SECURITY

PROTECTING YOUR INFORMATION AS IF IT WERE OUR OWN

Contents

Introduction to Iron Mountain Security Practices

Security is our #1 core value! We protect customer information as if it were our own – and we have more than 19,000 people around the world focused on that priority.

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.

We start with a robust commitment to maintain high levels of governance by engaging a security-conscious workforce, developing rigorous standards and implementing the best practices to comply with a multitude of ever-evolving industry and regulatory requirements – all with the aim of protecting the information customers entrust to Iron Mountain.

These practices extend into the physical design and construction of Iron Mountain's facilities, environmental controls and computer systems – which serve to protect the confidentiality, integrity and availability of information stored in buildings and computer systems, transported in vehicles or touched by people.

Our security practices come full circle within our company. In addition to serving 97% of the Fortune 1,000, Iron Mountain is one of its own customers. We diligently leverage our records management, data protection, secure shredding and archiving services in order to maintain the same level of security we provide to our customers.

Throughout this paper, you will have the opportunity to learn more about the depth and breadth of Iron Mountain Security Practices in the following areas:

- Information Security
- Physical Security, Safety and Business Continuity
- Investigative Services

THE QUALIFICATIONS OF IRON MOUNTAIN SECURITY PROFESSIONALS

Our security professionals have a wide range of industry, law-enforcement and government experience, with such skills and credentials as:

- Certified Fraud Examiner (CFE)
- Certified Public Accountant (CPA)
- Licensed Private Investigator (LPI)
- Legal, Privacy and Law Enforcement (LPLE)
- Certified Information System Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Privacy Professional (CIPP)
- Certified Information Privacy Professional/ Government (CIPP/G)
- Certified Protection Professional (CPP)
- Physical Security Professional (PSP)
- Certified Business Continuity Planner (CBCP)
- Certified Ethical Hacker (CEH)
- Certified Web Application Penetration Tester (GWAPT)

Information Security

Information technology resources play a vital role in the conduct and success of Iron Mountain businesses and are protected to ensure confidentiality, integrity and availability. As a result, our Information Security team provides a wide range of services to safeguard assets, ensure compliance and maintain the high level of trust placed in Iron Mountain by so many customers. And in order to maintain this trust, Iron Mountain manages an extensive set of security policies that covers a wide range of areas, including firewalls, network security, intrusion detection and prevention systems, cryptography and access controls.

For example, Iron Mountain Information Security practices are structured upon – but not limited to – the International Organization for Standardization/International Electrotechnical Commission 27002 "Code of Practice for Information Security Management" standard. This standard incorporates required elements for initiating, implementing and maintaining an information security management system.

ALIGNMENT OF SECURITY SERVICES

Iron Mountain's Information Security team has a broad mission that includes minimizing risks within our software and computing infrastructure. Its responsibilities include managing compliance and governance and assessing third-party security and privacy controls.

The team has developed an internally hosted security application called COMPASS (COMpliance, Privacy And Security Services), which automates security, compliance and risk governance processes and data consolidation. The COMPASS application provides centralized reporting and dashboards the team can use to quickly assess security program metrics and measure and improve the effectiveness of security standards across the company.

As an example, the team developed a comprehensive Security Assessment Program and regularly performs penetration tests to determine the likelihood of a network or application attack – and to assess the business impact of a threat. In the unlikely event that any security issues are identified, they are swiftly evaluated and remediated to mitigate the risk.

In addition, Iron Mountain has a dedicated Security Operations Center where analysts monitor our networks and systems and respond to computer security events. Furthermore, the team conducts information security training across Iron Mountain's organization.

ACHIEVING COMPREHENSIVE COMPLIANCE

The compliance experts within the Information Security team are dedicated to ensuring that Iron Mountain adheres to various governmental and regulatory requirements. For example, Iron Mountain currently complies with numerous industry, government and banking regulations and certifications (see sidebar).

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.

COMPLIANCE WITH REGULATORY REQUIREMENTS

Iron Mountain adheres to a broad and comprehensive set of requirements, including those established by:

- Payment Card Industry (PCI)
- Financial Institution Shared Assessment Program (FISAP)
- Federal Financial Institution Examination Council (FFIEC)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Association for Information Destruction (NAID®)
- 36 Code of Federal Regulations 1228 subpart K compliant facilities (CFR)
- National Archives and Records Administration (NARA)
- Nevada Data Privacy Security and Encryption Law (NRS 597.970)
- Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (201 CMR 17.00)
- American Institute of Certified Public Accountants (AICPA)
  - SysTrust

Physical Security, Safety and Business Continuity

Iron Mountain's Business Continuity and Crisis Management team is dedicated to ensuring that all critical businesses and processes are protected from interruptions — as well as producing sound, prudent continuity plans that ensure compliance with laws, regulatory requirements and our customers' service level agreements (SLAs).

