TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

# Management van mobiele apparaten

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

## Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Mobile Device Management’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

## Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

**Doel**

Dit document beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het beleid voor het management van mobiele apparaten, zoals smartphones, tablets en laptops, voor organisaties binnen de Rijksoverheid. Deze uitgangspunten over informatiebeveiliging zijn afkomstig uit de BIR en het beleid voldoet daarmee aan de BIR.

**Doelgroep**

Dit document is van belang voor de directie voor wat betreft de aanvulling van het informatiebeveiligingsbeleid voor mobiele apparaten, en voor ICT-beheerders.

**Reikwijdte**

Dit document heeft voornamelijk betrekking op maatregel 7.1.3 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen in relatie tot mobiele apparaten.

**Relatie met overige producten**

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI:2013)
- Informatiebeveiligingsbeleid
- Bring your own device
- Mobiele gegevensdragers

## Inhoudsopgave

# 1 Inleiding

Er is een toename van het gebruik van mobiele apparaten, zoals smartphones, tablets en laptops, door organisaties binnen de Rijksoverheid. Dit document heeft tot doel om vanuit verschillende gezichtspunten de risico's van het gebruik van mobiele apparaten weer te geven en handreikingen voor oplossingen te bieden om de risico's te verminderen. Het beschrijft het management van mobiele apparaten (Mobile Device Management (MDM)) als het stelsel van maatregelen, procedures en ondersteunende producten, die het mogelijk maken om mobiele apparaten binnen organisaties veilig te kunnen gebruiken en te kunnen beheersen. In dit document wordt tevens een voorzet gegeven voor aanvullend beleid op het gebied van MDM. Gezien de toenemende populariteit van smartphones en tablets voor zakelijk gebruik wordt in dit document specifiek aandacht besteed aan smartphones en tablets.

Dit document biedt geen volledige procesbeschrijving of productbeschrijvingen. Het bevat wel voldoende informatie om goede keuzes te maken ten aanzien van het management van mobiele apparaten en inzicht te bieden in informatiebeveiligingsaspecten betreffende mobiele apparaten.

In dit document wordt geen onderscheid gemaakt tussen mobiele apparaten van de organisatie en eigen mobiele apparaten van medewerkers (BYOD). Mobiele apparaten worden in beide toepassingsvormen steeds meer gebruikt binnen overheidsorganisaties, waardoor in toenemende mate data van de organisatie op de apparaten te vinden is. In beide gevallen blijft de data van eigendom van de organisatie, ongeacht of de organisatie of de medewerker eigenaar van het apparaat is.

Het is van belang om veilig om te gaan met mobiele apparaten en de data van de organisatie die erop kunnen staan, omdat:

- mobiele apparaten een besmetting met malware kunnen oplopen en daarmee de gehele organisatie kunnen infecteren (het mobiele apparaat wordt door hackers als aanvalsvector gebruikt);
- mobiele apparaten met data van de organisatie kunnen buiten de gebouwen van organisatie fysiek zoekraken of worden gestolen. Dit kan leiden tot dataschade en vervangschade van het apparaat;
- mobiele apparaten door malware hoge SMS of telefoonkosten kunnen veroorzaken;
- mobiele apparaten in sommige gevallen kunnen worden gebruikt om systemen van de organisatie te benaderen. Dit levert mogelijk privacy- en vertrouwelijkheidrisico's op.

# 2 Management van mobiele apparaten

Het management van mobiele apparaten is het stelsel van maatregelen, procedures en ondersteunende producten die het mogelijk maken om mobiele gegevensdragers binnen organisaties veilig te kunnen gebruiken en te kunnen beheersen. De maatregelen staan beschreven in de BIR en het afgeleide informatiebeveiligingsbeleid.

MDM is van toepassing op de volgende mobiele gegevensdragers:

- Telefoons en GSM's;
- Smartphones;
- Tablets, zoals iPad's;
- Dongels of MiFi voor mobiele toegang (MiFi is een Dongel met WiFi ingebouwd);
- Laptops.

