IRON MOUNTAIN®

Whitepaper

Iron Mountain InSight® Security

Zusammenfassung

Über Iron Mountain Security

Iron Mountain verfügt über einen umfassenden Sicherheitsansatz, der die Erfassung, Speicherung und Verarbeitung von Inhalten digitaler Dokumente sowie das Hosting in einem sicheren Rechenzentrum umfasst. Dabei setzen wir auf das Cyber Security Framework (CSF) des National Institute of Standards and Technology (NIST) als Rahmen für Unternehmenssicherheit. Wir sorgen für eine sichere Bereitstellung von Diensten, Datenspeicherung unter Berücksichtigung des Datenschutzes der Endnutzer:innen, Kommunikation zwischen Dienstleistungen, und verwaltungstechnischen Support mit Aufgabentrennung.

Schulungen

Iron Mountain arbeitet mit stark regulierten Branchen zusammen, die Datensicherheits- und Datenschutzschulungen der Mitarbeiter:innen erfordern. Die Mitarbeiter:innen nehmen das ganze Jahr über an verschiedenen Kursen und Schulungen im Bereich Datensicherheit und Datenschutz teil, die in unserem unternehmensweiten Schulungsprogramm vorgeschrieben sind. Das Schulungsprogramm umfasst jährliche Schulungen zu den Themen Sicherheitsbewusstsein, Datenschutz, Sicherheitscode, Verhaltenskodex und Geschäftsgebaren. Wir arbeiten mit unseren Kund:innen zusammen, um das Personal sorgfältigen Prüfungen zu unterziehen. Eine Anstellung hängt von einer Überprüfung, die aufgrund verschiedener lokaler und kundenspezifischer Anforderungen durchgeführt wird, ab.

Iron Mountain InSight-Produkte

I. Compliance-Programme

Iron Mountain InSight hat ein umfassendes und spezifisches Programm zur Einhaltung von Sicherheitsbestimmungen entwickelt, das an die Anforderungen der Branchen und öffentlichen Stellen angepasst ist. Dazu gehören die Einhaltung von Sicherheitsbestimmungen und Datenschutz.

Konformitätsbescheinigungen

- ISO 27001: InSight wird seit 2020 kontinuierlich zertifiziert. Dies ist eine internationale Norm, die Unternehmen bei dem Schutz ihrer Informationen unterstützt. Sie bietet einen Management-Rahmen für die Implementierung eines Information Security Management System (ISMS), um die Vertraulichkeit, Integrität und Verfügbarkeit aller Daten zu gewährleisten.

- SOC2 Typ 2: Iron Mountain InSight ist seit 2020 SOC2-Typ-2-konform. Der SOC2-Typ-2-Bericht ist ein SOC-Audit (Service Organization Control) darüber, wie ein cloudbasierter Dienstanbieter mit sensiblen Informationen umgeht.

Einhaltung von Branchenstandards

- InSight erfüllt die Anforderungen von Title 21 CFR Part 11.
- InSight hat den Status „StateRAMP – Ready" im Januar 2024 erhalten.
- FedRAMP (NIST 800-53/37): Prüfung durch Dritte anhand der NIST 800-53 Rev.-4-Kontrollen sowie zusätzlichen FedRAMP-Anforderungen. InSight hat FedRAMP-Betriebszulassungen (ATO) sowie den FedRAMP-Status „Ready" erhalten.

Datenschutz

- Datenschutz-Grundverordnung (DSGVO): InSight wurde einer DSGVO-Beurteilung unterzogen. Eine Kopie des Berichts ist auf Anfrage erhältlich.
- Health Insurance Portability and Accountability Act (HIPAA): InSight ist HIPAA-konform und hat Datenschutz- und Sicherheitsmaßnahmen implementiert, um den Datenschutz personenbezogener Daten zu gewährleisten.

II. Überblick über operative Sicherheit

Identitätsmanagement

- Wir implementieren und gewährleisten eine rollenbasierte Zugriffskontrolle für berechtigte Benutzer:innen, bei der ihre Nutzung und Zuweisung eingeschränkt ist. Die Multi-Faktor-Authentifizierung (MFA) ist obligatorisch, sodass der Zugriff auf authentifizierte Benutzer:innen beschränkt ist. Das Least-Privilege-Prinzip ist für autorisierte Benutzer:innen und Prozesse implementiert.

Überwachung

- Sicherheitsscan: Die InSight-Umgebung umfasst ein Überwachungssystem, das Container-Images und -Systeme scannt und Schwachstellen erkennt.
- Anwendungssicherheitstests: InSight führt statische Anwendungssicherheitstests (SAST), dynamische Anwendungssicherheitstests (DAST) und manuelle Penetrationstests durch.
- Systemüberwachung und Prüfprotokolle: InSight umfasst ein SIEM-System (Security Information and Event Management) für Protokollverwaltung, Echtzeitüberwachung von Sicherheitsereignissen, Korrelationen und Benachrichtigung bei Sicherheitsereignissen sowie Auditprotokolle.
- Reaktion auf Vorfälle: Unser „Cyber Incident and Response-Team" (CIRT) ist verantwortlich für die Klassifizierung von Audit-Ereignissen, die für das Informationssystem Iron Mountain InSight von besonderem Interesse sind, sowie für die Durchführung von Prüfungen und Analysen von Audit-Aufzeichnungen.
- Vorfallmanagement: Unser „Cyber Incident and Response-Team" (CIRT) führt einen Cyber-Reaktionsplan für Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellung in Echtzeit, um eine umfassende Protokollierung und Überwachung unserer Produkte und Infrastruktur zu ermöglichen. Darüber hinaus fördern wir das Bewusstsein unserer Mitarbeiter:innen und führen Schulungsprogramme durch, die interne Richtlinien und Verfahren zur Informationssicherheit beinhalten.

