

Devicemanagementbeleid

Voorbeelddocument

Versie: Augustus 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je bij het maken van een eigen devicemanagementbeleid. Elke school en elk schoolbestuur is anders. Pas het beleid daarom aan, zodat het past bij jouw situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het beleid definitief maakt.
* Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Het is nodig geel gearceerde teksten te vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///C%3A%5CUsers%5Cjhgerrits%5CDocuments%5C1.%20Kennisnet%20voorbeeldocumenten%5Cnormenkaderibp.kennisnet.nl%5Cgroeipad)of stuur een e-mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Vul in wie het beleid vaststelt.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld. |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties>. |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 5](#_Toc209505900)

[1.1 Doelstelling 5](#_Toc209505901)

[1.2 Reikwijdte 5](#_Toc209505902)

[1.3 Verantwoordelijkheden 6](#_Toc209505903)

[2 Devices 7](#_Toc209505904)

[2.1 Type devices 7](#_Toc209505905)

[2.1.1 Managed devices 7](#_Toc209505906)

[2.1.2 Unmanaged devices 7](#_Toc209505907)

[2.2 Managed & unmanaged devices 7](#_Toc209505908)

[2.3 Registratie van devices 7](#_Toc209505909)

[2.3.1 Managed devices 7](#_Toc209505910)

[2.3.2 Unmanaged devices 8](#_Toc209505911)

[2.4 Levenscyclus 8](#_Toc209505912)

[3 Security 9](#_Toc209505913)

[3.1 Toegang 9](#_Toc209505914)

[3.1.1 Medewerkers 9](#_Toc209505915)

[3.1.2 Leerlingen 9](#_Toc209505916)

[3.1.3 Externe partijen en bezoekers 10](#_Toc209505917)

[3.2 Beveiligingsmaatregelen 10](#_Toc209505918)

[3.2.1 Managed devices 10](#_Toc209505919)

[3.2.2 Unmanaged devices 10](#_Toc209505920)

[4 Herziening 11](#_Toc209505921)

[4.1 Beleidsherziening 11](#_Toc209505922)

# Inleiding

## Doelstelling

***Toelichting***

* *In deze paragraaf beschrijf je de doelstellingen van je beleid. Pas onderstaande voorbeelddoelstellingen aan, zodat ze passen bij jouw organisatie.*
* *Bepaal ook of je wilt voldoen aan een concreet volwassenheidsniveau van de bijbehorende norm (Verwijzing opnemen naar Norm SM.03 Mobiele apparaten en telewerken) en neem dit op in de doelstelling.*

Het doel van dit beleid is het waarborgen van een veilig, verantwoord en efficiënt gebruik van alle apparaten – zoals laptops, tablets, smartphones en randapparatuur – binnen alle onder dit bestuur vallende onderwijsinstellingen. Hiermee willen we het volgende bereiken:

1. Beschermen van leerlingen, medewerkers en externe partijen door middel van passende maatregelen om de fysieke en digitale veiligheid van apparaten te garanderen.
2. Centraliseren en standaardiseren van het beheer van devices, zodat apparaten op een uniforme wijze worden ingericht, onderhouden en beveiligd.
3. Vergroten van digitale weerbaarheid door misbruik, verlies, diefstal en onbevoegde toegang tot apparaten en de daarop aanwezige gegevens te voorkomen.
4. Optimaliseren van beheerprocessen door een efficiënte aanpak voor het uitgeven, onderhouden, updaten en innemen van apparaten te hanteren.

Door dit beleid wordt een stevige basis gelegd voor een toekomstbestendige, veilige en gebruikersvriendelijke digitale leer- en werkomgeving, waarin apparaten betrouwbaar en doelgericht ingezet kunnen worden.

## Reikwijdte

***Toelichting***

*In deze paragraaf beschrijf je de reikwijdte van je beleid. Pas de voorbeeldbeschrijving aan, zodat die past bij jouw organisatie.*

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers en derde partijen die gebruikmaken van – of toegang hebben tot – apparaten van <vul naam schoolbestuur in>. Binnen de scope van dit beleid vallen ook de privéapparaten die gebruikt worden om toegang te verkrijgen tot applicaties of data van de instelling.

