****

**Mobile Device Management**

Handreiking aangeleverd door Lumen Group incl. voorbeeld “Bring your own device beleid” ter ondersteuning in de naleving van de wettelijke verplichting uit de AVG

(Artikel 32 AVG)

|  |  |
| --- | --- |
| **Versie** | V1.0  |
| **Auteur** | Lumen Group |
| **Opsteldatum** | 17 oktober 2022 |
|  |  |

Mobile Device Management

**Versiebeheer**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datum** | **Auteur** | **Versie** | **Status** | **Aanpassing** |
|  |  |  |  |  |

**Goedgekeurd**

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Naam goedkeurder** | **Functie** | **Handtekening** |
|  |  |  |  |


Template Mobile Device Management aangeleverd door Lumen Group inclusief bijlagen ter ondersteuning in de naleving van de wettelijke verplichting uit artikel 32 AVG van [Lumen Group](https://www.lumengroup.nl/) is in licentie gegeven volgens een [Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen 4.0 Internationaal-licentie](http://creativecommons.org/licenses/by-nc-sa/4.0/).Toestemming met betrekking tot rechten die niet onder deze licentie vallen zijn beschikbaar via <https://www.lumengroup.nl/disclaimer/>.

De verantwoordelijkheid en aansprakelijkheid blijft bij de gebruiker voor: 1. Het bestuur en bedrijfsvoering van de organisatie. Hieronder valt onder andere de uitoefening van de bedrijfsactiviteiten in het kader van de verwante zakelijke aangelegenheden; en 2. De genomen beslissingen van de gebruiker die in een bepaalde mate gebaseerd zijn op de door Lumen Group geleverde adviezen, aanbevelingen of documenten.

**Inhoudsopgave**

[**1** **Inleiding** 3](#_Toc117865513)

[**2** **Uitgangspunten Mobile Device Management** 3](#_Toc117865515)

[**2.1** **Acceptabel gebruik** 4](#_Toc117865516)

[**2.2** **Bewustwording** 4](#_Toc117865517)

[**2.3** **Classificatie gegevens** 4](#_Toc117865518)

[**3** **Mobile Device Management-tool** 4](#_Toc117865519)

[**3.2 Beveiligingsfuncties** 5](#_Toc117865520)

[**3.3 Applicatie beheer** 5](#_Toc117865521)

[**3.4 Document managementfuncties** 6](#_Toc117865522)

[**3.5 Netwerkbeheer** 6](#_Toc117865523)

[**3.6 Integratie** 6](#_Toc117865524)

[**3.7 Rapporten** 6](#_Toc117865525)

[**3.8 Toekomstbestendigheid** 7](#_Toc117865526)

[**Bijlage A - Risico’s & maatregelen** 8](#_Toc117865527)

[**Bijlage B – Bring Your Own Device beleid ORGANISATIENAAM** 10](#_Toc117865528)

[**1. Introductie** 10](#_Toc117865529)

[**2. Doel** 10](#_Toc117865530)

[**3. Reikwijdte** 10](#_Toc117865531)

[**4. Verantwoordelijkheden** 10](#_Toc117865532)

[**4.1 Verantwoordelijkheden ORGANISATIENAAM** 10](#_Toc117865533)

[**4.2 Verantwoordelijkheden medewerkers** 11](#_Toc117865534)

[**5. Do’s en dont’s** 11](#_Toc117865535)

[**6. Bezwaar en beroep** 12](#_Toc117865536)

[**7. Inwerkingtreding beleid** 12](#_Toc117865537)

# **Inleiding**

Het gebruik van mobiele apparaten zoals laptops, smartphones en tablets (hierna: devices[[1]](#footnote-1)) is tegenwoordig voor bijna alle medewerkers binnen een organisatienoodzakelijk om hun werkzaamheden te kunnen verrichten. Bij deze werkzaamheden worden meestal veel gegevens verwerkt, waaronder persoonsgegevens.

Van medewerkers binnen een organisatie wordt verwacht dat zij verantwoord omgaan met deze devices. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de organisatie uit te voeren.

