

# Beperk de risico's van werken op afstand

Een betere balans tussen werk en privé, hogere productiviteit en besparing van tijd en geld zijn slechts enkele redenen waarom steeds meer bedrijven open staan voor thuiswerken. Maar deze verandering in manier van werken gaat gepaard met een hoger risico op datalekken.

Deze eenvoudige maatregelen geven u gemoedsrust, bescherming en productievere medewerkers.

## 1. Stel richtlijnen op

Zorg voor een aantal heldere richtlijnen voor werken op afstand alsmede de beveiligde vernietiging van vertrouwelijke informatie die we produceren tijdens het werken op een andere locatie.

## 2. Train uw werknemers

Train werknemers in beste praktijken voor veilig beheer en veilige vernietiging van informatie. Zorg ervoor dat alle werknemers goed begrijpen wat vertrouwelijke informatie inhoudt, en wat de gevolgen zijn voor het bedrijf als een datalek plaatsvindt.

## 3. Beperk toegang tot vertrouwelijke gegevens

Controleer of de werknemers op een need-to-know-basis de juiste toegang tot de juiste bestanden hebben.

## 4. Beveilig digitale apparatuur

Zorg ervoor dat alle bestanden, laptops en internetverbindingen beveiligd zijn met veilige wachtwoorden en dat de beveiligingsinstellingen en firewalls zijn geactiveerd.

## 5. Beveiligd werken op afstand

Stimuleer werknemers die regelmatig vanuit huis werken om een afsluitbare opslagplek te plaatsen om belangrijke en vertrouwelijke documenten veilig te bewaren.

## 6. Beveilig papieren documenten

Zorg ervoor dat werknemers die op een andere locatie werken papieren documenten mee terugnemen naar kantoor, voor veilige opslag of veilige vernietiging.

## 7. Voer een Shred-it-All beleid in

Voer een shred-it-all-beleid (alles versnipperen) in om ervoor te zorgen dat alle documenten of vertrouwelijke informatie veilig worden vernietigd, om te helpen het risico van een datalek te voorkomen.

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

