron Mountain remains compliant with the requirements set forth in the Sarbanes-Oxley Act of 2002 and to support the overall organizational business objectives from a Financial Internal Controls perspective. The SOX program focuses on the business and IT processes throughout Iron Mountain's Operations.

Our SOX risk assessment approach is systematic and rational, utilizing a top-down and risk-based approach and a business process approach. The design of the control framework is formally assessed throughout the year; in addition, key personnel must attest that the controls within their respective areas are designed and operating effectively.

Provided by Internal Audit Department | 03.21.2016

## CERTIFICATE OF LIABILITY INSURANCE – GENERAL



## CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)  
10/30/2015

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

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

<b>PRODUCER</b> Marsh USA, Inc. 1166 Avenue of the Americas New York, NY 10036 Attn: Norwalk.certrequest@marsh.com Fax: 212-948-0929  849434-GAWU-15-16		<b>CONTACT</b> NAME: PHONE (A/C, No, Ext): E-MAIL: ADDRESS: INSURER(S) AFFORDING COVERAGE <b>INSURER A:</b> ACE American Insurance Company <b>INSURER B:</b> Indemnity Insurance Company of North America <b>INSURER C:</b> ACE Property and Casualty Insurance Company <b>INSURER D:</b> Agri General Insurance Company <b>INSURER E:</b> N/A <b>INSURER F:</b>		<b>NAIC #</b> 22667 43575 20699 42757 N/A
<b>INSURED</b> IRON MOUNTAIN INCORPORATED ONE FEDERAL STREET BOSTON, MA 02110				

<b>COVERAGES</b>		<b>CERTIFICATE NUMBER:</b> NYC-007381347-12		<b>REVISION NUMBER:</b> 10		
THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.						
INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER:		HDOG27400826	11/01/2015	11/01/2016	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 25,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 10,000,000 PRODUCTS - COMP/OP AGG \$ 1,000,000 \$
A	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS		ISAH08864986	11/01/2015	11/01/2016	COMBINED SINGLE LIMIT (Ea accident) \$ 2,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
C	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$ 10,000		G27918359 001	11/01/2015	11/01/2016	EACH OCCURRENCE \$ 10,000,000 AGGREGATE \$ 10,000,000 \$
B	<input checked="" type="checkbox"/> WORKERS COMPENSATION AND EMPLOYERS' LIABILITY <input type="checkbox"/> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) <input type="checkbox"/> If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	WLRC48592958 (AOS) WLRC48592971 (AZ,CA,MA) WLRC48593227 (TN) SCFC4859296A (WI)	11/01/2015 11/01/2015 11/01/2015 11/01/2015	11/01/2016 11/01/2016 11/01/2016 11/01/2016	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
A	EXCESS WC & EMP. LIABILITY		WCUC48592983 (OH, WA)	11/01/2015	11/01/2016	Each Accident/Emp for Disease 1,000,000 SIR 500,000
<b>DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)</b> Coverage includes Iron Mountain Inc and all subsidiaries and affiliates including: Iron Mountain Information Management, LLC, Iron Mountain Information Management Services, Inc. and Iron Mountain Secure Shredding Inc., and Iron Mountain Fulfillment Services, Inc. and Iron Mountain Intellectual Property Management Inc.						


<b>CERTIFICATE HOLDER</b> Iron Mountain Incorporated One Federal Street Boston, MA 02110	<b>CANCELLATION</b> SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE of Marsh USA Inc. Steve Ruisi
---	--

© 1988-2014 ACORD CORPORATION. All rights reserved.

ACORD 25 (2014/01)

The ACORD name and logo are registered marks of ACORD

## CERTIFICATE OF LIABILITY INSURANCE – WAREHOUSE

 <b>CERTIFICATE OF LIABILITY INSURANCE</b>						DATE: 10/30/15			
THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.									
IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).									
PRODUCER Willis of New York, Inc. 200 Liberty Street New York, NY 10281				CONTACT NAME: Willis Certificate Center PHONE (A/C, No, Ext): 877-945-7378 E-MAIL: certificates@willis.com ADDRESS:				FAX (A/C, No):	
INSURED Iron Mountain and all subsidiaries Iron Mountain Information Management One Federal Street Boston, MA 02110				INSURER(S) AFFORDING COVERAGE INSURER A: National Union Fire Insurance Company of Pittsburgh, PA INSURER B: Allianz Underwriters Insurance Company				NAIC# 19445 36420	
COVERAGES									
CERTIFICATE NUMBER:									
REVISION NUMBER:									
THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN. THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.									
INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS		
	<input type="checkbox"/> GENERAL LIABILITY <input type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR <input type="checkbox"/> GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC						EACH OCCURRENCE DAMAGES TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS-COMP/OP AGG		
	<input type="checkbox"/> AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS						COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$		
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION \$						EACH OCCURRENCE \$ AGGREGATE \$ \$		
	<input type="checkbox"/> WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A					<input type="checkbox"/> WC STATUTORY LIMITS <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$		
A	Professional Liability / Errors & Omissions and Security and Privacy Liability			01-825-57-99	11/1/15	11/1/16	\$4,000,000		
B	Excess Professional Liability / Errors & Omissions and Security and Privacy Liability			ART20132260	11/1/13	11/1/16	\$5,000,000 (excess)		
DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)									
Coverage includes Iron Mountain Inc. and all subsidiaries and affiliates including Iron Mountain Information Management, LLC, Iron Mountain Information Management Services, Inc. and Iron Mountain Secure Shredding Inc., and Iron Mountain Fulfillment Services, Inc. and Iron Mountain Intellectual Property Management Inc. Cyber Liability is included under the E&O policy.									
CERTIFICATE HOLDER					CANCELLATION				
Iron Mountain Information Management Services, Inc. One Federal Street Boston MA 02110 USA					SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <i>Willis of New York, Inc.</i>				

ACORD 25 (2010/05)

 ©1988-2010 ACORD CORPORATION. All rights reserved  
 The ACORD name and logo are registered marks of ACORD



## FM GLOBAL CERTIFICATE OF PROPERTY INSURANCE



Factory Mutual Insurance Company  
 1175 Boston-Providence Turnpike  
 P.O. Box 9102  
 Norwood, Massachusetts  
 02062  
 United States of America  
 Tel: (1) 781 440-8000  
 Fax: (1) 781 440-8742

**POLICY INFORMATION FORM**

This document is issued as a matter of information only and confers no rights upon the document holder. This Policy Information Form does not amend, extend, or alter the coverage, terms, exclusions, conditions, or other provisions afforded by the policy. We hereby certify that insurance coverage is now in force with our Company as outlined below.

<b>Policy No.:</b>	1007574	<b>Policy Term</b>	
<b>Account No.:</b>	1-53244	<b>Effective Date:</b>	01 November 2015
		<b>Expiration Date:</b>	01 November 2016

**NAMED INSURED:**

Iron Mountain Incorporated

**DESCRIPTION AND LOCATION OF PROPERTY COVERED:**

Real and Personal Property

**Location No.:**

**INDEX No.:**

MULUS

All Insured Locations

USA

**COVERAGE IN FORCE:** (subject to limits of liability, deductibles and conditions in the Policy)

<b>Insurance Provided:</b>	<b>Peril:</b>	<b>Limit Of Liability:</b>
Property Damage	All Risk	USD 10,000,000
<b>CERTIFICATE TERM:</b>		<b>Effective:</b> 01 November 2015
		<b>Expires:</b> 01 November 2016

Real and Personal Property in which the Insured owns or has an insurable interest.

This Policy Information Form is to show evidence of "All Risk" of Physical Loss or Damage coverage, including flood, wind and earthquake as respects all locations of Iron Mountain (includes all worldwide locations, operating entities and business lines including: Records Management, Information Management, Off-Site Data Protection, Secure Shredding, Intellectual Property Management, Film & Sound, Consulting, Digital Services, National Underground Storage, Fulfillment Services, Connected Corporation, Archives One Inc., Live Vault, RMS Services - USA and Stratify).

Replacement Value Basis; Coverage includes Boiler & Machinery and Loss of Rents

Thirty (30) days prior written notice of cancellation applies

Certificate No: 00341-001



Iron Mountain Incorporated  
 One Federal Street  
 Boston, Massachusetts 02110-2004, USA

Authorized Signature / Issue Date  
 Michael J. Ryan / 12 November 2015


For questions, contact: Tina Burke



## CERTIFICATE OF INSURANCE - CRIME

 <b>CERTIFICATE OF LIABILITY INSURANCE</b>		DATE (MM/DD/YYYY) 11/05/2014				
THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.						
<b>IMPORTANT:</b> If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).						
<b>PRODUCER</b> Willis of New York, Inc. c/o 26 Century Blvd. P. O. Box 305191 Nashville, TN 37230-5191		<b>CONTACT NAME:</b> PHONE (AC, NO, EXT): 877-945-7378 FAX (AC, NO): 888-467-2378 E-MAIL: certificates@willis.com ADDRESS:				
<b>INSURED</b> Iron Mountain One Federal Street Boston, MA 02110		INSURER(S) AFFORDING COVERAGE INSURER A: Allianz Underwriters Insurance Company NAIC# 36420-001 INSURER B: INSURER C: INSURER D: INSURER E: INSURER F:				
<b>COVERAGES</b> <b>CERTIFICATE NUMBER:</b> 22341499 <b>REVISION NUMBER:</b>						
THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.						
INSR LTR	TYPE OF INSURANCE	ADDL INSD SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
	<b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:					EACH OCCURRENCE \$ DAMAGE TO RENTED PREMISES (EA OCCURRENCE) \$ MED EXP (Any one person) \$ PERSONAL & ADV INJURY \$ GENERAL AGGREGATE \$ PRODUCTS - COMPIOP AGG \$ \$
	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS					COMBINED SINGLE LIMIT (Ea accident) \$ BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
	<b>UMBRELLA LIAB</b> <input type="checkbox"/> OCCUR <b>EXCESS LIAB</b> <input type="checkbox"/> CLAIMS-MADE DED <input type="checkbox"/> RETENTION \$					EACH OCCURRENCE \$ AGGREGATE \$ \$
	<b>WORKER'S COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? <input type="checkbox"/> Y/N (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A				PER STATUTE <input type="checkbox"/> OTH-ER <input type="checkbox"/> E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
A	Crime		ART 2013 2260	11/1/2013	11/1/2016	\$5,000,000 Limit
DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required) Coverage includes Iron Mountain Inc and all subsidiaries and affiliates including: Iron Mountain Information Management, LLC, Iron Mountain Information Management Services, Inc. and Iron Mountain Secure Shredding Inc., and Iron Mountain Fulfillment Services, Inc. and Iron Mountain Intellectual Property Management Inc.						
<b>CERTIFICATE HOLDER</b>  Evidence of Insurance :				<b>CANCELLATION</b> SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE 		
ACORD 25 (2014/01)      Coll:4557543 Tpl:1885775 Cert:22341499      © 1988-2014 ACORD CORPORATION. All rights reserved. The ACORD name and logo are registered marks of ACORD						