Aan het gebruik van devices zijn immers risico’s verbonden, zoals het fysiek zoekraken van devices door diefstal of onopzettelijk verlies en malwarebesmettingen op devices, met mogelijk verlies of onbevoegd inzien van (persoons)gegevens. Het is daarom noodzakelijk afspraken te maken over het gebruik.

In hoofdstuk 2 staan de uitgangspunten van Mobile Device Management, gevolgd door informatie over gebruik van een Mobile Device Management Tool om het management te ondersteunen in hoofdstuk 3.

In bijlage A staan de oorzaken, mogelijke gevolgen en te nemen maatregelen behorende bij de risico’s van gebruik van devices schematisch weergegeven. In bijlage B is een voorbeeld opgenomen van een “Bring your own device” beleid.

1.

# **Uitgangspunten Mobile Device Management**

Mobile Device Management legt de regels vast binnen de organisatie die gehanteerd moeten worden als er devices worden geïntroduceerd. Het doel hiervan is te voorkomen dat de organisatie hinder ondervindt in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur en hardware.

Het bepaalt ook welke diensten wel, en welke diensten zeker niet uitgevoerd mogen worden op devices.

De organisatie maakt vooraf een keuze welke devices worden ingezet. Hiervoor zijn twee mogelijkheden (of een mix daarvan):

Wanneer medewerkers gebruik maken van eigen privé devices om werkzaamheden te verrichten ten behoeve de organisatie (“Bring Your Own Device”, BYOD), zijn zij zelf verantwoordelijk voor het nemen van adequate beveiligingsmaatregelen. De organisatie wijst haar medewerkers erop dat zij bij BYOD voldoen aan de minimale eisen aan beveiligingsmaatregelen zoals de organisatie die zelf hanteert. De organisatie kan hierop controles uitvoeren. De medewerker moet aan kunnen tonen op verzoek de organisatie welke maatregelen er zijn toegepast.

Wanneer de organisatie bepaalt welke devices de medewerker kan kiezen, is er sprake van “Choose Your Own Device” (CYOD). Medewerkers krijgen hierbij de keuze uit een aantal devices welke passen bij hun werkzaamheden en voorkeuren. Devices bij CYOD blijven eigendom van de organisatie, maar kunnen onder voorwaarden ook voor privédoeleinden gebruikt worden. Hierbij kan er ook voor worden gekozen, dat de medewerker de device(s) op den duur overneemt. Vervolgens worden de gebruiksregels in beleid omtrent Mobile Device Management of in gebruikersovereenkomsten vastgelegd. Deze regels dienen regelmatig herzien te worden naar de stand van de nieuwste ontwikkelingen op het gebied van informatiebeveiliging en door de OR/(G)MR en door de medewerker geaccepteerd en getekend te worden. Hiermee verklaren zij bewust te zijn van de gevaren van het werken met devices en dat zij zich houden aan hetgeen in het beleid of de gebruikersovereenkomst is vastgelegd. Tijdens bewustwordingscampagnes dient veilig mobiel werken en het beleid hieromtrent te worden meegenomen.

Bij het (opstellen van) beleid voor acceptabel gebruik van devices neemt de organisatie minimaal de volgende genoemde onderwerpen hierin mee:

# **Acceptabel gebruik**

Het opstellen van regels voor acceptabel gebruik. Hierbij is aandacht voor:

* Het proces in geval van verlies of diefstal van mobile devices, waarbij incidenten zo snel mogelijk gemeld moeten worden;
* Niet voldoen aan beleid en regels kan resulteren in een disciplinaire maatregelen;
* Een verbod op het downloaden van illegale software en/of software uit niet-vertrouwde bronnen;
* Een verbod op rooten en jailbreaken van een device (dit vergroot de kans op illegale software of toegang krijgen tot de telefoon)[[2]](#footnote-2);
* Regels over excessief gebruik in Nederland en/of en tijdens ‘roaming’ in het buitenland;
* Bij bellen of gebruik in de auto zich houden aan wettelijke regels;
* Houden aan hetgeen is vastgelegd in de gebruikersovereenkomst en het informatiebeveiligingsbeleid de organisatie.

