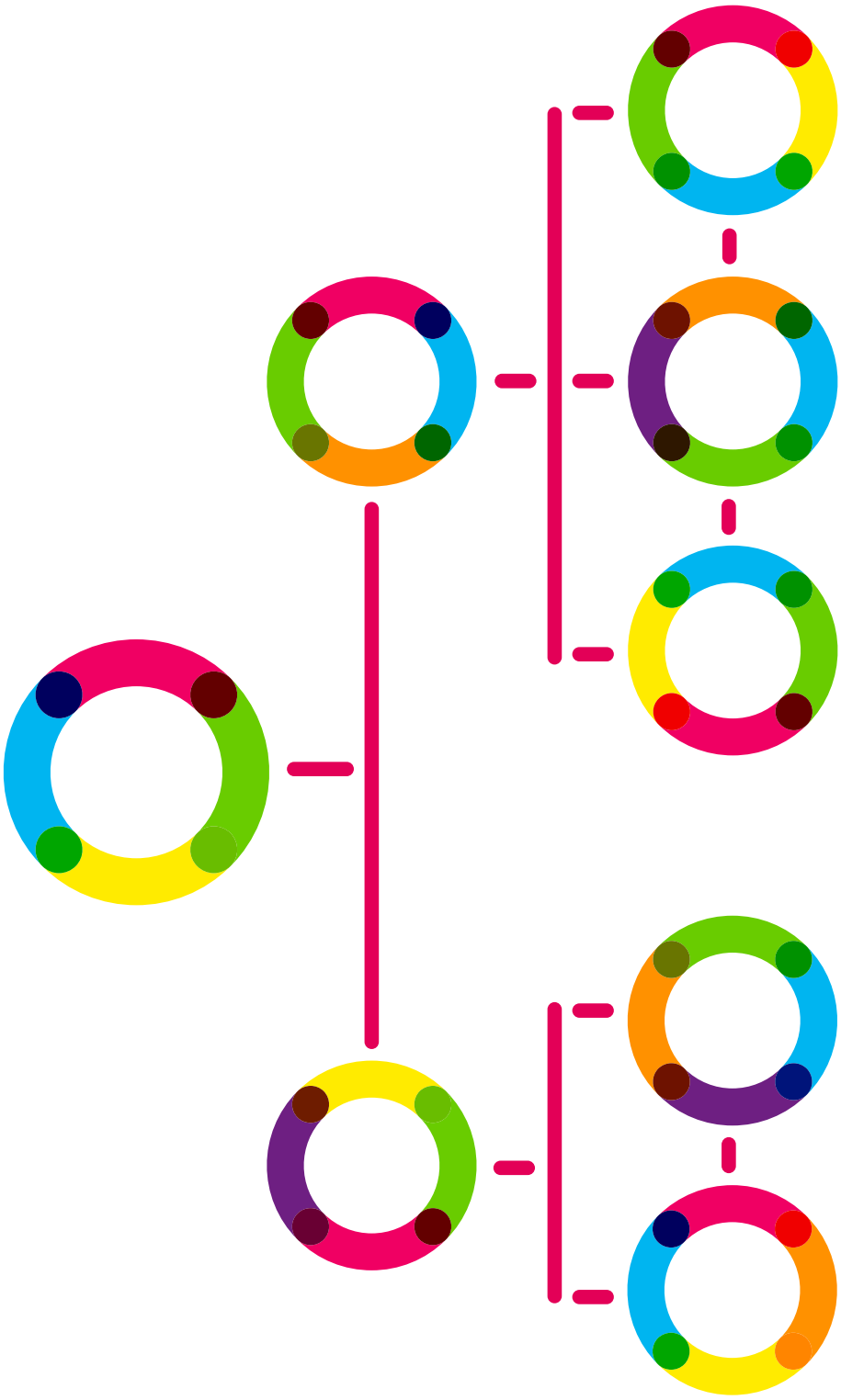

Beleid mobile device management 2024-2027

Gemeente *Stein*

Versiebeheer

Datum	Versie	Wie	Omschrijving
10-09-2016	0.1	CISO	Basisdocument
02-11-2016	1.0	CISO	Opzet en tekstuele aanpassingen
15-02-2024	2.0	CISO	Actualisatie volledig beleidsdocument

Inhoudsopgave

1. Inleiding

Medewerkers krijgen steeds meer mogelijkheden om informatie in te zien of te verwerken op afstand. Dit kan erg handig zijn als bijvoorbeeld medewerkers buiten het gemeentehuis informatie moeten inzien of als er bijvoorbeeld thuis gewerkt wordt. Na een aantal jaren ervaring op te hebben gedaan met het werken met mobiele apparaten is er meer inzicht in de behoeften en benodigdheden van medewerkers. Technische ontwikkelingen bieden ons daarnaast mogelijkheden om hier beter bij aan te sluiten.

