Gemeente Aalsmeer

GEMEENTEBLAD

Officiële uitgave van de gemeente Aalsmeer

Nr. 60419

22 maart

2018

Gemeentebreed informatieveiligheidsbeleid

Z-2018/004201

Burgemeester en wethouders van gemeente Aalsmeer besluiten vast te stellen het Gemeentebreed informatieveiligheidsbeleid (versie 1.05 van 22-12-2017).

Versiebeheer

Versie en datum	Wijziging	status
1.0 - 17 november 2016	Eerste oplevering	Vastgesteld college Amstelveen en Aalsmeer
1.01 - 16 december 2016	• CORV beheerder aangepast (in bijlage 1)	
1.02 - 24 september 2017	• Tekst 'Beleid en procedures voor informatie-uitwisseling' verplaatst van 10.4 naar 6.10	
1.03 - 13 oktober 2017	• Aanpassing van Wbp naar AVG, betreft gehele document echter met name bij het onderdeel rollen FG en privacybeheerder • Aanpassing rol- en functiescheiding bij rol Security Officer SUWI en explicitering aansluitbeleid SUWI	
1.04 - 24 november 2017	• Toegevoegd beveiligingsbeheerder BGT	
1.05 - 22 december 2017	• Actualisatie namen beheerders	

I. Voorwoord

I.I Totstandkoming

In dit document is het gemeentebrede informatieveiligheidsbeleid beschreven van de gemeenten Amstelveen en Aalsmeer.

Het informatieveiligheidsbeleid is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (van VNG/IBD) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd. De uitgangspunten uit deze baseline zijn integraal opgenomen in dit gemeentebrede informatieveiligheidsbeleid. Hierdoor is een actueel en naar de laatste inzichten opgesteld beleidsplan voor de gemeenten Amstelveen en Aalsmeer ontstaan.

Het beleid is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en management die in het kader van lijnwerkzaamheden of een project moeten weten aan welke kwaliteitsaspecten aandacht moet worden besteed. De intentie is niet dat alle medewerkers exact weten wat er in het gemeentebrede informatieveiligheidsbeleid staat, maar men moet wel weten dat het beleid er is, hoe het te gebruiken en wat de belangrijkste uitgangspunten zijn.

Afspraken die we maken over de rol- en taakverdeling bij de uitvoering van ons informatieveiligheidsbeleid geven uitdrukking aan de 3 leidende principes binnen onze gemeentelijke organisatie, zoals verwoord in "Het Huis AA", namelijk: verantwoordelijkheid nemen, aangesloten zijn en de boel op orde hebben.

De basis van dit informatieveiligheidsbeleid wordt gevormd door de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG - VNG/IBD). De specifieke vertaling en inrichting voor de gemeenten Amstelveen en Aalsmeer heeft plaatsgevonden in workshops in aanwezigheid van een brede afvaardiging uit de organisatie. Tijdens deze bijeenkomsten zijn de specifieke gemeentelijke inzichten en accenten opgehaald en samengebracht in dit document.

I.II Leeswijzer en ambitieniveau

Dit document bevat een groot aantal beleidsuitgangspunten op het gebied van de veiligheid van gemeentelijke informatieprocessen. De gemeentelijke informatieprocessen worden tijdens de fase van risicoanalyse geanalyseerd en vervolgens op basis van een risico van een prioriteit voorzien. De gemeente maakt tijdens dit proces zelf keuzes over de prioritering en fasering van de implementatie van de onderdelen van het beleidsplan.
Daarnaast richten de gemeenten Amstelveen en Aalsmeer zich, indien nodig, op de toepassing van specifiek op de gemeenten Amstelveen en Aalsmeer afgestemde maatregelen, die eveneens invulling geven aan de betreffende norm uit de BIG. Hierbij kunnen mogelijke alternatieve maatregelen worden ingezet om aan de in de BIG vastgestelde normen te voldoen.

Enkele beleidsuitgangspunten hebben betrekking op aandachtgebieden die pas actueel worden indien de gemeente voor een dergelijke keuze of vraagstuk staat, bijvoorbeeld de inzet van Cloudtechnologie, gezamenlijk uitbesteden van software-ontwikkeling of de aanschaf van een nieuw informatiesysteem. In dat specifieke geval hanteert de gemeente de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Met dit document wordt daarnaast bepaald dat de gemeente bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt hanteert.

II. Waarom informatieveiligheid?

II.I Inleiding

De gemeenten Amstelveen en Aalsmeer zijn informatie-intensieve organisaties met een primaire focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de gemeenten moeten kunnen beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. Voor een optimale, moderne dienstverlening is een koppeling van informatiesystemen noodzakelijk. Bovendien moeten burgers en bedrijven er op kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Informatisering speelt een steeds prominentere rol in de gemeentelijke organisatie. Deze rol wordt in het kader van het stelsel van basisregistraties en de toenemende complexiteit van het digitale dienstverleningskanaal steeds belangrijker. Ook de gemeenten Amstelveen en Aalsmeer richten zich op het koppelen van systemen waardoor grote gegevensverzamelingen ontstaan die vervolgens weer specifieke informatie opleveren voor interne en externe afnemers.

