IRON MOUNTAIN®

White paper

Iron Mountain InSight® security

Executive summary

About Iron Mountain security

Iron Mountain incorporates an in-depth security approach that covers content ingestion, storage, and processing of digital documents as well as hosting in a secure data center. 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.

Training

Iron Mountain works with highly regulated industries requiring workforce security and privacy training. Employees take various security courses and training developed throughout the year as mandated by our enterprise-wide training program. The training includes annual security awareness, data privacy training, secure code training, code of ethics, and business conduct. We work with customers so that personnel are properly vetted with background checks. Our employment is contingent upon a background investigation as applied through various local and client requirements.

Iron Mountain InSight products

I. Compliance programs

Iron Mountain InSight has established a broad and specific security compliance program aligning with industry and regulatory customer needs. This includes security compliance and data privacy.

Compliance attestations

- ISO-27001 - InSight has been continuously certified since 2020. This is an international standard that helps organizations manage the security of their information assets. It provides a management framework for implementing an information security management system (ISMS) to ensure the confidentiality, integrity, and availability of all data.
- SOC2 Type 2 - Iron Mountain has maintained a SOC2 Type 2 attestation for InSight since 2020. SOC2 Type 2 Report is a Service Organization Control (SOC) audit on how a cloud-based service provider handles sensitive information.

Industry compliance

- InSight is 21 CFR Part 11 capable.
- StateRAMP - Ready status received in January 2024.
- FedRAMP (NIST 800-53/37) - Third-party testing performed against the NIST 800-53 Revision 5 controls, as well as additional FedRAMP requirements. InSight has received FedRAMP Authorizations to Operate (ATO) as well as FedRAMP Ready status.

Data privacy

- General Data Protection Regulation (GDPR) - InSight has undergone a GDPR assessment and a copy of the report is available upon request.
- Health Insurance Portability and Accountability Act (HIPAA) - InSight is HIPAA-compliant and has implemented privacy and security measures to protect the privacy and security of personally identifiable information (PII).

II. Operational security overview

Identity and access management

- We implement and enforce role-based access control for privileged users wherein their use and allocation is restricted. Multi-factor authentication (MFA) is mandatory so that access is limited to authenticated users. Least privilege is implemented for authorized users and processes.

Monitoring

- Security scanning - The InSight environment includes a monitoring system which scans container images and systems, and detects vulnerabilities.
- Application security testing - InSight conducts static application security testing (SAST), dynamic application security testing (DAST) and manual penetration testing.
- System monitoring and audit logs - InSight includes a security information and event management (SIEM) system for log management, real time monitoring of security events, correlation and alerting of security events, and audit logs.
- Incident response - Our cyber incident and response team (CIRT) is responsible for classifying audit events that are of particular interest for the Iron Mountain InSight information system, and for conducting reviews and analysis of audit records.
- Incident management - Our cyber incident and response team (CIRT) maintains a cyber response plan to identify, protect, detect, respond, and recover in real time to include comprehensive logging and monitoring of our products and infrastructure. We also maintain employee awareness and training programs to include internal information security policies and procedures.

Business continuity

- InSight's Recovery Time Objective (RTO) for Tier 1 business applications is between 10 - 24 hours and the Recovery Point Objective (RPO) was assessed to be 1 hour in our last business continuity plan (BCP) test conducted in Q4 2023. RTO/RPO can be modified based upon customer needs.

Disaster recovery

- InSight's disaster recovery test is designed so that we can effectively recover objects, databases, and indices from accidental deletion or update, as those are the sources of persistent data for the InSight application within the given RTO/RPO as documented in our business continuity plan (BCP).

Capacity planning

- Our capacity planning is geared towards monitoring workload performance and allowing capacity to meet current and future demands. This includes measuring performance and monitoring so that we do not reach capacity limits.

Patching and vulnerability management

- Patching and vulnerability management, anti-malware, endpoint disk encryption, and intrusion prevention are managed through our Information Technology asset and endpoint management solutions.

Encryption

- All data is encrypted in flight and at rest following the Federal Information Processing Standards (FIPS 140-2) using industry standards such as Advanced Encryption Standard (AES) 256 and service managed keys.

III. Data privacy

Data residency

- To help comply with data residency requirements, InSight has the ability to control where data is stored at rest and also customize and restrict data storage to certain regions.

Data protection

- InSight applies appropriate technical, organizational and administrative measures, including encryption and multi-factor authentication (MFA) so that customer data remains secure at all times. InSight can deploy a web application firewall (WAF) at a customer's request.
- Any type of customer data (including confidential and personal data) may reside on the InSight platform and the customer has full discretion as to what data is submitted to the platform for processing. Customer data is retained only for the duration of the services and then either returned or deleted upon the customer's direction.
- Iron Mountain is aware that many countries have laws governing international data transfers and relies on Standard Contractual Clauses for internal and external transfers of personal data, as applicable, e.g., EU/ UK personal data transfers to countries such as the U.S. and India. Iron Mountain complies with the EU-U.S. Data Privacy Framework (DPF), the UK extension to the EU-U.S. DPF, and the Swiss-U.S. DPF.

- Iron Mountain Data Processing Agreement sets out our responsibilities and commitments related to the processing of customer personal data.

NOTE: Please view Iron Mountain's Privacy Notice to learn more about our privacy and data protection practices.

IRON MOUNTAIN®

800.899.IRON | ironmountain.com

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 225,000 organizations around the world, and with a real estate network of more than 98 million square feet across more than 1,400 facilities in over 60 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 centers, art storage and logistics, and cloud services, Iron Mountain helps organizations lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.

USDXP-WP-022825A