

Is uw kantoor klaar voor de terugkeer van de werknemers?

Dedrijven kunnen terug naar het kantoor - wat de langverwachte terugkeer naar persoonlijke samenwerking en kameraadschap terugbrengt! Maar deze terugkeer brengt natuurlijk ook extra risico's voor gegevensbeveiliging met zich mee.

Zorg voor een veilige terugkeer naar kantoor met Shred-it.

De hieronder beschreven stappen kunnen uw bedrijf en werknemers helpen bij een veilige terugkeer naar het kantoor.

» Moedig personeel aan om documenten terug te brengen



Thuiswerken is sinds het begin van COVID-19 een pijler geweest van het leven van velen. In deze tijd hebben werknemers waarschijnlijk belangrijke documenten mee naar huis genomen of hebben ze mogelijk vertrouwelijke informatie uitgeprint. Vraag alle werknemers om documenten die niet langer nodig zijn veilig naar kantoor terug te brengen, zodat u ervoor kunt zorgen dat ze worden verzameld en veilig worden vernietigd om de risico's van een datalek te helpen voorkomen.

» Ruim op om het kantoor klaar te maken



Voordat de werknemers terugkeren, moet u zich voorbereiden en documenten opruimen. Moeten bureaus worden leeggemaakt? Heeft u opbergkasten die al enige tijd niet zijn georganiseerd? Het boeken van een eenmalige vernietigings-service is de perfecte manier om het kantoor op te ruimen en mogelijke risico's van een datalek te verkleinen.

» Train werknemers



Als werknemers nu terugkeren naar de werkplek, is dat het perfecte moment om ze (opnieuw) te trainen in de best practices op het gebied van veilig beheer en vernietiging van informatie. Neem de tijd om ervoor te zorgen dat alle medewerkers begrijpen wat vertrouwelijke informatie is en wat de gevolgen zijn voor het bedrijf als zich een datalek voordoet.

» Voer een risicobeoordeling voor informatiebeveiliging uit



Bewustwording is de eerste stap naar het aanpakken en verbeteren van best practices op het gebied van informatiebeveiliging. Loopt uw bedrijf risico op een datalek? Het uitvoeren van een eigen beoordeling van de beveiliging van kantoordocumenten, het bewaren van documenten en het bewustzijn en training van werknemers kan helpen bij het identificeren van gebieden waar een lek kan plaatsvinden.

FACT SHEET

» Voer een “leeg bureau”-beleid in



De introductie van een “leeg bureau”-beleid zorgt ervoor dat het personeel alle ongewenste, gevoelige informatie verwijdert en beveiligt. Ook helpt het de risico's op een datalek te verkleinen. Moedig werknemers aan om hun bureau te ontdoen van alle papieren, met name die met gevoelige informatie zoals persoonlijke gegevens, rekeningnummers en commercieel gevoelige gegevens, plus alle andere niet-essentiële documenten en notities (inclusief de alomtegenwoordige post-its). Zorg er ook voor dat verwijderbare media, documenten en notitieboekjes aan het eind van de dag en elke keer dat medewerkers hun bureau verlaten, worden opgeborgen.

» Introduceer een beleid voor documentbeheer



Niet juist opgeborgen en verkeerd behandelde papieren documenten zijn de oorzaak van veel spraakmakende datalekken. Door een beleid voor documentbeheer te implementeren, krijgt u een volledig beeld van de documenten die uw bedrijf in- en uitgaan, welke informatie ze bevatten, wie er toegang toe heeft en hoelang ze moeten worden bewaard.

» Als u twijfelt, vernietig dan alles



De werkplek ligt vol met vertrouwelijke informatie, maar het kan tijdrovend en verwarrend zijn om te bepalen of een document al dan niet vertrouwelijk is. Verminder dus de belasting voor de werknemers en help het risico op een datalek te verkleinen met een “vernietig alles”-beleid – hierbij worden alle zakelijke documenten in een veilige, vergrendelde console geplaatst en op een veilige manier vernietigd zodra ze niet meer nodig zijn.



Neem voor uw gemoedsrust vandaag nog contact op met Shred-it® 0800 0114 | shredit.nl

Shred-it® is een oplossing van Stericycle. © 2021 Shred-it® International. Alle rechten voorbehouden.

 **Shred-it®**