Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER BESPREKING

Nota actief openbaar
ja

Aan -
Van CIO Rijk

Onze referentie
2025-0000237148

Datum
25 oktober 2024

Opgesteld door
[redacted]

Samengewerkt met

Bijlage(n)
0

nota

Appbeleid

Colofon

Naam	App-beleid
Type	Beleid
Status	Finaal
Versie	1.0
Vastgesteld door	CIO-rijk
Datum vaststelling	ntb
Beheer	CIO Rijk
Contact	CIORijk-IB&P@minbzk.nl

Versiebeheer

Versie	Omschrijving
0.1	Versie besproken in eerste rijksbrede workshop
0.3-0.5	Versies besproken met de werkgroep
0.6	Versie besproken in tweede rijksbrede workshop
0.65	Versie besproken met bestuurlijke en politieke lijn
0.7	Versie besproken in gremia
0.81	Versie voor nieuwe aanbieding aan gremia
0.82	Versie met verwerkte opmerkingen CISO-raad okt '24
1.0	Versie aangenomen door ICBR

0. Uitgangspunten

Bij het opstellen van dit beleid zijn de volgende uitgangspunten gehanteerd:

Uitvoerbaarheid is essentieel
De inhoud van het beleid moet goed uitvoerbaar zijn. Om dit te bewerkstelligen zijn de SSO's betrokken en ontwikkelen we parallel met het beleid ook de handreikingen, de allowlist en de toetsingsleidraad.

Risicogebaseerde uitrol van appbeleid
Eerdere versies van het appbeleid hadden als doel om het beleid in één keer uit te rollen voor de mobiele apparaten voor álle rijksambtenaren. In de behandeling van dit conceptbeleid in de gremia (CTO-, CISO- en CIO-raad) bleek echter dat deze grootschalige aanpak de uitvoerbaarheid in de weg zat. Dit nieuwe conceptbeleid geeft gehoor aan het voorstel vanuit de CIO-raad om **een risico-gebaseerde aanpak te nemen, waarbij dit appbeleid in**

eerste instantie alleen wordt uitgerold voor zogenaamde hoogrisicoambtenaren. Deze term worden verderop toegelicht bij paragraaf 1.4 Definities. De ervaringen die worden opgedaan met de uitrol van het appbeleid voor deze kleinere groep ambtenaren met verhoogd risicoprofiel, kunnen later worden gebruikt om het appbeleid naar een bredere groep rijksambtenaren uit te rollen.

Goede professionele ondersteuning: voorkomen van Shadow IT
De medewerkers krijgen alle apps die ze nodig hebben om hun werk te doen. Dit voorkomt dat medewerkers zelf oplossingen bedenken en ook inzet van privé apparatuur voor zakelijk gebruik.

Regime: Comply or explain
Het beleid stelt centrale kaders die rijksbreed gelden voor hoogrisicoambtenaren. De rijksorganisaties hebben eigen eindverantwoordelijkheid rondom IT, informatiebeveiliging en privacy. Het beleid is verplicht met een comply-or-explain regime

Doelstelling: risicobeheersing via allowlist
Doel van het beleid is risicobeheersing rondom app-gebruik: spionage risico's, beveiligingsrisico's en privacy-risico's. De gekozen technische richting is de allowlist: je reduceert het aantal apps en je beoordeelt de apps op risico's. Conform het vorige uitgangspunt zijn hier explains op mogelijk.

1. Scope

1.1 Dit beleid is van toepassing op de Rijksdienst en door het Rijk verstrekte mobiele apparatuur. Voor organisaties van de overheid die geen onderdeel zijn van de rijksdienst geldt dit beleid als advies.

1.2 Het opknippen van de uitrol tussen in eerste instantie hoogrisicioambtenaren zorgt ervoor dat er vooralsnog niets verandert voor de rest van de rijksambtenaren. Pas na een positieve evaluatie van deze eerste uitrol Q1 2025 kunnen we gaan bepalen of en wanneer andere groepen ambtenaren aan de beurt zijn, of dat we wellicht de groep moeten inperken.

1.3 Buiten scope vallen:
Mobiele apparatuur van externe dienstverlenende organisaties en andere zakelijke partners van de rijksoverheid.

1.4 Definities

Apps
Apps zijn applicaties voor mobiele devices **inclusief** de onderdelen waar ze uit bestaan: de functionaliteiten zelf, de software development kit (SDK) en de software libraries.