1.1 Doelstelling mobile device management

Mobiele apparaten (vaak ook mobile devices genoemd) zoals smartphones, tablets en laptops worden veel gebruikt om gemeentelijke informatie in te zien of te verwerken. Dit heeft enerzijds te maken met de informatiesamenleving en het feit dat gemeenten steeds meer digitaal gaan werken, aan de andere kant verandert het concept van werken waarbij steeds meer tijd- en plaats onafhankelijk gewerkt wordt. Het is belangrijk om beleid vast te leggen om de risico's van de data op de mobiele apparaten in kaart te brengen en hiervoor maatregelen te treffen.

Het is belangrijk veilig om te gaan met mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan, omdat:

- Mobiele apparaten malware- en virus besmettingen kunnen oplopen en daarmee ook andere apparatuur van de gemeente kunnen infecteren (het mobiele apparaat wordt door hackers als aanvalsvector gebruikt);
- Mobiele apparaten die gebruik maken van onveilige (publieke/ openbare) wifi kunnen worden afgeluisterd;
- Mobiele apparaten (persoons) gegevens bevatten en doorgaans buiten de gemeentelijke gebouwen zijn. Deze (persoons) gegevens kunnen zoekraken of worden ingezien door onbevoegden. Dit kan een datalek tot gevolg hebben.
- Mobiele apparaten door malware hoge SMS verbruik en telefoonkosten kunnen veroorzaken;
- Mobiele apparaten kunnen zoekraken of gestolen worden (vervangschade en inzien van gegevens);
- Mobiele apparaten kunnen worden gebruikt om gemeentelijke systemen te benaderen (privacy, bewerken gegevens).

Dit beleidsdocument verwoordt de concrete beleidsregels die nodig zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen de gemeente Stein en op de beschikbaar gestelde mobiele apparaten te beschermen. Dit document bevat onder andere informatie over het gebruik en beheer van zowel de hardware als de software en welke beveiligingsmaatregelen hierbij worden genomen.

Het doel van dit beleid is te voorkomen dat de dienstverlening van de gemeente hinder ondervindt in het geval er gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur en hardware plaatsvindt.

1.2 Toepassingsgebied

Dit document is van toepassing op alle medewerkers werkzaam voor de gemeente Stein die gebruik maken van mobiele apparaten met daarop toegang tot de gegevens van de gemeente en toegang tot onze gemeentelijke informatiesystemen.

1.3 Te behalen resultaten

Door dit beleid te volgen wil de gemeente de volgende resultaten bereiken:

- Het minimaliseren van risico's rondom het gebruik van mobiele apparaten en de gegevens die hierop staan.
- Voldoen aan de wettelijke plicht uit de Algemene Verordening Gegevensbescherming, de Uitvoeringswet Algemene Verordening Gegevensbescherming en de Wet Politiegegevens waarbij de gemeente passende technische en organisatorische maatregelen moet treffen voor de veiligheid van (persoons)gegevens.
- Voldoen aan de normen uit de Baseline Informatiebeveiliging Overheid (BIO).
- Een cultuur waarin iedere medewerker veilig gebruik kan maken van een mobile device.
- Duidelijkheid over de rollen, taken en verantwoordelijkheden.
- Zorgen voor een efficiënte en effectieve procesgang rondom de uitgifte van mobile devices.

1.4 Verantwoordelijkheden

De gemeentesecretaris is eindverantwoordelijk voor de naleving van dit beleid. Het beheer en de uitvoering van dit document ligt bij de CISO en team Informatiemanagement. De Functionaris Gegevensbescherming heeft een adviserende en toezichthoudende taak. Iedere medewerker dient zich te houden aan de in dit document beschreven en daaruit voortvloeiende instructies.