# **Bewustwording**

* Aandacht voor het gebruik van devices, het tekenen van een gebruikersovereenkomst en de risico’s in bewustwordings- trainingsmateriaal van de organisatie;
* De organisatie informeert haar medewerkers welke informatie zij wel of niet mogen inzien of verwerken met hun device, of er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden.

# **Classificatie gegevens**

De organisatie hanteert voor de te verwerken gegevens classificatieniveau’s, waarop de verschillende soorten verwerkingen (bijvoorbeeld het inzageniveau) op de verschillende soorten devices wordt afgestemd. Deze classificatie is meestal opgenomen in het informatiebeveiligingsbeleid van de organisatie.

# **Mobile Device Management-tool**

Devices van zowel de organisatie als privé-devices, waarop gegevens kunnen staan van de organisatie, worden bij voorkeur beheerd met een Mobile Device Management-tool of -software (hierna: MDM-tool). De organisatie gebruikt deze MDM-tool op de eigen hardware of in de Cloud/SaaS.

Let op: wanneer de organisatie voor het eerst gebruik maakt van een MDM-tool of er niet vertrouwd mee is, voert zij hierop een DPIA uit. Als uit de DPIA blijkt dat de MDM-technologie in bepaalde gevallen noodzakelijk is, moet nog steeds worden beoordeeld of er geen andere minder ingrijpende maatregelen mogelijk zijn en of de functionaliteiten zo zijn ingesteld dat ze passend bij de situatie zijn.[[3]](#footnote-3)

Bij het selecteren van een MDM-tool zijn de volgende functionaliteiten belangrijk ter overweging:

**3.1 Managementfuncties**

Instelbaarheid van:

* Wachtwoordbescherming;
* Wachtwoord reset;
* Leegmaken van device op afstand (remote wipe);
* Device selectief leegmaken;
* Op afstand blokkeren device;
* Aanpassen van de netwerkinstellingen;
* Uitschakelen functies zoals: netwerk, bluetooth, mobiele data, camera;
* Automatische software- en policyupdates;
* Monitoring configuraties;
* Logging van gebruikers.

# **3.2 Beveiligingsfuncties**

Instelbaarheid van:

* Applicatie-blacklisting en applicatie-whitelisting;
* Detectie device-compromitering (rooting en jailbreaking detectie);
* Detectie wisselen sim-card ;
* Dataprotectie;
* Device encryptie;
* Folder/ map encryptie;
* Encryptie van e-mail en bijlagen;
* Geofencing (instellen geografische grenzen waarbij overschrijding zorgt voor een alarm);
* Opleggen tijdrestricties (instellen tijdstippen waarbinnen het apparaat gebruikt mag worden);
* VPN-functies (voor veilige encrypted verbindingen);
* Virusscanners;
* Firewall;
* Multi- of tweefactorauthenticatie;
* Single Sign-on ondersteuning.

# **3.3 Applicatie beheer**

Mogelijkheden voor:

* Opzetten van een eigen App Store waaruit de user kan/mag kiezen, ook voor desktopapplicaties ;
* Integratie met een andere App Store (bijvoorbeeld Apple);
* Beveiliging tegen verwijdering MDM-software en geassocieerde apps ;
* Applicatie-sandboxing (applicatie draait dan in een eigen afgeschermde omgeving);
* Tools voor sandboxing;
* Virtuele desktopfuncties of -applicaties.

# **3.4 Document managementfuncties**

Mogelijkheden voor:

* Aparte encrypted document container/ locatie;
* E-mail beveiliging;
* Toegang tot (eigen) bestanden op servers;
* Integratie met Sharepoint of ander Document Management Sofware (bij voorkeur met die de organisatie zelf al heeft).

# **3.5 Netwerkbeheer**

Mogelijkheden voor:

* Dataverbruikbeheer (over Wi-Fi maar ook mobiele netwerken);
* Controle over roaming-kosten, of blokkeren roaming;
* Diagnose;
* Monitoren gebruik;
* Blokkeren van devices als bijvoorbeeld instellingen worden aangepast of als policies niet geaccepteerd worden;
* Service management / ICT-beheer;
* Helpdesk support;
* Service monitoring.

