Gemeente Haarlem

Gebruik en ondersteuning mobile devices

Dit document beschrijft het beleid m.b.t. mobile devices voor decentrale politieke ambtsdragers

30 oktober 2019

Afdeling InformatieVoorziening

Inhoudsopgave

1. Inleiding

Op vrijwel alle terreinen van het taakveld van de gemeente speelt Informatie- en CommunicatieTechnologie (ICT) een rol. Met ICT zijn aanzienlijke kosten gemoeid.
Dit document verwoordt het beleid en de concrete regels die nodig zijn om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen onze organisatie en op de beschikbaar gestelde mobile devices te beschermen.

1.1 Snelle ontwikkelingen op het gebied van ICT

Alle Informatie en Communicatie Technologie (ICT) voorzieningen van de gemeenten Haarlem & Zandvoort[1] zijn ondergebracht bij de afdeling Informatie Voorziening (IV). De ontwikkelingen bij de afdeling IV op het gebied van hardware & software verlopen erg snel. Zowel voor het gebruik als door wet- en regelgeving wordt wekelijks software geüpdatet, dagelijks worden er technische aanpassingen gerealiseerd, kwetsbaarheden verholpen, virus- malware en internet aanvallen afgeslagen, mobile devices uitgeleverd en hardware vervangen. Duidelijke afspraken zijn daarom nodig.

2. Beleid en regels

De organisatie stelt aan de ambtsdragers mobile devices beschikbaar voor het uitvoeren van hun werkzaamheden. Om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie binnen onze organisatie te beschermen, is er informatiebeveiligingsbeleid, een privacyreglement voor de medewerkers, een privacyverklaring voor burgers en een Regeling Integriteit (integriteitswijzer gemeente Haarlem 2016) vastgesteld binnen de organisatie.

Beleid en technische maatregelen alleen, zijn niet voldoende om de goede werking van de mobile devices te waarborgen. Ongewenst gebruik kan grote hinder en schade opleveren. Het onderstaande beleid voorziet in een aantal regels voor verantwoord gebruik van de mobile devices door de ambtsdragers en Beheerders. De essentie van dit beleid is als volgt samen te vatten:

a. Gebruik. De beschikbaar gestelde mobile devices zijn bedoeld voor zakelijk en privé gebruik. Privégebruik is toegestaan voor zover dit niet indruist tegen de in dit document gestelde regels en geen extra kosten voor de organisatie tot gevolg heeft.
b. Vertrouwelijkheid. Ambtsdragers moeten zich er van bewust zijn dat ze met vertrouwelijke gegevens te maken hebben. Ambtsdragers mogen alleen vertrouwelijke informatie benaderen als ze hiervoor gemachtigd zijn. Het gebruik van mobile devices mag eventuele vertrouwelijkheid of gevoeligheid van gegevens niet schenden of in strijd zijn met wettelijke of contractuele beperkingen.
c. Privacy. Op zowel het gebruik als controle op het gebruik van mobile devices is de Nota Privacy beleid, het privacyreglement en het Informatiebeveiligingsbeleid van de organisatie van toepassing.
d. Overlast voorkomen. Het gebruik van internet en e-mail is aan bepaalde regels en beperkingen gebonden. Hierbij gelden de zakelijke omgangsvormen bij communicatie.
e. Zorgvuldigheid. De ambtsdrager dient zorgvuldig om te gaan met de beschikbaar gestelde mobile devices en zich te houden aan de in dit document gestelde regels. Onder zorgvuldig wordt o.a. verstaan: geen beschadigingen aan mobile devices aanbrengen, het mobile device in een beschermhoes of tas vervoeren, software/apps gebruiken zoals geïnstrueerd.

[1] Hierna te noemen: organisatie

f. Security. De beschikbaar gestelde mobile devices zijn voorzien van de laatste security updates. Van de ambtsdrager wordt verwacht dat er zorgvuldig met gebruiker gegevens en wachtwoorden wordt omgegaan en onregelmatigheden zo spoedig mogelijk gemeld worden. Verderop in dit document lees je meer over wat er precies van je verwacht wordt en hoe je incidenten / onregelmatigheden kunt melden.