## CERTIFICATE OF LIABILITY INSURANCE - CYBER SECURITY

 <b>CERTIFICATE OF LIABILITY INSURANCE</b>		DATE: 10/30/15	
THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.			
IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).			
PRODUCER Willis of New York, Inc. 200 Liberty Street New York, NY 10281		CONTACT NAME: Willis Certificate Center PHONE (A/C, No, Ext): 877-945-7378 FAX (A/C, No): E-MAIL: certificates@willis.com ADDRESS:	
INSURED Iron Mountain and all subsidiaries Iron Mountain Information Management One Federal Street Boston, MA 02110		INSURER(S) AFFORDING COVERAGE INSURER A: National Union Fire Insurance Company of Pittsburgh, PA INSURER B: Allianz Underwriters Insurance Company NAIC# 19445 36420	
COVERAGES		CERTIFICATE NUMBER:	
THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN. THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.		REVISION NUMBER:	
INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD
	GENERAL LIABILITY <input type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC		
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS <input type="checkbox"/> NON-OWNED AUTOS		
	UMBRELLA LIAB <input type="checkbox"/> OCCUR EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input type="checkbox"/> RETENTION \$		
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? <input type="checkbox"/> YES (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	N/A	
A	Professional Liability / Errors & Omissions and Security and Privacy Liability		01-825-57-99
B	Excess Professional Liability / Errors & Omissions and Security and Privacy Liability		ART20132260
			11/1/15 11/1/16
			11/1/13 11/1/16
			\$4,000,000
			\$5,000,000 (excess)
DESCRIPTION OF OPERATIONS/LOCATIONS/VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)			
Coverage includes Iron Mountain Inc. and all subsidiaries and affiliates including Iron Mountain Information Management, LLC, Iron Mountain Information Management Services, Inc. and Iron Mountain Secure Shredding Inc., and Iron Mountain Fulfillment Services, Inc. and Iron Mountain Intellectual Property Management Inc. Cyber Liability is included under the E&O policy.			
CERTIFICATE HOLDER		CANCELLATION	
Iron Mountain Information Management Services, Inc. One Federal Street Boston MA 02110 USA		SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE <i>Willis of New York, Inc.</i>	

ACORD 25 (2010/05)

 ©1988-2010 ACORD CORPORATION. All rights reserved  
 The ACORD name and logo are registered marks of ACORD

## CANADA GENERAL LIABILITY INSURANCE



## Certificate of Insurance

No.: 2015-39

Dated: October 29, 2015

This document supersedes any certificate previously issued under this number

This is to certify that the Policy(ies) of insurance listed below ("Policy" or "Policies") have been issued to the Named Insured identified below for the policy period(s) indicated. This certificate is issued as a matter of information only and confers no rights upon the Certificate Holder named below other than those provided by the Policy(ies).

Notwithstanding any requirement, term, or condition of any contract or any other document with respect to which this certificate may be issued or may pertain, the insurance afforded by the Policy(ies) is subject to all the terms, conditions, and exclusions of such Policy(ies). This certificate does not amend, extend, or alter the coverage afforded by the Policy(ies). Limits shown are intended to address contractual obligations of the Named Insured.

Limits may have been reduced since Policy effective date(s) as a result of a claim or claims.

<b>Certificate Holder:</b> Iron Mountain Incorporated 195 Summerlea Road Brampton, ON L6T 4P6	<b>Named Insured and Address:</b> Iron Mountain Incorporated 195 Summerlea Road Brampton, ON L6T 4P6
--	---

**This certificate is issued regarding:**

Evidence of Insurance

Type(s) of Insurance	Insurer(s)	Policy Number(s)	Effective/ Expiry Dates	Sums Insured Or Limits of Liability	
COMMERCIAL GENERAL LIABILITY • Occurrence Format	ACE INA Insurance	CGL324533	Nov 01, 2015 to Nov 01, 2016	Each Occurrence	USD 1,000,000
				Products & Completed Operations Aggregate	USD 1,000,000
				General Aggregate	USD 10,000,000
				Personal & Advertising Injury	USD 1,000,000
				Tenants Legal Liability	USD 1,000,000
UMBRELLA	ACE INA Insurance	XBC324056	Nov 01, 2015 to Nov 01, 2016	Per Occurrence	USD 25,000,000
				Aggregate	USD 25,000,000

**Notice of cancellation:**

Should any of the above described policies be cancelled before the expiration date thereof, notice will be delivered in accordance with policy provisions.

<b>Marsh Canada Limited</b> 120 Bremner Boulevard Suite 800 Toronto, ON M5J 0A8 Telephone: 416-349-4577 Fax: 416-815-3309 shawna.reed@marsh.com	Marsh Canada Limited   By: _____ Shawna Reed
---	---

# Information Security Incident Management

---

## BREACH NOTIFICATION POLICY

---

<b>Policy Name</b>	Breach Notification Policy
<b>Policy Purpose</b>	This Iron Mountain Records Management Policy (Policy) establishes that Iron Mountain management will promptly notify its customers of security breaches affecting their material, in accordance with law and/or their contract.
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Breach Notification</li><li>– Time Tables</li></ul>

---

## INCIDENT MANAGEMENT PROGRAM



---

### Incident Management Program

---

Iron Mountain's #1 Core Value is security and protecting customers' information is of paramount importance to us. To preserve our customers' trust and support our #1 value, our Incident Management and Response Program was developed with a tactical and business strategy, including governance, industry standard and best practices. Our program has executive support and commitment, which is visible in their role of monitoring the program. This is delivered by corporate and business-focused teams, and is put in practice every day by Iron Mountain employees.

Iron Mountain's Incident Management program is structured upon the International Organization for Standardization/International Electrotechnical Commission 27001/27002 "Code of Practice for Information Security Management" standard better known as ISO-27001/27002. Specifically, it incorporates standards and guidelines under this code, for use by those responsible for initiating, implementing or maintaining our Incident Management program where all events and incidents are promptly managed.

In the event of an incident, it is our policy to report incidents including any potential breach of personal data, whether it involves employee, clients' or customer information, which is entrusted to Iron Mountain. Additionally, a continuous workflow analysis is performed to ensure our standard operational procedures and the risks potentially associated with the Program's growth are mitigated.

Incidents are reported via a single point-of-contact incident management tool called the Event Reporting and Management System (ERMS). The ERMS is a central reporting system designed to capture incidents globally. The tool was created to streamline the reporting process, enabling Iron Mountain employees to register vital incident information quickly, thoroughly, and efficiently about any event that occurs at Iron Mountain.

Once an incident is reported via ERMS, the appropriate team is alerted to begin triaging the matter. Iron Mountain response team members coordinate customer notifications rapidly in accordance with laws, regulations and customer agreements. Additionally, they perform tracking and metrics to allow for the identification of trends, and develop processes and procedures to proactively prevent reoccurring events.

Iron Mountain treats customer information with the highest level of security to safeguard and protect our customers' most valuable assets: information.

## ENTERPRISE EVENT REPORTING POLICY GLOBAL

---

<b>Policy Purpose</b>	<p>The purpose of this policy is to describe and document the requirements for reporting events (as defined in 2.2), or potential events, that may impact Iron Mountain (the “Company”), its employees, officers, directors, shareholders, customers or other business partners.</p> <p>This policy applies to all employees and contractors, of wholly owned entities and majority-owned joint ventures performing services for, or on the behalf of Iron Mountain regardless of the capacity in which they do so (“Iron Mountain Employees and Associates”), in all business lines and functions.</p> <p>This policy is not designed to capture employee misconduct</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Enterprise Event Reporting</li><li>– Triage, investigate, and escalate the event to internal support resources</li><li>– Mitigate the event and its impact</li><li>– Coordinate notifications in compliance with legal, regulatory and contractual requirements</li><li>– Notify appropriate insurance partners</li><li>– Develop trending and reporting</li><li>– Develop processes and procedures to prevent recurring events</li></ul>

---

## VEHICLE INCIDENT MANAGEMENT POLICY

---

<b>Policy Purpose</b>	<p>To describe and document Iron Mountain's policy related to handling of vehicle collision incidents and the subsequent repair of vehicles when damaged.</p> <p>This Policy applies to all employees of wholly owned entities and majority-owned joint ventures who operate vehicles, manage the vehicles and the operators of said vehicles for or on the behalf of Iron Mountain ("Iron Mountain Employees") in all geographies, business lines and functions.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Incident Claims</li><li>– Incident Reporting</li><li>– Vehicle Repairs</li></ul>

---



# Information Security Aspects of Business Continuity Management

---

## BUSINESS CONTINUITY POLICY

---

<b>Policy Name</b>	Business Continuity Policy (Global)
<b>Policy Purpose</b>	<p>To describe and document Iron Mountain's policy related to business continuity and the plans that provide for the prompt and effective continuation of all business critical functions in the event of a disruption of service at each Iron Mountain facility or those facilities that come under their direct control or jurisdiction.</p> <p>Iron Mountain is committed to ensuring its organizational resilience through an effective global business continuity program that ensures effective delivery of essential products and services in the event of emergencies or disruptions. This Policy ensures Iron Mountain continues operating its core business during unplanned disruptions, meeting its obligations to customers and regulators, and protecting the Iron Mountain brand and stakeholders' interests.</p> <p>This Policy applies to all employees, contractors, customers, vendors, guests or other parties performing services for or on the behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates") in all geographies, business lines and functions, including joint ventures.</p>
<b>Key Points</b>	<ul style="list-style-type: none"><li>– Additional Information</li><li>– Plan Implementation</li><li>– Policy Exceptions</li><li>– Policy Violations</li></ul>

---

## ABSTRACT OF BUSINESS CONTINUITY MANAGEMENT (BCM) PROGRAM



---

## Business Continuity Management Abstract of BCM Program

---

**Revised Tuesday, January 4, 2016**

The information within this abstract is valid on the day it was approved. Iron Mountain reserves the right to make any changes with the business continuity and or disaster recovery plan that enhances its ability to mitigate any threat, risk, or vulnerability. Safeguarding and protecting life, assets, and property is our Business Continuity Management program priority.

### A. Abstract Introduction

---

#### IRON MOUNTAIN'S APPROACH TO DISASTER RECOVERY & BUSINESS CONTINUITY

---

The Office of Business Continuity Management (BCM) develops policy and provides executive governance and leadership in all business continuity, crisis management, and disaster recovery strategic programs. Operationally, business Line and business function leaders are identified as Business Continuity "Plan Owners" that contribute in developing and executing tactical and operational plans that address emergency and crisis response, business recovery and continuity, and pandemic planning. The Plan Owners' maintain BC plans within their respective business line or business functional SharePoint. The BCM program provides the oversight to ensure that Business Impact Analysis, Threat, Risk, and Vulnerability assessments, and annual testing and exercises are included in tactical plan development, implementation, and execution.

From an Information Technology perspective, Iron Mountain Disaster Recovery strategies adhere to industry standard best practices by utilizing a multi-tiered approach in the physical and logical management of all infrastructure hardware and software components. This applies to the following areas:

- Daily Operations,
- Disaster Recovery Preparedness,
- Business Continuity and Recovery.

Within the Information Technology arena, specific Recovery Time Objectives and Recovery Point Objectives are critical elements in the recovery plans which are defined based upon the individual systems/applications' RTO and RPO that is being hosted. These plans are typically developed by identifying the service offering to address the respective needs of our customers.

In developing IT infrastructure contingencies that ensure business continuity, our business operations use redundancy and automated fail-over to provide high availability for critical processes via our divisional headquarter facilities in Collegeville, PA. Each functional department manager has the responsibility for ensuring that its critical processes are identified and that capability for recovery exists. The overall design of our disaster recovery effort utilizes our existing highly available infrastructure and diverse geographic locations to provide for immediate fail over of our critical business applications in the event of disaster. Iron Mountain's multi-tiered approach encompasses physical diversity of data centers/critical operations, redundant network connectivity over diverse Tier-1 services providers, and highly available secure ingress gateways.