# **3.6 Integratie**

Mogelijkheden voor:

* Integratie met PC beheer tooling;
* Integratie met andere desktop tooling;
* Gebruik integratie-API’s;
* Gebruik Management Console voor mobile devices en PC’s.

# **3.7 Rapporten**

Mogelijkheden voor:

* Alarmering;
* Instelbare geautomatiseerde respons op alarmen;
* Real-time overzichten;
* Analyse tot op deviceniveau;
* Analyse tot op appniveau.

# **3.8 Toekomstbestendigheid**

* Er komen steeds nieuwe (mobiele) apparaten en versies van Operating Systemen uit. Een MDM-oplossing dient zo ontworpen te zijn en ingericht kunnen worden dat deze mee kan gaan met deze nieuwe (mobiele) apparaten en Operating Systemen.
* Een MDM-oplossing dient meerdere versies van een Operating Systeem te ondersteunen.
* Een MDM-oplossing moet zo snel mogelijk bij het verschijnen van een nieuwe versie van een Operating Systeem en/of veiligheidsupdate deze nieuwe versie ondersteunen.

**Bijlage A - Risico’s & maatregelen**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risico** | **Oorzaken** | **Mogelijke gevolgen** | **Preventiemaatregelen** |
| **Fysiek zoekraken device** | * Diefstal;
* Onopzettelijk verlies.
 | * (Onbevoegde) toegang tot systemen van de organisatie met het device (met datalek van persoonsgegevens als gevolg);
* Inzien (persoons)gegevens door onbevoegden met datalek van persoonsgegevens als gevolg;
* Kopiëren van gegevens (met datalek van persoonsgegevens als gevolg);
* Wijzigen van gegevens (met datalek van persoonsgegevens als gevolg);
* Vernietigen van gegevens en misbruiken van gegevens (met datalek van persoonsgegevens als gevolg);
* Risico voor de rechten en vrijheden van betrokkenen;
* Meldingsplicht richting de betrokkene(n) en/of Autoriteit Persoonsgegevens.
 | * Vaststellen en implementeren device-beleidsregels en/of gedragsregels voor de medewerkers;
* Implementeren device-encryptie (bijvoorbeeld Bitlocker), in ieder geval beveiligde opslag van gegevens van de organisatie, als die al worden toegestaan op het device;
* Waar mogelijk zero footprint software gebruiken;
* Waar informatie lokaal wordt opgeslagen dient het device van afstand te wissen zijn;
* Implementeren MDM-software;
* Implementeren van een apparaat-opzoekfunctie (in de MDM-software);
* Implementeren van Mobile Application Management software (MAM-software);
* Toegang tot systemen afdwingen door implementatie van tweefactorauthenticatie;
* Specifieke bewustwordingscampagnes;
* Invoeren incidentmanagement.
 |
| **Malware besmetting op het device** | * Ontbreken vastgesteld beleid over welke applicaties zijn toegestaan, niet-vertrouwde applicatiebronnen gebruiken kan risico verhogend werken;
* Ongeautoriseerde applicaties downloaden;
* Phishing;
* Verbinden via onveilige open netwerken, waar men gestuurd kan worden naar kwaadaardige websites;
* Openen van met malware besmette bestand, bijvoorbeeld een bijlage van een e-mail.
 | * Installatie kwaadaardige software die gegevens steelt, zichzelf toegang verschaft, maar ook zichzelf verspreidt over andere systemen binnen een organisatie. Met als gevolg dat de gegevens niet meer betrouwbaar zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid;
* Installatie malware die sms’jes zenden of bellen met dure nummers, met als gevolg hoge kosten;
* Hoog dataverbruik door installatie van kwaadaardige software;
* Versleutelen van gegevens op mobiele apparaten (ransomware, cryptoware); waardoor deze niet meer beschikbaar zijn;
* Negatieve publiciteit en reputatieschade.
 | * Vaststellen en implementeren device-beleidsregels en gedragsregels voor de medewerkers;
* Implementeren van MDM-software;
* Implementeren van MAM-software;
* Uitzetten van services die niet direct nodig zijn;
* Geen netwerken gebruiken die onbetrouwbaar zijn;
* Specifieke bewustwordingscampagnes;
* Patchen en updates tijdig uitvoeren;
* Detecterende maatregelen treffen (op basis van logging, waaronder bijvoorbeeld een Security Information Managament System (SIEM)/ Security Operation Centre (SOC).
 |