Daarnaast is de gemeente steeds afhankelijker van goed werkende informatievoorziening en systemen. Dit betekent dat de gemeenten Amstelveen en Aalsmeer alert zijn op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet zijn ontworpen met het oog op veiligheid. De veiligheid die met de technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en -procedures. Daarnaast speelt echter de menselijke factor (het menselijk gedrag) een steeds grotere rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk. Deze factor speelt, door de steeds complexer wordende informatieprocessen, veelal zelfs een doorslaggevende rol.

Informatie komt in verschillende vormen voor. Het kan zijn geschreven, gesproken, gedrukt of digitaal zijn verwerkt en/of opgeslagen. Al deze verschijningsvormen van informatievragen voor een deel eenzelfde generieke aanpak, maar kennen ook verschillen. Dit document besteedt hier aandacht aan.

De veiligheid van informatie speelt binnen een groot aantal gebieden van de gemeente een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom de SUWI, DigiD, BRP, WD of BAG) separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatieveiligheidsbeleid op te stellen. In dit gemeentebrede informatieveiligheidsbeleid worden beleidsuitgangspunten vastgelegd ten aanzien van alle onderliggende informatiedomeinen. Hieronder vallen niet alleen de informatie-intensieve domeinen als sociaal domein, publieksdiensten of financiën, maar eveneens domeinen als beheer en onderhoud, ruimtelijke ordening en facilitaire zaken.

In het gemeentebrede informatieveiligheidsbeleid wordt op strategisch en tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid van de gemeenten Amstelveen en Aalsmeer. Dit document zal samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatie binnen alle domeinen van de organisatie zijn gewaarborgd.

II.II De informatieveiligheidspiramide

Ook de centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet- en regelgeving op dit gebied uit zich deze aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De ontwikkeling door VNG/IBD van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatieveiligheid NEN/ISO 27001 en 27002, bieden een meetlat voor gemeenten om hun informatieveiligheid op orde te brengen en te houden.

Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking worden gesteld, zoals de Wet Basisregistratie Personen (Wet BRP), Algemene Verordening Gegevensbescherming (AVG), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet Openbaarheid Bestuur (Wob). Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet Basisregistratie

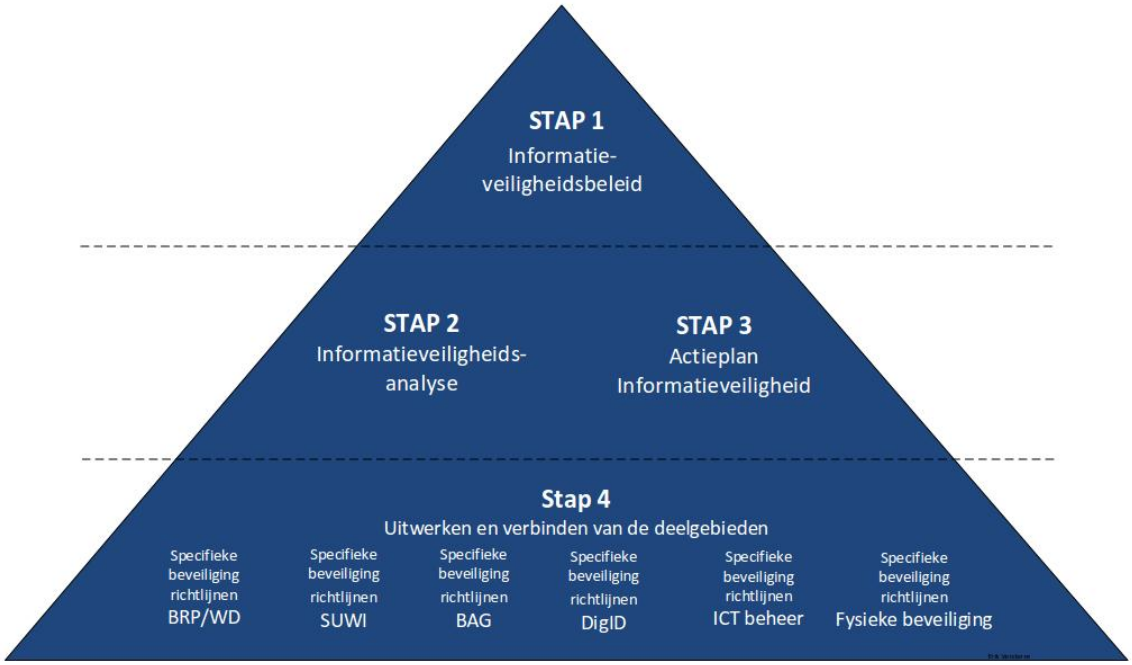
Adressen en Gebouwen (BAG), Wet Kenbaarheid Publiekrechtelijke Beperkingen (Wkpb), de nieuwe Wet Ruimtelijke Ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

Teneinde de scope van dit document te verduidelijken, is in figuur 1 aangegeven welke niveaus van informatieveiligheid zijn te onderkennen.

