SOLUTION BRIEF

IRON MOUNTAIN INSIGHT SECURITY OVERVIEW

IRON MOUNTAIN®

EXECUTIVE SUMMARY

Security is a primary concern for our customers. They demand a proven solution that provides protection for them and their customers against hackers, malware, and unsafe operations. They also require a solution that extends their current security practices so that they can meet critical certification and compliance requirements, provide granular control over user access, and access easy-to-use auditing and tracking capabilities.

Iron Mountain InSight® incorporates an end-to-end security strategy that covers content ingestion to storage of digital documents and metadata. Iron Mountain leverages the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) as our enterprise security framework.

We provide secure deployment of services, data storage with end-user privacy safeguards, communications between services, and administration support with separation of duties.

The infrastructure is designed in progressive layers starting from the physical security of the hosted data centres, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes that support operational security following compliance specifications (ISO 27001 and SOC 2 Type II).

IRON MOUNTAIN SECURITY OVERVIEW

Our 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.

To protect our customers' information, Iron Mountain InSight® maintains high levels of governance by:

- Engaging a security-conscious, highly vetted workforce
- Developing and following rigorous standards
- Implementing best practices that comply with evolving industry and regulatory requirements

These practices originate in the physical design and construction of our facilities, environmental controls, and computer systems. And with our cloud partners like Google and Amazon Web Services, we ensure that the confidentiality, integrity, and availability of information stored in the cloud is as secure as the information stored in our physical buildings and computer systems.

The Iron Mountain InSight® framework for security compliance follows the NIST standard of Identify, Protect, Detect, Respond, and Recover.

IDENTIFY

This function assists in developing an organisational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities. This includes:

- Risk assessments following NIST 800-53/53A
- Information Security Management System (ISMS) to protect PII
- Asset, risk, and supply chain management

PROTECT

This function outlines the safeguards to ensure delivery of critical infrastructure services and supports the ability to limit or contain the impact of a potential cybersecurity event. This includes:

- Web Application Firewall (WAF) and Data Loss Prevention (DLP) solutions
- Identity and Access Management (IAM)
- Regular penetration tests
- Encryption of data at rest and in transit with AES256, TLS 1.2 / 3
- Data protection, privacy, and security training for all employees

DETECT

This function defines the appropriate activities to identify the occurrence of a cybersecurity event. This includes:

- Security Information and Event Management (SIEM) solution for system monitoring
- Scanning of all environments, containers, and code
- Full audit, system, and network logs for all user and admin activity

RESPOND

This function includes appropriate activities to take action in the event of a detected cybersecurity incident. This includes:

- Virtual Security Operations Centre (vSOC) with Federally cleared resources for security monitoring
- Defined and approved incident response procedures

RECOVER

This function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired from a cybersecurity incident. This includes:

- Defined and approved business continuity, contingency, and disaster recovery plans (RTO under 24 hours; RPO within 1 hour)
- Regular tests and assessments of these plans

In addition to this strong security foundation, Iron Mountain InSight® provides extra security features that can be used to grant or restrict access to content within the platform. These user controls are applied at the role level and can be enhanced by adding criteria based on content metadata to further restrict access to sensitive information. All business functions are logged, ensuring that there is a comprehensive audit trail available.

Please contact us for additional information.

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organisations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centres, art storage and logistics, and cloud services, Iron Mountain helps organisations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working.

UK-WP-031422A