The hallmark of Iron Mountain is in the value it places on the security of its customer's information assets. To that end, specific Iron Mountain Disaster Recovery plans are considered company propriety and not for disclosure. This ensures that we fulfill our obligations to protect our customers in all aspects of their records and information management needs.

## **B. Enterprise Wide Business Continuity**

### **BUSINESS IMPACT ANALYSIS (BIA) AND CONTINUITY STRATEGIES**

---

The need for comprehensive business continuity plans has long been clearly understood as an essential function. Its importance was driven home decisively in response to Y2K. Preparations for that event were undertaken months in advance and written plans were built based upon existing strategies for continuation of business-critical functions.

Following Y2K, Iron Mountain continues to conduct more comprehensive planning and exercising the Business Continuity and Disaster Recovery Plan. Iron Mountain begins the process with an enterprise wide formal Business Impact Analysis (BIA) and Threat, Risk, and Vulnerability assessments (TRV). These efforts served to identify both critical processes and critical infrastructure, and the necessary security strategies to protect them.

Due to the continuing evolution and consolidation of legacy systems, Iron Mountain's infrastructure has become more streamlined and efficient. As part of this effort, Iron Mountain's corporate critical business operations have deliberately migrated towards full redundancy utilizing the technical infrastructure available at our Boston, MA; Collegeville, PA; Boyers, PA; and Renton, WA locations. This has served to help meet all identified Recovery Time Objectives (RTO) when a BIA is completed.

The RTO of business functions is dependent upon the timing of the event. Business functions have cycles of activity; accounting, reporting, meeting filing cycles. These cycles are considered in establishing the criticality level of the Iron Mountain business functions.

The following example represents the criticality of the Iron Mountain business functions at 745 Atlantic Avenue based upon the BIA and TRV:

- **Major Business Process Criticality**

Investor Relations/Cash Management/Treasury/Payroll/Human Resources/Information Systems/Corporate Applications/Digital/Core Service Operations/Real Estate/Banking Relationship/Benefits/Accounting/AP/AR/GL/Tax/Security/Travel/CSG Operations/Legal

- **Business Process Criticality Level**

The failover capability for all key operational processes to our alternate locations is an effective and best-practice recovery strategy for business. Such capability limits the reliance on specific written plans for each business process which require the intervention of a "human resource" to activate or implement.

### **Information Systems Operations and Corporate Applications**

*Criticality: Mission Critical*

SafeKeeperPlus (SKP), Oracle, SecureBase, Digital Record Center for Compliant Messaging, Data Protector, Live Vault, E-Search, and Data Defense are all critical automated systems. Periods of criticality for corporate applications are quarter-end, year-end, 10K preparation, payroll, and budgeting. All systems (inventory and applications) are backed up via the redundancy previously stated. New data receipt will be addressed immediately, with a Recovery Point Objective of 24 hours. The Recovery Time Objective is defined in the customer contract or SLA.

### **Investor Relations, Cash Management and Treasury**

*Criticality: High Level of Importance*

Critical items include funding and interest payment on Bonds. Four priority external groups of concern are Shareholders, Analysts, Bond Holders and Banks. All required blank reporting forms are kept off-site at the residences of two senior Treasury executives who can execute all critical process with telecommunications and remote computer access. Shareholder communications are addressed via our Corporate Crisis Communication plan.

Recovery Time Objective for these processes is 1 hour.

**Payroll and Human Resources***Criticality: High Level of Importance*

Payroll has a high level of criticality. Data feeds to the outsourced payroll vendor can be handled at one of the alternative sites. All other processes have a medium criticality and can be handled remotely.

Recovery Time Objective for these processes is 1 hour.

**Real Estate/Facility Issues for the Corporate Offices***Criticality: High Level of Importance*

If the office space at the corporate headquarters were suddenly no longer viable, there are multiple existing locations from which essential work can be performed. In addition, Corporate Real Estate and Corporate Procurement have a Recovery Time Objective of 24 hours for the establishment of newly equipped space if required.

**Communications**

A formal crisis communication plan has been developed and is administered by the Iron Mountain Vice President, Corporate Communications.

Senior Management emergency contact information to include office, home and cell phone, as well as business and alternate email addresses is maintained centrally and updated and published quarterly.

**C. Facility Continuity of Operations****SAFEGUARDING AND PROTECTING LIFE, ASSETS, AND PROPERTY**

---

Since an identical business interruption scenario (for example, severe weather) can result in single or compound problems (for example, personal injury, transportation disruptions, power loss and building damage) remediation, recovery, and facility continuity of operation efforts will be dictated by the extent of the event. We have established the following priority for our business resumption efforts:

1. Saving of lives and first aid to the injured
2. Reduction and/or prevention of further damage
3. Restoration and recovery of damaged property

## WATER AND FIRE DAMAGE REMEDIATION

---

One of the most prevalent threats and vulnerabilities to any business is water and fire. In order to ensure the appropriate recovery of customer assets stored at Iron Mountain facilities, recovery plans maintain national account relationships with international disaster recovery vendors, which include BMS Catastrophe, Polygon and Belfor Disaster Recovery Solutions. The specific methodology for recovery of an asset will depend upon the nature of the damage and the media involved. Wet paper records for example, can be effectively recovered through the use of freeze drying and/or desiccant dehumidification. Magnetic media requires more careful handling and cleaning in addition to appropriate drying techniques.

Iron Mountain is committed to the protection of its customer assets. Our relationship with our vendors is designed to provide our customers with the best emergency services available. While it remains our goal to do everything possible so that we never require the services of our recovery partners, we take our responsibility to be prepared seriously.

## WORKFORCE /PANDEMIC PLANNING

---

Iron Mountain is committed to influenza and pandemic readiness and preparedness in order to maintain business continuity, including our customer's requirements to have plans tested and the results available to them. To improve on the outcome of business continuity success, management continually verifies the viability of the workforce/ pandemic plan. Iron Mountain is committed to ensure contingency viability with annual exercises that are appropriate for the anticipated event.

## EMERGENCY AND CRISIS MANAGEMENT

---

The depth of Iron Mountains' emergency and crisis management plans are presented as a *Table of Contents* from our most recent facility continuity of operations planning template. All of our facilities utilize this template for creating tactical and operational plans that can be executed during any emergency or crisis:

### Facility Continuity of Operations Plans at Iron Mountain

#### Table of Contents

---

##### **Section 1 Introduction**

- 1.1 Overview
- 1.2 Scope
- 1.3 Purpose
- 1.4 Objectives

##### **Section 2 Structure**

- 2.1 Logical Structure
- 2.2 Physical Structure
- 2.3 Business Support Structure
- 2.4 Response & Recovery Structure

##### **Section 3 Roles and Responsibilities**

- 3.1 Crisis Management Team (CMCT)
- 3.2 Regional Event Management Team
  - 3.2.1 Site Event Response Team (SERT)

##### **Section 4 Phases**

- 4.1 Alert Phase
- 4.2 Assess Phase
- 4.3 Activation Phase
- 4.4 Recovery Phase



#### 4.5 Return Phase

### Section 5 Prevention of and Preparation for General Emergencies

- 5.1 Aircraft Flight Pattern
- 5.2 Fire Prevention/Preparation
- 5.3 Fire Emergency
- 5.4 Bomb Threats
- 5.5 Protests & Civil Disorder
- 5.6 Riots & Civil Disorder
- 5.7 Individual Medical Emergencies
- 5.8 Tornado
- 5.9 Earthquake
- 5.10 Racking Collapse – Structural Damage
- 5.11 Sprinkler System Damage/Pipe Leak
- 5.12 Clean Agent Fire Equipment Damage/Activation
- 5.13 Fire System Impairment
- 5.14 Hot Work
- 5.15. Shelter in Place
- 5.16 Flood
- 5.17 Severe Weather
- 5.18 Power Outage
- 5.19 Technology/Telecommunications Outage
- 5.20 Damaged Inventory
- 5.21 Hazardous Chemical Spill
- 5.22 Terrorism
- 5.23 Suspicious Packages and Letters

### Section 6 Prevention of and Preparation for Site Risk Specific Emergencies

- 6.1 Risk-Based Supplemental BCP Plans

### Section 7 Contact Information

- 7.1 Site Event Response Team (SERT)
- 7.2 Employee Contact List
- 7.3 Employee Emergency Contact List
- 7.4 External Service Providers
- 7.5 Hotel Accommodations

### Section 8 Facility Information

### Section 9 Appendix

- 9.1 General Documents
  - 9.1.1 Market/Territory Internal Communications
  - 9.1.2 Damage Assessment Checklist (General Facility)
  - 9.1.3 Vendor Expense Tracking
- 9.2 Risk-Based Supplemental BC Plans

## Crisis Management Plan at Iron Mountain

### Table of Contents

---

#### Section 1 Introduction

- 1.1 Overview
- 1.2 Scope
- 1.3 Purpose
- 1.4 Objectives

#### Section 2 CMP Structure

- 2.1 CMP Logical Structure
- 2.2 CMP Physical Structure
- 2.3 CMP Business Support Structure

- 2.4 CMP Response & Recovery Structure
- Section 3 CMP Roles & Responsibilities**
  - 3.1 Crisis Management Core Team (CMCT) Mission
  - 3.2 Regional Event Management Team (REMT) Mission
  - 3.3 Crisis Support Team (CST) Mission
  - 3.4 Site Event Response Team (SERT) Mission
- Section 4 CMP Phases**
  - 4.1 Phase Activities Timeline
  - 4.2 Phase Descriptions
- Section 5 CMP Phase Activities**
  - 5.1 Alert Phase
  - 5.2 Assess Phase
  - 5.3 Activation Phase
  - 5.4 Recovery Phase
  - 5.5 Return Phase
- Section 6 Appendix**
  - 6.1 CMP – Revision History
  - 6.2 CMP – Exercise History
  - 6.3 Employee Contact list
  - 6.4 Xmatters Teams
  - 6.5 External Service Providers
  - 6.6 Crisis Command Center (Virtual & Physical)
  - 6.7 Initial – Event Status Meeting Agenda
  - 6.8 Damage Assessment Checklist (General Facility)
- Section 7 Supplemental Plans**
  - 7.1 Emergency Action Fire Safety Plans (EAFSP)
  - 7.2 BCP – Annual Testing
  - 7.3 Flood Emergency Response Plan (FERP)
  - 7.4 Hurricane
  - 7.5 Earthquake/Tornado
  - 7.6 Racking Collapse
  - 7.7 Wildfire
  - 7.8 Winters Storm
  - 7.9 Labor Plan
  - 7.10 Fire Drill
  - 7.11 Evacuation Drill
  - 7.12 Earthquake Drill
  - 7.13 Tornado Drill

## D. Data Processing Continuity

### NETWORK DISASTER RECOVERY/BUSINESS CONTINUITY

Iron Mountain's network consists of two data centers interconnected by a redundant high-speed ATM backbone with diversified switching to provide a fault tolerant, high-capacity infrastructure. The network is engineered with high capacity connections to diverse ISPs providing redundant Internet connectivity. An Autonomous System Number permits the use of BGP to provide fault tolerant inbound access. Security of this network is achieved using firewall inspection modules running on scalable appliance solutions, providing fault tolerance and redundancy. The architecture has been engineered in accordance with industry best practices to support multiple DMZ networks allowing for secure redundant private connections to our customers and partners. These connections are facilitated via our private SONET ring network. Recent strategic alliances and business partnerships allow for bandwidth on demand through optical technologies to support both public and private connectivity requirements.

