
BELEID VOOR MOBIELE APPARATUUR

Beleidsnotitie

Bedrijfsvertrouwelijk

BIO 06.2.1

Gemeente Almere



Status	Concept, versie 1.0 vastgesteld CIO in 2016
Versie	2.0
Ingangsdatum	01-01-2020
Revisiedatum	31-12-2022
Opdrachtgever	Gemeente Almere
Team/taakveld	CIO-Office / Informatieveiligheid
Auteur(s)	J.A. Blok, CISO W.O. Meijer, IBO M.M. de Boer – de Wit, PIO G. King, Technisch architect K. Speelman, Senior beleidsadviseur IV R. Snellenburg, Technisch Security Specialist

Doelstelling

De doelstelling van het tactische informatieveiligheidsbeleid van de Gemeente Almere is om de dreigingen van binnen en buiten de organisatie m.b.t. informatie en systemen het hoofd te bieden door de (grootte van de) risico's vast te stellen en adequate maatregelen te nemen. Hiervoor heeft de gemeente tactisch en operationeel beleid geformuleerd gebaseerd op de eisen van de "Baseline Informatieveiligheid Overheid (BIO)".

Centrale verantwoordelijkheid

Vanuit de BIO is de Gemeentesecretaris van de gemeente Almere eindverantwoordelijk voor informatieveiligheid en voor de inrichting en werking van de beveiligingsorganisatie. Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen en processen vast, technisch ondersteund door de afdeling ICTAR, onder verantwoordelijkheid van de afdelingsmanager ICTAR.

Algemene beleidsuitgangspunten

- Alle relevante wet- en regelgeving wordt nageleefd.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering en handhaving van de informatieveiligheidsactiviteiten binnen hun verantwoordelijkheidsgebied en zorgen voor instructie en naleving van de overeengekomen maatregelen door hun medewerkers.
- Advies, ondersteuning en coördinatie van alle activiteiten op het gebied van informatieveiligheid op gemeenteniveau gebeurt door de Chief Information Security Officer (CISO).
- Voorzieningen voor informatie en informatieverwerking worden door de CISO beoordeeld op de risico's t.a.v. informatieveiligheid. De noodzakelijk geachte maatregelen worden gerealiseerd door de afdelingsmanager, daarbij technisch ondersteund door de manager van de afdeling ICTAR.
- Voor de gewenste en noodzakelijke maatregelen voor het realiseren van de informatieveiligheid worden contacten met relevante overheidsinstanties en met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties onderhouden.
- Jaarlijks worden het beleid en de maatregelen t.a.v. het realiseren en handhaven van voldoende informatieveiligheid beoordeeld op actualiteit en effectiviteit. Over deze beoordeling wordt door de CISO gerapporteerd aan de Concerndirectie. Noodzakelijke maatregelen worden voorgesteld en na goedkeuring geïmplementeerd. Informatieveiligheid is een standaard onderdeel van de P&C-cyclus.
- Al het tactisch beleid wordt centraal gepubliceerd (direct na vaststelling) en is daarmee toegankelijk voor alle medewerkers (huidige platform is de Wiki van Alforum).

* Deze beleidsuitgangspunten zijn gebaseerd op de BIO en uitgewerkt voor gemeente Almere, vervolgens vastgesteld door de CIO.

1. Mobiele Apparatuur

Er is een toename van het gebruik van mobiele apparatuur zoals smartphones, tablets en laptops binnen de gemeente Almere. Deze beleidsnotitie is geschreven om vanuit verschillende gezichtspunten de risico's, randvoorwaarden en oplossingen weer te geven die de gemeente kan inzetten bij de keuzes voor mobiele apparatuur. Het maakt voor deze beleidsnotitie niet uit of het een gemeentelijk mobiel apparaat is of een eigen mobiel apparaat (in het geval van Bring Your Own Device), immers op mobiele apparatuur kan in meer of mindere mate data van de gemeente staan. Los van het feit of het mobiele apparaat fysiek kan zoekraken, de data valt in beide gevallen onder de verantwoordelijkheid van de gemeente. Daarnaast wordt er binnen de gemeente flexibel gewerkt met mobiele apparaten.

Veilig omgaan met mobiele apparatuur en de gemeentelijke gegevens die erop kunnen staan is noodzakelijk om de risico's te beperken. Deze risico's kunnen mogelijk leiden tot beveiligingsincidenten en datalekken. Enkele voorbeelden maar niet gelimiteerd tot:

- Mobiele apparatuur een malware besmetting kan oplopen en daarmee ook de gemeente infecteren (het mobiele apparaat wordt door hackers als aanvalsvector gebruikt);
- Mobiele apparatuur (persoons) gegevens bevat en doorgaans buiten de gemeentelijke gebouwen zijn. Deze (persoons) gegevens kunnen zoekraken of worden ingezien door onbevoegden;
- Mobiele apparatuur door malware hoge SMS of telefoon kosten kan veroorzaken;
- Mobiele apparatuur kan zoekraken of gestolen worden (vervangschade en inzien van gegevens / datalekken);
- Mobiele apparatuur gebruikt kan worden als brug om gemeentelijke systemen te benaderen.