De bovenstaande gegevensdragers kunnen al dan niet door de organisatie verstrekt zijn.

## 2.1 Bring Your Own Device (BYOD)

BYOD houdt in dat medewerkers van de organisatie eigen apparaten kunnen gebruiken voor hun werk. Deze apparaten kunnen onderweg, maar ook op kantoor worden gebruikt. Deze mobiele apparaten kunnen toegang krijgen tot vertrouwelijke informatie van de organisatie en deze informatie kan ook op het betreffende apparaat terechtkomen.

Op dit moment worden mobiele apparaten ook zonder toestemming zakelijk gebruikt. Doordat de organisatie eigendom blijft van de data op het apparaat is het noodzakelijk dat er nadrukkelijk toestemming voor zakelijk gebruik wordt gegeven.

Mobiele apparaten die eigendom zijn van de organisatie, dienen te worden bijgehouden in de ICT-Configuratie Management Database. Bij BYOD (privéapparaten) is dit lastiger, tenzij er wordt afgedwongen dat alle apparaten waar zakelijke informatie op kan staan, geregistreerd worden. Binnen MDM-tooling bestaat hier functionaliteit voor. Voor MDM-tooling op privéapparaten (BYOD) is op grond van artikel 27, eerste lid, onder K en l, van de Wet op de Ondernemingsraden instemming van de ondernemingsraad (OR) nodig.

## 2.2 Drie risico's van gebruik mobiele apparaten

In de inleiding werden kort enkele risico's beschreven die van toepassing kunnen zijn op mobiele apparaten. Hieronder worden drie belangrijke beveiligingsrisico's voor het gebruik van mobiele apparaten nader toegelicht.

### 1. Malware besmetting op het mobiele apparaat

MOGELIJKE OORZAKEN:

- Er is geen vastgesteld beleid over welke applicaties zijn toegestaan, waardoor niet-vertrouwde applicatiebronnen ook worden gebruiken;

- Jailbreaken of rooten van apparaten[1];
- Klikken op links in mail, webpagina's en in SMS-berichten die niet-vertrouwd zijn;
- Verbinden via onveilige open netwerken.

MOGELIJKE GEVOLGEN

Besmetting met malware kan verschillende gevolgen hebben. Er kan kwaadaardige software worden geïnstalleerd die (vertrouwelijke) gegevens steelt, of zichzelf toegang verschaft tot of verspreidt naar andere systemen van organisatie. Ook is installatie mogelijk van dialers die sms'jes zenden of bellen met dure nummers met hoge kosten als gevolg.

MAATREGELEN

- Vaststellen en implementeren beleidsregels voor mobiele apparaten;
- Implementeren MDM Software om beleid af te dwingen op mobiele apparaten (ook toepasbaar op BYOD apparaten);
- Uitzetten van diensten die niet direct nodig zijn;
- Geen niet-vertrouwde netwerken gebruiken;
- Specifiek aandacht voor dit onderwerp in bewustwordingscampagnes.

## 2. Gegevensverlies, of onbevoegde toegang tot gegevens

MOGELIJKE OORZAKEN

- Er is geen vastgesteld beleid over welke gegevens op mobiele apparaten mogen staan. Er is geen beleid voor dataclassificatie;
- Malware op het apparaat;
- Klikken op links in mail, webpagina's en in SMS-berichten die niet vertrouwd zijn;
- Verbinden via onveilige open netwerken;
- Man in the middle attack[2];
- Niet locken van het apparaat;
- Geen encryptie op inhoud en verbindingen.

MOGELIJKE GEVOLGEN

Mogelijke gevolgen zijn het inzien gegevens door onbevoegden, het kopiëren van gegevens, het vernietigen van gegevens of het veranderen van gegevens.