Iron Mountain has a pair of underground data centers. Iron Mountain has constructed a state of the art data center 200 feet underground in our 113-acre highly secure facility in Western Pennsylvania. In addition, we have a fully redundant DR data center in Missouri. These facilities utilize high capacity and redundant optical technology such as SONET terminals, ATM switches and optical IP routers. This engineering approach provides flexible and scalable growth with potentially unlimited capacity within two of the worlds most secure locations.

Iron Mountain exceeds industry standard best practices related to the management of all infrastructure hardware and software components, both in terms of their daily operations and in relation to disaster recovery preparedness and business continuity. Iron Mountain has a BCM Director and staff with business continuity and disaster recovery certifications and are regarded in the industry as experts. The overall design of our disaster recovery effort utilizes our existing highly available infrastructure to provide for immediate fail over of our production database in the event of a disaster. Dual methods are used: Mirroring and Log Ship every 15 minutes from our production site to our disaster recovery site over our secure private network. Copies of all encrypted production tapes are created daily and shipped offsite to a secure location. In the event of a disaster these tapes would immediately be shipped to our recovery site. The disaster recovery plan associated with the query and ingestion process for external access to our archive utilizes an implementation of TCP/IP and BGP. This implementation allows us automatically, within our private TCP/IP address space to redirect any network traffic to our disaster recovery site in the event of a disaster. This architecture affords us the ability to continuously ingest data and accept query traffic from our external customers.

### **E. Information Technology Disaster Recovery Protocol Strategy**

Iron Mountain has instituted documentation that streamline the development of application/system recovery planning process as well as documentation that detail the disaster recovery testing execution guidelines. Iron Mountain has further refined its recovery process by the establishment of a formal recovery protocol strategy. Senior level Vice Presidents have been trained as Disaster Response Managers. These individuals coordinate all aspects of facility level recovery efforts from infrastructure to customer communication to DR Vendor management. The extent of this process is shown in the Table of Contents from our Recovery Coordination manual.

#### **APPENDIX 1. SAFEKEEPERPLUS DISASTER RECOVERY OVERVIEW**

##### **Strategy**

Iron Mountain SafeKeeperPlus (SKP) has taken significant steps to provide redundancies in personnel, systems and infrastructure. Our systems have been designed with redundancy in mind, in many cases residing on highly available or fault-tolerant systems. Our most critical systems are duplicated in our hot-site environment, providing redundancy in components ranging from data to facilities. In spite of our best efforts to mitigate risk, outages will happen, though Data currency will not exceed fifteen minutes.

The SKP System has been created and is maintained to provide the Iron Mountain operations staff the automated ability to efficiently store and retrieve the boxes and files contained in our record centers.

The SKP System is comprised of numerous databases and processes used to manipulate and control these databases:

- PROGRESS Databases, startup and shutdown scripts, startup parameters
- Disk storage and file system space used to contain the databases
- CPU and memory to operate the databases
- Disk storage and file systems to contain reports and data files generated by the SKP system

- Software to enable printing, emailing and faxing of reports and bar-coded labels
- Software used to read and write data to bar-code scanner devices (Spectrum 1, Spectrum 24 and MCL RF units)
- Software used to provide a web interface to the databases for your customers, along with an Oracle based search engine for the web interface
- An FTP service used to allow customers to send and receive maintenance and order data files
- Together, these elements provide an efficient Inventory Control system.
- SKP System Backups and contingency
- In order for Iron Mountain to perform business operations on a continuous basis, the SKP System is protected and backed up in various ways.
- Localized or small scale component failures and damage risks are minimized by
- Mirrored system disks
- Redundant computer systems and related hardware
- Multiple network connections
- Redundant networking system components
- Daily Computer backups of the Operating System, control files and scripts
- Daily computer backups of the system generated report and data files
- Weekly database backups with up “to-the-second” recovery files for the databases
- Large scale catastrophic or regional disasters, failures and system damage risks are minimized by
- A remote site with a complete copy of all the SKP System databases and other critical operating components.
- An automated process that keeps the remote site databases in sync with the main Production site.

Iron Mountain tests our disaster recovery plans at least once a year to test their accuracy, efficacy, and speed. Tests are used to improve the disaster recovery process where needed.

## APPENDIX 2. SECURE BASE DISASTER RECOVERY OVERVIEW

### **Service Level Agreement**

Iron Mountain Records management is committed to providing systems availability with unplanned outages of one hour or less once it has been determined that an event has occurred that effectively takes SecureBase, VaultTracker, or SecureSync offline. Data currency will not exceed fifteen minutes.

### **Strategy**

Iron Mountain Data Backup & Recovery has taken significant steps to provide redundancies in personnel, systems and infrastructure. Our systems have been designed with redundancy in mind, in many cases residing on highly available or fault-tolerant systems. Our most critical systems are duplicated in our hot-site environment, providing redundancy in components ranging from data to facilities. In spite of our best efforts to mitigate risk, outages will happen.

Our strategy for business continuity planning is to design manual processes that will allow the branch to continue operating on a limited basis, under a variety of outage scenarios.

Operating on a “Limited basis” refers to the desire to limit transactions processed manually, due to both the reduced capacity associated with backup systems, infrastructure and personnel, and the requirement that all manual transactions be reconciled to the supporting information system, prior to returning to normal operation.

Understanding these restrictions, we have prioritized transactions from a customer perspective, allocating our operating resources based on customer need. For example: We assign processing priority to a customer DR request over a customer Special request and a customer special request over a customer add-on request.

Unlike a branch outage scenario, the continuity plan for a disaster which affects one or more of the systems within our Western Pennsylvania data center in a manner which is deemed critical to continued operation must be handled in such a way as to fail over the entire system to the Missouri hot standby site. Failing over one critical system without failing over all critical systems could result in data inconsistency that would be counter-productive to maintaining our Service Level Agreement.

Iron Mountain tests our disaster recovery plans at least once a year to test their accuracy, efficacy, and speed. Tests are used to improve the disaster recovery process where needed.

### APPENDIX 3. DIGITAL RECORD CENTER FOR COMPLIANT MESSAGING DISASTER RECOVERY OVERVIEW

---

#### **Strategy**

Iron Mountain's Digital Record Center for Compliant Messaging (DRCCM) has been designed to maximize availability of the systems to our customers for ingestion and retrieval of their data. As the main value of the Digital Archive is its ability to ingest customer data, Iron Mountain has taken significant steps to provide redundancies in personnel, systems and infrastructure to ensure that this service is always available to take in customer data, store it safely, and to have information about that data available for search, review, and reporting. Our systems have been designed with resiliency in mind, in many cases residing on highly available or fault-tolerant systems. These provisions ensure that Iron Mountain DRCCM Disaster Recovery provides:

- Complete system recovery, with 100% data reliability
- Recovery without re-processing data (restore, not reingest)
- A trusted custodian of backlog data during the recovery window
- No changes in processes or system access (assuming Iron Mountain is providing media transportation)

In the event of communications failure with the primary site, multiple communication channels are available. In the event these also fail, EVAA includes automated failover to access alternative systems available for continued customer data ingestion. The Digital Archives application is prepared to continue in its function of collecting data to be added to customer archives.

Iron Mountain maintains two secure underground data centers with full redundancy located in Western Pennsylvania and Missouri.

In the event of a disaster occurring to a data center, Iron Mountain will repoint asset delivery to a remote data center. New customer data will be retained securely until the backup data center is ready to ingest the reappointed assets. Original assets on tape media will be delivered from their secure offsite storage location and restored at the alternate site. There is no need to ingest those assets again.

In addition to on-line availability, a copy of all customer data, and the meta-data that describes it, is stored in an ultra-secure Iron Mountain off-site data underground repository like the one described above. This data can be recovered to more immediate on-line availability as needed.

Iron Mountain tests our disaster recovery plans at least once a year to test their accuracy, efficacy, and speed. Tests are used to improve the disaster recovery process where needed.



---

**APPENDIX 4. CORPORATE APPLICATIONS DISASTER RECOVERY OVERVIEW**

---

**Strategy**

Iron Mountain CSG has taken significant steps to provide redundancies in personnel, systems and infrastructure. Our systems have been designed with redundancy in mind, in many cases residing on highly available or fault-tolerant systems. Our most critical systems are duplicated in our hot-site environment, providing redundancy in components ranging from data to facilities. In spite of our best efforts to mitigate risk, outages will happen.

Against that possibility:

- The DR database is kept in sync with Production by sending the change logs every 30 minutes
- The change logs are applied to the DR instance, which then becomes “in sync” with the Production database
- The Web Server is kept in sync once a day since the data on the Web tier infrequently changes
- Both the Production and Web servers are also backed-up on a daily basis
- Vendor Interface files and key encryption files are backup up daily as part of \home\ftp\pora directory
- DR strategy leverages our Oracle cloning technique, which is often done multiple times per week.
- Oracle is available 24x7.
- DR Server Infrastructure (Kansas City)
- A current DR database exists in a shared Oracle application environment. It is hosted on a server that is also hosting additional Oracle test & development instances
- While less powerful than the full production cluster, the DR server set retains all business data and can be used for most business applications for a limited time.

Our strategy for business continuity planning is to design manual processes that will allow the businesses to continue operating.

Understanding these restrictions, we have prioritized transactions from a customer perspective, allocating our operating resources based on customer need. For example: We assign processing priority to a customer DR request over a customer Special request and a customer special request over a customer add-on request. The expected recovery window is 4-24 hours.

Iron Mountain tests our disaster recovery plans at least once a year to test their accuracy, efficacy, and speed. Tests are used to improve the disaster recovery process where needed and availability for all key operational processes to our alternate locations is an effective and best-practice recovery strategy for business. Such capability limits the reliance on specific written plans for each business process which require the intervention of a “human resource” to activate or implement.

**Final Comment**

At Iron Mountain, our number one core value is security. Every employee at Iron Mountain takes security, safety, and life saving measures seriously to safeguard and protect all of our resources and assets. The Business Continuity Management program is supported at the highest level at Iron Mountain, our Chief Executive Officer. With a Senior Executive Steering Committee providing leadership direction, the Director of Business Continuity Management can provide the highest quality level of programs to our employees and customers.

## BUSINESS CONTINUITY PLAN, PANDEMIC PLAN, AND EXECUTIVE SUMMARY

### Revised Thursday, February 18, 2016

The information within this abstract is valid on the day it was approved. Iron Mountain reserves the right to make any changes with the business continuity and or disaster recovery plan that enhances its ability to mitigate any threat, risk, or vulnerability. Safeguarding and protecting life, assets, and property is our Business Continuity Management program priority.

### Introduction of the Business Continuity Plan (BCP) for Pandemic Response

The objective of the pandemic plan is to provide multi-strategic contingency efforts with several key decision matrices, various allocation and deployment of resources, and identifiable trigger points to reduce and/or maintain a minimal business impact to Iron Mountain employees, company assets, and to our customers. The success of Iron Mountain's BCP is its enablement of customers to experience a seamless, transparent, and effective execution of its continuity of operations.

In the event that a pandemic is imminent and/or does occur, the Crisis Management Core Team will declare the implementation of the pandemic plan with the established contingency efforts identified by Iron Mountain to mitigate disruption of business operations for customers, vendors, service providers, and safeguard human resources and physical assets.