1.5 Herziening

De gemeente hanteert sinds 2016 regels rondom mobile devices. Wegens de vele ontwikkelingen rondom mobile device management vervangt dit beleidsdocument, bij vaststelling door het college van Burgemeester en Wethouders de notitie Mobile Devices 2016-2018. Wegens de controlerende aspecten in dit beleid rondom medewerkers is er een instemmingsaanvraag bij de OR gedaan alvorens deze is vastgesteld door het college.

Uitleg van begrippen

2. Uitleg van begrippen

Medewerker
Burgemeester, wethouders, gemeenteraadsleden, commissieleden op grond van de gemeentewet en alle overige medewerkers werkzaam binnen de gemeente Stein (waaronder intern, inhuur etc.).

Gebruiker
Leveranciers of personen die in samenwerking met of in opdracht van de gemeente werkzaamheden uitvoeren en hiervoor tijdelijk een mobile device ter beschikking wordt gesteld.

Mobile devices
Een mobiel apparaat dat zich kenmerkt door een computer functionaliteit waarop applicaties beschikbaar zijn. Hiermee kunnen via mobiel internet of wifi informatiesystemen benaderd worden. Hieronder vallen bijvoorbeeld mobiele telefoons, laptops, tablets en smartwatches.

Beveiligingsincident
Een beveiligingsincident is een inbreuk op onze beveiliging, waarbij de beschikbaarheid, integriteit of de vertrouwelijkheid van informatie in gevaar is of kan komen.

Datalek
Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

2 factor authenticatie
Een authenticatie methode waarbij je twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen. Naast het traditionele wachtwoord moet je een extra code invoeren (per SMS of app).

Baseline Informatiebeveiliging Overheid (BIO)
De BIO is een uniform normenkader voor de beveiliging van de informatiehuishouding van alle overheidsorganisaties.

Encryptie
Het versleutelen van gegevens op basis van een willekeurige code. Wegens de complexiteit van deze versleuteling kan er niemand meer bij de gegevens.

Zero footprint
Er worden geen gegevens opgeslagen op het apparaat zelf.

Beleidsregels mobiele apparaten

3. Beleidsregels mobiele apparaten

3.1 Mobile Device management

Mobile Device Management (MDM) is het stelsel van maatregelen, procedures en ondersteunende producten die het mogelijk maken om mobiele apparaten veilig te kunnen gebruiken en te kunnen beheersen. MDM is van toepassing op de volgende mobiele apparaten waar gemeentedata op wordt verwerkt. Gemeente Stein maakt in haar bedrijfsvoering gebruik van:

- Smartphones
- Tablets
- Laptop
- Computer

Ten behoeve van Mobile Device Management dienen er regels binnen de gemeente te zijn die gehanteerd moeten worden als er mobiele apparaten worden gebruikt. Zo dient alle (mobiele) apparatuur in gebruik bij de gemeente bij team Informatiemanagement bekend en geregistreerd te zijn in de MDM beheeromgeving. Mobiele apparaten dienen altijd te zijn voorzien van de laatste updates en beveiligingsinstellingen (zie hiervoor paragraaf 4.2.)
Met MDM-tooling kan de gemeente hiervoor zorgdragen.

3.2 Mobile Application Management

Anders dan Mobile Device Management, richt Mobile Application Management (MAM) zich meer op de uitrol, inrichten en configuratie van software op apparaten. MAM-software zorgt ervoor dat data in een container (aparte omgeving) staat en niet lokaal wordt opgeslagen. De gemeente beheert die container en daarmee de zakelijke gegevens die hierin staan. Hiermee hoeft niet een volledig device te worden gemanaged. Met het gebruik van MAM software worden gemeentelijke gegevens opgeslagen in een container. Deze kunnen op afstand worden gewist zonder de privé gegevens van de gebruiker mee te nemen. Wanneer er gebruik wordt gemaakt van een privé apparaat, wordt er alleen een MAM omgeving op het apparaat geïnstalleerd.

Ondernemingsraad
Voor MAM-tooling is op grond van artikel 27, eerste lid, onder K en l, van de Wet op de Ondernemingsraden instemming van de ondernemingsraad (OR) nodig.

3.3 Beheer mobiele apparaten

Wegens de (toenemende) beveiligingsrisico's bij het gebruik van mobiele apparaten en de (persoons)gegevens die hierop worden verwerkt stelt de gemeente een mobiel apparaat zoals een smartphone, laptop en tablet beschikbaar aan alle medewerkers voor de uitvoering van hun werkzaamheden. Deze mobiele apparaten worden beheerd door de gemeente. In de BIO is in norm 6.2.1 de verplichting opgenomen dat de gemeente vastgesteld beleid behoort te

hebben om de risico's die het gebruik van mobiele apparatuur met zich mee brengt te beheren.

