

Basis op Orde

De information protection baseline voor Microsoft 365



Cloud Security Care

Binnen elke organisatie is informatie één van de meest belangrijke bedrijfsmiddelen. Informatie kan bijvoorbeeld om medische redenen privacygevoelig zijn, of wellicht is het intellectueel eigendom of betreft het concurrentiegevoelige informatie. Als organisatie bent u verantwoordelijk om te zorgen dat wordt voldaan aan de BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid)-classificatie. De basis hiervoor is aanwezig binnen wet- en regelgeving en normeringen als de AVG en ISO27001.

Informatiebeveiliging met Microsoft 365

Het is zaak om werk te maken van informatiebeveiliging vanuit de bron: de gevoeligheid van de informatie zelf. Gebaseerd op deze gevoeligheid worden de juiste beveiligingsmaatregelen genomen. Deze maatregelen zorgen ervoor dat de vertrouwelijkheid van de informatie wordt gewaarborgd, ongeacht waar de informatie is opgeslagen, wordt geraadpleegd of met wie deze wordt gedeeld. Microsoft Information Protection biedt deze mogelijkheden.

Microsoft Information Protection is de oplossing voor het detecteren, classificeren en beschermen van informatie, zowel binnen Microsoft 365 als andere cloud-toepassingen en is daarmee zeer breed inzetbaar. Documenten en e-mail berichten worden voorzien van een zogenaamd classificatielabel. Dit label (bijvoorbeeld 'privacygevoelig') biedt hierbij zowel beschermingsmaatregelen als visuele markeringen (bijvoorbeeld een watermerk).

Doelgroep Basis op Orde traject

- Chief Compliance Officer (CCO)
- Chief Risk Officer (CRO)
- Chief Information Security Officer (CISO)
- Privacy Officer (PO)
- Legal Department
- IT Management

Basis op Orde traject

Het Basis op Orde traject is opgebouwd uit de volgende vier componenten:



Tijdens de **awareness workshop (2 uur)** worden de functionaliteit, het beheer en het licentiemodel van Microsoft Information Protection gepresenteerd en besproken.



Tijdens de **requirements workshop (4 uur)** worden de requirements opgesteld die de input vormen voor het prototype ontwerp.



Tijdens de **prototype ontwerpfase (40 uur)** worden de scope en functies op basis van de eerder vastgelegde requirements verder gedetailleerd. Dit bevat onder meer het aantal deelnemers aan de proof of concept, het ontwerp voor de gevoeligheidslabels, het uitrollen van de client (indien nodig) en de beveiligingsregels bij datalekken.



Deelnemers aan de proof of concept worden tijdens de **kick start (8 uur)** geïnformeerd en geïnstrueerd over het verdere verloop van het project. De kick start bestaat uit een awareness- en inspiratiesessie en de realisatie en de presentatie van een ondersteunende website.



Tijdens de uiteindelijke **proof of concept (1-3 maanden)** worden de functies toegepast. Middels enquêtes worden de deelnemers gevraagd naar hun ervaringen. Tussentijdse evaluatiesessies worden gebruikt om vragen te beantwoorden en eventuele problemen te verhelpen. Na afloop van de proof of concept volgt een evaluatie waarbij de vervolgstappen worden bepaald.

Meer weten of direct aan de slag?

Wilt u meer weten over wat het Basis op Orde traject uw organisatie kan opleveren of een offerte op maat? Neem dan contact op met uw Motion10 Accountmanager of [Ron Witjes](#), Modern Work & Security Lead bij Motion10