Collegevoorstel
Openbaar

Onderwerp
Regionaal ‘Mobile Device Management’ beleid

Programma	Bestuur en Organisatie	**Behandeldatum**	10 maart 2026
Portefeuillehouder	T.F.A. van Elferen	**Status**	Openbaar

Advies

1. Een regionaal ‘Mobiel Device Management’ beleid vast te stellen dat voldoet aan de geldende wet- en regelgeving.
2. Daarbij omwille van betere en (kosten) efficiëntere beveiliging van onze ICT-voorzieningen de vier pijlers als uitgangspunt voor dit beleid over te nemen:
    a. Persona gedreven beveiliging
    b. Risico gestuurde toegang per persona
    c. Transparantie en proportionaliteit
    d. Governance en eigenaarschap
3. De financiële consequenties van de MDM-implementatie aan te gaan, waarbij iRvN de implementatie verder zal uitwerken en de kosten 2026 via de eerstvolgende voortgangsmonitor zullen worden meegenomen. De kosten voor 2027 en verder worden meegenomen in de oplading van het begrotingsproces vanaf 2027.
4. De WOR-bestuurder de OR te laten informeren over de inhoud van het beleid en de functionele impact op het gebruik van de diverse apparaten

Aanleiding
De digitale transformatie is ook binnen onze gemeente in volle gang. Medewerkers en bestuur werken steeds vaker hybride, maken gebruik van mobiele apparaten en hebben toegang tot Cloud toepassingen zoals Microsoft 365 en de vele vak applicaties. Deze ontwikkeling biedt kansen voor flexibiliteit en efficiëntie, maar brengt ook risico’s met zich mee. Europees en Nationaal leidt dat tot toenemende wet- en regelgeving waaraan we moeten voldoen. Denk hierbij aan regels rondom de Algemene verordening gegevensbescherming (AVG), de Baseline Informatievoorziening Overheid (BIO) en de Network Information Security guideline 2.0 (NIS2). Het is onontkoombaar om onze digitale werkomgeving beter te beschermen. Daarom stellen we een nieuw regionaal Mobile Device Management (hierna MDM) -beleid voor.

Met dit beleid regelen we wat gebruikers met zakelijke apparatuur mogen doen en welke zakelijke toepassingen vanaf privé apparatuur zijn toegestaan. Dit heeft gevolgen voor het gebruik van de apparatuur door de eindgebruikers. Met het vaststellen van dit beleid komen er beperkingen bij. Denk bijvoorbeeld aan het blokkeren van onveilige apps of websites op een zakelijk device of het gebruik in het buitenland, mocht bijvoorbeeld het land van bestemming op een zwarte lijst staan. Ook het benaderen van zakelijke mail op een privé device wordt anders. Om daar toegang toe te krijgen en te behouden moet met behulp van een extra multifactor authenticatie de identiteit van de gebruiker worden vastgesteld. Ook bij gebruik van een privé apparaat moet het apparaat, de locatie en de gebruiker voldoen aan vast te stellen voorwaarden. Dit is een extra handeling voor de gebruiker, maar noodzakelijk om de werkomgeving te beschermen.

Beoogde impact: kaderstelling
Bij de implementatie van het MDM-beleid worden duidelijke kaders vastgesteld die ervoor zorgen dat het gebruik van mobiele devices voldoet aan de volgende vereisten:

1. Bescherming van gemeentelijke data, inclusief de persoonsgegevens van inwoners, tegen verlies, diefstal en ongeautoriseerde toegang.
2. Naleving van wet- en regelgeving om juridische risico's en aansprakelijkheid te minimaliseren.
3. Regionale afstemming van het MDM-beleid met centraal beheer en configuratie zodat de beheerlast niet onnodig toeneemt en waar mogelijk de eindgebruikers niet onnodig veel extra handelingen hoeven uit te voeren.
4. Mogelijkheid om devices op afstand te vergrendelen en/of te wissen, om de veiligheid te vergroten.
5. Scheiding van zakelijke informatie en persoonlijke data om privacy te waarborgen.

Hoewel dit MDM-beleid een regionale insteek kent past het nemen van de genoemde maatregelen ook binnen de ambitie een betrouwbare en omgevingsbewuste gemeente te zijn in onze eigen doelenboom. De maatregelen dragen bij aan het doel ons werk zorgvuldig, slagvaardig en volledig uit te voeren. Veiligheid is daarin een belangrijk criterium en het door ontwikkelen van onze interne digitale werkomgeving een van de kernactiviteiten.