Iron Mountain introduced an improved customer notification system for inclement weather service-related disruptions. We conducted an in-depth Business Impact Analysis (BIA) to ensure our recovery time objectives (RTOs) and recovery point objectives (RPOs) are in line with the requirements of our different business segments. In-depth business continuity plans were developed as a result of the BIA to ensure rapid recovery in the event of a business disruption.

The team also developed a global crisis management plan that details immediate response procedures when dealing with a business disruption. This plan includes an automated crisis communication system that allows the right people to be promptly notified, and get the right resources on the ground quickly. In addition, each Iron Mountain facility has a comprehensive Emergency Action Plan that details proper procedures to follow before, during and after an emergency situation. Iron Mountain personnel receive extensive training on emergency preparedness and response.

INFORMATION MANAGEMENT UNDERGROUND

Another key to Iron Mountain's Business Continuity and Crisis Management practices is our underground facilities, the first of which is located in Boyers, Pennsylvania. Known as Data Bunker 220 (DB 220), it hosts Iron Mountain's primary data center, which is solidly constructed 220 feet below ground away from environmental hazards.

Given the vast size of the facility and the number of people working there, its remote and subterranean location, the value of property being stored there (including many one-of-a-kind, irreplaceable items) and the unique value it provides to customers, the importance of providing exceptional security at DB 220 cannot be overstated (see sidebar).

Located in Kansas City, Missouri, and solidly constructed 110 feet below ground away from environmental hazards, Data Bunker 110 (DB 110) is the primary backup facility for North America. The data center is a "hot" online facility that stores near-real-time backups and can host additional backup systems restored from tape if required. In addition, full data center operations from DB 220 can fail over to DB 110.

DATA BUNKER 220 BY THE NUMBERS

On any given weekday, there are close to 2,500 individuals inside the Boyers facility:

- 2,200 are government employees or government contractors
- 180 are Iron Mountain employees
- 100 are employed by private entities
- The remaining are contractors, service technicians and/or vendors

The facility's 1.2 million square feet of developed space has 142 different record centers/leased areas. There are 12 governmental agencies and private institutions occupying each of these record centers.

The failover capability for all key operational processes is an effective, best-practice recovery strategy for business. It limits the reliance on specific written plans for each business process, which requires the intervention of a "human resource" to activate or implement. Together, DB 220 and DB 110 form the foundation for many of Iron Mountain's Business Continuity and Crisis Management services, and they enable us to provide customers with high availability and peace of mind that critical data and information is protected — no matter what.

STRENGTHENING THE WAY WE PROTECT CUSTOMER INFORMATION

The Physical Security team provides critical services for Iron Mountain's global business operations. Often in direct support of our customers and the local management team, the group is dedicated to successfully supporting field operations in physical security matters.

Iron Mountain has made a robust commitment to maintaining high levels of governance and implementing security standards and best practices as they evolve. Our security team has developed and maintained a layered security approach to protect customer information and assets, commencing with a robust employee background investigation program, chain-of-custody integrity via internal controls and physical security systems incorporating intrusion detection, card access, CCTV and fire suppression.

The Physical Security team works on critical incidents, natural disasters, special projects and certification requirements. It also provides Iron Mountain with vital physical security services, from managing emergency response to providing subject matter expertise for building safety and security designs.

To date, the program has been very successful and ensures that the company is protecting the customer information that is entrusted to us. An example of this is making sure that Iron Mountain facilities are in compliance with the Code of Federal Regulation (CFR), International Traffic in Arms Regulations (ITAR), PCI, National Industrial Security Program Operating Manual (NISPOM) and the National Association for Information Destruction (NAID) requirements.

The Physical Security team works closely with field operations to optimize and strengthen the way we protect customer information. The team extensively reviews and provides subject matter expert recommendations for physical security improvement. What's more, continuous security infrastructure and process improvements are also performed with field operations to enhance our program. We also continually evaluate our security programs and standards to maintain and provide optimal protection of our customers' information and assets.

Investigative Services

Iron Mountain employs a team focused on the protection of customer information and the people and assets of Iron Mountain. This team's responsibilities include Incident Management, Corporate Investigations, Background Investigations and a Fraud, Waste and Abuse program.