2.1 Definities

Ambtsdrager	Burgemeester, wethouders, gemeenteraadsleden en commissieleden op grond van de gemeentewet.
ICT-middelen	De door of namens de organisatie ter beschikking gestelde hardware, software en netwerkfaciliteiten, evenals de door of namens de organisatie aangeboden voorzieningen t.b.v. elektronisch data- en spraakverkeer. Waaronder: desktop- en laptopcomputers en de daarop geplaatste programmatuur, internettoegang, e-mail, maar ook printer, scanner, (mobiele) telefoon en mobile devices.
Beheerder Technisch	De ICT-verantwoordelijke medewerker van de afdeling IV. Deze medewerkers hebben uitgebreide ICT bevoegdheden, zijn verantwoordelijk voor het beheer, de beveiliging en het onderhoud van het geautomatiseerde informatiesysteem, waarbij ook aspecten van softwareontwikkeling en systeemontwikkeling tot het takenpakket behoren. Hun gedrag wordt uitvoerig vastgelegd in audit trails welke niet muteerbaar zijn. Deze audit trail bevat wie, wat, waar, wanneer aangaande; Alle bewerkingen: het inloggen, wijzigingen, afsluiten, aanmaken en verwijderen van zaken. Alle activiteiten: het aanmaken, wijzigen, beëindigen, verwijderen van autorisaties of rollen. Alle wijzigingen aan een werkproces.
Beheerder Functioneel	De verantwoordelijke medewerker van de afdeling ID en/of de hiervoor aangewezen medewerkers. Deze medewerkers hebben ICT bevoegdheden, zijn verantwoordelijk voor het beheer, de beveiliging en het onderhoud van het geautomatiseerde informatiesysteem. Hun gedrag wordt vastgelegd in audit trails welke niet muteerbaar zijn. Deze audit trail bevat wie, wat, waar, wanneer aangaande; Alle bewerkingen: het inloggen, wijzigingen, afsluiten, aanmaken en verwijderen van zaken. Alle activiteiten: het aanmaken, wijzigen, beëindigen, verwijderen van autorisaties of rollen. Alle wijzigingen aan een werkproces.
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.
Derden	Onder derden wordt verstaan iedereen die geen medewerker of ambtsdrager is van de organisatie.
Beveiligings-Incident	Een incident waarbij de reputatie van de organisatie op het spel zou kunnen staan of de bedrijfsvoering buiten proportioneel kan worden verstoord, met het risico dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(middelen) worden aangetast of attractieve waarde goederen worden ontvreemd.
Internet-gebruik	Het uitwisselen of doorgeven van gegevens en/of berichten via E-mail, het bezoeken van internetsites, het binnenhalen (downloaden) van gegevens alsmede het binnenhalen van software, apps en/of het gebruiken van software vanaf internet.
Mobile device	Een draadloos apparaat, niet zijnde een PC, dat zich kenmerkt door computer functionaliteit waarop applicaties beschikbaar zijn, waarmee via mobiel internet of wifi organisatie informatiesystemen kunnen worden benaderd. Hieronder vallen een daarvoor geschikte mobiele telefoon, laptop of tablet.
Representatieve staat	Het mobile device dient voor hergebruik uit te leveren zijn. Hiermee word o.a. bedoeld: geen stickers op het mobile device aanbrengen, moedwillig beschadigingen en/of markeringen aanbrengen, het mobile device schoon houden.

2.2 Geldigheid beleid en regels

2.2.1 Het beleid Gebruik en ondersteuning mobile devices van de organisatie is vastgesteld voor uitgifte en gebruik van mobile devices. De organisatie is bereid om aan de ambtsdrager de apparatuur ten behoeve van zijn/haar functie bij de organisatie in bruikleen te geven, onder bepalingen zoals vastgesteld in onderhavig beleidstuk en de bruikleenovereenkomst. (bijlage 1).

2.2.2 Dit beleid en regels, gebruik en ondersteuning mobile devices geldt voor alle ambtsdragers van de organisatie. De gemeentesecretaris is verantwoordelijk en het presidium is eindverantwoordelijk voor de naleving van dit beleid en de regels.

2.2.3 Iedere ambtsdrager dient zich te houden aan de in dit document beschreven en daaruit voortvloeiende instructies, geboden en verboden. Dit document is niet vrijblijvend. Het presidium kan bij overtreding van de in dit document omschreven regels passende maatregelen nemen.

