meijers
makelaars in assurantiën

De Meijers informatiebeveiligingsmaatregelen

Beschikbaarheid, integriteit en vertrouwelijkheid van informatie(voorzieningen) vinden we belangrijk binnen Meijers. Daarom nemen we maatregelen op het gebied van informatiebeveiliging.

Beheer van bedrijfsmiddelen

Bedrijfsmiddelen die toegang geven tot bedrijfsgevoelige informatie registreren we. En we benoemen een gebruiker. Ook zorgen we voor onderhoud en implementatie van bijbehorende beveiligingsmaatregelen.

Business Continuity Management & Disaster Recovery

Voor het omgaan met grote calamiteiten die de bedrijfsvoering ernstig kunnen verstoren, hebben we een BCP & DR plan. Het bijwerken en testen van dit plan vindt periodiek plaats om de werking te garanderen.

Dataopslag

Klantdata slaan we op in datacenters binnen Nederland. In specifieke gevallen staan deze datacenters in andere landen binnen de Europese Unie.

Personeel en inhuur

Nieuw personeel en derde partijen screenen we. Zij tekenen ook een geheimhoudingsverklaring. Informatiebeveiligingsverantwoordelijkheden leggen we contractueel vast.

Logische toegangsbeveiliging

Maatregelen zorgen dat de authenticatie en autorisatie van gebruikers en beheerders op een juiste en volledige manier plaatsvindt. In het authenticatie- en wachtwoordbeleid is minimale wachtwoordcomplexiteit, lengte- en wijzigingsfrequentie opgenomen.

Incidentmanagement en datalekken

Beveiligingsincidenten leggen we vast en volgen we op om bedrijfsschade te beperken en herhaling te voorkomen.

Fysieke beveiliging

Alleen geautoriseerde personen hebben toegang tot de Meijers omgevingen. Gasten worden altijd door een Meijers medewerker begeleid. Bedrijfsgevoelige informatie laat niemand onbeheerd achter. Voor werkplekken geldt een 'clean desk' en 'clear screen' procedure.

Informatiebeveiliging en leveranciers

Van leveranciers verwachten we dat zij hun beveiliging, voor zover deze Meijers informatie en/of informatiebeveiliging raakt, minimaal op hetzelfde niveau hebben als Meijers zelf. Leveranciers die belangrijk zijn voor onze informatiebeveiliging controleren we op naleving hiervan.

Operationeel ICT management

Om betrouwbare informatieverwerking te garanderen, zijn er belangrijke beveiligingsmaatregelen. Bijvoorbeeld beleid over updates en back-ups, bescherming tegen malware, omgang met mobiele gegevensdragers en netwerkbeveiliging.

Van Heuven Goedhartlaan 935 | 1181 LD Amstelveen | Postbus 707 | 1180 AS Amstelveen | (020) 642 0524 | info@meijers.nl | meijers.nl