IRON MOUNTAIN®

FAKT Z PRAXE

„MENŠÍ PODNIKY JSOU VŮČI KYBERNETICKÉ KRIMINALITĚ ZRANITELNĚJŠÍ, PROTOŽE NA ROZDÍL OD VĚTŠÍCH FIREM JE MÉNĚ PRAVDĚPODOBNÉ, ŽE BUDOU MÍT K DISPOZICI TÝMY IT SPECIALISTŮ, KTEŘÍ BY PORUŠENÍ ZABEZPEČENÍ ÚDAJŮ ZABRÁNILI NEBO NA NĚJ REAGOVALI, NEBO ŽE BUDOU MASIVNĚ INVESTOVAT DO KYBERNETICKÉ BEZPEČNOSTI.“

ZURICH INSURANCE UK

TŘI PRAVIDLA PRO ZACHOVÁNÍ BEZPEČNOSTI INFORMACÍ A BEZPEČNOU SPRÁVU DOKUMENTŮ A DAT PŘI PRÁCI NA DÁLKU

OSVĚDČENÉ POSTUPY PRO MALÉ PODNIKY

S každým dalším zaměstnancem pracujícím na dálku se může bezpečnost informací začít otřásat v základech. Kybernetické útoky, vyděračský software a phishingové e-maily jsou na vzestupu. Hackeři dobře vědí, jak zranitelná místa zneužít a dosáhnout finančního zisku. To poslední, co vaše malá firma potřebuje, je další neúspěch při snaze o růst. Pomozte svým týmům zvládnout všechny změny v souvislosti s prací na dálku a informujte je o osvědčených postupech v oblasti bezpečnosti informací.

VNITŘNÍ PŘEDPISY

Poskytněte všem zaměstnancům jasné a stručné písemné vnitřní předpisy týkající se klíčových aspektů bezpečnosti informací. Měly by zahrnovat i popis dovoleného způsobu užívání jejich notebooků, telefonů a dalších zařízení. Jako výchozí bod pro zabezpečení práce na dálku zvažte vytvoření vnitřních předpisů týkajících se následujících bodů:

- Výkon pracovních povinností na osobních počítačích nebo telefonech
- Kopírování obchodních informací do osobních zařízení
- Odesílání obchodních dat na soukromou e-mailovou adresu nebo jakoukoli jinou e-mailovou adresu mimo firemní doménu
- Tisk pracovních dokumentů doma
- Používání soukromých flash disků k ukládání údajů o pracovní činnosti

Předpisy nemusí být dlouhé. Musí být jen jasné, snadno dostupné a srozumitelné. V případě práce na dálku doporučujeme poskytnout předpisy v digitální podobě s více kontakty pro případné dotazy.

OCHRANA

Pracovníci na dálku musí být extrémně ostražití, pokud jde o zabezpečení informací na všech jejich zařízeních. Naučte je, aby si dávali pozor na kybernetické útoky, vyděračský software a phishingové e-maily. Upozorněte je, že zločinci chtějí šíření onemocnění COVID-19 využít k hackerským útokům. Požádejte je, aby používali privátní filtry a chránili tak své informace.

ABYCHOM VÁM POMOHLI UDRŽET VYSOKOU ÚROVEŇ MONITOROVÁNÍ BEZPEČNOSTI, PŘINÁŠÍME SEZNAM DOPORUČENÝCH A ZAKÁZANÝCH ČINNOSTÍ PRO ZAMĚSTNANCE PRACUJÍCÍ NA DÁLKU:

Doporučeno	Zakázáno
Používání zabezpečeného Wi-Fi připojení	Používání veřejných hotspotů Wi-Fi
Bezpečné uložení nepoužívaných zařízení, aby byla chráněna před neoprávněným přístupem	Sdílení zařízení nebo hesel s dalšími osobami v domácnosti nebo na jakémkoli veřejném místě
Ukládání všech pracovních dokumentů do podnikové sítě	Ukládání pracovních dokumentů na osobní plochu
Netištění pracovních dokumentů doma	Tisk dokumentů doma nebo na veřejnosti
Skartace nebo bezpečné uložení všech vytištěných dokumentů při první příležitosti	Vyhození vytištěných dokumentů do odpadkových košů nebo kontejnerů na tříděný odpad doma nebo na veřejnosti

DŮVĚRNOST INFORMACÍ

Abyste zabránili poškození značky nebo pověsti, je nutné zachovat důvěrnost osobních údajů zákazníků nebo klientů a ochránit práva duševního vlastnictví. Zaměstnanci, kteří vzdáleně pracují s citlivými záznamy, by měli absolvovat formální školení o zásadách ochrany osobních údajů a nástrojích, které zabrání jejich zneužití.

FAKT Z PRAXE

„ZAMĚSTNANCŮM PRACUJÍCÍM NA DÁLKU JE DŮLEŽITÉ PŘIPOMÍNAT OSVĚDČENÉ POSTUPY PRO SPRÁVU A BEZPEČNOST INFORMACÍ. VE STRESOVÝCH SITUACÍCH SI LIDÉ CHTĚJÍ PRÁCI USNADNIT, KOMUNIKUJTE S NIMI PROTO SROZUMITELNĚ A VĚCNĚ.“

ARLETTE WALLS, GLOBÁLNÍ VEDOUCÍ SPRÁVY DOKUMENTŮ A INFORMACÍ, SPOLEČNOST IRON MOUNTAIN

PROČ ZROVNA SPOLEČNOST IRON MOUNTAIN?

- Nejprodávanější řešení pro malé a střední podniky
- Obchodní zástupce jen pro vás
- Nonstop zákaznický servis

+420 233 900 638 | IRONMOUNTAIN.CZ

O SPOLEČNOSTI IRON MOUNTAIN

Společnost Iron Mountain Incorporated (NYSE: IRM), založená v roce 1951, je celosvětovým lídrem v oblasti služeb pro ukládání a správu informací. Společnost Iron Mountain, které důvěřuje více než 220 000 organizací po celém světě a která disponuje sítí nemovitostí o rozloze více než 85 milionů čtverečních stop ve více než 1 400 zařízeních ve více než 50 zemích, ukládá a chrání miliardy informačních aktiv, včetně kritických obchodních informací, vysoce citlivých dat a kulturních a historických artefaktů. Společnost Iron Mountain poskytuje řešení, která zahrnují bezpečné ukládání, správu informací, digitální transformaci a bezpečnou likvidaci, ale také datová centra, úložiště artefaktů a jejich logistiku i cloudové služby, a pomáhá tak organizacím snižovat náklady a rizika, dodržovat předpisy, zotavovat se z katastrof a umožnit digitální způsob práce. Další informace naleznete na adrese www.ironmountain.com.