**Bijlage B – Bring Your Own Device beleid ORGANISATIENAAM**

# **1. Introductie**

ORGANISATIENAAM verwacht van haar medewerkers dat zij de devices, die van medewerker zelf zijn en waarop activiteiten worden uitgevoerd voor ORGANISATIENAAM (hierna: BYOD), op een verantwoorde manier gebruikt.

ORGANISATIENAAM erkent het voordeel van een BYOD-beleid met de mogelijkheid voor medewerkers om thuis, op kantoor of onderweg te kunnen werken met de eigen mobile devices.

ORGANISATIENAAM verwacht van haar medewerkers dat minimaal de maatregelen worden genomen en nageleefd, zoals hierin aangegeven.

# **2. Doel**

Dit beleid is bedoeld om een veilige omgeving te creëren voor de organisatie- en persoonsgegevens, die ORGANISATIENAAM verwerkt, op BYOD.

Het naleven van dit BYOD-beleid zorgt er niet alleen voor dat organisatie- en persoonsgegevens worden beschermd, maar het beperkt ook de impact van een cyberaanval, datalek of andere illegale beschadigende activiteiten op de rechten en vrijheden van de betrokkenen.

# **3. Reikwijdte**

Dit beleid is van toepassing op medewerkers die voor hun werkzaamheden eigen devices (BYOD) gebruiken. Dit beleid kan ook van toepassing zijn op externe medewerkers [en (sub)verwerkers] die op enige manier werkzaamheden verrichten voor ORGANISATIENAAM en daarbij eigen devices gebruiken.

Onder devices wordt in ieder geval de volgende hardware verstaan: *desktop computer, laptop, notebook, tablet, Personal Digital Assistants (DPA’s), (smart)phone, maar ook een USB-stick en bijvoorbeeld een hardware token (tag) en enig ander persoonlijk apparaat die de mogelijkheid heeft om de diensten van ORGANISATIENAAM te raadplegen.*

# **4. Verantwoordelijkheden**

# **4.1 Verantwoordelijkheden ORGANISATIENAAM**

ORGANISATIENAAM is verantwoordelijk voor het onderhouden en updaten van het BYOD-beleid en het actief monitoren van het device. ORGANISATIENAAM heeft het recht om het gebruik van de device(s) tijdelijk of permanent te verbieden. ORGANISATIENAAM kan de volgende acties uitvoeren:

* Het controleren van de door de medewerkers te nemen maatregelen. Op verzoek van ORGANISATIENAAM moet de medewerker zelf aantonen dat hij of zij de in 5.1 genoemde maatregelen toepast.
* Het weigeren van de toegang tot diensten van ORGANISATIENAAM om beveiligingsincidenten op te lossen of te voorkomen.
* Alle mogelijke en wettelijk toegestane acties om verloren gegevens terug te halen en gegevens te verwijderen binnen de beveiligde omgeving van ORGANISATIENAAM.
* Het monitoren en loggen van gegevensuitwisseling tussen het device en ORGANISATIENAAM.

ORGANISATIENAAM weegt hierbij haar gerechtvaardigde belang om ORGANISATIENAAM te beschermen af tegen de redelijke verwachtingen met betrekking tot privacy van medewerkers.

# **4.2 Verantwoordelijkheden medewerkers**

Medewerker gaat akkoord met de volgende regels betreffende het gebruik van de diensten van ORGANISATIENAAM

* [VUL HIER BELEID BETREFFENDE DE KOSTEN VAN DEVICES IN ZOALS, VERGOEDINGEN, KOSTEN VOOR REPARATIE, MOBIELE DATA, BELKOSTEN]
* Medewerker zorgt voor de geheimhouding, integriteit en toegankelijkheid, in verband met de werkzaamheden voor en de diensten van ORGANISATIENAAM.
* Medewerker probeert geen gegevens te verwijderen, downloaden of verplaatsen van de beschermde omgeving van ORGANISATIENAAM naar omgevingen die niet door ORGANISATIENAAM wordt beschermd, zonder daarvoor toestemming te hebben van ORGANISATIENAAM.
* Medewerker houdt rekening met opgestelde informatiebeveiligingsbeleid van ORGANISATIENAAM.
* Medewerker meldt direct beveiligingsincidenten met betrekking tot het device aan [VERANTWOORDELIJK ORGAAN].