Hoogrisicoambtenaren
Dit is een groep ambtenaren die door hun profiel aantrekkelijk worden geacht voor spionage door bijvoorbeeld statelijke actoren en Advanced Persistent Threats (APT's – groepen cybercriminelen met sterke banden met statelijke actoren). Mobiele apparaten en de apps kunnen door dezen worden misbruikt voor spionage, wat de grondslag voor dit appbeleid vormt.
Concreet zijn hoogrisicoambtenaren leden van de Algemene Bestuursdienst en

ambtenaren in een vertrouwensfunctie met een Verklaring Geen Bezwaar (VGB) B, A en A+ zoals uitgegeven door de AIVD en MIVD.
Het staat organisaties ook vrij om andere medewerkers aan te merken als hoogrisicoambtenaar.

Landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen
Landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen zijn onder meer opgesomd in de 'Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland' van de AIVD[1]. Omdat dat kan wijzigen wordt in dit document alleen naar dat document verwezen.

Mobiele devices
Mobiele devices betreffen doorgaans mobiele telefoons, laptops en tablets. In de context van beleid gaat het alleen om smartphones en tablets. Zakelijke laptops worden al integraal beheerd. Eenvoudige mobiele telefoons, dus geen smartphones, zijn zeer beperkt aan deze risico's onderhevig.

Managed devices
Managed devices zijn mobiele devices die met behulp van zogenaamde Mobile Device Managementooling (MDM-tooling) beheerd worden. In het kader van dit beleid is het daarbij van belang dat de MDM-tooling ten minste in staat is om een allow-list te handhaven en het gebruik en het installeren van niet-toegestane apps te blokkeren.

Spionage-achtige apps
De AIVD heeft in de 'Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland'[2] aangegeven dat het gebruik van apps en mobiele devices inherente spionage risico's met zich meebrengt. Spionage-achtige apps in dit beleid zijn apps afkomstig uit de landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen die, al dan niet transparant, toegang hebben tot de gegevens op het devices en sensoren zoals de camera's, microfoon en de GPS.

Zakelijke apparatuur
Apparatuur die eigendom is van de werkgever en de medewerker ter beschikking wordt gesteld om zijn werkzaamheden mee uit te voeren.

2. Doel

Iedere rijksorganisatie beperkt risico's rondom het gebruik van apps, waaronder spionage, privacy en securityrisico's. Voor dit doel is er ten minste een lijst met apps die niet ingezet mogen worden (zie art. 3) en wordt er gezorgd dat alleen vooraf goedgekeurde apps mogen worden ingezet (zie art. 4).

2.1 Impact op Bring Your Own Device

[1] Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland | Brief | Rijksoverheid.nl
[2] Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland | Brief | Rijksoverheid.nl

Gelet op de implementatie van het Appbeleid bij hoogrisicoambtenaren en de steeds meer toenemende dreigingen in het mobiele landschap is het raadzaam een eventueel BYOD-beleid te heroverwegen.

3. Niet in te zetten apps

3.1 Apps van bedrijven uit landen met een offensief cyberprogramma gericht tegen Nederland en/of Nederlandse belangen zijn niet toegestaan.

3.2 Uitzondering op 3.1 is wanneer een applicatie nodig is voor het uitoefenen van een primaire taak van een rijksorganisatie. Hierbij kan gedacht worden aan inspectie en toezicht, opsporingsonderzoek of inlichtingenbelang.

3.3 Indien een rijksorganisatie gebruik maakt van de uitzonderingsgrond onder 3.2, maken ze daarvoor een door de CIO vastgestelde uitleg (explain). De explainprocedure wordt toegelicht in hoofdstuk 4 van de BIO. Daarvoor gelden de volgende eisen:

- Er is een door de directie van de rijksorganisatie vastgestelde risicoanalyse waarover de (departementale) CISO geadviseerd heeft.
- In die analyse wordt uiteengezet:
  - Waarom de app noodzakelijk is voor de taken van de organisatie;
  - Welke risico's er zijn waaronder spionage-achtige risico's; en
  - Welke maatregelen worden genomen om de risico's te beheersen.
- De vastgestelde analyse wordt gedeeld met de CISO Rijk zodat zij haar monitorende rol kan uitvoeren en de uitzondering en de onderbouwing kunnen worden meegenomen in de evaluatie van het beleid.