In norm 6.2.1.1 is daarnaast de verplichting opgenomen dat mobiel apparatuur zo is ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Wanneer zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, worden deze gegevens versleuteld. In het geval van opslag van vertrouwelijke informatie moet op mobiele apparatuur 'wissen op afstand' mogelijk zijn.

Omdat er geen beheer mogelijk is op privé toestellen zonder hierbij mogelijk de privacy te schenden van de gebruiker, stelt de gemeente altijd een mobiel apparaat beschikbaar. Alleen in uitzonderlijke situaties is het mogelijk om gebruik te maken van een eigen privé toestel. De direct leidinggevende van de medewerker of team Informatiemanagement dient altijd schriftelijk toestemming te geven voor het gebruik van een privé apparaat met de onderbouwing waarom hiervoor wordt gekozen.

4. Uitgangspunten

De uitgangspunten die gehanteerd worden in dit beleid 'Mobile device management' zijn ontleend aan de Baseline Informatiebeveiliging Overheid (BIO).

4.1 Gebruik van mobiele apparaten

1. Het gebruik van mobiele apparaten door de medewerker is primair ten behoeve van het vervullen van de taak of functie. Mobiele apparaten mogen door de medewerker privé gebruikt worden mits men veilig, zorgvuldig en integer om gaat met het apparaat én gegevens van de organisatie.

2. In sommige situaties is het mogelijk om tijdelijk een mobiel apparaat ter beschikking te stellen aan een leverancier of persoon die in opdracht van of in samenwerking met de gemeente werkzaamheden uitvoert. Deze gebruiker dient vooraf altijd een geheimhoudingsverklaring te tekenen en in de gelegenheid te worden gesteld kennis te nemen van het beleid Mobile Devices van de gemeente Stein. De medewerker die de aanvraag bij team Informatiemanagement in dient, is verantwoordelijk voor het vooraf laten tekenen van de geheimhoudingsverklaring en het informeren over de uitgangspunten in dit beleid. De geheimhoudingsverklaring maakt onderdeel uit van het contract en dient door de contracteigenaar hierbij te worden gearchiveerd.

3. Het is verplicht om op de laatste werkdag[1] de mobiele apparaten met de toegangsdruppel, lockersleutel in goede staat en werkend te retourneren inclusief alle toebehoren. De direct leidinggevende is verantwoordelijk voor het maken van afspraken hierover met de medewerker.

[1] Onder de laatste werkdag valt de dag waarna er geen werkzaamheden meer voor de gemeente Stein worden uitgevoerd. Dit kan dus afwijken van de daadwerkelijke uitdienstdatum.

4. Ter beschikking gestelde mobiele apparaten mogen alleen door de medewerker/ gebruiker zelf worden gebruikt.

5. Reparaties aan en opening van apparatuur mag uitsluitend door team Informatiemanagement of een door hun aangewezen derde(n) geschieden. De daaraan verbonden kosten zijn voor rekening van de gemeente, tenzij wordt geconstateerd dat sprake is van een onzorgvuldig gebruik en/of nalatigheid.

6. Veilige apps en software installeren mag voor privé en zakelijk gebruik. Bij constatering van het gebruik van onveilige apps, software of diensten, aangeboden goederen, pornografische, racistische en/of ander kwetsend of aanstootgevend materiaal zullen er passende maatregelen genomen worden. Het is niet toegestaan vooraf geïnstalleerde software zonder toestemming van team Informatiemanagement te verwijderen.

7. De medewerker/ gebruiker is niet aansprakelijk voor schade en/of verlies van het door de gemeente ter beschikking gestelde mobile device, behalve in geval van schade als gevolg van grove schuld, nalatigheid en/of opzet van de zijde van de medewerker/ gebruiker zoals het downloaden en installeren van illegale software.

8. Het is mogelijk om bij uitdiensttreding van de medewerker een mobiel nummer welke is verstrekt door de gemeente, mee te nemen naar een andere provider. Dit dient zo spoedig mogelijk na bekendmaking van de uitdiensttreding bij P&O of direct leidinggevende bekend te worden gemaakt aan team Informatiemanagement.