Het beleid heeft betrekking op het beheer en gebruik van alle soorten apparaten, waaronder laptops, tablets, smartphones, randapparatuur en overige digitale hulpmiddelen die eigendom zijn van of beheerd worden door <vul naam schoolbestuur in>. Het beleid heeft ook betrekking op apparaten die worden beheerd door externe leveranciers die namens <vul naam schoolbestuur in> optreden.

## Verantwoordelijkheden

***Toelichting***

*In deze paragraaf bepaal je wie er verantwoordelijk is voor het toepassen van de beveiligingseisen uit dit beleid.*

Rollen en verantwoordelijkheden met betrekking tot het toepassen van de beveiligingseisen die voortvloeien uit dit beleid zijn als volgt belegd:

* De **centrale IT-beheerder** past de device-specifieke maatregelen toe.
* De **systeemeigenaar** van het betreffende systeem bepaalt in combinatie met de **proces-eigenaar** of toegang is toegestaan vanaf een unmanaged device en is verantwoordelijk voor het afdwingen van de juiste maatregelen.

|  |  |
| --- | --- |
| **Rol** | **Verantwoordelijkheden** |
| **Eerste lijn** |
| Bestuur, directie, schoolleiding | * Stelt het devicemanagementbeleid vast.
* <Vul aan met verantwoordelijkheden>.
 |
| **Tweede lijn** |
| Proceseigenaar | * Bepaalt met systeemeigenaar of toegang is toegestaan vanaf een unmanaged device.
* <Vul aan met verantwoordelijkheden>.
 |
| Systeemeigenaar | * Bepaalt met proceseigenaar of toegang is toegestaan vanaf een unmanaged device.
* Is verantwoordelijk voor het afdwingen van de juiste maatregelen op systeemniveau.
* <Vul aan met verantwoordelijkheden>.
 |
| Beheerder van de devices | * Past de device-specifieke maatregelen toe.
 |
| IBP’er, CISO, security officer, privacy officer | * <Vul aan met verantwoordelijkheden>.
 |
| **Derde lijn** |
| Functionaris gegevensbescherming | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |
| Interne audit | * Bepaal of deze rol een functie heeft binnen dit proces.
* <Zo ja, vul aan met verantwoordelijkheden>.
 |

# Devices

## Type devices

### Managed devices

Managed devices zijn apparaten die door <vul naam schoolbestuur in> of leveranciers worden geleverd, ingericht, beheerd en beveiligd. Deze devices worden centraal voorzien van updates, beveiligingsinstellingen en toegangsrechten.

### Unmanaged devices

Unmanaged devices zijn apparaten van leerlingen, docenten of bezoekers (Bring Your Own Device: BYOD) die niet centraal worden beheerd door <vul naam schoolbestuur in>.

## Managed & unmanaged devices

***Toelichting***

*Beschrijf hier op basis van welke criteria toegang tot applicaties vanaf unmanaged devices wel of niet wordt toegestaan. Er is hier voor een aantal criteria een voorzet gedaan. Deze kun je zelf aanpassen en aanvullen.*

De afweging of een applicatie vanuit een unmanaged device benaderd mag worden, wordt per applicatie gemaakt op basis van de volgende criteria:

* **Gevoeligheid van de gegevens**.Hoe gevoeliger de applicaties en informatie die via het apparaat worden verwerkt, hoe groter de noodzaak om dit te doen via managed devices.
* **Risico op beveiligingsincidenten**.Hoe groot is de kans op beveiligingsincidenten, zoals datalekken, malware-infecties of verlies/diefstal van apparaten.
* **Beheerbaarheid**.In welke mate is het mogelijk om op afstand updates, configuraties en beveiligingsinstellingen door te voeren?
* **Ondersteuningsbehoefte**.Hoeveel hulp hebben gebruikers nodig bij installatie, updates of probleemoplossing?
* **Kosten en efficiëntie**. Wat is de balans tussen aanschaf- en beheerkosten en de risico’s bij unmanaged gebruik?
* <Vul aan>.