2.3 Gebruik van de mobile devices

2.3.1 Het gebruik van de mobile devices door de ambtsdrager is primair ten behoeve van het vervullen van zijn taak of functie. Voor zover dit niet indruist tegen de gestelde regels, niet storend is voor de overeengekomen werkzaamheden en geen extra kosten voor de organisatie tot gevolg heeft, is privé gebruik toegestaan.

2.3.2 Het presidium behoudt de bevoegdheid een ambtsdrager de mogelijkheid tot het gebruik van ter beschikking gestelde mobile devices te ontzeggen.

2.3.3 Het installeren of gebruiken van software of apps voor privé en/of zakelijke doeleinden zonder een geldige licentie of abonnement is verboden.

2.3.4 Mede met het oog op beheer van licenties en de ondersteuning van de gebruikers kan de Beheerder controles uitvoeren ten aanzien van geïnstalleerde software of apps, alsmede ter zake instructies geven. Dit met inachtneming van de Nota Privacy beleid.

2.3.5 Op alle door de organisatie beheerde mobile devices is een antivirusprogramma en/of een beheerapp actief. Geadviseerd wordt om op niet door de organisatie beheerde mobile devices een antivirusprogramma te installeren en up-to-date te houden. Hiervoor zijn op het internet of in de appstore gratis versies te vinden. De securityofficer van de organisatie kan hierin adviseren.

2.3.6 Met uitzondering van niet draagbare hardware geldt dat hardware nimmer onbeheerd achtergelaten dient te worden.

2.3.7 De ambtsdrager is verantwoordelijk voor het in goede en representatieve staat houden van de mobile devices.

2.3.8 In geval van schade, vermissing of diefstal van ICT-middelen dient de beheerder snel op de hoogte te worden gesteld. Dit kan via 023-5115252 tijdens kantooruren en buiten kantooruren via servicedesk.iv@haarlem.nl. Waar mogelijk en relevant, zoals bij inbraak, dient bij de politie aangifte te worden gedaan en van het betreffende proces-verbaal een afschrift aan de beheerder te worden overgelegd.

2.3.9 Na melding van diefstal of vermissing zal de beheerder het mobile device blokkeren en wissen. De beheerder maakt tevens melding bij datalekmelden@haarlem.nl. Om het device op afstand te blokkeren en wissen is door de beheerder Airwatch op het device geinstalleerd. Airwatch is geconfigureerd met inachtname van de Nota Privacy beleid.

2.3.10 Reparaties aan en opening van apparatuur mag uitsluitend door de beheerder en of door beheerder aangewezen derden te geschieden.

2.3.11 Bij vervanging van een defect of vermist mobile device wordt dit vervangen. De beheerder bepaalt of het mobile device daadwerkelijk defect is. (Een matige batterij is bijvoorbeeld geen defect).

2.3.12 Accessoires die bij het mobile device zijn aangeschaft worden bij vermissing of defect door de ambtsdrager zelf vervangen.

2.3.13 Als een mobile device storingen vertoond is het mogelijk om het mobile device aan te bieden bij de beheerder. Hiervoor dient contact opgenomen te worden met de servicedesk van IV. (Zie 2.7.3) Vervolgens wordt er beoordeeld of de storing verholpen kan worden. Het is mogelijk dat het mobile device ter reparatie ingenomen wordt. Mogelijk wordt het device teruggezet naar fabriekswaarden.

2.3.14 Afhankelijk van de locatie van een werkplek (kantoor, trein, etc.), gaat het gebruik van mobile devices gepaard met risico's, waarvoor ambtsdragers bijbehorende beveiligingsmaatregelen dienen te treffen. Te denken valt aan het opbergen in lockers en het mijden van verbinding met openbare WiFi netwerken.

2.3.15 De ambtsdrager is zelf verantwoordelijk voor de back-up van lokaal opgeslagen data op het mobile device. Denk hierbij ook aan foto's, WhatsApp historie en dergelijke. Het gebruik van de C- en D-schijf van laptops voor data opslag wordt ontraden.
Bij gebruik van het mobile device wordt dataopslag op OneDrive geadviseerd.
Opslag in de iCloud is gratis tot 5 gigabyte bij overschrijding van deze opslag zijn de kosten voor de ambtsdrager. Als de extra opslag gekoppeld wordt aan het @Haarlem.nl of @Zandvoort.nl email adres vervalt deze extra opslag als het email adres wordt verwijderd.

