

Begeleidende tekst uitrol MDM (Mobile Device Management) voor raads- en commissieleden bij gemeente Tiel

Waarom MDM?

Alle mobiele apparaten van de gemeente Tiel, waaronder de door raadsleden gebruikte iPad, moeten voorzien worden van MDM (Mobile Device Management). Zo ook die van de raads- en commissieleden. Dit betreft o.a.

- De in gebruik zijnde iPads.
- (In een later stadium) Privé telefoons indien deze ook zakelijk gebruikt worden (bijvoorbeeld voor het ophalen van mail, adresboek en agenda).

Met MDM wordt de data op de telefoon en tablet beter beschermd. Deze maatregel is een onderdeel van de (verplichte) Baseline Informatieveiligheid Overheid (BIO).

Een veilige werkplek

Met de uitrol van MDM 'splitsen' we het mobiele apparaat (telefoon, iPad) als het ware in een zakelijk deel en een privé deel. Hierdoor zorgen we ervoor dat zakelijke mail of bestanden uitsluitend binnen dit – beveiligde – zakelijke deel zichtbaar en gebruikt kunnen worden. MDM zorgt ervoor dat, ingeval van verlies of diefstal van een mobiel apparaat (telefoon, tablet), de zakelijke data op afstand (door de helpdesk) gewist kan worden en/of het apparaat vergrendeld. Hierdoor kan deze data niet in handen van derden vallen.

Voor het privé gedeelte verandert er in feite niets behoudens dat er een afscherming is ontstaan tussen het zakelijke en het privé gedeelte van een mobiel apparaat. Na de uitrol van MDM is het niet meer toegestaan en niet meer mogelijk om bijvoorbeeld zakelijke mail in je google mail omgeving te ontvangen.

Via MDM software kunnen IT-beheerders alle mobiele bedrijfsapparaten, zoals smartphones en tablets van medewerkers op afstand beheren. Alle toestellen staan in verbinding met een MDM server waardoor het mogelijk is om op een eenvoudige manier toezicht te houden op de werking van deze apparaten.

Een scheiding tussen werk en privé op smartphones

Het komt vaak voor dat medewerkers één mobiel toestel zowel zakelijk als privé gebruiken. Hierdoor komen datastromen door elkaar te lopen. Denk bijvoorbeeld aan de installatie van een bedrijfsapplicatie op een privésmartphone. De IT-beheerder heeft geen controle over het privét toestel waar de zakelijke applicatie op staat, met als gevolg dat de bedrijfsgegevens buiten de grenzen van het afgeschermd netwerk terecht komen. Een MDM oplossing biedt uitkomst.

Gegevens veiligstellen bij diefstal

Stel dat er een mobiel apparaat wordt gestolen waarop belangrijke en/of vertrouwelijke bedrijfsinformatie staat. De Mobile Device Manager kan op een snelle en eenvoudige manier ervoor zorgen dat het apparaat wordt geblokkeerd en dat de gegevens die erop staan worden gewist.

Meerdere categorieën gebruikers en apparatuur

Door de afzonderlijke werkgevers (gemeenten, BWB) is er de afgelopen jaren aan vele medewerkers een telefoon of tablet – in bruikleen – uitgereikt. Dit noemen we zakelijke apparaten (vakterm COD, Company Owned Devices). Daarnaast zijn er diverse medewerkers die eigen apparatuur (telefoons, tablets) inzetten en daarvoor een vergoeding ontvangen. Dit noemen we BYOD (Bring Your Own Device). Beide categorieën medewerkers vallen onder de BIO-voorwaarden en deze apparatuur zal van MDM voorzien moeten worden.

In een volgende fase zullen ook de door raads- en commissieleden ingezette eigen laptops of PC's van MDM moeten worden voorzien.