MAATREGELEN

- Vaststellen en implementeren beleidsregels voor mobiele apparaten;

[1] Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS-apparaat, waardoor ook mailware gedraaid kan worden. Rooten is het proces dat het mogelijk maakt men meer rechten krijgt op het apparaat (Android) en daardoor het complete besturings systeem te wijzigen of te vervangen, en daarmee mailware introduceren en beveiligingsinstellingen te omzeilen.
[2] Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt, zonder dat beide partijen daar weet van hebben. Dit terwijl de computer van de aanvaller zich tussen deze partijen bevindt.

- Implementeren van encryptie op toegestane data op het apparaat;
- Indien mogelijk ‘zero footprint’ software gebruiken;
- Implementeren MDM software;
- Implementeren apparaatauthenticatie;
- Implementeren kanaal encryptie en ‘two factor authenticatie’;
- Specifiek aandacht voor dit onderwerp besteden in bewustwordingscampagnes.

## 3. Zoekraken apparatuur (fysiek)

MOGELIJKE OORZAKEN

- Diefstal
- Verlies

MOGELIJKE GEVOLGEN

- Mogelijk inzien gegevens door onbevoegden, evenals het kopiëren van gegevens, het vernietigen van gegevens of het veranderen van gegevens;
- Onbevoegd toegang tot organisatiesystemen;
- Het mobiele apparaat moet worden vervangen.

MAATREGELEN

- Vaststellen en Implementeren beleidsregels voor mobiele apparaten;
- Implementeren van encryptie op toegestane data op het apparaat;
- Indien mogelijk ‘zero footprint’ software gebruiken;
- Implementeren MDM software;
- Implementeren van een apparaat opzoekfunctie (in de MDM software);
- Implementeren van een functie om het apparaat op afstand te wissen;
- Implementeren ‘two factor authenticatie’ voor toegang tot organisatiesystemen;
- Specifiek aandacht voor dit onderwerp in bewustwordingscampagnes.

## Bijlage 1: Aanvulling beleid voor Management van mobiele apparaten

### Uitgangspunten Management van mobiele apparaten (Mobile Device Management, MDM)

Ten behoeve van het management van mobiele apparaten (MDM) dienen er regels binnen de organisatie te zijn die moeten worden gehanteerd voor het gebruik van mobiele apparaten. Het doel van deze beleidsaanvulling is het voorkomen van vermijdbare schade voor de organisatie.

### Aanvullende maatregelen MDM

De volgende maatregelen dienen terug te komen in aanvullend beleid omtrent MDM:

1. Het opstellen van regels voor acceptabel gebruik. Deze regels dienen door de medewerker geaccepteerd en getekend te worden. Binnen de regels voor acceptabel gebruik is aandacht voor:
   - Het proces in geval van verlies of diefstal van alle mobiele gegevensdragers, waarbij meldingen binnen 4 uur gedaan moeten worden;
   - Niet voldoen aan beleid en regels kan resulteren in een disciplinair proces;
   - Een verbod op het downloaden van illegale software en software uit niet-vertrouwde bronnen;
   - Een verbod op rooten en jailbreaken van een mobiel apparaat (dit vergroot de kans op illegale software of toegang krijgen tot de telefoon);
   - Regels over excessief gebruik in Nederland en tijdens ‘roaming’ in het buitenland;
   - Bij gebruik als bestuurder van een voertuig voldoen aan wettelijke normen;
   - Zich houden aan ICT-standaarden en nadere afspraken.

2. Gebruikers hebben kennis van de regels:
   - Het gebruik van mobiele apparatuur dient aandacht te hebben in bewustwordings-trainingsmateriaal van de organisatie.

3. Toevoegen van regels voor het meenemen van informatie:
   - De organisatie dient ook aandacht te hebben voor de impliciete toestemming aan gebruikers welke informatie zij wel of niet mogen inzien met hun apparaat, of;
   - Er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording kan worden geroepen.

4. Detailregels om te zorgen voor bescherming van gegevens op apparaten:
   - De organisatie hanteert classificatie regels van organisatiegegevens en zorgt voor passende maatregelen om dit op apparaten (al of niet) te ondersteunen.