The pandemic plan owner(s) are identified as members of the Crisis Management Core Team as key leaders in Safety & Security, Business Continuity, Risk Management, Real Estate, Communication, Information Technology, Legal, Procurement and Human Resources,. The key executive leaders within these disciplines comprise the CMCT and provide the expertise to create the guidelines and framework that develop the strategic, tactical, and operational plans that will be executed by the appropriate designated managers.

Furthermore, the core team members are permitted the flexibility to address new actionable information as it relates to a declared global pandemic, ensuring that Iron Mountain's key stakeholders within each of the organization's business lines are provided a consistent and prudent decision matrix to enhance business decisions.

Iron Mountain's Crisis Management Core Team will provide the executive oversight necessary for the pandemic plan, while the Business Continuity Management Team creates the plan's framework with guidance and recommendations from such organizations as the World Health Organization (WHO); the Centers for Disease Control and Prevention (CDC); the U.S. Department of Health and Human Services (HHS); the Department of Homeland Security (DHS); and from industry organizations and leaders that have identified "best practices", as well as from certain customers that operate under strict government regulation, such as the Federal Financial Institutions Examination Council (FFIEC). The office of BCM facilitates the planning and testing of all plans.

When a declaration of a pandemic outbreak has been made, Iron Mountain's Crisis Management Core Team will monitor the evolution of the pandemic threat and immediately initiate the appropriate action(s) as outlined in the plan.

### Context of a Pandemic Response

Iron Mountain actively monitors pandemic conditions as defined by the World Health Organization (WHO) as well as other US Departments responsible for the health and welfare of human life, including other acceptable international sources who are capable to advise that there is a significant risk of a human influenza pandemic occurring at some point, whether in the short-term or further into the future.

The current consensus by leading subject matter experts agree that the threat of a pandemic outbreak necessitates the need for organizational planning that will address the potential loss of life, serious illness, and extreme numbers of employee absenteeism. On serious illness alone, the expected absent rate will average between 5 and 8 days. Subsequently, work disruption will be severely impacted across all private and public organizations at all levels of employment.

Given the likelihood and potential impact of a (influenza) pandemic, it is essential that the organizations, like Iron Mountain, have a contingency plan in place to cover such an eventuality.

### **Monitoring the Phases of a Pandemic**

The World Health Organization (WHO) has defined six phases in the evolution of an influenza pandemic which define a staged approach to preparedness planning and response, leading up to the declaration of the onset of a pandemic.

Iron Mountain BCM recognizes the notification and recommendation by WHO and the CDC when evidence of a pandemic may be threatening. The implementation of the Pandemic Plan is executed to protect Iron Mountain resources and business interests. The Crisis Management Core Team monitors the evolution of the potential threat of the pandemic and immediately initiates the review of pandemic plan. The review includes the monitoring of the pre-establish Iron Mountain four 'Trigger Stages' in the event a phase 6 is declared by the World Health Organization.

### **Declared Pandemic – Phase 6**

Iron Mountain's Crisis Management Core Team and Regional Event Management Teams are in position strategically within the global organization are prepared to declare a pandemic based on one of the four WHO trigger stages:

- Trigger Stage 1 (*Standby*) – Virus/cases only outside of your domain.
- Trigger Stage 2 (*Minimize Risk Transmission*) – Virus isolated within your domain.
- Trigger Stage 3 (*Containment*) – Outbreaks within your domain.
- Trigger Stage 4 (*Full Pandemic Recovery*) – Widespread activity across the entire Territory/Area/Region.

### **Pandemic Plan – Structure and Priority Objectives**

The strategic plan is structured to provide long term mission objectives, while the tactical plan is designed to provide the planner with guidance and assist in identifying the resources to develop and create an actionable and executable operational plan. Together, the final result is a finished written plan that is actionable and provides the mechanism (checklist) that defines appropriate phases, trigger points, steps, processes, escalation, notifications, and immediate actions that will effect a successful business contingency operation.

With proper structure and priority objectives, along with appropriate urgency levels that correspond with the pandemic impact, effective deployment of resources are focused on the impacted areas where the organization needs to react to mitigate, contain, or recover operations. Iron Mountain's responses are structured to address five critical objectives:

- Leadership, organization & coordinating operations
- Communications
- Surveillance, information gathering, situation reporting & risk assessment
- Containment: health, safety & welfare issues
- Business Continuity

The critical objectives are structured to meet the following set of priorities but are not limited to:

- Initiate a preventive program to reduce the likelihood Iron Mountain's operations will be significantly affected by a pandemic event,
- Reduce the impact of a pandemic on the organization's employees and services,
- Conduct surveillance and monitoring of employee absence levels and service impact,
- Assure the welfare of employees, including the potential impact to our customers,
- Monitor the impact of the developing situation on critical activities and services, and take remedial action as required, and

- Create a testing program to ensure ongoing review and updates to the pandemic plan.

The creation of strategic, tactical, and operational plans is structured to effectively meet short term and long term business disruption demands as well as provide the flexibility to address critical activities and services with our customers and strategic business partners, including a post pandemic recovery with the goal of quickly returning systems, services, and operational activities to normal.

Finally, Iron Mountain continually reviews its entire Business Continuity Management Program to determine its ability to meet the needs of its employees, resources, customers, strategic business partners and shareholders. A core value of Iron Mountain's business continuity commitment is to ensure our ability to provide uninterrupted business services, safeguard our employees, and protect company assets during any event that threatens to disrupt our operation and organization.

# Compliance

## LEGAL, COMPLIANCE AND REGULATORY POLICY

<b>Policy Name</b>	36.0 Legal, Compliance and Regulatory
<b>Policy Purpose</b>	This policy provides guidance on complying with legislative, regulatory and contractual requirements affecting information resources.
<b>Policy Statement</b>	All personnel must comply with relevant national and local legal, regulatory and contractual requirements.
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– All relevant statutory, regulatory and contractual requirements must be explicitly defined and documented for each information resource</li> <li>– All personnel must comply with copyright laws and packaged system license agreements</li> <li>– Information assets must be protected from loss, destruction and alteration for the period of retention required by statutory and regulatory requirements</li> <li>– The Privacy and Compliance Department at <a href="mailto:Compliance@IronMountain.com">Compliance@IronMountain.com</a> will provide guidance to managers and users as to their responsibilities and limitations regarding the collection and distribution of personal information</li> <li>– Information security reviews will be performed by Information Security to measure the organization's awareness of and compliance to the Iron Mountain Information Security Policy</li> <li>– Independent information security audits will be performed through Iron Mountain Internal Audit to measure compliance with the Iron Mountain Information Security Policy, standards, procedures and guidelines</li> <li>– Business managers are responsible for monitoring the information security practices of all personnel under their supervision</li> <li>– All personnel are responsible for reporting information security violations to Information Security</li> <li>– Access to system audit tools must be protected to prevent any misuse or compromise</li> <li>– Iron Mountain will engage independent information security specialists to assess the strengths, weaknesses and vulnerabilities of Iron Mountain's information resources</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>– Adhering to Copyright Laws and License Agreements</li> <li>– Certification Internal Audit (UK)</li> <li>– Collecting Personal Data</li> <li>– Competence of Independent Assurance Function</li> <li>– Confidentiality of Test Plans and Results</li> <li>– Customer Must be Able to "Opt Out" of Marketing Lists</li> <li>– Displaying the Iron Mountain Privacy Policy</li> <li>– Disseminating Personal Information</li> </ul>



- 
- Frequency of Testing
  - Independent Testing of Information Resources and Practices
  - Internal Audit
  - Iron Mountain Privacy Policies Must Consider Privacy Regulations
  - Maintenance of the Record Retention Schedule
  - Measurement and Interpretation of Test Results
  - Obtaining and Processing Personal Data
  - Procurement Control
  - Protecting Customer Data from Third Parties
  - Record Retention Schedule Supports Regulatory Requirements
  - Records Retention must follow the Iron Mountain Retention Schedule
  - Reporting on the Security Posture of Iron Mountain
  - Restricted Use of System Audit Tools
  - Retention of Collected Personal Data
  - Technical Compliance Testing (UK)
  - Test Results Distribution
  - Transferring Personal Data Outside of the European Economic Area
  - Updating Collected Personal Data
-

## HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) POLICY

<b>Policy Name</b>	Health Insurance Portability and Accountability Act (HIPAA) Policy (NA)
<b>Policy Purpose</b>	<p>Iron Mountain (the “Company”) recognizes its status as a business associate as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the HITECH Act of 2009, along with any implementing regulations including those implemented as part of the final Omnibus Rule (collectively referred to as the “HIPAA Rules”) and is committed to comply with the corresponding HIPAA Rules.</p> <p>The purpose of this policy is to ensure compliance by its workforce with the HIPAA Rules and other state laws protecting Protected Health Information (“PHI”). i) Specifically, to ensure the confidentiality, integrity and availability PHI that Iron Mountain Processes, ii.) to protect PHI against any reasonably anticipated threats or hazards to the security or integrity of it and against any reasonably anticipated unauthorized uses or disclosures, and iii.) to protect patients’ rights.</p> <p>This policy applies to all employees, contractors, vendors or other parties of wholly owned entities and majority-owned joint ventures who may perform services for or on behalf of Iron Mountain regardless of the capacity in which they do so (“Iron Mountain Employees and Associates”), and who have access or may have access to PHI or supervise such individuals in all geographies, business lines and functions. This policy also applies to all employees and officers of Iron Mountain who are responsible for providing the infrastructure, processes and procedures so that Iron Mountain can comply with the HIPAA Rules</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– HIPAA Business Associate</li> <li>– HIPAA Compliance and Evidence</li> <li>– HIPAA Compliance Documentation</li> <li>– HIPAA Customer Notification of Individual Requests</li> <li>– HIPAA Disclosure Risk Mitigation</li> <li>– HIPAA Legal Department Guidance</li> <li>– HIPAA Minimum PHI Use or Disclosure</li> <li>– HIPAA Permitted or Required Disclosure</li> <li>– HIPAA PHI Approved Disclosures</li> <li>– HIPAA PHI Breach</li> <li>– HIPAA PHI Sale and Market</li> <li>– HIPAA Violations</li> </ul>

## GLOBAL PRIVACY POLICY

<b>Policy Name</b>	Privacy Policy (Global)
<b>Policy Purpose</b>	<p>To promote and implement Iron Mountain's Core Values of Security, Integrity, Accountability and Teamwork as they relate to the protection of Personal Data, to provide adequate and consistent safeguards for the Processing of Personal Data by Iron Mountain Employees and Associates and to inform each Iron Mountain Employees and Associates as to how his or her Personal Data is processed by Iron Mountain.</p> <p>This policy applies to all employees, contractors, customers, vendors, guests or other parties of wholly owned entities and majority-owned joint ventures who may perform services for or on behalf of Iron Mountain regardless of the capacity in which they do so ("Iron Mountain Employees and Associates") in all geographies, business lines and functions. For additional guidance regarding regional data protection, please refer to the documents referenced in Section 8.</p>
<b>Key Points</b>	<ul style="list-style-type: none"> <li>– Privacy Cross Border Transfers Europe</li> <li>– Privacy Cross Border Transfers Other International</li> <li>– Privacy Cross Border Transfers Safe Harbor</li> <li>– Privacy Personal Data Accuracy</li> <li>– Privacy Personal Data Collection</li> <li>– Privacy Personal Data Processing</li> <li>– Privacy Personal Data Processing and Use</li> <li>– Privacy Personal Data Protection</li> <li>– Privacy Personal Data Relevancy</li> <li>– Privacy Personal Data Retention</li> <li>– Privacy Personal Data Safeguards</li> <li>– Privacy Personal Data Third Party Processing</li> <li>– Privacy Policy Violations</li> </ul>

## EMPLOYEE CONFIDENTIALITY AND NON-COMPETITION AGREEMENT

## EMPLOYEE CONFIDENTIALITY AND NON-COMPETITION AGREEMENT

FOR AND IN CONSIDERATION of my employment and of the salary, benefits, and any other compensation hereafter to be paid me by or on behalf of Iron Mountain Information Management, Inc. and/or any of its parent corporations, subsidiaries, affiliates, successors, or assigns (hereinafter "Iron Mountain"), as well as other consideration, the sufficiency of which is hereby acknowledged, and acknowledging that Iron Mountain is employing me in reliance upon my full compliance with this Agreement, I covenant, promise and agree as follows:

**1. Confidentiality.** I shall carefully guard and keep confidential all information concerning the business, contemplated future business, prospects and any other affairs of Iron Mountain that Iron Mountain regards as confidential, proprietary, or private in nature, whether or not so labeled (hereafter, "Confidential Information"). I acknowledge and agree that (a) Iron Mountain's methods of operation, software and computer programs developed by or for Iron Mountain for use in its business, the identity of customers and prospects, pricing and marketing strategies, service offerings and sales techniques, and other forms of non-public information developed or used by Iron Mountain and maintained on a confidential basis, constitute Confidential Information and are highly valuable to Iron Mountain; (b) my unauthorized disclosure or use of Confidential Information could irreparably damage Iron Mountain; and (c) as an employee of Iron Mountain, I have or will have access to (and receive compensation from Iron Mountain to use, develop and/or contribute to the development of) such Confidential Information.

