INFORMATIEBLAD

Checklist Databeveiliging voor de onboarding van nieuwe medewerkers

Heeft u onlangs nieuwe medewerkers bij uw organisatie verwelkomd? Zo ja, dan is het van cruciaal belang om vanaf het begin van hun dienstverband aandacht te besteden aan informatiebeveiliging. Fouten of onachtzaamheid van werknemers zijn belangrijke oorzaken van datalekken; een gedegen oriëntatie kan een grote bijdrage leveren aan het verminderen van risico's. Managers en leiderschapsteams kunnen de algehele beveiligingscultuur van een bedrijf bevorderen door strategieën uit te stippelen en ervoor te zorgen dat werknemers zich bewust zijn van hun eigen rol bij het veilig bewaren van gegevens.

WIST U DAT?

Bijna de helft (49%) van de ondervraagde zakelijke leiders geeft aan dat een gebrek aan inzicht in de bedreigingen en risico's voor de organisatie de grootste drempel is voor werknemers om het beleid inzake informatiebeveiliging na te leven.1

Hier is een checklist met onderwerpen inzake informatiebeveiliging, zowel elektronisch als op papier, om door te nemen tijdens de onboarding.

☐ **Regelgeving inzake informatiebeveiliging.**
Datalekken kunnen leiden tot boetes en de reputatie van een bedrijf schaden. Wanneer ervoor wordt gezorgd dat medewerkers vertrouwd zijn met de belangrijkste aspecten van relevante databeveiligingswetten, kan dat waardevolle context bieden voor belangrijke discussies over databeveiliging.

☐ **Incidentenrapportage.**
Ondanks de welgemeende inspanningen van een bedrijf kan er toch een datalek plaatsvinden. Werknemers moeten weten wanneer en hoe ze deze gebeurtenissen moeten melden. Ook moeten ze de garantie hebben dat ze niet zullen worden bestraft als ze van zich laten horen. Zorg ervoor dat u uw nieuwe medewerkers direct op de hoogte brengt van percepties en verwachtingen over incidentenrapportage, zodat zowel nieuwe als huidige werknemers begrijpen wat ze moeten doen als er zich een datalek voordoet.

☐ **Afdrukprocedures.**
Veelvoorkomende fouten, zoals het onbedoeld achterlaten van vertrouwelijke documenten in de buurt van bijvoorbeeld printers, verhogen het risico op datalekken. Het is cruciaal om het belang van het snel ophalen van gedrukt materiaal uit de printer te benadrukken, omdat dit de kans op diefstal van informatie kan verkleinen. Als uw bedrijf de printers beschermt middels een wachtwoord, vergeet dan niet om nieuwe werknemers te laten zien hoe ze toegang kunnen krijgen tot deze wachtwoorden en hoe de wachtwoorden veilig kunnen worden bewaard.

☐ **Beleid voor elektronische apparaten.**
Persoonlijke mobiele telefoons en tablets op de werkplek zijn wellicht handig, maar ze kunnen ook een verhoogd risico vormen op beveiligingsincidenten. Zorg er bij de onboarding van nieuwe medewerkers voor dat ze begrijpen hoe ze hun apparaten te allen tijde kunnen beschermen.

Bron: 1. Shred-it Gegevensbeschermingsrapport 2021.

Wij beschermen wat van belang is

Shred-it®
Een Stericycle®-Oplossing

CHECKLIST DATABEVEILIGING VOOR DE ONBOARDING VAN NIEUWE MEDEWERKERS

☐ **Houd bureaus opgeruimd.**
Als uw bedrijf een officieel clean desk-beleid heeft, doet u er verstandig aan om uit te leggen wat dat precies betekent voor nieuwe medewerkers. Een dergelijk beleid vereist doorgaans dat werknemers alle papieren met vertrouwelijke informatie achter slot en grendel bewaren; niet-essentiële documenten van hun bureau verwijderen; en het vergrendelscherm van hun computer inschakelen voordat ze voor langere tijd of aan het einde van de dag vertrekken.

Klik hier voor een clean desk-beleid.

☐ **Grondige documentvernietiging.**
Nieuwe medewerkers dienen te begrijpen wat ze moeten doen met bedrijfsdocumenten die niet langer bewaard moeten worden. Door nieuwe medewerkers te informeren over uw bestaande procedures voor documentvernietiging, kunnen risico's en problemen op het gebied van databescherming worden beperkt. Het is misschien het beste om een Shred-it All-beleid in te voeren en medewerkers te adviseren om alle overbodige documenten in een beveiligde console te doen om veilige vernietiging te garanderen. Zo hoeven zij zich niet af te vragen wat vertrouwelijk is en wat niet. Dit versterkt niet alleen de beveiliging van vertrouwelijke documenten; het is ook een best practice op het gebied van duurzaamheid, aangezien al het versnipperde papier gerecycled wordt.

Klik hier voor een Shred-it All-beleid.

☐ **Wachtwoordprotocollen.**
Wachtwoorden zijn een essentiële veiligheidsmaatregel. Nieuwe werknemers moeten volledig op de hoogte worden gebracht van het wachtwoordbeleid van uw organisatie en weten wat het betekent om sterke wachtwoorden te maken. Een goed wachtwoord bevat hoofdletters en kleine letters, cijfers en symbolen, en moet regelmatig worden bijgewerkt. Als uw bedrijf een programma voor verplichte wachtwoordupdates heeft, zorg er dan voor dat nieuwe werknemers daarvan op de hoogte zijn

☐ **Voorzorgsmaatregelen voor e-mail.**
Veel incidenten op het gebied van cyberbeveiliging vinden plaats doordat werknemers op onveilige e-mails klikken. Nieuwe medewerkers dienen te worden getraind in het herkennen van verdachte e-mails, zoals malware, phishing-trucs en ransomware, zodat ze schadelijke situaties leren te vermijden.

Ga voor meer best practices omtrent informatiebeveiliging naar shredit.nl of bel 0800 0114

Wij beschermen wat van belang is

Shred-it®
Een Stericycle®-Oplossing