2. Beleid voor gebruik mobiele apparatuur

De volgende beleidsdoelstellingen zijn van toepassing:

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé apparatuur die (ook) zakelijk wordt gebruikt ('Bring Your Own Device'). Op privé apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: de onmogelijkheid om illegale software te downloaden, controle op wachtwoordbeleid, encryptie, aanwezigheid van malware, et cetera.
- Het gebruik van privé apparatuur waarop beveiligingsinstellingen zijn verwijderd (zoals bijvoorbeeld: 'jailbreak', 'rooted device', ontwikkelaars unlock) is niet toegestaan.¹
- De medewerkers van de gemeente die gebruik maken van mobiele apparatuur dienen de installatie van Mobile Device Managementsoftware toe te staan om bovenstaand beleidsuitgangspunt te handhaven. (De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand, hiervoor is een internetverbinding vereist.
- Er is altijd een mogelijkheid tot het wissen van informatie op mobiele apparatuur (smartphone en tablet), hiervoor is een internetverbinding vereist.
- Gebruik van encryptie is verplicht. Apparatuur zonder encryptie worden niet ondersteund.
- Zakelijke en privégegevens worden van elkaar afgeschermd.

3. Externe toegang tot netwerk en applicaties

De gemeente maakt gebruik van two-factorauthenticatie voor externe toegang tot het gemeentelijk netwerk. Hiervoor is een aanmeldingsprocedure inclusief autorisatie van kracht.

¹ Jailbreak 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 daardoor het complete besturingssysteem te wijzigen of te vervangen, en daarmee ook malware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

4. Medewerkers

Voor medewerkers gelden de volgende afspraken:

- Externe toegang tot het gemeentelijk netwerk is alleen mogelijk voor medewerkers en derden die expliciet door de gemeente zijn geautoriseerd.
- Alle personen die met mobiele apparatuur toegang krijgen tot applicaties of systemen van de gemeente worden op het moment dat zij hiervoor worden gefaciliteerd expliciet geïnformeerd over de technische regels en de gedragsregels voor mobiele apparatuur van de gemeente.
- De betrokken personen tekenen een verklaring dat zij akkoord gaan met deze regels en overeenkomstig deze regels zullen handelen.
- Niet naleven van deze regels kan leiden tot intrekken van de toegang tot informatie, applicaties en/of systemen van de gemeente met mobiele apparatuur. Verder kan het leiden tot disciplinaire maatregelen overeenkomstig de aanstelling (eigen medewerkers) of het contract met de gemeente (ingehuurde medewerkers en medewerkers van ingehuurde derde partijen).
- Bij het vermoeden of het constateren van een datalek² of beveiligingsincident dient altijd direct melding te worden gemaakt bij de Servicedesk door gebruik te maken van MijnICT op Alforum.
- Bij verlies en / of diefstal dient altijd direct melding te worden gemaakt bij de Servicedesk door gebruik te maken van MijnICT op Alforum.

5. Review uitvoering beleid

Eénmaal per jaar moeten de uitgangspunten van het gebruik van mobiele apparatuur door de CISO worden beoordeeld. Deze beoordeling heeft als doel:

- Het beleid toetsen aan de nieuwe ontwikkelingen zowel binnen als buiten de gemeente;
- Bevindingen vanuit beveiligingsincidenten, datalekken en audits van het afgelopen jaar verwerken.

6. Documentatie en vastlegging procedure

- De procedure rond het toekennen, muteren en verwijderen van gebruikers(rechten) wordt gedocumenteerd.
- De procedure rond de uitgifte van mobiele apparatuur wordt gedocumenteerd.
- Eenmaal per jaar vindt een review van de procedures plaats (nieuwe versie) ter beoordeling of een aanpassing gewenst is (PDCA).
- Eenmaal per 3 jaar, of na grote structurele wijzigingen in beleidsomgeving en/of informatieomgeving, vindt een totale review van de procedure plaats.

7. Afwijkingen

Alle afwijkingen van bovenstaande regels moeten vooraf worden voorgelegd en besproken met de CISO. Aan de hand van een risicobeoordeling kan worden bepaald of er van de regels afgeweken kan worden en onder welke omstandigheden. Afwijkingen dienen vastgelegd te worden in een register. Dit register wordt gedeeld met de betrokken afdelingsmanager.

² Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie.

Taken verantwoordelijkheden en bevoegdheden

Voor het beleid zijn de volgende taken en verantwoordelijkheden volgens het RACI-model³:

	CISO	CIO-Of- fice	CIO / Afd. Manager ICTAR	CD	Afdelings- manager	ICTAR	HRM
Opstellen van een beleidsvoorstel	R	C	A			C	
Goedkeuren van beleid			R	A			
Opstellen en uitwerken maatregelen voor de uitvoering	C	I	C		A	R	I
Implementatie maatregelen en procedures	C		R		A		
Review beleid en procedures	R		A		C	C	I

Relaties met andere documenten

- Protocol mobiele apparatuur versie 2.0
- Instemmingsbesluit van de DOOR gemeente Almere
- Operationeel beleid voor mobiele apparatuur (onderhanden bij TSS)

³ RACI-model: R (*Responsible, NL: Verantwoordelijk*), A (*Accountable, NL: Eindverantwoordelijk*), C (*Consulted, NL: Geraadpleegd*), I (*Informed, NL: Geïnformeerd*)