mint
ADVOCATEN

Checklist informatieveiligheid

Om te voorkomen dat de alsmaar toenemende cybercriminaliteit de overhand neemt, moet men de nodige aandacht schenken aan informatieveiligheid.

In dat kader hebben wij een overzicht gemaakt met 6 praktische leidraden om de beveiliging van de informatie binnen uw onderneming te verbeteren in de dagdagelijkse praktijk.

Informatieveiligheidsbeleid- en plan

In dit beleid streeft u ernaar een aantal doelstellingen te behalen om de veiligheid van uw organisatie naar een hoger niveau te tillen.

Wees u ervan bewust dat de beveiligingsmaatregelen worden genomen afhankelijk van de vastgestelde risico's. Ook hier zal de ISO-normering gelden als uitgangspunt waarbij er een onderscheid wordt gemaakt op basis van organisatie, techniek en beleid.

Beleid in-en uitdiensttreding medewerkers

Als u grip wilt op wie toegang heeft tot onder andere uw systemen, applicaties,... kan u een in- en uitdiensttredingsbeleid opstellen.

Zo dient u bijvoorbeeld de mailbox te blokkeren uiterlijk op het tijdstip van uitdiensttreding. Deze blokkering moet gebeuren nadat de werknemer daarvan vooraf is verwittigd en een automatisch bericht werd ingesteld. Dit bericht mag worden gebruikt gedurende een redelijke periode van één maand, eventueel te verlengen tot drie maanden.

ICT-code

Volledigheidshalve vat u al deze informatieveiligheidsregels nog even samen in een ICT-code, als bijlage bij het arbeidsreglement.

Dit kan worden beschouwd als een soort ‘morele’ gedragscode hoe er zo optimaal mogelijk wordt omgesprongen met ICT-materiaal.

Telewerkbeleid

Na de COVID-pandemie zijn we massaler beginnen telewerken.

De grootste risico’s op incidenten en datalekken doen zich namelijk voor in een thuiswerkomgeving, door een slecht beveiligd netwerk.

Beleid datalekken en incidenten

Elke werknemer moet op de hoogte zijn van zijn of haar verantwoordelijkheid. Indien er zich een incident of datalek voordoet, dan moet het management van de organisatie hier zo snel mogelijk over worden ingelicht.

Een onderneming heeft namelijk de plicht om binnen 72u aan de toezichthoudende autoriteiten een datalek te melden om latere sancties te vermijden.

Wachtwoordbeleid

Hackers kennen alle trucjes en ezelbruggetjes die we gebruiken wanneer we een wachtwoord verzinnen.

Neem daarom de tijd om een sterk wachtwoord in te stellen aan de hand van een duidelijk wachtwoordbeleid binnen uw onderneming. Dit is namelijk een belangrijke oorzaak voor het ontstaan van datalekken.

Mint Advocaten helpt u graag op weg!

Samengevat, kan informatieveiligheid worden omschreven als:

“maatregelen die ervoor zorgen dat de betrouwbaarheid van informatie behouden blijft, en incidenten worden vermeden.”

Wij staan u dan ook graag bij om deze documenten op te maken en verdere advies op uw maat te verlenen.

mint
ADVOCATEN

09 391 79 18

karel@mintadvocaten.be

/company/mint-advocaten

/mintadvocaten