INCIDENT MANAGEMENT

Incidents involving customer material are reported via our Incident Reporting Center (IRC) and are triaged, investigated and escalated by an experienced team of security professionals, including analysts and investigators with backgrounds in privacy, law and investigations. The IRC allows the team to efficiently track incidents, identify trends and develop processes and procedures to prevent recurring incidents.

CORPORATE INVESTIGATIONS

The Corporate Investigations team has global responsibility for conducting fact-finding investigations, including employee wrongdoing, accidents and responding to the loss of customer or Iron Mountain assets. In addition to our experienced investigators, a team of qualified and vetted licensed private investigators throughout North America has been identified to assist with ongoing investigations by providing additional expertise, regional coverage and a network connection with local law enforcement communities. This has improved incident response time, proven effective in supporting several high-profile incidents and will be expanded globally as investigative resources and expertise are needed.

FRAUD, WASTE AND ABUSE

Iron Mountain has established and maintains a Global Fraud, Waste and Abuse (FWA) program whose goal is to ensure complete and accurate financial reporting, eliminate inefficiencies and detect and prevent fraud, waste and abuse. In order to implement policies and reporting tools, Iron Mountain maintains a professional staff that is dedicated to maintaining the program and investigating allegations. Members of the staff hold the following designations: Certified Public Accountant (CPA), Certified Fraud Examiner (CFE) and the primary investigative staff are former Federal Bureau of Investigation Agents.

BACKGROUND INVESTIGATIONS

People are Iron Mountain's greatest asset and the face of the company. Therefore, it is imperative that we employ individuals who positively reflect our core values and demonstrate superior service and commitment to Iron Mountain's customers. The Background Investigations (BI) team partners with Human Resources to ensure Iron Mountain hires and retains employees who share our vision and core values.

Recently, Iron Mountain enhanced its BI process to better align with our commitment to security and the safety of our customers and employees. Our policy includes a 7-year review of employment verifications and a 10-year review of criminal records via domestic and international law enforcement repositories. A criminal record review is conducted every three years henceforth for all employees. We have also designed and implemented a risk-based assessment program that, depending on various risk categories, will impose different levels of due diligence upon new and existing third parties that provide services to Iron Mountain — which helps ensure that our partners are subject to the same rigorous standards by which we operate.

Finally, Iron Mountain employs a Code of Ethics and Business Conduct that makes sure we value honesty and integrity as much as quality service. We believe that acting with the highest ethical standards isn't just the right thing to do — it helps build trust with our customers and contributes to successful long-term relationships.

Unparalleled Security, Today and Tomorrow

While new security opportunities and challenges are always on the horizon, our goal remains the same: to secure and protect customers' information as if it were our own. And we continue to actively pursue this goal by infusing our security expertise and best practices into every solution and service we offer.

Additionally, we understand that security is a constantly moving target. As such, we continue to work closely with our customers, business associates and strategic partners to monitor, assess and evolve our security programs on a regular basis. As a result of these efforts, our customers are able to benefit from:

- **Unparalleled protection of assets:** Iron Mountain customers can rest assured that their critical information is protected by the right people – in transit and while stored – and in accordance with industry standards and best practices.
- **Comprehensive security assurance:** By applying numerous certification and industry standards that meet or exceed established requirements, Iron Mountain solutions can reduce the costs and risks associated with compliance, litigation, disaster recovery and preservation of vital assets.
- **Industry leading expertise:** Iron Mountain regularly updates customers on the latest information management, storage and security issues businesses are facing, so they can stay ahead of the curve and limit risks to their bottom line and their brand.

Iron Mountain provides a broad portfolio of solutions and services that are tailored to your unique needs and designed to help you maximize the business value of your information. We are unique in the industry due to our consistent management of information regardless of location and media type or format. And of course, strong security and chain-of-custody measures are at the core of every service we offer.

Finally, within the Security organization, Iron Mountain employs a Business Integration team whose responsibility is to work directly with the sales force as a liaison between our customers and the business for security matters. The team coordinates cross-functional activities amongst Iron Mountain stakeholders by defining consistent security and compliance responses to appropriately address specific needs of customers by leveraging the expertise of Iron Mountain Security personnel throughout the organization. Additionally, the team prepares and regularly updates the Security Assurance Package (SAP), which customers can request at any time to learn more about Iron Mountain's Security practices.

For more information about Iron Mountain Security Practices, Compliance and Certifications please request our Security Assurance Package (SAP) from your Iron Mountain sales representative or account manager, or visit www.ironmountain.com.

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 for more information.