Argumenten

1. *Met dit beleid zorgen we ervoor dat we aan wet- en regelgeving voldoen*
   Dit beleid zorgt ervoor dat we voldoen aan recente wet- en regelgeving. Een deel van deze wet- en regelgeving (NIS2, Cyberbeveiligingswet, en BIO2) voorziet in bestuurdersaansprakelijkheid.

2. *Met het overnemen van het regionaal MDM-beleid zorgen we voor een betere en (kosten) efficiëntere beveiliging van onze ICT-voorzieningen gebaseerd op vier pijlers:*
   Een gezamenlijk beleid biedt de kans om zo (kosten)efficiënt mogelijk de beveiliging van onze systemen en informatie in te regelen. Technisch maatwerk per organisatie is mogelijk, maar voor het geheel van de IRvN een inefficiënte en – binnen de huidige kostenverdeelsleutel – een kostbare oplossing voor alle organisaties. Daarbij kan gefragmenteerd beleid leiden tot het principe van de zwakste schakel in de beveiligingsketen van alle betrokken organisaties in de ICT-samenwerking. Daarom stellen we een gezamenlijk beleid voor gebaseerd op de volgende pijlers:
   a. *Met persona-gedreven beveiliging zorgen we voor proportionele maatregelen.*
      Niet elke gebruiker heeft dezelfde digitale risico's. Bestuurders, raadsleden, medewerkers, IT-beheerders en externen hebben verschillende rollen en verantwoordelijkheden. Daarom adviseren we een indeling in persona's, waarbij de beveiligingsmaatregelen worden afgestemd op het risicoprofiel van de gebruikersgroep. Daarbij kunnen we aan specifieke rollen een hoger veiligheidsniveau toewijzen. Dit

wordt gedaan in overleg met de CISO's en de FG's van de betreffende deelnemende gemeenten.

b. *Risico gestuurde toegang per persona*
Risico gestuurde toegang per persona zorgt voor optimale digitale weerbaarheid. Toegang tot gemeentelijke systemen, zoals Citrix, I-Babs en andere applicaties, wordt alleen verleend als het apparaat, de locatie en de gebruiker voldoen aan vooraf vast te stellen voorwaarden. Dit voorkomt misbruik en verhoogt de digitale weerbaarheid.

c. *Transparantie en proportionaliteit*
We monitoren het gebruik van apparaten en applicaties, maar doen dit proportioneel, transparant en niet ongevraagd. Bijvoorbeeld bij verlies/diefstal wordt het apparaat uitgelezen of op afstand leeg gemaakt. Zijn er problemen met de apparatuur dan moet de gebruiker toestemming geven dat het device wordt overgenomen door een systeembeheerder. Gebruikers worden geïnformeerd over wat we monitoren.

d. *Governance en eigenaarschap*
De specifieke regels voor de inrichting en het beheer van de IT-systemen ligt bij iRvN. De kaders van dit beleid zijn vooraf door de diverse gremia meegegeven. Met dit beleid worden de kaders door de deelnemers vastgesteld. De governance blijft zoals die is: lokaal bestuurlijk, centraal technisch.

3. *Door de financiële consequenties van MDM-implementatie (vooralsnog ingeschat op € 190 per gebruiker per jaar) aan te gaan zorgen we ervoor dat deze met de eerstvolgende begrotingswijziging zullen worden meegenomen.*
De nieuwe maatregelen zijn nodig om onze digitale weerbaarheid te vergroten. Dit doen we door risicoprofielsegmentatie toe te passen, de logging en monitoring 24/7 te organiseren en te voldoen aan de extra toegangseisen. IRvN zal de implementatie uitwerken. De kosten zijn ingeschat op structureel €1,1 miljoen en incidenteel op € 268.800.

4. *Door in te stemmen met het verzoek aan de WOR-bestuurder zorgen we ervoor dat de OR geïnformeerd wordt over de inhoud van het beleid en de functionele impact op het gebruik van de zakelijke apparaten*
Zakelijke smartphones, laptops en tablets worden nog steeds door de werkgever verstrekt. Met dit voorstel worden vanuit zakelijk oogpunt beperkingen toegevoegd wat je met de diverse zakelijke devices kunt doen. Het betreft geen grote inhoudelijke wijziging van de huidige secundaire arbeidsvoorwaarden, wel een inperking van bijvoorbeeld gebruik van apps zoals TikTok of websites die niet veilig worden bevonden en die je dan niet meer kan benaderen.

