IRON MOUNTAIN®

kertas putih

Gambaran umum keamanan Iron Mountain

Gambaran umum keamanan Iron Mountain

Ringkasan eksekutif

Keamanan adalah perhatian utama bagi pelanggan kami. Mereka menuntut solusi teruji yang memberikan perlindungan bagi mereka dan pelanggan mereka dari peretas, malware, dan operasi yang tidak aman. Mereka juga memerlukan solusi yang memperluas praktik keamanan mereka saat ini sehingga dapat memenuhi persyaratan sertifikasi dan kepatuhan penting, menyediakan kontrol terperinci atas akses pengguna, serta mengakses kemampuan audit dan pelacakan yang mudah digunakan.

Iron Mountain InSight® menggabungkan strategi keamanan menyeluruh yang mencakup penyerapan konten hingga penyimpanan metadata dan dokumen digital. Iron Mountain memanfaatkan Kerangka Kerja Keamanan Siber (CSF) dari National Institute of Standards and Technology (NIST) sebagai kerangka kerja keamanan perusahaan kami.

Kami menyediakan penerapan layanan yang aman, penyimpanan data dengan perlindungan privasi pengguna akhir, komunikasi antarlayanan, dan dukungan administrasi dengan pemisahan tugas.

Infrastruktur dirancang dalam lapisan progresif mulai dari keamanan fisik pusat data yang dihosting hingga keamanan perangkat keras serta perangkat lunak yang mendasari infrastruktur, dan terakhir, kendala teknis serta proses yang mendukung keamanan operasional sesuai dengan spesifikasi kepatuhan (ISO 27001 dan SOC 2 Tipe II).

Gambaran umum keamanan Iron Mountain

Praktik keamanan kami berpandu pada standar perusahaan yang tinggi dan didorong oleh tim yang berfokus pada bisnis serta berdedikasi untuk melindungi informasi dan aset—sekarang dan pada tahun-tahun mendatang.

Untuk melindungi informasi pelanggan kami, Iron Mountain InSight® mempertahankan tata kelola tingkat tinggi dengan:

- Melibatkan tenaga kerja yang sadar akan keamanan dan sangat teruji
- Mengembangkan dan mematuhi standar yang ketat
- Menerapkan praktik terbaik yang sesuai dengan persyaratan peraturan dan industri yang berkembang

Praktik ini berasal dari desain fisik dan konstruksi fasilitas, kontrol lingkungan, dan sistem komputer kami. Bersama mitra cloud kami, seperti Google dan Amazon Web Services, kami juga memastikan bahwa kerahasiaan, integritas, dan ketersediaan informasi yang disimpan di cloud seaman informasi yang disimpan di bangunan fisik dan sistem komputer kami.

Kerangka kerja Iron Mountain InSight® untuk kepatuhan keamanan mengikuti standar NIST, yaitu Mengidentifikasi, Melindungi, Mendeteksi, Menanggapi, dan Memulihkan.

Mengidentifikasi

Fungsi ini membantu mengembangkan pemahaman organisasi dalam mengelola risiko keamanan siber terhadap sistem, orang, aset, data, dan kemampuan. Fungsi ini mencakup:

- Penilaian risiko yang mematuhi NIST 800-53/53A
- Sistem Manajemen Keamanan Informasi (ISMS) untuk melindungi informasi identitas pribadi (PII)
- Manajemen aset, risiko, dan rantai pasokan

Melindungi

Fungsi ini menguraikan pengamanan untuk memastikan penyampaian layanan infrastruktur penting dan mendukung kemampuan untuk membatasi atau menahan kemungkinan terjadinya peristiwa keamanan siber. Fungsi ini mencakup:

- Solusi Firewall Aplikasi Web (WAF) dan Pencegahan Kehilangan Data (DLP)
- Manajemen Identitas dan Akses (IAM)
- Uji penetrasi reguler

- Enkripsi data at rest dan in transit dengan AES256, TLS 1.2 / 3
- Pelatihan tentang perlindungan data, privasi, dan keamanan untuk semua karyawan

Mendeteksi

Fungsi ini menentukan aktivitas yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber. Fungsi ini mencakup:

- Solusi Manajemen Peristiwa dan Informasi Keamanan (SIEM) untuk pemantauan sistem
- Memindai semua lingkungan, kontainer, dan kode
- Log jaringan, sistem, dan audit lengkap untuk semua aktivitas pengguna dan admin

Menanggapi

Fungsi ini mencakup aktivitas yang sesuai untuk mengambil tindakan jika terjadi insiden keamanan siber yang terdeteksi. Fungsi ini mencakup:

- Pusat Operasi Keamanan Virtual (vSOC) dengan sumber daya izin Federal untuk pemantauan keamanan
- Prosedur tanggap insiden yang ditetapkan dan disetujui

Memulihkan

Fungsi ini mengidentifikasi aktivitas yang sesuai untuk mempertahankan rencana ketahanan dan memulihkan kemampuan atau layanan yang terganggu akibat insiden keamanan siber. Fungsi ini mencakup:

- Rencana keberlangsungan bisnis, kontingensi, dan pemulihan bencana yang ditetapkan dan disetujui (RTO di bawah 24 jam; RPO dalam 1 jam)
- Pengujian dan penilaian rutin atas rencana ini

Selain landasan keamanan yang kuat ini, Iron Mountain InSight® menyediakan fitur keamanan tambahan yang dapat digunakan untuk memberikan atau membatasi akses ke konten di dalam platform. Kontrol pengguna ini diterapkan pada tingkat peran dan dapat disempurnakan dengan menambahkan kriteria berdasarkan metadata konten untuk lebih membatasi akses ke informasi sensitif. Semua fungsi bisnis dicatat, sehingga memastikan tersedianya jejak audit yang komprehensif.

Harap hubungi kami untuk mendapatkan informasi tambahan.

IRON MOUNTAIN®

+62 21 3973 9999 | ironmountain.com/id

Tentang Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), didirikan pada tahun 1951, merupakan perusahaan global terkemuka di bidang jasa penyimpanan dan manajemen informasi. Telah dipercaya oleh lebih dari 225.000 perusahaan di seluruh dunia, dan lebih dari 26 juta meter persegi jaringan real estat pada lebih dari 1.400 fasilitas di lebih dari 50 negara. Iron Mountain menyimpan dan melindungi milyaran aset bernilai, termasuk informasi bisnis penting, data yang sangat sensitif, dan artefak sejarah dan budaya. Dalam menyediakan solusi yang mencakup manajemen informasi, transformasi digital, penyimpanan dan pemusnahan dokumen yang aman, dan pusat data, layanan cloud, serta penyimpanan dan logistik karya seni, Iron Mountain membantu pelanggan mengurangi biaya dan risiko, mematuhi peraturan, melakukan pemulihan dari bencana, dan memungkinkan cara kerja yang lebih digital.