Toelichting Handreiking Mobile Device Management

Waarom Mobile Device Management?

Gegevensverwerkingen vinden veelal digitaal plaats via mobiele apparaten zoals smartphones, tablets en laptops (hierna: devices). Tegelijkertijd verandert het concept van werken waarbij steeds meer tijd- en plaatsonafhankelijk, en dus ook thuis, gewerkt wordt. Medewerkers krijgen daardoor meer mogelijkheden om informatie in te zien of te verwerken op afstand. Dit brengt risico's met zich mee, zoals onder meer malwarebesmettingen van devices, inzage van persoonsgegevens door onbevoegden, maar ook het kwijtraken van devices. Dit alles met mogelijke datalekken als gevolg. Om de potentiële risico's in goede banen te leiden en datalekken te voorkomen, is het nodig om van te voren na te denken over mobile device management en welke oplossingen er allemaal zijn.

Voor wie is deze Handreiking Mobile Device Management bedoeld?

Deze handreiking is bedoeld voor de IT-coördinatoren of - beheerders en andere personen die verantwoordelijk zijn voor het opstellen van beleidsdocumenten en gedragsregels (eerste lijn) die over informatiebeveiliging gaan. De beleidsverantwoordelijke binnen de organisatie dient aantoonbaar goedkeuring te verlenen. Betrek hierbij ook de medezeggenschap (OR/GMR) door het OR/(G)MR met deze aanvulling op het algemene informatie- en beveiligingsbeleid in te laten stemmen. Een Functionaris Gegevensbescherming (tweede lijn) kan bij dit proces adviseren en het Mobile Device Management onderdeel maken van het toezichtskader.

Deze handreiking is opgesteld aan de hand van de Handreiking van de Informatiebeveiligingsdienst voor gemeenten en het Centrum Informatiebeveiliging en Privacybescherming (CIP).

Hoe moet je deze Handreiking Mobile Device Management gebruiken?

Deze handreiking is bedoeld ter informatie en als richtlijn bij het opstellen van een eigen beleid met betrekking tot het gebruik van alle devices, als aanvulling op het algemene informatiebeveiligingsbeleid. Dit is geschreven om informatiebeveiligingsmaatregelen met betrekking tot mobile device management te duiden en scherper de mogelijkheden op dit gebied weer te geven. Als voorbeeld is er een "Bring your own device" beleid bijgevoegd, welke gedeeltelijk gebruiksklaar is, maar organisatie-neutraal geformuleerd. In geel is in het voorbeeld gemarkeerd waar nog invulling of toevoeging vereist is om het voor de eigen organisatie te specificeren.

Lumen Group kan ondersteunen bij het implementeren van dit Mobile Device Management. Neem vrijblijvend contact op via fg@lumengroup.nl of 030 889 65 75 om de mogelijkheden te bespreken.

Versie 1.0 – 31-10-2022