2.3.16 Een mobile device dient beveiligd te zijn. Laptops zijn beveiligd met een inlog account. Smartphones dienen een simkaart code te hebben die niet 0000 of 1234 is. Voor smartphones en tablets geld dat het unlock scherm moet zijn voorzien van een code (niet 0000 of 1234), vingerscan, gezichtsscan of beveiligingspatroon.

2.4 Termijn van gebruik en aanschaf van mobile devices

2.4.1 Ambtsdragers hebben recht op maximaal twee mobile devices.

2.4.2 Een aanvraag voor mobile devices kan bij de Griffier gedaan worden. De Griffier maakt een fixmelding voor de aanvrager(s) met vermelding van de naam van de ambtsdrager en vermelding van de gewenste mobile devices. De mogelijkheden zijn: Smartphone, Smartphone + laptop of Smartphone + tablet.

2.4.3 Voor levering van de mobile devices wordt door de griffier contact opgenomen door de Servicedesk IV of de afdeling FAZA.
(Fix- STARTPAGINA > MIJN WERKPLEK > WERKPLEK > AANVRAAG NIET REGULIERE HARDWARE)

2.4.4 De ambtsdrager dient de mobile devices bij beëindiging van de aanstelling of lidmaatschap op eerste verzoek in volledige staat inclusief accessoires te retourneren. Bij verzuim tot retourneren zal het presidium de ambtsdrager hierop aanspreken gezien de wettelijke verplichting tot retourneren van mobile devices.

2.4.5 Bij inleveren van het mobile device wordt in het bijzijn van de ambtsdrager alle data en accountgegevens gewist, teruggezet naar fabriekswaarden en de beveiligingscodes ingesteld op 0000.

2.4.6 De afschrijvingstermijn voor smartphones en tablets is 36 maanden. Voor laptops geldt 48 maanden. Na de afschrijvingstermijn worden de devices vervangen.

2.5 Mobiel telefoon/data abonnement

2.5.1 Mobile devices mogen privé gebruikt worden. Mits men veilig, zorgvuldig en integer omgaat met het mobile device én gegevens van de organisatie.

2.5.2 Legale Apps en software installeren mag voor privé en zakelijk gebruik. Bij constatering van niet legale apps, software of malicieuze diensten, aangeboden goederen, pornografisch en/of racistisch en/of ander kwetsend of aanstootgevend materiaal zal de beheerder contact met de gemeentesecretaris opnemen.

2.5.3 Reikwijdte mobiel abonnement binnen Europese Unie(EU):
- Onbeperkt zakelijk bellen in EU naar vaste en mobiele nummers
- Onbeperkt privé bellen in EU naar vaste en mobiele nummers
- 4G

- Maximum datagebruik 5GB per maand op basis van fair use
- SMS/MMS (zonder extra kosten)
- 0900-nummer (servicenummer) Niet toegestaan.
- 0906-nummer (erotisch karakter) is geblokkeerd
- 0909-nummer (amusement en spelletjes) is geblokkeerd

2.5.4 Reikwijdte mobiel abonnement buiten EU:
- Bellen buiten de EU is toegestaan mits noodzakelijk voor de uitoefening van het ambt.
- Bellen/SMS/MMS buiten de EU is toegestaan mits noodzakelijk voor de uitoefening van het ambt.
- Data-gebruik buiten de EU is toegestaan mits noodzakelijk voor de uitoefening van het ambt.

2.5.5 Ambtsdragers die een simkaart in bruikleen hebben geven toegang tot alle door de telecom provider vastgelegde gegevens omtrent het gebruik van de simkaart voor monitoring doeleinden.

2.5.6 Het verwijderen van de simkaart uit het geleverde mobile device door de ambtsdrager is niet toegestaan.

2.5.7 Het is mogelijk om een privé mobiel nummer over te zetten naar het provider-contract van de organisatie. De organisatie doet geen afkoop van contracten en abonnementen. Kosten van afkoop zijn voor eigen rekening. Ook is het mogelijk om het mobiele nummer welke is verstrekt door de organisatie, mee te nemen naar een andere provider bij beëindiging van de aanstelling of lidmaatschap.

