IRON MOUNTAIN®

DIE DREI GRUNDPFEILER FÜR DATENSCHUTZ UND INFORMATIONSSICHERHEIT IM HOMEOFFICE

BEST PRACTICES FÜR KLEINE UNTERNEHMEN

ZAHLEN & FAKTEN

„KLEINERE UNTERNEHMEN KÖNNEN LEICHTER OPFER VON CYBERBEDROHUNGEN WERDEN, WEIL SIE, ANDERS ALS GROSSE KONZERNE, MEIST KEINE EXPERT:INNEN VOR ORT HABEN, DIE SOFORT AUF DATENPANNEN REAGIEREN ODER DIESEN VORBEUGEN KÖNNEN. AUCH INVESTIEREN SIE WENIGER IN DIE CYBERSICHERHEIT."

ZURICH INSURANCE UK

Je mehr Menschen im Homeoffice oder von unterwegs aus arbeiten, desto größer sind die Risiken für die Informationssicherheit. Hacker wissen genau, wie sie Schwachstellen ausnutzen, um sich finanziell zu bereichern – Cyberangriffe, Ransomware und Phishing-Mails nehmen immer weiter zu. Ein einziger solcher Vorfall kann das ganze Wachstum Ihres Unternehmens in Gefahr bringen. Deshalb sollten Sie Ihre Best Practices zum Thema Informationssicherheit so klar wie möglich kommunizieren, wenn jemand ins Homeoffice wechselt.

RICHTLINIEN

Formulieren Sie klare und deutliche Richtlinien zu den wichtigsten Aspekten der Informationssicherheit und stellen Sie diese allen Mitarbeiter:innen schriftlich zur Verfügung. Erklären Sie u. a., wie Laptops, Telefone und andere Geräte richtig genutzt werden. Wenn Sie noch dabei sind, diese Richtlinien zu entwickeln, denken Sie an die folgenden Punkte:

- Dürfen Ihre Angestellten geschäftliche Aufgaben auf privaten Computern oder Telefonen erledigen?
- Dürfen sie Geschäftsunterlagen auf eigene Geräte kopieren?
- Dürfen sie Geschäftsunterlagen an ihre private E-Mail-Adresse oder andere E-Mail-Adressen außerhalb der Unternehmensdomain senden?
- Dürfen sie Geschäftsunterlagen zu Hause ausdrucken?
- Dürfen sie eigene USB-Sticks zum Speichern von Geschäftsinformationen nutzen?

Dafür müssen Sie keine langen Abhandlungen verfassen. Es ist vor allem wichtig, dass die Richtlinien leicht zugänglich und gut verständlich sind. Damit Sie Ihre Mitarbeiter:innen im Homeoffice gut erreichen, empfehlen wir, die Richtlinien digital bereitzustellen und mehrere Ansprechpartner:innen anzugeben, falls Fragen aufkommen.

SCHUTZ

Angestellte im Homeoffice müssen ganz besonders auf die Sicherheit der Informationen auf all ihren Geräten achten. Wenn Sie sie entsprechend schulen, sind sie für Gefahren durch Cyberangriffe, Ransomware und Phishing-Mails sensibilisiert. Weisen Sie darauf hin, dass Kriminelle die Coronapandemie für Hacking-Kampagnen missbrauchen. Halten Sie Ihre Angestellten auch dazu an, immer einen Sichtschutz zu verwenden, damit keine Daten einsehbar sind.

DIE FOLGENDEN DOS UND DON'TS FÜR REMOTE-MITARBEITER:INNEN TRAGEN ZU EINEM HOHEN MASS AN SICHERHEIT BEI:

Do	Don't
Eine sichere WLAN-Verbindung nutzen	Öffentliche WLAN-Hotspots nutzen
Bei Nichtgebrauch Geräte sicher aufbewahren, um sie vor unbefugtem Zugriff zu schützen	Geräte und Passwörter mit anderen Personen im Haushalt oder an öffentlichen Orten teilen
Alle geschäftlichen Unterlagen im Firmennetzwerk speichern	Geschäftliche Unterlagen auf dem eigenen Rechner speichern
Unterlagen nicht zu Hause ausdrucken	Unterlagen zu Hause oder an öffentlichen Orten ausdrucken
Gedruckte Unterlagen bei der ersten Gelegenheit vernichten oder sicher aufbewahren	Gedruckte Unterlagen in privaten oder öffentlichen Papierkörben oder Altpapiertonnen entsorgen

DATENSCHUTZ

Um Ihrer Marke und Ihrem guten Ruf nicht zu schaden, müssen Sie jederzeit dafür sorgen, dass personenbezogene Daten Ihrer Kund:innen sowie geistiges Eigentum geschützt bleiben. Angestellte im Homeoffice, die mit sensiblen Aufzeichnungen zu tun haben, sollten ausführlich zu Datenschutzrichtlinien und Tools geschult werden, um Missbrauch zu vermeiden.

ZAHLEN & FAKTEN

„ES IST WICHTIG, AUCH IM HOMEOFFICE DARAN ZU ERINNERN, WELCHE BEST PRACTICES FÜR INFORMATIONS-MANAGEMENT UND SICHERHEIT GELTEN. UNTER STRESS NUTZEN DIE MENSCHEN GERN ABKÜRZUNGEN, ALSO KOMMUN-IZIEREN SIE EINFACH UND AUF DEN PUNKT."

ARLETTE WALLS, GLOBAL RECORDS & INFORMATION MANAGER BEI IRON MOUNTAIN

WARUM IRON MOUNTAIN?

- Erfolgreiche KMU-Lösungen
- Individuelle Kundenbetreuung
- Kundendienst rund um die Uhr

DE: 0800 408 0000 | WWW.IRONMOUNTAIN.COM/DE
AT: +43 (0) 2287 30 544 | WWW.IRONMOUNTAIN.COM/AT
CH: 0800 00 24 24 | WWW.IRONMOUNTAIN.COM/CH

ÜBER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) ist ein weltweit führender Anbieter von innovativen Services in den Bereichen Archivierung und Lagerung, Datacenter-Infrastruktur, Lifecycle IT Asset Management und Informationsmanagement. Auf Iron Mountain vertrauen mehr als 225.000 Unternehmen weltweit. Das 1951 gegründete Unternehmen unterstützt seine Kund:innen bei ihrer Business Transformation. Mit seinem breiten Dienstleistungsspektrum, das von der digitalen Transformation, Rechenzentren, IT Lifecycle Management über sichere Archivierung und Vernichtung bis hin zur Kunstarchivierung und -logistik reicht, hilft Iron Mountain Unternehmen, Licht ins Dunkel ihrer Daten zu bringen. So können Sie den Wert und die Intelligenz Ihrer gespeicherten digitalen und physischen Assets schnell und sicher erschließen und gleichzeitig sicherstellen, dass Sie Ihre Umweltziele erreichen. Weitere Informationen finden Sie auf unserer Unternehmenswebsite unter www.ironmountain.com/de / www.ironmountain.com/at / www.ironmountain.com/ch