## Registratie van devices

### Managed devices

***Toelichting***

* *Geef hier aan waar managed devices geregistreerd worden. Dit kan binnen het CMDB of andere programma’s die al worden gebruikt, zoals Intune of een overzicht in Excel.*
* *Geef ook aan welke kenmerken worden vastgelegd. Je kunt daarvoor onderstaande eisen overnemen en aanpassen of aanvullen.*

Alle managed devices worden geregistreerd in het centrale devicebeheersysteem van <vul naam schoolbestuur in> vóór uitgifte aan de gebruiker. De registratie bevat minimaal:

* Apparaattype en merk/model
* Beheerstatus: managed/unmanaged
* Serienummer of uniek identificatienummer
* Naam of ID van de toegewezen gebruiker
* Datum van uitgifte en (indien van toepassing) inname
* <vul eisen voor de registratie aan>

De registratie wordt minimaal **jaarlijks gecontroleerd en geactualiseerd**. Bij verlies, diefstal, vervanging of einde gebruik, wordt het apparaat direct afgemeld in het beheersysteem en worden eventuele toegangsrechten ingetrokken.

### Unmanaged devices

***Toelichting***

*Vul in of en waar unmanaged devices geregistreerd worden. De registratie van unmanaged devices hangt af van keuzes die je maakt met betrekking tot beheer. Kies je voor Mobile Application Management (MAM) (zie 3.2, Beveiligingsmaatregelen)? Dan kunnen de unmanaged devices geregistreerd worden binnen de MAM-oplossing.*

<Geef aan op welke manier unmanaged devices geregistreerd worden>.

## Levenscyclus

* *Hier beschrijf je de levenscyclus die een apparaat doorloopt binnen jouw schoolorganisatie. Neem onderstaande stappen over en/of pas ze eventueel aan.*

De levenscyclus beschrijft de fasen die een apparaat en het bijbehorende account doorlopen binnen de schoolorganisatie.

**1. Aanschaf en registratie**

* **Managed devices**: aanschaf via geautoriseerde leverancier. Serienummer en specificaties registreren in MDM-systeem.
* **Unmanaged devices: geen registratie of registratie binnen MAM vanaf stap 2.**

**2. Configuratie en uitrol**

* **Managed devices**: automatische configuratie via MDM: apps, netwerkprofielen, beveiligingsinstellingen.
* **Unmanaged devices**: instructies voor installatie van schoolapps en inschrijving in MAM (indien van toepassing).

**3. Operationeel gebruik**
Continue naleving van beveiligingsmaatregelen (zie 3.2).

**4. Onderhoud**

* Periodieke controles op hardwarestatus, beveiligingsinstellingen en software-updates.
* Eventuele herconfiguratie bij beleidswijzigingen of nieuwe veiligheidsvereisten.

**5. Incidentbeheer**
Aansluiting op het incidentmanagementproces.

* **Managed devices**: remote wipe of blokkering via MDM.
* **Unmanaged devices**: remote wipe van schooldata via MAM.

**6. Terugname en deprovisioning**

* **Managed devices**: terugname aan het einde van gebruiksperiode, volledige datawipe, herinstallatie of veilige recycling.
* **Unmanaged devices**: intrekken van toegang, verwijderen van schoolprofielen en -apps.

**7. Einde levensduur (voor managed devices)**

Veilige fysieke vernietiging of gecertificeerde recycling van hardware.

# Security

## Toegang

***Toelichting***

*In deze paragraaf beschrijf je hoe je als organisatie wilt omgaan met toegang tot schoolapplicaties vanaf managed en unmanaged devices. Bepaal of je gebruik wilt maken van Mobile Application Management (MAM) tools bij het beveiligen van applicaties die toegankelijk zijn vanaf unmanaged devices. Maak je hier gebruik van? Dan is het belangrijk dat je ervoor zorgt dat applicaties alleen via MAM beschikbaar worden gesteld op unmanaged devices.*

### Medewerkers

Medewerkers werken in principe uitsluitend met managed devices. Alleen het bestuur of de ICT-coördinator kan toestemming verlenen. In dat geval is het nodig dat er passende beveiligingsmaatregelen zijn getroffen, zoals gebruik van een beveiligde VDI-omgeving.

### Leerlingen

Leerlingen maken bij voorkeur gebruik van managed devices, vooral als zij werken met onderwijsapplicaties waarin persoonsgegevens worden verwerkt of waar gevoelige processen in voorkomen, zoals het afnemen van toetsen. Unmanaged devices kunnen worden toegestaan voor de toegang tot specifieke onderwijsapplicaties. <naam schoolbestuur> beoordeelt per systeem of toegang vanaf een unmanaged device toegestaan is.