Geschäftskontinuität

- Das Recovery Time Objective (RTO) von InSight für Geschäftsanwendungen der Stufe 1 beträgt 10 bis 24 Stunden. Das Recovery Point Objective (RPO) betrug bei unserem letzten, im 4. Quartal 2023 durchgeführten BCP-Test (Business Continuity Plan) 1 Stunde. Das RTO/RPO kann je nach Kundenbedürfnissen angepasst werden.

Notfallwiederherstellung

- Der InSight-Notfallwiederherstellungstest ist so konzipiert, dass wir Objekte, Datenbanken und Indizes nach versehentlichem Löschen oder Aktualisieren effektiv innerhalb des gegebenen RTO/RPO, wie in unserem Geschäftskontinuitätsplan (BCP) dokumentiert, wiederherstellen können, da dies die Quellen persistenter Daten für die InSight-Anwendung sind.

Kapazitätsplanung

- Unsere Kapazitätsplanung ist darauf ausgerichtet, die Workload-Leistung zu überwachen und Kapazitäten für aktuelle und zukünftige Anforderungen sicherzustellen. Dazu gehören die Messung der Leistung und die Überwachung, damit wir die Kapazitätsgrenzen nicht erreichen.

Patching und Schwachstellenmanagement

- Patching und Schwachstellenmanagement, Anti-Malware-Maßnahmen, Endpunkt-Datenträgerverschlüsselung und Intrusion Prevention werden über unsere IT-Asset- und Endpunkt-Management-Lösungen verwaltet.

Verschlüsselung

- Alle Daten werden gemäß FIPS 140-2 (Federal Information Processing Standards) anhand von Industriestandards wie AES 256 (Advanced Encryption Standard) und Service-Managed Keys gespeichert und übermittelt.

III. Datenschutz

Data Residency

- Data Residency beschreibt, wo die Daten des/r Kund:in gespeichert werden. Um die Anforderungen an die Data Residency zu erfüllen, kann InSight steuern, wo die Daten gespeichert werden, und die Datenspeicherung kann auf bestimmte Regionen angepasst und beschränkt werden.

Datenschutz

- InSight setzt geeignete technische, organisatorische und administrative Maßnahmen ein, darunter Verschlüsselung und Multi-Faktor-Authentifizierung (MFA), damit Kundendaten jederzeit geschützt bleiben. InSight kann auf Kundenanfrage eine Web Application Firewall (WAF) bereitstellen.

Datenschutz-Folgenabschätzungen (DPIAs)

- Iron Mountain verarbeitet private und personenbezogene Daten im Namen anderer. Als Datenverantwortlicher oder Auftragsverarbeiter kann Iron Mountain Kundeninformationen verarbeiten, ohne Kenntnis des tatsächlichen Inhalts oder Ursprungs der Daten zu erhalten.
- Wenn wir als Datenverantwortlicher oder Auftragsverarbeiter aus dem Europäischen Wirtschaftsraum (EWR) und der Schweiz agieren (oder aus den USA auf Daten im EWR oder in der Schweiz zugreifen), werden die Daten gemäß den geltenden Grundsätzen des Privacy Shield verarbeitet.
- Wir führen in regelmäßigen Abständen Datenschutz-Folgenabschätzungen (DPIAs) durch, die im Zusammenhang mit der Verarbeitung personenbezogener Daten vorgeschrieben sind.

HINWEIS: Informationen über die Arten von personenbezogenen Daten und die Zwecke, zu denen diese Daten übertragen und verarbeitet werden, sowie über die Dritten, an die diese Daten weitergegeben werden können, finden Sie in der Datenschutzerklärung von Iron Mountain.

Elevate the power of your work

Seit mehr als 70 Jahren ist Iron Mountain Ihr strategischer Partner für Ihre Informationen und Ressourcen. Als weltweit führendem Unternehmen im Bereich Archivierung und Informationsmanagement vertrauen uns mehr als 225.000 Unternehmen weltweit, darunter über 90 % der Fortune 1000. Wir schützen, erschließen und steigern den Wert Ihrer Arbeit – egal, wo sich die Informationen befinden und wie sie gespeichert sind.

DE: 0800 408 0000 | ironmountain.com/de-de
AT: +49 40 521 08 170 | ironmountain.com/de-at
CH: 0800 00 24 24 | ironmountain.com/de-ch

Über Iron Mountain

Iron Mountain Incorporated (NYSE: IRM) wurde 1951 gegründet und ist weltweit führender Dienstleister für Archivierung und Informationsmanagement. Wir genießen das Vertrauen von mehr als 225.000 Organisationen weltweit und verfügen über ein Immobiliennetzwerk von mehr als 9,1 Millionen Quadratmetern in über 1.400 Einrichtungen in mehr als 60 Ländern weltweit. Wir lagern und schützen Milliarden von Informationen, darunter kritische Geschäftsinformationen, hochsensible Daten sowie kulturelle und historische Artefakte. Iron Mountain bietet ein breites Lösungsportfolio an. Vom sicheren Speichern, Verwalten und Vernichten von Informationen, über Rechenzentren bis hin zu Cloud-Services. Wir unterstützen Unternehmen dabei, Kosten und Risiken zu senken, Richtlinien einzuhalten und eine digitale Arbeitsweise zu ermöglichen. Mehr Infos erhalten Sie unter www.ironmountain.com/de-de.