4. Vooraf goedgekeurde apps

4.1 CIO Rijk stelt een rijksbrede basis allowlist vast en maakt daarbij gebruik van input vanuit de rest van rijksoverheid. Hierbij maakt CIO Rijk een afweging aan de hand van de volgende selectiecriteria:

- Er is functionele noodzaak voor de app;
- Er is geen bruikbaar alternatief in de vorm van een (voor mobiel gebruik geoptimaliseerde) website die dezelfde functionele behoefte invult;
- Er is geen standaard platform app (zoals de rekenmachine app) die een bruikbaar alternatief is;
- Er is aandacht voor de privacyaspecten waarbij ten minste beoordeeld wordt of de permissies die app vraagt en de verwerkingsdoelen proportioneel zijn voor het doel waarvoor de app wordt ingezet
- De risico's van de app en de leverancier zijn in relatie tot het belang van de app in voldoende mate beoordeeld en beheerst met inachtneming van het bepaalde in 3.1.
- Er is beoordeeld dat, indien nodig, de app voldoet aan andere wet- en regelgeving zoals de Woo en de Archiefwet.
- CIO Rijk en de rijksorganisaties geven bij inzet van apps ook aandacht aan publieke waarden waaronder open source, mensenrechten en duurzaamheid.

De bovenstaande criteria zijn niet zwart-wit, maar er is sprake van een zorgvuldige afweging.

4.2 Rijksorganisaties stellen zelf hun organisatiespecifieke allowlist vast met aanvullingen en inperkingen ten opzichte van de rijksbrede basis allowlist en met inachtneming van het bepaalde in artikelen 3 en 5. Ze hanteren hierbij ten minste dezelfde selectiecriteria als in 4.1.
De organisatiespecifieke allowlist wordt in ieder geval afgestemd met de (departementale) CISO of iemand die hiertoe gedelegeerd is. Organisaties zijn zelf in staat om te bepalen op welk niveau het toevoegen (of verwijderen) van een app afgestemd dient te worden.

4.3 CIO Rijk faciliteert en stimuleert samenwerking op dit gebied voor effectiviteit en efficiëntie bijvoorbeeld door oprichten van een community van experts.

4.4 De organisatiespecifieke allowlist wordt technisch geborgd met volledig managed devices.

4.5 Indien organisaties een andere methodiek toepassen dan onder 4.4 beschreven methodiek maken ze daarvoor een door de bestuurder vastgestelde uitleg (explain). Daarin worden ten minste de volgende vragen beantwoord:
- Hoe wordt geborgd dat alleen vooraf goedgekeurde apps worden ingezet;
- Hoe worden de risico's van spionage-achtige apps beheerst.

4.6 Nieuwe apps worden aangevraagd op de reguliere wijze voor ICT-middelen. De ICT-serviceorganisatie controleert of de aanvraag aan de selectiecriteria voldoet, zie 4.1, en maakt de app beschikbaar (voor de aanvrager of algemeen). De ICT-serviceorganisatie legt periodiek de toevoegingen en verwijderingen voor aan de CISO inclusief onderbouwing. Dit stelt de CISO in staat om daar desgewenst op bij te sturen..

5. Aanwijzingen CISO Rijk

Op grond van artikelen 13 en 14 uit het 'Besluit CIO-stelsel Rijksdienst 2021[3]' kan de CISO Rijk indien nodig apps aanwijzen als niet te gebruiken. Hierbij geldt onverminderd het hiervoor bepaalde in art. 3.2

6. Planning en governance

6.1 Departementen en hun dienstonderdelen maken zelf een plan en planning voor de implementatie van het beleid.

6.2 Als uitgangspunt geldt dat de implementatie uiterlijk 2 jaar na vaststelling van het beleid afgerond is.

6.3 Indien die planning niet haalbaar is, stellen de organisaties een door de CIO vastgestelde uitleg (explain). Hierin wordt ten minste ingegaan op de volgende aspecten:
- Waarom de planning niet haalbaar is;
- Een alternatieve planning;
- Te nemen tussentijdse beheersmaatregelen.

6.4 De voortgang van de implementatie wordt door de departementen en hun dienstonderdelen initieel halfjaarlijks gerapporteerd aan de CIO Rijk en

[3] Besluit CIO-stelsel Rijksdienst 2021 | Besluit | Rijksoverheid.nl

vervolgens jaarlijks. CIO Rijk zal met de departementen hiervoor een compact rapportage format opstellen.

6.5 De organisatiespecifieke allowlist wordt ten minste jaarlijks geëvalueerd ten opzichte van de selectiecriteria, dan wel vaker bij belangrijke wijzigingen in een app, zoals een nieuwe eigenaar.

6.6 Jaarlijks sturen de rijksorganisaties hun organisatiespecifieke allowlist naar de CIO-Rijk. CIO-Rijk gebruikt dit om de rijksbrede basis allowlist te evalueren en bij te stellen.

6.7 CIO Rijk herziet ten minste 2-jaarlijks het beleid, dan wel CIO Rijk stelt vast dat herziening nog niet nodig is. CIO Rijk past het beleid aan in rijksbrede samenwerking en vaststelling via de reguliere lijnen.