IRON MOUNTAIN®

3P DLA BEZPIECZEŃSTWA INFORMACJI I ZARZĄDZANIA DOKUMENTACJĄ W MODELU PRACY ZDALNEJ

NAJLEPSZE PRAKTYKI DLA MAŁYCH PRZEDSIĘBIORSTW

INFORMACJA BRANŻOWA

"MNIEJSZE FIRMY SĄ BARDZIEJ NARAŻONE NA CYBERPRZESTĘPCZOŚĆ, PONIEWAŻ W PRZECIWIEŃSTWIE DO WIĘKSZYCH ORGANIZACJI, RZADZIEJ DYSPONUJĄ ZESPOŁAMI SPECJALISTÓW, KTÓRZY MOGLIBY ZAPOBIEC NARUSZENIU DANYCH LUB ZAREAGOWAĆ NA NIE, A TAKŻE MNIEJSZYMI MOŻLIWOŚCIAMI POZWALAJĄCYMI NA ZNACZNE INWESTYCJE W CYBERBEZ-PIECZEŃSTWO".

ZURICH INSURANCE UK

W modelu pracy zdalnej lub hybrydowej, problemy z bezpieczeństwem danych mogą się zwiększać. Cyberprzestępcy wiedzą, jak wykorzystywać luki w zabezpieczeniach, aby osiągnąć korzyści finansowe dzięki cyberatakom, oprogramowaniu ransomware i phishing. Ostatnią rzeczą, jakiej potrzebuje Twoja firma, to dodatkowe trudności w prowadzeniu biznesu. Pomóż sobie i swojej organizacji ze zmianami związanymi z praca zdalną poprzez dzielenie się i komunikowanie najlepszych praktyk w zakresie bezpieczeństwa danych.

POLICIES - POLITYKA

Zapewnij wszystkim pracownikom jasne, zwięzłe i spisane zasady dotyczące kluczowych aspektów bezpieczeństwa danych. Powinny one obejmować również odpowiedzialne korzystanie z laptopów, telefonów i innych urządzeń. Jako punkt wyjścia do zapewnienia bezpieczeństwa podczas pracy zdalnej, rozważ stworzenie zasad firmowych w następujących obszarach:

- Realizacja zawodowych obowiązków na prywatnym komputerze lub telefonie
- Kopiowanie dokumentacji biznesowej na urządzenia prywatne
- Wysyłanie dokumentów służbowych na prywatną skrzynkę pocztową lub inną poza domeną firmy
- Drukowanie dokumentów służbowych w domu
- Używanie prywatnych dysków przenośnych do przechowywania danych biznesowych

Opracowana polityka nie musi być długa. Zasady muszą być łatwo dostępne i zrozumiałe, a także jasno zakomunikowane. W przypadku pracy zdalnej rekomendujemy udostępnienie zaleceń w formie cyfrowej z uwzględnieniem danych kontaktowych w razie ewentualnych pytań.

PROTECTION - OCHRONA

Pracownicy zdalni muszą zachować szczególną czujność w kwestii bezpieczeństwa danych na wszystkich swoich urządzeniach. Powinni być świadomi zagrożeń związanych z cyberatakami, oprogramowaniem ransomware i e-mailami phishingowymi. Ostrzeż ich, że przestępcy po pandemii COVID-19 nasilili swoje ataki hakerskie. Zachęcaj pracowników do korzystania z tzw. privacy screens, aby chronić swoje dane.

OTO LISTA NASZYCH WSKAZÓWEK, ABY POMÓC W UTRZYMANIU WYSOKIEGO POZIOMU BEZPIECZEŃSTWA:

Zalecamy:	Odradzamy:
Korzystanie z bezpiecznego połączenia Wi-Fi	Korzystanie z publicznych hot spotów Wi-Fi
Bezpieczne przechowywanie urządzeń, gdy nie są używane, aby uchronić je przed nieautoryzowanym dostępem	Udostępnianie urządzenia lub hasła osobom w Twoim domu lub dowolnej przestrzeni publicznej
Zapisywanie wszystkich dokumentów służbowych w swojej sieci firmowej	Zapisywanie dokumentów biznesowych na pulpicie
Unikania drukowania dokumentów w domu	Drukowanie dokumentów z lokalizacji domowych lub publicznych
Niszczenie lub bezpieczne przechowywanie wydrukowanych dokumentów	Wyrzucanie wydrukowanych dokumentów do osobistych lub publicznych pojemników na śmieci i do recyklingu

PRIVACY - PRYWATNOŚĆ

Aby zapobiec zagrożeniom dla marki i reputacji, należy koniecznie zadbać o prywatność danych osobowych i własność intelektualną Klientów. Pracownicy zdalni, którzy mają do czynienia z poufnymi danymi, powinni przejść formalne szkolenie w zakresie polityki prywatności i narzędzi zapobiegających nadużyciom.

INFORMACJA BRANŻOWA

„WAŻNE JEST, ABY PRZYPOMINAĆ OSOBOM PRACUJĄCYM ZDALNIE O NAJLEPSZYCH PRAKTYKACH W ZAKRESIE ZARZĄDZANIA I BEZPIECZEŃSTWA DANYCH. W STRESUJĄCYCH CZASACH SZUKAMY NIESKOMPLIKOWANYCH ROZWIĄZAŃ, DLATEGO KOMUNIKACJA POWINNA BYĆ PROSTA I KONKRETNA ".

ARLETTE WALLS, GLOBAL RECORDS & INFORMATION MANAGER, IRON MOUNTAIN

DLACZEGO IRON MOUNTAIN?

- Najlepiej sprzedające się rozwiązania SMB
- Dedykowani przedstawiciele skoncentrowani na danym Kliencie
- Obsługa Klienta 24/7

801800802 | IRONMOUNTAIN.PL

O IRON MOUNTAIN

Firma Iron Mountain Incorporated (NYSE: IRM), założona w 1951 roku, jest światowym liderem w dziedzinie usług zarządzania pamięcią masową i danymi. Firma Iron Mountain, której zaufało ponad 220 000 organizacji na całym świecie, dysponuje siecią nieruchomości o powierzchni prawie 8 milionów metrów kwadratowych, w ponad 1400 obiektach, w przeszło 50 krajach, przechowuje i chroni miliardy zasobów danych, w tym krytyczne dane biznesowe oraz artefakty kulturowe i historyczne. Firma dostarcza rozwiązania obejmujące bezpieczne przechowywanie, zarządzanie danymi, transformację cyfrową, bezpieczne niszczenie, a także centra danych, przechowywanie i logistykę dzieł sztuki oraz usługi w chmurze. Iron Mountain pomaga organizacjom obniżyć koszty i ryzyko, zachować zgodność z przepisami (compliance), odzyskać sprawność po awarii i wprowadzić bardziej cyfrowy sposób pracy. Więcej informacji można znaleźć na stronie www.ironmountain.com.