**2. Non-Disclosure.** I shall not, at any time, either while I am employed by Iron Mountain or after the termination of such employment, disclose any Confidential Information to any person or entity or employ the same in any way other than for the benefit of Iron Mountain and with its full knowledge and consent. I shall similarly keep confidential any

information that belongs or pertains to any current or prospective Iron Mountain customer or client.

**3. Non-Competition.** During my employment with Iron Mountain and for one year following the termination thereof, I shall not, in any location that is within a 50-mile radius of any Iron Mountain facility at which I worked during the final twelve months of my employment (the "Territory"), provide direct or indirect services to a Competitor, whether as an employee, consultant, independent contractor, agent, or owner (other than of an interest of 5% or less in a publicly traded entity). For the purposes of this Agreement, a "Competitor" shall mean any person or entity that competes or is actively preparing to compete in the United States with any product, service or business of the unit, division or subsidiary of Iron Mountain by which I am employed. I understand and agree that this covenant is necessary to protect Iron Mountain's business interests, including its relationships with its customers and clients and its Confidential Information. I further understand that this covenant does not prohibit me from working for or rendering services to a Competitor outside the Territory.

**4. Non-Solicitation.** During my employment with Iron Mountain and for one year following the termination of employment, I shall not, directly or indirectly, on behalf of myself or any other person or entity, solicit business from any actual or

prospective customer or client of Iron Mountain with which I had contact during my Iron Mountain employment, nor shall I attempt to induce any such actual or prospective customer or client to terminate its relationship with Iron Mountain. I also agree that for such one-year period, I will not, directly or indirectly, on behalf of myself or others, hire, attempt to hire, solicit for employment, seek to retain on an independent contractor or consultant basis, or in any way encourage the departure, resignation or other termination of employment of, any employee of Iron Mountain.

**5. Business Reputation.** During my employment with Iron Mountain and for all time thereafter, I will not do any act, engage in any conduct, or make or publish any untrue or misleading statement that will demean or otherwise adversely affect the name, reputation, or business interests of Iron Mountain.

**6. Return of Property.** Upon the termination of my employment with Iron Mountain, I will return to Iron Mountain all its property, including, without limitation, keys, telephones, computers, PDAs, documents, records, electronic data and files, notes, papers, reports and customer lists, and shall not keep originals or copies of such property, regardless of the medium on which it is stored.

\_\_\_\_\_ Initials

**7. Duration of Obligations.** No change as regards my duties or position with Iron Mountain shall in any way affect my obligations under employment, whether initiated by me or by Iron Mountain, shall not release me from my covenants and obligations under this Agreement.

**8. Entire Agreement/No Oral Modification.** This Agreement represents the entire understanding between me and Iron Mountain and supersedes all prior or contemporaneous agreements between the parties (whether written or oral) related to confidentiality and/or non-competition and cannot be amended except by a written agreement signed by the parties hereto that specifically refers to it. The failure of Iron Mountain from time to time to insist on my strict compliance with the terms of this Agreement will not be deemed a waiver of any right granted to Iron Mountain.

**9. Remedies/Severability.** I acknowledge and agree that Iron Mountain may be without an adequate remedy at law should I breach this Agreement and I, therefore, agree that, in addition to legal relief, Iron Mountain, without needing to post a bond or other security, may enforce this Agreement by equitable relief including a temporary, preliminary, and/or permanent injunction and/or specific performance. I understand and agree that each provision of this Agreement is of great importance to Iron Mountain; is separate, severable, and

independent; and, if severed, would be enforceable as if it were made the subject of a separate agreement with Iron Mountain. Should a court of competent jurisdiction find any provision of this Agreement unenforceable, in whole or in part, I specifically agree that (a) such finding shall not affect the enforceability of any other part of this Agreement and (b) such court may amend such unenforceable provision to render it enforceable in accordance with the spirit and intent of this Agreement, to the maximum extent permitted by law.

**10. Choice of Law/Jury Waiver.** This Agreement shall be deemed to have been made in the Commonwealth of Massachusetts, shall take effect as an instrument under seal within Massachusetts, and the validity, interpretation and performance of this Agreement shall be governed by, and construed in accordance with, the internal law of Massachusetts, without giving effect to conflict of law principles. Any action, demand, claim or counterclaim relating to the terms and provisions of this Agreement, or to its breach, may be commenced in Massachusetts in a court of competent jurisdiction and shall be resolved by a judge alone; both parties hereby waive and forever renounce the right to a trial before a civil jury.

**11. Successors and Assigns.** Iron Mountain shall have the right to assign this Agreement and its rights hereunder to its successors and assigns, and all covenants and

agreements hereunder shall be enforceable by such successors or assigns.

**12. At Will Employment.** This Agreement does not constitute a contract of employment for any specific period of time. I acknowledge and agree that I am and will remain an "at will" employee, which means that either I or Iron Mountain may terminate the employment relationship at any time, with or without cause or prior notice.

**13. Voluntary Assent.** I UNDERSTAND THAT THIS AGREEMENT CONTAINS SIGNIFICANT RESTRICTIONS WHICH, AMONG OTHER THINGS, PROHIBIT ME FROM WORKING FOR AN IRON MOUNTAIN COMPETITOR DURING THE EFFECTIVE PERIOD HEREOF, AND I AM WILLING TO, AND DO, ACCEPT SUCH RESTRICTIONS. I ACKNOWLEDGE THAT IRON MOUNTAIN HAS ADVISED ME TO SEEK THE ADVICE OF MY OWN LEGAL COUNSEL IF I AM UNSURE ABOUT THE EFFECT OF ANY OF THE OBLIGATIONS AND RESTRICTIONS IN THIS AGREEMENT.

**14. Addendum.**

☐ If this box is checked, this Agreement is modified by the Addendum annexed hereto.

IN WITNESS WHEREOF, I hereunto set my hand and seal this \_\_\_\_\_ day of \_\_\_\_\_, 20 \_\_\_\_\_.

**Agreed and Accepted:**

IRON MOUNTAIN INFORMATION MANAGEMENT, INC.

By: \_\_\_\_\_  
(Employee Signature)

By: \_\_\_\_\_

\_\_\_\_\_  
Name (Print)

Title: \_\_\_\_\_



## PRIVACY, DATA PROTECTION, & COMPLIANCE POLICIES AND PROCEDURES SUMMARY

### Iron Mountain and Its Commitment to Privacy, Data Protection, and Compliance

July 1, 2015

Iron Mountain recognizes the importance of privacy, data protection, and compliance, to our Customers, Vendors, and other business partners and to our Employees. To evidence its commitment, Iron Mountain has appointed the following individuals to manage the Company's privacy and compliance programs:

Jason E. Lomax - Chief Compliance Officer  
E-mail: [Jason.Lomax@ironmountain.com](mailto:Jason.Lomax@ironmountain.com)

Michael Zurcher - Director, Privacy and Compliance  
E-mail: [Michael.Zurcher@ironmountain.com](mailto:Michael.Zurcher@ironmountain.com)

1. **Privacy, Data Protection, Compliance, and Security Overview** - Iron Mountain has had in place for many years the following programs that are integral to a sound confidentiality, privacy, data protection, and compliance program:

- a) **Security Program** - In the United States, all new employees hired since June 1998 have undergone: (i) a 5-year background investigation which, effective January 1, 2003, was expanded to a 7-year background investigation, and subsequently effective July 1, 2011 has been expanded to a 10-year background investigation and (ii) drug-screening.
  - i. Since January 1, 2006, the following background and related checks have been conducted prior to hiring for all United States employees: Social Security Trace; Criminal Records Search; Federal Felony Search; U.S. Secretary of State Terrorist List review; review of Medicare and other healthcare and fraud convictions published by the Office of the Inspector General and Government Management Services.
  - ii. Since January 1, 2005, prospective employees in Canada have undergone background investigations equivalent to those of the United States program.
  - iii. Similar background checks are performed in other countries as permitted by law in those jurisdictions. Please consult with the local country management as to the applicability or permissibility of these programs in the respective countries outside the United States.
  - iv. Pursuant to Executive Order 13224 by the Office of Foreign Assets Control ("OFAC") of the Department of the Treasury, with respect to its employees, since September 1, 2005, Iron Mountain has reviewed the OFAC list to ensure that no prospective employees were listed on the OFAC list.
  - v. In 2006 and 2007, Iron Mountain carried out a program to re-perform background investigations of all its employees in North America, including those who were hired prior to January 1, 2006.
  - vi. In 2009 Iron Mountain implemented a program whereby background investigations of all its employees in North America are re-performed every three years from the date

of hire.

- vii. Since prior to 1998, all new employees in the United States have signed confidentiality agreements pursuant to which employees agree to protect the confidentiality of information and data of both Iron Mountain and its customers. Iron Mountain has established similar programs for Iron Mountain business operations outside the United States.

**b) Compliance Program** - Iron Mountain has a formal compliance program supervised by the Privacy and Compliance Department, and with a separate staff dedicated to compliance and privacy matters. The compliance program consists of training and education of employees regarding compliance issues, establishment of compliance standards, monitoring for compliance, and participating in investigations and decisions regarding compliance issues. In addition, a custom video regarding data protection is incorporated into new employee orientation as well as being a requirement for all temporary personnel to view and to acknowledge adherence to confidentiality and privacy. Compliance and confidentiality are periodically reinforced at the national and local level as well through the following policies and programs:

- i) Employees are required to annually certify adherence to the Company's Code of Ethics and Business Conduct which provides additional support related to the Company's focus on compliance and confidentiality. Iron Mountain's Code of Ethics and Business Conduct is available in multiple languages at: [www.ironmountain.com/code](http://www.ironmountain.com/code).
- ii) The Company has regional privacy resources throughout the enterprise which support the program.
- iii) The Company regularly communicates to its employees about privacy & compliance issues.
- iv) Other compliance, confidentiality, and privacy initiatives are introduced from time to time. Efforts by the security team support these initiatives.