9. Er mogen er geen kopieën van gegevens en programmatuur aan derden worden verstrekt.

10. In een openbare ruimte mag een mobile device niet onbeheerd worden achtergelaten.

11. Een mobiel apparaat dient bij het verlaten van de werkplek altijd te worden vergrendeld.

4.2 Beveiligingsinstellingen

1. De gemeente is bevoegd om beveiligingsinstellingen af te dwingen op mobiele apparaten. Dit betreft onder meer:

- Controle op en toepassen van wachtwoordbeleid (o.a. sterk wachtwoord, apparaat vergrendeling en resetten van wachtwoorden);
- Toepassen van encryptie van apparaat en op verbindingen;
- Toepassen van zero footprint;
- Controle op de aanwezigheid van virussen en malware;
- Verplichten van gebruik antivirus / anti- malware toepassingen;
- Controle van internet en mail content op aanwezigheid van virussen en malware;
- Het plaatsen van onveilige applicaties en websites op de blacklist van gemeente Stein;
- Controle op het verwijderen van beveiligingsinstellingen (jailbreak, rooted device);
- Toepassen van beperkingen voor het aansluiten van (USB) devices zoals een dvd apparaat, cd apparaat, opslagapparaat etc.;
- Verplichten van 2 factor authenticatie voor het raadplegen van specifieke informatiesystemen;
- De aanwezigheid van een iCloud account op het mobiele apparaat.

2. In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals het traceren, blokkeren en/of wissen van apparatuur op afstand.

3. Informatie die via een mobiel apparaat van de gemeente worden uitgewisseld via mail of andere apps, kunnen mogelijk op grond van de Wet Open Overheid opgevraagd worden en openbaar worden gemaakt.

4. In geval van schade, vermissing of diefstal van een mobiel apparaat dienen team Informatiemanagement en de CISO direct op de hoogte te worden gesteld. Bij inbraak dient bij de politie aangifte te worden gedaan. Na melding van diefstal of vermissing zal team Informatiemanagement het mobile device blokkeren en op afstand wissen.

5. Afhankelijk van de locatie van een werkplek (gemeentehuis, thuis, openbare ruimte etc.) gaat het gebruik van mobiele apparaten gepaard met risico's waarvoor de gebruiker beveiligingsmaatregelen moet treffen. Hierbij kun je denken aan het vermijden van verbinding met openbare WiFi netwerken (gebruik hiervoor je persoonlijke hotspot) en het niet onbeheerd achterlaten van mobile devices.

6. Mobiele apparaten dienen indien mogelijk beveiligd te zijn met een 2-factor authenticatie. In het geval van een smartphone of tablet geldt dat deze voorzien is van een toegangscode (gebruik hiervoor geen geboortedatum of ander makkelijk te raden code), vingerscan of gezichtsscan.

4.3 Technische en organisatorische maatregelen

De gemeente legt bij het nemen van technische beveiligingsmaatregelen op het apparaat de focus op beveiliging middels een daarvoor ingerichte virtuele werkomgeving, oftewel een MAM-software omgeving. Gemeentelijke informatiesystemen bevinden zich altijd in een beveiligde container en zullen bij verlies van een mobiel apparaat niet meer toegankelijk zijn. Dit geldt echter niet voor e-mails, agenda, contactpersonen en lokaal opgeslagen documenten.
Om deze reden is bewustwording aan medewerkers op het gebied van privacy en informatiebeveiliging een terugkerend patroon wat door de CISO/ Adviseur Privacy in samenwerking met de Functionaris Gegevensbescherming en team Informatiemanagement wordt verzorgd.

Elke medewerker/ gebruiker is verplicht integer te handelen en dient zich te houden aan de geheimhoudingsplicht.

4.4 Cloudtoepassingen en apps

De gemeente stelt haar informatiesystemen beschikbaar via MAM software en beschouwd deze omgeving als veilig. De gemeente staat toe dat buiten deze digitale werkplek gebruikers andere Cloud toepassingen en apps gebruiken, mits zij zich bewust zijn van de beveiligingsrisico's die daaraan verbonden zijn.

Het is niet toegestaan om vertrouwelijke informatie zoals persoonsgegevens op te slaan anders dan in de werkomgeving. Gegevens komen dan op onbekende servers te staan op onbekend locaties. Het opslaan van gemeentelijke informatie in een niet beveiligde omgeving kan leiden tot een beveiligingsincident en/of een datalek. Om gegevens veilig met derden te kunnen delen heeft de gemeente een aantal diensten beschikbaar gesteld. Het uitwisselen van vertrouwelijke informatie via niet veilige bronnen is niet toegestaan.