5. Alle mobiele apparaten, zowel van de organisatie of privé, waarop organisatiegegevens kunnen staan, worden bij voorkeur beheerd met een MDM-tool met passende functionaliteiten.

## Bijlage 2: Functionele eisen MDM-software

In deze bijlage worden mogelijke functionele eisen voor software voor management van mobiele apparaten beschreven.

Om een goede keuze te kunnen maken voor MDM-software zijn de volgende vragen van belang:

- Kan de software binnen de organisatie worden gebruikt op eigen hardware of is er een cloud?

- Mogelijkheid tot SaaS-oplossing?

- Welke platforms is de organisatie bereid te ondersteunen en kan de tool deze ook ondersteunen, denk hierbij aan: iOS, Android, BlackBerry, Windows Phone, Symbian, overige?

- Zijn de volgende MDM-functies aanwezig?
    - Wachtwoord bescherming instelbaar;
    - Wachtwoord reset functie beschikbaar;
    - Op afstand het device leegmaken (remote wipe);
    - Selectief leegmaken apparaat;
    - Op afstand blokkeren;
    - Instellen netwerk settings;
    - Uitschakelen camera functies zoals: netwerk, bluetooth, 3G data, camera;
    - Automatische uitrol software en policies;
    - Monitoring configuraties.

- Zijn de volgende beveiligingsfuncties aanwezig?
    - Applicatie backlisting en applicatie whitelisting;
    - Apparaat compromittering (rooting en jailbreaking detectie);
    - Wisselen sim-card detectie;
    - Data protectie (DLP);
    - Apparaat encryptie;
    - Folder / map encryptie;
    - Encryptie van e-mail en ook bijlagen;
    - Geofencing (instellen geografische grenzen waarbij overschrijding zorgt voor een alarm);
    - Tijd restricties kunnen opleggen (instellen tijdstippen waarbinnen het apparaat gebruikt mag worden);
    - VPN functies (voor veilige encrypted verbindingen);
    - Antivirus functies/ detective;
    - Firewall;
    - Single Sign-on Support.

- Zijn de volgende applicatie beheerfuncties aanwezig?

  - Kun je een eigen App Store opzetten waaruit de user kan/mag kiezen? Kan die App Store ook voor desktop applicaties gebruikt worden?
  - Is applicatie sandboxing mogelijk (applicatie draait dan in een eigen afgeschermde omgeving)?
  - Zijn er tools aanwezig voor sandboxing?
  - Is er een integratie mogelijk van een andere App Store (bijvoorbeeld Apple)?
  - Zijn virtuele desktop functies of applicaties beschikbaar?

- Document/content management functies?
  - Is er een aparte encrypted document container/locatie mogelijk?
  - Is e-mailbeveiliging mogelijk?
  - Is toegang tot (eigen) bestanden op servers mogelijk?
  - Is er integratie met Sharepoint of andere Document Management Sofware? (bij voorkeur die de organisatie zelf al heeft)?

- Netwerk beheer functies?
  - Data verbruik beheer (over Wi-Fi maar ook mobiele netwerken)?
  - Controle over roaming-kosten, of blokkeren roaming?
  - Diagnose functies?
  - Monitoren gebruik?
  - Blokkeren van devices als bijvoorbeeld instellingen worden aangepast of als policies niet geaccepteerd worden?

- Service management / ICT beheer
  - Helpdesk support functies
  - Service monitoring

- Integratie
  - Mogelijkheden om te integreren met PC Beheer Tooling?
  - Met welke andere desktop tooling kan worden geïntegreerd?
  - Zijn er integratie API’s?
  - Is er een Management Console voor Mobile Devices en PC’s?

- Rapporten
  - Zijn er alarmen?
  - Geautomatiseerde respons op alarmen instelbaar?
  - Real-time overzichten beschikbaar?
  - Analyse tot op device niveau?
  - Analyse tot op app niveau?