**c) Privacy Program** - Iron Mountain maintains a privacy program that is reasonably designed to ensure a high level of privacy with respect to all information it processes, including information regarding its employees and information belonging to its customers. The following are descriptions of specific aspects of Iron Mountain's privacy and data protection programs. Additional information is available upon request.

- i. **Web-Site/On-line Privacy Notice:** This privacy notice may be found at <http://www.ironmountain.com/Utility/Legal/Privacy-Policy.aspx>.
- ii. **Global Privacy and Data Protection Policy**
- iii. **General Privacy Principles:** Iron Mountain has adopted certain privacy principles that apply to its general, day-to-day business operations. These privacy principles may be found at: <http://www.ironmountain.com/Utility/Legal/Privacy-Policy.aspx>.
- iv. **(U.S.A.) HIPAA:** Except with respect to certain of its employee benefit plans, Iron Mountain is not a covered entity.

The HITECH Act and the Omnibus Rules require Iron Mountain as a business associate to comply with certain of the HIPAA Privacy, Security and

Breach Notification Rules. In order to satisfy these requirements, Iron Mountain conducts compliance and risk assessments for services that store, destroy or release PHI, and has remediated its practices to satisfy the applicable requirements of these Rules Rule. This program includes appropriate measures designed to satisfy the requirements of the Rules applicable to Iron Mountain, including appropriate safeguards to restrict access to, and control the use and disclosure of PHI, in accordance with the provisions of a customer's business associate agreement. Further, this program requires all employees with access to or potential access to health information, or who manage those with access or potential access to health information, to take our annual HIPAA training. Many employees take additional trainings on privacy and security as appropriate to their individual responsibilities.

As part of Iron Mountain's overall privacy program, Iron Mountain has established a system that tracks and reports potential unauthorized acquisition, access, use, or disclosures of personal information, including those that may be reportable under HIPAA. In addition, Iron Mountain has procedures and personnel trained in investigations of any such events, together with protocols for notification and remediation of any potential disclosures.

- v. **(U.S.A.) Gramm-Leach-Bliley Act:** Pursuant to the Interagency Guidelines Establishing Information Security Standards and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Iron Mountain's privacy and information security programs include safeguards designed to manage and control access to customer information in Iron Mountain's possession, including, without limitation, the following: (1) limiting access to customer information and to the Company's facilities where customer information is managed by Iron Mountain, (2) establishing internal controls such as the pre-employment screening procedures described above, (3) installing and maintaining security and monitoring systems, (4) maintaining disaster recovery plans, and (5) designing facilities with protection against certain environmental events. Iron Mountain will also promptly notify a customer in the event that the Company becomes aware of any unauthorized access to customer information.
- vi. **(U.S.A.) Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule:** Iron Mountain has implemented and maintains a program to assist customers that are required to comply with the FACTA Disposal Rule. Except for those records that a customer specifically identifies in writing as not containing consumer information (as defined in 16 CFR Section 682.1) or personal data, reasonable measures are used to protect against unauthorized access to or use of consumer information. Iron Mountain has implemented and monitors compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed. Additionally, Iron Mountain has implemented and monitors compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

- vii. **(U.S.A.) State Privacy Legislation:** Legislation has been enacted in at least 47 states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands requiring or further refining the requirement that companies and/or state agencies disclose to consumers a security breach involving their personal information. In order to assist customers with complying with these state laws, Iron Mountain maintains a list of current state legislation regarding breaches of data security and reporting requirements, and has established a process to report personal data privacy and security breaches.
- viii. **(U.S.A.) Massachusetts CMR 201 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth:** Iron Mountain has developed, implemented, and maintains a comprehensive written information security program that is reasonably designed to be in compliance with the provisions of Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.
- ix. **Investigation of Breaches of Data Security:** In North America, potential breaches involving personal data are managed through the Company's Event Reporting Management Tool and by the Incident Management team with the support of Iron Mountain's Global Security Department. Depending on the nature of the incident involved, this Department will conduct or supervise an investigation. Any determination of a breach will be promptly reported to the affected customer or employee, as the case may be.
- x. **The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks:** Iron Mountain certifies its compliance with the European Union/USA Safe Harbor Framework, and with the Swiss/USA Safe Harbor Framework. To review Iron Mountain's certification to these Safe Harbor Frameworks, please refer to the U.S. Department of Commerce's directory of companies that have certified compliance with Safe Harbor at: <https://safeharbor.export.gov/list.aspx>. Iron Mountain's specific Safe Harbor certification for the EU and Switzerland is available at: <https://safeharbor.export.gov/swisslist.aspx>
- xi. **Canada – Personal Information Protection and Electronic Documents Act (PIPEDA):** Iron Mountain Canada Corporation has implemented practices designed to comply with the requirements of PIPEDA. There is a separate statement of privacy principles for Iron Mountain Canada Corporation that supplements the privacy policy of the U.S. parent corporation. A copy of these principles follows on pages 10 and 11. There is also a template for a Data Protection Agreement available from Iron Mountain Canada Corporation to amend existing Service Agreements.
- xii. **Vendor Privacy Agreements and Assessments:** In order to comply with applicable privacy and data protection laws, rules, and regulations, Iron Mountain's policy, in general, requires vendors and/or subcontractors that handle and have access to Iron Mountain employee or customer information to:
  - Sign a Vendor Privacy Agreement whereby such vendors and/or subcontractors agree to protect personal information in accordance with Iron Mountain's privacy and security standards.
  - Complete a privacy assessment that must be approved by Iron Mountain's Global Security Department prior to commencing a business relationship.

- Depending upon the specific services being offered by a particular vendor/subcontractor, undergo a full information security and privacy review by Iron Mountain.

**Further Information:** For information that is country-specific or that is applicable to certain industry segments or other more geographically-specific areas and that is not referred to above, or, if you have further questions regarding Iron Mountain's privacy program, please e-mail the persons named above.



## PRIVACY PROTECTION IN CANADA

### Iron Mountain Canada Corporation

Iron Mountain Canada Corporation (“Iron Mountain Canada”) is dedicated to the protection of personal data which its customers entrust to it, as well as to the safeguarding of personal data it maintains about its own employees. As you might expect, privacy is a cornerstone of the data management services, which Iron Mountain Canada offers to its customers. It is with this in mind, that Iron Mountain Canada sets forth below additional information concerning how Iron Mountain Canada intends to protect the privacy of personal data entrusted to it.

The privacy principles set forth below are designed to (1) establish the off-line privacy principles of Iron Mountain Canada and (2) to complement the online privacy policy of Iron Mountain Incorporated, the parent corporation of Iron Mountain Canada, a copy of which can be found at <http://www.ironmountain.ca/en/legal/privacy.asp>

### The Personal Information Protection and Electronics Documents Act (“PIPEDA”)

PIPEDA became applicable to Iron Mountain Canada and other commercial organizations effective as of January 1, 2004. PIPEDA is based on Ten Principles established in 1996 by the Canadian Standards Association’s *Model Code for the Protection of Personal Information*. Those Ten Principles are set forth in greater detail below.

PIPEDA was enacted, among other things, to fill a void since the majority of the Provinces had not yet passed legislation to protect personal information. While many Provinces had legislation enacted that protected healthcare information or that asserted certain rights of privacy under freedom of information acts, PIPEDA was designed to be a much broader umbrella of legislation that not only protected the privacy of such personal information, but also set forth the clear requirements for the collection, use and disclosure of such personal information.

Even with the passage of PIPEDA, individual Provinces have nonetheless been encouraged to enact legislation similar to PIPEDA in order to govern how commercial entities manage personal data in their possession. Well in advance of the enactment of PIPEDA, Quebec enacted an act *Respecting the Protection of Personal Information in the Private Sector*. Provinces with their own legislation on the topic govern the protection of personal information and the collection, use and disclosure of personal information within the respective Provinces.

With respect to cross-border, inter-provincial and international trade and commerce, PIPEDA will be the governing law for these transactions.

### THE TEN PRINCIPLES:

**Principle 1, Accountability.** In support of its commitment to protect personal information and its possession and to appropriately collect, use and disclose personal information, privacy concerns in regard to Iron Mountain Canada should be addressed to mail to: [compliance@ironmountain.com](mailto:compliance@ironmountain.com).

**Principle 2, Identifying Purposes.** The purposes for which personal information is collected by Iron Mountain Canada must be identified at or before the time the information is collected.

**Principle 3, Consent.** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where required or permitted by law.

**Principle 4, Limiting Collection.** The collection of personal information shall be limited to that which is necessary for the purposes identified by Iron Mountain Canada. All information so collected shall be collected by fair and lawful means.

**Principle 5, Limiting Use, Disclosure and Retention.** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

**Principle 6, Accuracy.** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

**Principle 7, Safeguards.** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

**Principle 8, Openness.** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

**Principle 9, Individual Access.** Upon request, an individual must be informed of the existence, use and disclosure of his or her personal information and must be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. However, in the case of personal information, which customers of Iron Mountain Canada store with it, since, in the majority of instances, Iron Mountain Canada does not manage customers' data based on individual records, the company will refer the individual to the customer of Iron Mountain Canada so that the customer may respond to such request for individual access. Employees of Iron Mountain Canada shall, however, have access to his/her personal information in accordance with existence policies and procedures governing personnel data.

**Principle 10, Challenging Compliance.** An individual shall be able to address a challenge concerning compliance with the above principles to Iron Mountain Canada at [compliance@ironmountain.com](mailto:compliance@ironmountain.com).

For more information regarding PIPEDA, please visit the official web-site of the Privacy Commissioner of Canada at <http://www.privcom.gc.ca>.

## GLOBAL ANTI-CORRUPTION & ANTI-BRIBERY PROGRAM OVERVIEW

### Iron Mountain and Its Commitment to Anti-corruption & Anti-bribery Prevention, Detection, & Compliance

July 1, 2015

Iron Mountain is a publicly traded, global corporation that operates in over 30 countries. As such, Iron Mountain is subject to a number of Anti-corruption & Anti-bribery laws and conventions including but not limited to the United Kingdom Bribery Act 2010 ("Bribery Act") and the United States Foreign Corrupt Practices Act ("FCPA").

In order to comply with applicable laws and conventions, Iron Mountain has implemented and maintains a Global Anti-corruption and Anti-bribery program that is reasonably designed to prevent and detect corruption and bribery. Some of the key elements of this program are:

- A comprehensive Global Code of Ethics and Business Conduct that is distributed to, trained on, and certified to by every employee upon employment and annually thereafter. The Code is available in multiple languages at [www.ironmountain.com/code](http://www.ironmountain.com/code).
- The development, dissemination, and enforcement of a broad range of global policies including:
  - Anti-corruption & Anti-bribery,
  - Compliance & Ethics,
  - Gifts & Hospitality,
  - Travel & Entertainment,
  - Background Investigations,
  - Charitable Contributions, and
  - Political Contributions.
- An annual risk assessment - Iron Mountain conducts a multi-factor, annual risk assessment of all the countries in which it has operations.
- Annual certification to the program by each country and senior leadership.
- Training - Iron Mountain has an on-going program of in-person and on-line training.
- An anonymous "Hotline" - Iron Mountain maintains a global "hotline" for reporting – where permitted by law – corruption via telephone and internet portal at [www.IMEthicsLine.com](http://www.IMEthicsLine.com).
- An on-going audit program - Iron Mountain's Internal Audit Department conducts audits regarding Anti-corruption & Anti-bribery.
- Risk based pre-contract risk assessment of subcontractors, agents, and consultants.
- Inclusion of Anti-corruption & Anti-bribery language in applicable third party contracts,
- Assessments of target firms and partners pre-merger, pre-acquisition, and pre-joint venture formation.
- A post-merger, acquisition, and joint-venture assessment, training, and integration program.
- A translation program – All relevant documents are translated into the local language.
- Iron Mountain's Global Security Services, Internal Audit, and Legal Departments are available to promptly investigate any allegations and assist in any other matters.