Kanttekeningen

Effect op gebruiksvriendelijkheid

Met dit beleid regelen we wat gebruikers met zakelijke apparatuur mogen doen en andersom. Daarnaast gaan we monitoren welke apps er op zakelijke telefoons, tablets en laptops staan. Als dit beleid wordt ingevoerd, heeft het beperkte gevolgen voor de gebruiksvriendelijkheid van de zakelijke devices en de toegang tot zakelijke apps op privé devices. Voorbeeld: als iemand toegang wil tot MS365 op zijn privé device, dan kan dit

alleen als de persoon is geïdentificeerd. Hiervoor maken we gebruik van multifactor – authenticatie welke een extra handeling van de gebruiker zal afdwingen.

Openbaarheid
Regionaal is afgesproken dat de bijlagen bij het onderliggende beleidsstuk niet openbaar zijn. In de bijlagen staan beveiligingsmaatregelen genoemd die we als vertrouwelijk beschouwen. Dit collegevoorstel en het beleidsstuk zelf zijn wel openbaar.

Gesprek met de stad
Er heeft geen gesprek met de stad plaatsgevonden. Het betreft de interne bedrijfsvoering.

Communicatie
Na vaststelling van het beleid zal de WOR-bestuurder de OR informeren over inhoud en functionele impact van het MDM-beleid. De fasering en uitrol is na vaststelling van dit stuk in handen van de IRvN en zal gefaseerd over de deelnemers plaatsvinden. Communicatie verloopt dan ook via de IRvN.

Financiën
De kosten die gemoeid zijn met de implementatie van het MDM-beleid zullen naar schatting €190,- per gebruiker per jaar zijn. Dit is gebaseerd op een verdeling van de totaal benodigde investering over de 5600 regionale gebruikers, zowel medewerkers als bestuurders. Na vaststelling van het MDM-beleid zal IRvN met de planvorming en de realisatie gaan starten. De meerkosten krijgen een plek in de begroting van de MGR en worden via de huidige verdeelsleutel aan u doorbelast. De verwachting is dat de eenmalige implementatiekosten van €268.800 via de reguliere verdeelsleutel zullen worden doorbelast aan alle deelnemers. Voor Nijmegen betekent dit een bedrag van circa € 155.000 voor de implementatie in 2026. De structurele kosten zijn nu begroot op € 632.000 voor Nijmegen (peildatum maart 2026). Deze kosten zullen via een melding in de voortgangsmonitor worden opgevoerd, gezien de noodzaak om onze digitale weerbaarheid op korte termijn te versterken. De structurele kosten vanaf 2027 en verder worden meegenomen in iRvN begroting en wordt vervolgens opgeladen in het begrotingsproces 2027.

Vervolg
De input van het Portefeuilehoudersoverleg (PFO) Digitalisering, de Kring van Gemeentesecretarissen, het Regionaal Strategisch ICT Overleg (RSiO), het Regionaal Tactisch ICT Overleg (RTiO), het CISO-overleg en het FG-overleg is reeds verwerkt. De feedback van de Kring van Griffiers is besproken en wordt meegenomen bij de uitrol van dit beleid en het verstrekken van de devices aan raads- en commissieleden.
De griffie kan door de IRvN worden ondersteund bij informatie, toelichting en implementatie van dit beleid op de devices van raads- en commissieleden.

De tijdlijn zal er verder als volgt uit zien;

1. Regionale bestuurlijke vaststelling van het beleidskader;
    a. Kaderbrief MGR- iRvN (december 2025)
    b. Zienswijzen gemeenteraden (jan/feb 2026)
    c. Begroting MGR-iRvN 2027 (apr 2026)
    d. Zienswijzen gemeenteraden (jul 2026)
    e. Besluitvorming MGR (aug 2026)

    f. Vertaling in de Programma begroting (nov 2026)
2. Opstellen basis van plan van aanpak en uitwerkingen door projectgroepen techniek, privacy & beveiliging, adoptie (apr-dec 2026)
3. Meenemen medewerkers en bestuur informeren (dec 2026 – jan 2027)
4. Technische implementatie (vanaf jan 2027).
5. Uitvoering communicatie en adoptieplan (vanaf jan 2027)

Aan IRvN wordt de opdracht verstrekt het MDM-beleid samen met de gemeenten uit te laten werken en te implementeren. Het PFO Digitalisering, de Kring van Gemeentesecretarissen, het RSiO en RTiO worden bij de uitwerkingen betrokken.

Bijlage(n)

1. Regionaal MDM-beleid versie 1.4
2. Regionaal MDM-beleid versie 1.4 bijlagen