IRON MOUNTAIN®

DE 3 PIJLERS VAN INFORMATIEBEVEILIGING VOOR COLLEGA'S OP AFSTAND

DE BESTE AANPAK VOOR KLEINE BEDRIJVEN

FEIT UIT DE PRAKTIJK

"KLEINERE BEDRIJVEN ZIJN KWETSBAARDER VOOR CYBERCRIMINALITEIT, OMDAT ZE, IN TEGENSTELLING TOT GROTERE BEDRIJVEN, MEESTAL MINDER IT-SPECIALISTEN HEBBEN OM EEN DATALEK TE VOORKOMEN OF EROP TE REAGEREN, EN GEEN MIDDELEN OM FLINK TE INVESTEREN IN CYBERBEVEILIGING."

ZURICH INSURANCE UK

Werknemers die op afstand werken, kunnen voor barsten in uw informatiebeveiliging zorgen. En laten hackers nu heel goed weten hoe ze die kwetsbaarheden misbruiken: cyberaanvallen, ransomware en phishingmails komen steeds vaker voor. Zulke tegenslagen bent u liever kwijt dan rijk. Met duidelijke communicatie en tips over informatiebeveiliging lukt het uw teams toch om veilig op afstand te werken. We noemen 3 cruciale aandachtspunten.

BELEID

Deel een duidelijk en beknopt schriftelijk beleid over de belangrijkste aspecten van informatiebeveiliging met al uw medewerkers. Hierin zet u ook het acceptabele gebruik van hun laptops, telefoons en andere apparaten. Denk bijvoorbeeld aan afspraken over deze onderwerpen:

- Op privécomputers of -telefoons werken
- Bedrijfsgegevens naar persoonlijke apparaten kopiëren
- Zakelijke documenten naar een privéadres mailen of naar een ander e-mailadres buiten het bedrijf
- Thuis zakelijke documenten printen
- Bedrijfsinformatie op persoonlijke USB-sticks opslaan

Het beleid hoeft niet uitgebreid te zijn. De afspraken moeten alleen duidelijk gecommuniceerd, makkelijk toegankelijk en begrijpelijk zijn. We raden aan om het beleid in een digitaal formaat aan te bieden en te zorgen voor meerdere contactpersonen, zodat collega's vragen kunnen stellen.

BESCHERMING

Collega's die op afstand werken moeten extra letten op de beveiliging van al hun apparaten. Train ze om alert te zijn op cyberaanvallen, ransomware en phishing-e-mails. Waarschuw ze dat criminelen de verspreiding van COVID-19 gebruiken om bedrijven te hacken. En vraag medewerkers om privacyschermen te gebruiken om zo hun informatie te beschermen.

UW INFORMATIE VEILIG HOUDEN? DIT ZIJN DO'S EN DON'TS VOOR WERKNEMERS OP AFSTAND:

Do	Don't
Een veilige wifiverbinding gebruiken	Openbare wifi-hotspots gebruiken
Apparaten veilig opbergen wanneer ze niet in gebruik zijn	Apparaten of wachtwoorden delen met mensen in uw huishouden of in een openbare ruimte
Bedrijfsdocumenten op het bedrijfsnetwerk opslaan	Bedrijfsdocumenten op uw privécomputer opslaan
Thuis geen bedrijfsdocumenten printen	Thuis of op een openbare plek bedrijfsdocumenten printen
Geprinte documenten meteen veilig bewaren of versnipperen	Geprinte documenten in uw eigen of een openbare prullenbak gooien

PRIVACY

Om uw reputatie niet in gevaar te brengen is het cruciaal om persoonlijke klantgegevens en intellectueel eigendom privé te houden. Collega's op afstand die gevoelige gegevens verwerken, moeten een training krijgen over uw privacybeleid en de middelen krijgen om misbruik te voorkomen.

FEIT UIT DE PRAKTIJK

"HET IS BELANGRIJK OM MEDEWERKERS DIE OP AFSTAND WERKEN TE HERINNEREN AAN DE AFSPRAKEN OVER INFORMATIEBEHEER EN -BEVEILIGING. IN STRESSVOLLE TIJDEN ZOEKEN MENSEN ALTIJD DE SNELSTE MANIER, DUS HOUD DE COMMUNICATIE EENVOUDIG EN SPECIFIEK."

ARLETTE WALLS, GLOBAL RECORDS & INFORMATION MANAGER, IRON MOUNTAIN

010 425 4444 | IRONMOUNTAIN.COM/NL

OVER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), opgericht in 1951, is wereldwijd marktleider op het gebied van opslag- en informatiebeheerdiensten. Vertrouwd door meer dan 225.000 organisaties over de hele wereld en met een netwerk van meer dan 90 miljoen vierkante meter in meer dan 1.450 vestigingen in meer dan 50 landen, bewaart en beschermt Iron Mountain miljarden informatiedragers en documenten, waaronder bedrijfskritische informatie, zeer gevoelige gegevens en culturele en historische artefacten. Iron Mountain biedt oplossingen voor onder meer veilige opslag, informatiebeheer, digitale transformatie, veilige vernietiging en datacenters, kunstopslag en logistiek, en clouddiensten. Iron Mountain helpt organisaties om kosten en risico's te verlagen, te voldoen aan wet- en regelgeving, te herstellen van calamiteiten en een meer digitale manier van werken mogelijk te maken. Bezoek www.ironmountain.nl voor meer informatie.