## IRON MOUNTAIN CODE OF ETHICS AND BUSINESS CONDUCT OVERVIEW

**July 1, 2015**

Iron Mountain's Code of Ethics and Business Conduct empowers employees to achieve success by providing guidance and resources to help make legal and ethical business decisions. A copy of Iron Mountain's Code of Ethics and Business Conduct is available in multiple languages at: [www.ironmountain.com/code](http://www.ironmountain.com/code).

The Iron Mountain Board of Directors unanimously approved the Code of Ethics and Business Conduct at its February, 2015 meeting. The Code applies to all Iron Mountain business units, legal entities, controlled joint ventures, affiliates and partnerships. All employees, agents, officers, and members of the Board of Directors are required to follow the Code. Iron Mountain also seeks out suppliers, vendors, contractors, and consultants who maintain ethical standards in line with those written in the Code.

The Code is distributed to all employees worldwide. Further, every employee is trained annually on the Code and executes an annual Certification to abide by the Code. All new employees are also trained on and certify to the Code during onboarding.

The topics covered in the code include:

Our Core Values	Avoiding Conflicts of Interest
Who Must Follow the Code	Preventing Bribery and Corruption
Special Responsibilities for Management and Leadership	Appropriately Exchanging Gifts and Hospitality
Zero Tolerance for Retaliation	Adhering to International Sanctions and Trade Regulations
Investigations and Disciplinary Action	Contracting with Government Customers
The <a href="#">Iron Mountain Ethics Line</a>	Competing the Right Way
Promoting a Safe and Secure Workplace	Selling and Marketing with Integrity
Valuing Inclusion and Diversity	Gathering Competitive Intelligence
Preventing Harassment and Discrimination	Protecting the Environment and Building Sustainability
Safeguarding Our Confidential and Proprietary Information	Contributing to Our Communities
Managing Our Records Appropriately	Respecting Human Rights
Keeping and Disclosing Accurate Financial Records	Safeguarding Our Vehicles and Facilities
Responding to Inquiries from Investors, Analysts, and the Media	Respecting Privacy
Using Technology and Information Systems Responsibly	Effective and Responsible Use of Social Media
	Avoiding Insider Trading
	Participating in Politics and Government Affairs

## SOC 3 REPORT

To view the entire Ernst & Young Report of Independent Accountants SOC 3 Report, [click here](#).



Ernst & Young, LLP  
200 Clarendon Street  
Boston, Massachusetts 02116

Tel: +01 617 266 2000  
Fax: +01 617 266 5843  
ey.com

### Report of Independent Accountants

To the Management of Iron Mountain Information Management, LLC

We have examined management's assertion that Iron Mountain Information Management, LLC (Iron Mountain), during the period January 1, 2015 to December 31, 2015, maintained effective controls to provide reasonable assurance that:

- the Information Technology (IT) Infrastructure Environment and Application Hosting Services System was protected against unauthorized access, use, or modification;
- the Information Technology (IT) Infrastructure Environment Services and Application Hosting System was available for operation and use, as committed or agreed;
- information within the Information Technology (IT) Infrastructure Environment Services and Application Hosting System designated as confidential is protected as committed or agreed;

based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy updated as of July 1, 2015. This assertion is the responsibility of Iron Mountain's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Iron Mountain's relevant security, availability and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Iron Mountain's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

*Ernst & Young LLP*

Ernst & Young LLP  
March 7, 2016  
Boston, Massachusetts



IRON MOUNTAIN PCI ATTESTATION OF COMPLIANCE



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

Based on the results noted in the ROC dated 18 September 2015, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of 18 September 2015: (*check one*):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby Iron Mountain Information Management, Inc has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table><thead><tr><th>Affected Requirement</th><th>Details of how legal constraint prevents requirement being met</th></tr></thead><tbody><tr><td></td><td></td></tr><tr><td></td><td></td></tr></tbody></table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

## FACTA RED FLAGS SUMMARY

### July 1, 2015

Iron Mountain has implemented a physical and information security, privacy, and data protection infrastructure that is reasonably designed to protect the data and information that is entrusted to us by our customers. This infrastructure contains a range of controls and processes to prevent unauthorized access to and acquisition of customer data, and to identify unauthorized attempts to access or acquire customer data.

Should there be any activity, such as a call from a consumer, indicating that there has been a potential access or acquisition of a customer's data or information, Iron Mountain will promptly notify the customer, take corrective action, and, as provided in the customer contract, reasonably cooperate with the customer in investigating any unauthorized access or acquisition.

As indicated in the Federal Trade Commission Interim Final Rule "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, as Amended by the Red Flag Program Clarification Act of 2010" published at <http://www.gpo.gov/fdsys/pkg/FR-2012-12-06/pdf/2012-29430.pdf> in the Federal Register on December 6, 2012, Iron Mountain is not a creditor and therefore is not a covered entity but a service provider.

## MASSACHUSETTS DATA PRIVACY STATEMENT

### **MASSACHUSETTS 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth Iron Mountain Customer Inquiry Response**

Iron Mountain has developed, implemented, and maintains a written information security program that is reasonably designed to be in compliance with the provisions of Massachusetts 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth.

.

## GLOBAL FRAUD, WASTE, &amp; ABUSE PROGRAM SUMMARY



## Global Fraud, Waste, & Abuse Program Summary

### Iron Mountain and Its Commitment to Fraud, Waste, & Abuse Compliance

January 1, 2016

The goals of Iron Mountain's Fraud, and Fraud, Waste, & Abuse ("FWA") program are:

- The prevention, proactive identification, and resolution of deficient corporate processes to ensure complete and accurate financial reporting, elimination of inefficiencies, and the prevention and detection of Fraud, and Fraud, Waste, & Abuse.
- Compliance with applicable laws and regulations including but not limited to the False Claims Act and the Fraud Enforcement and Recovery Act.

For the purpose of this program summary, Fraud, and Fraud, Waste, & Abuse, includes illegal, improper, wasteful, or fraudulent activities. Examples of which include, but are not limited to:

- Theft or misappropriation of funds, supplies, property, or other resources
- Improper and wasteful use of resources
- Forgery or alteration of documents
- Bribery or attempted bribery
- Unauthorized use of records
- Unauthorized alteration or manipulation of computer files
- Unauthorized use of logos, trademarks, copyrights, etc.
- Falsification of reports to management or external agencies
- Pursuit of a benefit or advantage in violation of Iron Mountain's conflict of interest policy
- Improper handling or reporting of financial transactions
- Authorizing or receiving compensation for goods not received or services not performed
- Improper payments from vendors
- Acceptance of inappropriate gifts, entertainment, and/or travel
- Authorizing or receiving compensation for hours not worked
- Falsification or unauthorized alteration of time or leave records
- Falsification of expenses
- Willful violation of laws, regulations, or contractual obligations

In order to achieve its Fraud, and Fraud, Waste, & Abuse goals, Iron Mountain has established and maintains a Global Fraud, and Fraud, Waste & Abuse (FWA) program that is reasonably designed to prevent and detect Fraud, and Fraud, Waste & Abuse. This program is supported by Iron Mountain's

- Code of Ethics and Business Conduct – [www.ironmountain.com/code](http://www.ironmountain.com/code),
- Iron Mountain's IMComplianceHelpline - Iron Mountain's Global website - [www.IMComplianceHelpline.com](http://www.IMComplianceHelpline.com) and telephone "hotline" for reporting fraud, and fraud, waste, abuse, corruption, and other matters,
- Global Fraud Policy,
- Global Compliance and Ethics Policy,
- Global Anti-corruption and Anti-bribery Policy,
- Global Expense and Travel Policy,

- Iron Mountain's Global Incident Reporting Center, and
- Periodic Messaging and other relevant communication

In order to implement these policies and reporting tools, Iron Mountain maintains a professional staff that is dedicated to implementing and managing the Fraud, and Fraud Waste & Abuse program, and investigating allegations. This staff is part of Iron Mountain's Global Security Services Group. Members of the staff hold the following designations: Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), Certified Internal Auditor (CIA), and Certified Controls Specialist (CCS). Additionally, the primary investigative staff are former Federal Bureau of Investigation (FBI) Agents.

Additional resources supporting the FWA program include providing appropriate funding for the program, maintaining an appropriate professional staff for the program, and providing the staff with ongoing specialist training, professional organization membership, and the costs and tools necessary to perform internal reviews and execute the program.

To ensure appropriate project expertise, Global Security Services' Fraud, and Fraud, Waste, & Abuse team supplements its activities by partnering with other specialist corporate functions, including Internal Audit, Legal, and Human Resources.

In addition, the FWA program provides training and presentations to operations and process management and corporate leadership on red flags of fraud, fraud, waste, & abuse, and risk trends.

The FWA program is a risk based program. An annual risk assessment is performed that identifies and ranks the global fraud, and fraud, waste & abuse risks facing Iron Mountain, develops mitigation projects for a calendar year. The program is subject to ongoing assessment throughout the year, is realigned as risks change and events occur, and is reviewed annually to ensure that goals are met. Input for the risk assessment is provided by, but not limited to, the following;

- Cross functional area coordination - Global Internal Audit, Global Internal Controls, Finance, and Corporate Legal;
- Senior Global Operational Management;
- Trends identified by professional organizations and affiliations;
- Results of prior reviews and reported incidents.

The FWA program has identified core processes that are considered high risk and are subject to continuous data analysis; examples of such processes are;

- Accounts Payable; North American Accounts Payable masterfile and payables records are assessed for internal conflicts of interest and accuracy and completeness;
- Expense Reports; North American Senior Management and Employee base Travel & Entertainment (T&E) is performed for policy compliance and expense appropriateness;
- Payroll; detection of ghost employees; metrics analysis for the complete and accurate recording of employee time; appropriateness of payments for the North American commissioned sales employee base;
- Accounts Receivables; cash receipt application and methods of customer refunds for customer overpayment;
- Corporate Credit Card programs; fleet fuel card programs, corporate and employee liability card programs to ensure policy compliance and expense appropriateness;
- Billing; customer billing process; this would include testing operational processes involving SKP and OPIS systems, including cross functional reliance on customer inventory verification, to ensure completeness and accuracy of data capture for billing purposes;
- Vendor Management; address verification, purchasing patterns, segregation of duties, prices of goods and services relative to market, existence of, proper content in, and integrity of contracts.



The results of FWA reviews are maintained in accordance with Iron Mountain's established standards of record retention. FWA reports, which are proprietary, are made available to the Iron Mountain Board of Directors, Senior Corporate Management, and effected Management to assist in remediation efforts.

Non-compliance with Iron Mountain's Fraud, and Fraud, Waste, & Abuse Policy and Program is subject to discipline up to and including termination. Where indicated, violations are referred to Law Enforcement.



**ABOUT IRON MOUNTAIN.** Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at [www.ironmountain.com](http://www.ironmountain.com) for more information.

---

© 2016 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.