### Externe partijen en bezoekers

Externe partijen en bezoekers mogen uitsluitend gebruikmaken van unmanaged devices via een gescheiden gastennetwerk zonder toegang tot interne systemen of gevoelige data. Hebben externe partijen toegang nodig tot applicaties of systemen die niet beschikbaar zijn vanaf een unmanaged device? Dan wordt tijdelijk een managed device toegekend aan de externe partij.

## Beveiligingsmaatregelen

### Managed devices

***Toelichting***

* *Hier leg je vast welke beveiligingsmaatregelen je neemt om managed devices voldoende te beschermen.*
* *Maak bij applicatiebeheer een keuze voor werken met whitelisting (alleen goedgekeurde applicaties mogen geïnstalleerd worden) of blacklisting (niet-goedgekeurde applicaties worden geblokkeerd).*

<Naam schoolbestuur> implementeert de volgende maatregelen voor managed devices:

* **Volledige device-inschrijving**.Het device wordt geregistreerd in een mobile-device-managementtool.
* **Volledig beheer**. Besturingssysteeminstellingen, updates en patches worden centraal uitgerold.
* **Verplichte encryptie**.Er is verplichte encryptie van opslag (BitLocker, FileVault, Android/iOS native encryptie).
* **Authenticatie**. Er moet minimaal gebruikgemaakt worden van pincode/biometrie en time-out voor schermvergrendeling.
* **Applicatiebeheer**. Er mogen alleen goedgekeurde applicaties worden geïnstalleerd (whitelisting), niet-goedgekeurde apps mogen worden geblokkeerd (blacklisting).
* **Remote wipe**.Het moet mogelijk zijn het apparaatbij verlies, diefstal of einde dienstverband/leerperiode op afstand te wissen.
* **Content filtering**. Webfiltering via een applicatie op het device op basis van leeftijd en beleid.
* **Automatische logging**. Activiteiten en inbreukpogingen worden centraal gelogd.
* **Incidentmanagement**. Incidenten worden volgens het incidentmanagementproces gemeld.

### Unmanaged devices

***Toelichting***

*Hier leg je vast welke maatregelen je neemt om unmanaged devices voldoende te beschermen. In de voorbeeldmaatregelen die hieronder zijn opgenomen is uitgegaan van een toegepaste MAM-oplossing.*

<Naam schoolbestuur> implementeert de volgende maatregelen voor unmanaged devices:

* **Geen volledige devicecontrole**. Devices worden alleen beheerd op app- en dataniveau via MAM.
* **Verplicht schoolaccount**.Elke gebruiker maakt gebruik van een schoolaccount (Microsoft 365, Google Workspace) met multifactorauthenticatie.
* **App-gefocust beleid**. Beveiligingsregels worden alleen toegepast binnen schoolapps (Teams, Outlook, Classroom).
* **Data loss prevention**:
	+ Het kopiëren en plakken naar privéapps wordt geblokkeerd.
	+ Schoolbestanden worden niet opgeslagen in onbeheerde cloudopslag (Dropbox, privé-Google Drive).
* **Remote wipe**. Alleen schooldata wordt verwijderd bij verlies of vertrek. De privédata blijft intact.
* **Wachtwoord/pincode-eis**.Bij toegang tot schoolapps is een wachtwoord of pincode verplicht.
* **Device compliance-check**. Bij toegang tot de MAM-omgeving of applicaties die binnen MAM vallen.
* **In-app encryptie**.Binnen de MAM-omgeving wordt er gebruikgemaakt van encryptie van documenten en e-mail.
* **Voorlichting aan gebruikers**.Gebruikers krijgen voorlichting over veilig gebruik van schooldata op privéapparaten.
* **Incidentmanagement**. Incidenten worden volgens het incidentmanagementproces gemeld.

# Herziening

## Beleidsherziening

***Toelichting***

* *Beschrijf wie er betrokken worden bij eventuele wijzigingsvoorstellen van dit beleid.*
* *Beschrijf met welke interval dit devicemanagementbeleid herzien wordt.*

De eigenaar van het devicemanagementbeleid evalueert <beschrijf hoe vaak> keer per jaar het beleid en stelt verbeteringen voor waar nodig. Hierbij worden <beschrijf wie er betrokken dienen te worden bij eventuele wijzigingsvoorstellen> betrokken. Dit devicemanagementbeleid moet na <vul in welke interval> jaar formeel herzien en goedgekeurd worden door het schoolbestuur.