4.5 Gebruik van apps uit landen met een offensief cyberprogramma

Op 21 maart 2023 heeft de Rijksoverheid besloten dat het ambtenaren afgeraden wordt om applicaties van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen te installeren en te gebruiken op hun mobiele werkapparatuur. In het geval dat een applicatie in beheer is in een land met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen, dan is er sprake van een verhoogd spionagerisico. Voor meer informatie hierover wordt verwezen naar bijlage 1: advies gebruik apps uit landen met een offensief cyberprogramma. Dit document is tevens gepubliceerd in de intranetgroep informatiebeveiliging & privacy.

5. Vaststelling

Managementteam
Het managementteam van de gemeente Stein heeft dit document operationeel vastgesteld in de MT-vergadering van datum

De gemeentesecretaris,

Ondernemingsraad
De ondernemingsraad van de gemeente Stein heeft ingestemd met dit document in de OR-vergadering van datum

De voorzitter,

College van burgemeester en wethouders
Burgemeester en wethouders van de gemeente Stein hebben dit document bestuurlijk vastgesteld in de collegevergadering van datum .

Burgemeester en wethouders van Stein,

De secretaris, De burgemeester,

Bijlagen

Bijlage 1: Gebruik van apps uit landen met een offensief cyberprogramma

1. Inleiding

Op 21 maart 2023 heeft de Rijksoverheid besloten dat het ambtenaren wordt afgeraden om applicaties van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen te installeren en te gebruiken op hun mobiele werkapparatuur[2]. Aanleiding van dit besluit zijn de Kamervragen die zijn gesteld door een Tweede Kamer lid voor D66 over de mogelijkheid om de Chinese applicatie TikTok te weren op mobiele apparaten van medewerkers van de Rijksoverheid.

Op basis van deze vragen is aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) gevraagd een advies te geven. De conclusie van dit advies is dat het gebruik en de aanwezigheid van mobiele telefoons en de daarop geïnstalleerde applicaties altijd een inherent spionagerisico vormen. Het is daarom aan te raden altijd een grondige afweging uit te voeren tussen de noodzaak van het installeren van een bepaalde applicatie en het daarbij behorende risico. Het gebruik van apps van bedrijven uit landen met een offensief cyberprogramma door ambtenaren in dienst van de rijksoverheid verhoogt dit risico. De Vereniging Nederlandse Gemeenten (VNG) heeft aangegeven zich aan te sluiten bij het beleid van het Rijk[3].

2. Aanleiding

De oproep om de app TikTok te verbieden speelt al jaren, maar is dit jaar in een stroomversnelling gekomen. De reden daarvoor is dat de potentiële dreigingen de afgelopen tijd zijn toegenomen. Zo is er Chinese wetgeving die het mogelijk zou kunnen maken voor Chinese veiligheidsdiensten om informatie die TikTok verzamelt van bijvoorbeeld ambtenaren in te kijken. Dit is een potentieel gevaar en risico dat niet genomen wil worden. Of gegevens van TikTok daadwerkelijk in verkeerde handen zijn gevallen is op dit moment onbekend. “Mogelijk dat bepaalde inlichtingendiensten hier meer informatie over hebben, maar publiekelijk is dit niet bekend”, geeft een beveiligingsonderzoeker van cybersecuritybedrijf Computest aan.

TikTok heeft niet meer toegang tot gebruikersgegevens dan andere social media apps zoals Facebook en Instagram die ook locatiegegevens en toegang tot contactpersonen vragen. Toch zijn met name regeringen steeds voorzichtiger, omdat TikTok een bedrijf is dat een stuk dichter bij de Chinese overheid staat dan Facebook en Instagram bij de Amerikaanse overheid staan. Op dit moment doen de federale politiedienst FBI en het Amerikaanse OM onderzoek naar ByteDance (organisatie achter TikTok) wegens het bespioneren van Amerikaanse journalisten via de app.

---

[2] brief Tweede Kamer
[3] VNG advies

Medewerkers van het Chinese bedrijf zouden locatiedata en andere persoonlijke gegevens van Amerikaanse journalisten hebben gebruikt om hen via TikTok in de gaten te houden. Zo wilden ze naar verluidt achterhalen wie de bronnen van de journalisten waren.