# **5. Do’s en dont’s**

Medewerker gaat akkoord met de volgende gebruiken omtrent BYOD.

**5.1 Do’s**

Medewerker:

* Beveiligt het device met een wachtwoord, door gebruik te maken van een sterk wachtwoord of een wachtwoordmanager.
* Vergrendelt het device bij het verlaten van de werkplek (bijvoorbeeld via de windowstoets+L).
* Stelt tweefactorauthenticatie in waar mogelijk.
* Voert tijdig en minimaal maandelijks de updates uit van de software van het device. Dit kan bestaan uit het patchen van het device.
* Heeft anti-virus software geïnstalleerd als het device deze software ondersteunt.
* Slaat de documenten van ORGANISATIENAAM alleen in de beveiligde omgeving van ORGANISATIENAAM op.
* Meldt diefstal of verlies van het device zo snel mogelijk bij [VERANTWOORDELIJK ORGAAN].
* Meldt een (mogelijk) malware-, virus- of ransomware-aanval op het device direct bij [VERANTWOORDELIJK ORGAAN].
* Ondersteunt ORGANISATIENAAM bij het uitvoeren haar wettelijke en operationele taken in het geval een onderzoek aan of in een device noodzakelijk is.

**5.2 Dont’s**

Medewerker:

* Gebruikt het device niet om illegale of andere criminele activiteiten uit te voeren. Dit bestaat ook uit het gebruik van illegale software op het device.
* Slaat geen gegevens op van ORGANISATIENAAM buiten de beschermde omgeving van ORGANISATIENAAM.
* Mag het device niet rooten of jailbreaken.
* Mag geen anderen gebruik laten maken van het device dan zichzelf.

# **6. Bezwaar en beroep**

Als de medewerker het niet eens is met de (voorgenomen) beslissing van ORGANISATIENAAM om het gebruik van de device(s) tijdelijk of permanent te verbieden, of met andere door ORGANISATIENAAM uit te voeren acties zoals aangegeven in 4.1, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

# **7. Inwerkingtreding beleid**

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle
van het gedrag of de prestaties van medewerkers. De OR/(G)MR) is om deze reden instemmingsplichtig. De OR/(G)MR) heeft op <datum> ingestemd met de inhoud van deze gedragscode.

Dit beleid treedt direct na goedkeuring door het Bestuur van ORGANISATIENAAM in werking en geldt totdat een nieuwe versie van dit beleid wordt goedgekeurd.

Deze regeling wordt jaarlijks geëvalueerd door ORGANISATIENAAM en de OR/(G)MR.

De eerstkomende evaluatie vindt plaats op …...

Aldus in tweevoud opgemaakt en ondertekend,

|  |  |  |
| --- | --- | --- |
| Naam Ondergetekende | : |  |
| Functie: | : |  |
| Datum | : |  |
| Handtekening | : |  |

1. Onder mobile devices of mobiele apparaten wordt in ieder geval de volgende hardware verstaan: computer, laptop, tablet, telefoon, smartphone, maar ook een USB-stick en bijvoorbeeld een hardware token (tag). [↑](#footnote-ref-1)
2. Jailbreaken is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook malware gedraaid kan worden; rooten is het proces dat het mogelijk maakt dat men meer rechten krijgt op het apparaat (Android) en waardoor het complete besturingssysteem kan worden gewijzigd of vervangen, en daarmee malware kan worden geïntroduceerd en beveiligingsinstellingen worden omzeild. [↑](#footnote-ref-2)
3. WP29, Advies 2/2017 over gegevensverwerking op het werk, p. 20. [↑](#footnote-ref-3)