

# Richtlijnen voor de beheerder

Een kwart van alle inbreuken op informatiebeveiliging wordt veroorzaakt binnen een organisatie door nalatigheid van medewerkers<sup>1</sup>.

Vertrouwelijke informatie beveiligen beschermt uw werkomgeving en iedereen die er deel van uitmaakt. Een van de eerste stappen voor een beschermde werkomgeving is het invoeren van een *Documentbeheerbeleid*, zodat alle medewerkers weten wat ze moeten doen met ALLE bedrijfsdocumenten, zowel op papier als elektronisch. Dan hoeft niemand ernaar te raden!

## 1. Pas het bijgevoegde beleidssjabloon aan voor uw bedrijf.

Denk na over elk stadium van de informatie/documentcyclus om volledig te begrijpen hoe informatie wordt geproduceerd, gedeeld en opgeslagen in uw organisatie; van creatie en opslag tot vernietiging van documenten. U kunt navraag doen bij diverse medewerkers en afdelingen voor een holistisch inzicht, want, afhankelijk van de bedrijfssector/afdeling, zijn er veel specifieke regels en voorschriften met betrekking tot het bewaren, verspreiden, opslaan en vernietigen van documenten.

## 2. Win juridisch advies in.

Het kan nooit kwaad om advies in te winnen van een juridische expert voor complexe nalevingskwesaties binnen uw organisatie om te verzekeren dat uw beleid volledig en grondig is. En zorg ervoor dat u regelmatige evaluaties inplant, want de regels kunnen soms veranderen.

## 3. Train uw medewerkers.

Zodra u uw *Documentbeheerbeleid* hebt opgesteld en dit is goedgekeurd door de belangrijkste stakeholders binnen uw organisatie, is het tijd om uw personeel te trainen en op te leiden. U kunt beleidsambassadeurs op afdelingsniveaus benoemen om trainingssessies te houden en zo meer dialoog en begrip te kweken omtrent het nieuwe beleid. Dit geeft iedereen een meer persoonlijke en interactieve mogelijkheid om te begrijpen waarom het beleid zowel belangrijk als relevant is voor alle medewerkers binnen de organisatie.

## 4. Plaats herinneringen op plekken op kantoor waar papier wordt geproduceerd.

We hebben een poster voor u bijgevoegd die u op kantoor kunt verspreiden. U kunt deze ophangen op uw werkplek en in alle afdelingen om medewerkers te herinneren aan het belang van een consistente naleving van het beleid. Gevoelige informatie moet te allen tijde worden beschermd en afgesloten worden opgeslagen of op veilige wijze worden vernietigd.

## 5. Voer periodieke controles uit.

We bevelen aan dat u uw beleidsambassadeurs voor elke afdeling verantwoordelijk maakt voor periodieke controles. Een snelle audit van tijd tot tijd verzekert dat uw medewerkers uw nieuwe beleid volgen, versterkt het belang ervan, frist geheugens op en is een geweldige manier om iedereen er bij te betrekken.

---

<sup>1</sup> Onderzoek naar kosten van gegevensinbreuken, 2015: Wereldwijde analyse door het Ponemon Institute

## **6. Organiseer indien nodig nieuwe trainingen.**

Een *Documentbeheerbeleid* kan complex zijn om in te voeren. Medewerkers kunnen het moeilijk vinden om hun gedrag te veranderen en nieuwe procedures inzake informatieopslag en -vernietiging over te nemen. Om te verzekeren dat uw beleid met succes wordt ingevoerd, moet u beleidsinformatie doorlopend bespreken, aanpassen en verspreiden.

## **6. Valueer beleid in overeenstemming met nieuwe wetgeving.**

In deze steeds veranderende wereld moeten organisaties op de hoogte blijven van nieuwe wetgeving inzake gegevensbescherming en privacy. U moet uw *Documentbeheerbeleid* doorlopend evalueren, zodat het actueel is en in overeenstemming met gegevensbeschermings- en andere privacywetgeving.