2.6 Beveiligingsbeleid

2.6.1 Het is toegestaan om organisatie informatie in de vorm van e-mail op een Mobile device (zakelijk of privé) te gebruiken. Door Active Sync (push mail) te activeren, wordt informatie op het device opgeslagen. Als er organisatie informatie (bijv. e-mail) op een mobile device staat, is het IV beleid met betrekking tot Mobile Devices van toepassing en moet op het device een minimale vorm van beveiliging worden toegepast, bestaande uit een wachtwoord. Dit wordt door het e-mail systeem afgedwongen.

2.6.2 Ambtsdragers die als mobile device een door de organisatie verstrekte laptop gebruiken moeten de laptop eens in de 180 dagen met een fysieke netwerk kabel met het gemeente Haarlem netwerk verbinden om het gebruiker wachtwoord te wijzigen. Dit is om security en licentie technische redenen.
(Dit kan alleen op het gemeente Haarlem netwerk en geldt alleen voor laptops met fysieke netwerk aansluiting)

2.7 Ondersteuning servicedesk IV

2.7.1 De servicedesk van de afdeling IV ondersteunt alle ambtsdragers van de organisatie op het gebied van ICT gerelateerde zaken. Voorwaarde hiervoor is dat er wordt gewerkt op mobile devices geleverd door de organisatie en met software of apps geleverd door de organisatie.

2.7.2 IV biedt geen ondersteuning voor privé aangekochte apps en/of software welke geïnstalleerd zijn op mobile devices van de organisatie.

2.7.3 De servicedesk IV is op werkdagen telefonisch bereikbaar op nummer 5252 of 0235115252 van 7:45 t/m 17:00.

2.7.4 Digitale meldingen kunnen 24/7 gedaan worden via de FIX pagina op intranet.

2.7.5 Dagelijks van 09:00 t/m 13:00 is er een mogelijkheid om zonder afspraak langs te komen bij het ICT-Loket voor ICT gerelateerde vragen of problemen. Het ICT-Loket op de locatie Zandvoort is geopend op dinsdag van 09:00 t/m 12:00.

2.7.6 Voor een adequate ondersteuning door de servicedesk IV en gericht oplossen van problemen is het zaak jezelf hierop voor te bereiden door alle benodigde

informatie zoals Apple-id, wachtwoorden etc. paraat te hebben.

2.7.7 De afdeling IV, ICT loket en servicedesk IV zijn niet aansprakelijk voor het verlies van persoonlijke items (foto's, bestanden, etc.) indien dit na een consult (telefonisch of aan het loket) het geval is. Het is de verantwoordelijkheid van de ambtsdrager om zijn persoonlijke items vooraf veilig te stellen bijvoorbeeld door een kopie of back-up te maken.

2.8 Eigendom

2.8.1 Ter beschikking gestelde ICT-middelen mogen niet aan derden in gebruik worden gegeven. Evenmin mogen een of meer kopieën van programmatuur aan derden worden verstrekt.

2.8.2 De organisatie is eigenaar van het mobile device.

2.9 Revisie / evaluatie

2.9.1 Dit beleidsdocument wordt minimaal één keer per half jaar beoordeeld op effectiviteit en actualiteit waarbij het tijdig bijgewerkt wordt met betrekking tot de veranderende ICT-omgeving, richtlijnen, privacy, security, AVG en voortschrijdend inzicht.

Versie	Datum	Beschrijving
1.0	06-06-2019	Concept versie afgeleid van de medewerker versie
1.0	18-06-2019	Review Hardware & Softwarebeheer
1.01	16-10-2019	Review HRM. Aanpassingen aanvraag traject.
1.02	22-10-2019	Review HRM. Aanpassingen. Norm devices verwijderd. Artikel 1.2 verwijderd. Diverse kleine aanpassingen.
1.03	23-10-2019	Review HRM. Aanpassingen 2.5.3 & 2.5.4
1.04	30-10-2019	Opmerkingen JZ. Artikel 2.2.1 toegevoegd

Dit is een uitgave van gemeente Haarlem & Zandvoort,
30 oktober 2019

Tekst: Barry Halderman,
Fotografie: -,
Ontwerp: Barry Halderman,
Drukwerk: -

Postbus 511
2003 PB Haarlem
Tel. 14 023

haarlem.nl
zandvoort.nl