3. Om welke landen en om welke apps gaat het?

In het geval dat een applicatie in beheer is in een land met een offensief cyberprogramma gericht tegen Nederland en Nederlandse belangen dan is er sprake van een verhoogd spionagerisico. Voorbeelden van landen met een offensief cyberprogramma zijn Rusland, China, Iran en Noord-Korea. Van deze landen is bekend dat inlichtingendiensten de intentie en capaciteit hebben om spionageoperaties richting Nederlandse overheden, bedrijven en personen uit te voeren.

Zo kunnen veel offensieve inlichtingendiensten organisaties en datacentra verplichten hun gebruikersgegevens te delen of in bepaalde gevallen fabrikanten zelfs verzoeken om technische voorzieningen in de software aan te brengen. In bijlage A van het VNG advies is een overzicht van veel gebruikte apps uit deze landen opgenomen.

4. Advies vanuit de VNG

Voor gemeente Stein (en andere gemeenten) speelt de te maken afweging zich af op twee punten:

Punt 1: *Gebruik van apps die **niet** afkomstig zijn uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen.*

Gemeenten gebruiken bepaalde apps zoals Facebook, Instagram en Youtube om in contact te komen met hun inwoners en ondernemers. Daarbij maken ze gebruik van platforms waar deze doelgroepen zelf ook op aanwezig zijn. Om te bepalen of deze platforms wel of niet geschikt zijn als communicatiemiddel adviseert de VNG hierover intern het gesprek aan te gaan waarbij wordt gekeken naar het risico vs. noodzaak.

Op basis van de informatie die gemeente Stein plaatst op deze social media platforms wordt er nog geen noodzaak gezien om het gebruik van deze apps af te raden. De risico's worden periodiek gemonitord en beoordeeld.

Punt 2: *Gebruik van apps die **wel** afkomstig zijn uit landen met een offensief cyberprogramma tegen Nederland en/ of Nederlandse belangen wordt het gebruik*

Uit het advies van de AIVD blijkt dat er een risico is op spionage dat niet opweegt tegen de voordelen van het gebruik van dit soort apps. Gemeenten worden daarom geadviseerd om de lijn van het Rijk te volgen om apps afkomstig van landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen te weren van werktelefoons en niet in te zetten als communicatiekanaal voor inwoners.

5. Besluit gemeente Stein

Op basis van bovenstaande risico's heeft de gemeente Stein op 18 oktober 2023 besloten het advies van de VNG op te volgen.

Dit betekent concreet dat op mobiele apparaten van de gemeente Stein (mobiel, laptop, IPad) in lijn met andere Nederlandse gemeenten er geen gebruik (meer) wordt gemaakt van de apps die in bijlage A van het VNG advies zijn opgesomd. De meeste bekende app hiervan is TikTok.

Omdat gemeente Stein op dit moment geen apps uit landen met een offensief cyberprogramma inzet als specifiek communicatiekanaal richting inwoners blijft de huidige werkwijze voortbestaan. Bij medewerkers die op dit moment gebruik maken van ‘bring your own device’ is het niet mogelijk om het niet installeren, dan wel het verwijderen van dit soort apps af te dwingen. De gemeente zet hier in op bewustwording.

Dit besluit wordt meegenomen bij de aanschaf van de nieuwe mobiele apparaten en bij het actualiseren van het beleid Mobile Devices. Bij het actualiseren van het beleid mobile devices wordt daar waar mogelijk rekening gehouden met functies binnen de gemeente waarbij een ambtenaar ook in zijn privé leven het gezicht van de gemeente Stein is. Denk hierbij aan de Burgemeester, wethouders en raadsleden.

Bijlage 2: gerelateerde BIO normen

In onderstaande tabel zijn de normen/ controls uit de Baseline Informatiebeveiliging Overheid (BIO) benoemd waaraan met dit beleid geheel of gedeeltelijk wordt voldaan.

BIO norm	Titel	Omschrijving
6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende maatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich mee brengt te beheren.
6.2.1.1	-	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn
6.2.1.2	-	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: **a**. In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. **b**. Het device maakt deel uit van patchmanagement en hardening. **c**. Er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. **d**. Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. **e**. Periodiek wordt getoetst of de punten in lid a), b) en c) worden nageleefd.
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.
8.1.3.1	-	Alle medewerkers worden aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.
9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

Dat maakt Stein voor mij...

Gemeente *Stein*