Bovenaan de piramide treffen we het informatieveiligheidsbeleid aan. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar.

De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten in het gemeentebrede informatieveiligheidsbeleid getoetst met de praktijksituatie. Hier worden niet alleen de "harde aspecten" onderzocht. Dat wil zeggen de techniek, de regels en de procedures. Maar worden ook de "zachte aspecten" meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie. Na de risico-inventarisatie vindt risicoweging en -prioritering van maatregelen plaats. Tijdens deze stap worden de geconstateerde risico's gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van risico's en te treffen maatregelen.

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals het BRP, de BAG of het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.



Figuur 1: De informatieveiligheidspiramide

II.III Toelichting op ISO 27001 en ISO 27002 (code voor informatieveiligheid)
Het gemeentebrede informatieveiligheidsbeleid is volledig gebaseerd op de internationale standaard voor informatieveiligheid NEN-ISO/IEC 27001 en 27002. De eerste standaard (27001) biedt een richtlijn voor de implementatie en planmatige borging van Informatieveiligheid binnen de organisatie. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde "best practices" voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. De Baseline Informatiebeveiliging Nederlandse Gemeenten is afgeleid van deze beide internationale informatieveiligheidsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie specifiek is aangepast voor de situatie in gemeenten.

II.IV Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid
De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente (in hoofdstuk 3 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatieveiligheid uitgebreider beschreven), zo ook voor informatieveiligheid. De verantwoordelijkheid voor informatieveiligheid ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de algemene directeur.
De vaststelling en implementatie van de informatieveiligheidsstructuur (onder het begrip informatieveiligheidsstructuur wordt in dit verband de complete beheercyclus van het informatieveiligheidsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatieveiligheid wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid) en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeenten Amstelveen en Aalsmeer. Voor het nemen van operationele maatregelen is de algemeen directeur gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdelingsoverstijgende (informatie)systemen.

De afdelingshoofden zijn verantwoordelijk voor de informatiesystemen waarvan zij eigenaar zijn. Zij dienen deze systemen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

II.V Wettelijke basis en controle beveiligingsnormen
De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Algemene Verordening Gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen burgerservicenummer;
- Paspoortwet;
- Wet BasisRegistratie Personen (BRP);
- Wet Openbaarheid Bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Nieuwe Wet Ruimtelijke Ordening (nWRO).

Op grond van bovenstaande wet- en regelgeving worden eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

1. Informatieveiligheidsbeleid

Doelstelling:
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.

Resultaat:
Strategisch beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

1.1 Beleidsdocument voor informatieveiligheid
Het college van burgermeester en wethouders behoort een gemeentebreed beleidsdocument voor informatieveiligheid goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen.
Minimaal zijn de volgende aspecten in dit beleidsdocument aanwezig:
- De doelstellingen van informatieveiligheid voor de gemeente.

- De beveiligingseisen en -prioriteiten.
- De organisatie van de informatieveiligheidsfunctie (zie hoofdstuk 2).
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatie-beveiligingsrollen (zie hoofdstuk 2).
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie II.II) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie II.VI).
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie 1.5).

1.2 Scope van het informatieveiligheidsbeleid

De scope van dit beleid omvat alle gemeentelijke informatieprocessen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip en gebruikte apparatuur. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college en de gemeenteraad. Daarnaast bevat dit document de uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners.
Ook beleid ten aanzien van het specifieke aansluitbeleid SUWI is integraal opgenomen in dit gemeentebrede informatieveiligheidsbeleid, zodat alle beleidsuitgangspunten met betrekking tot informatieveiligheid in één gemeentebreed document zijn samengebracht.

1.3 Informatieveiligheidsanalyse

Op basis van dit strategische beleidsdocument worden door het managementteam de Informatieveiligheidsanalyse met het actieplan informatieveiligheid vastgesteld. Hierin wordt aangegeven op welke wijze het beleid uitgevoerd wordt.
De kernelementen in de informatieveiligheidsanalyse zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van de informatieveiligheidsanalyse wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau.
- Voor het bepalen van afhankelijkheden en risico's is een analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
  - Risico's die onvoldoende af te dekken zijn door maatregelen.
  - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen.
  - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden.
  - Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.

1.4 Aanvullende maatregelen

1.4.1 Afwijkend beveiligingsniveau

Als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist dan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), moet een daarvoor verantwoordelijk persoon aanvullende maatregelen treffen. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen (zie hoofdstuk 3).

1.4.2 Persoonsgegevens

Bij de verwerking van persoonsgegevens zijn aanvullende maatregelen vereist, afhankelijk van de klassenindeling van de Algemene Verordening Gegevensbescherming (AVG).

1.4.3. Aansluitbeleid SUWI

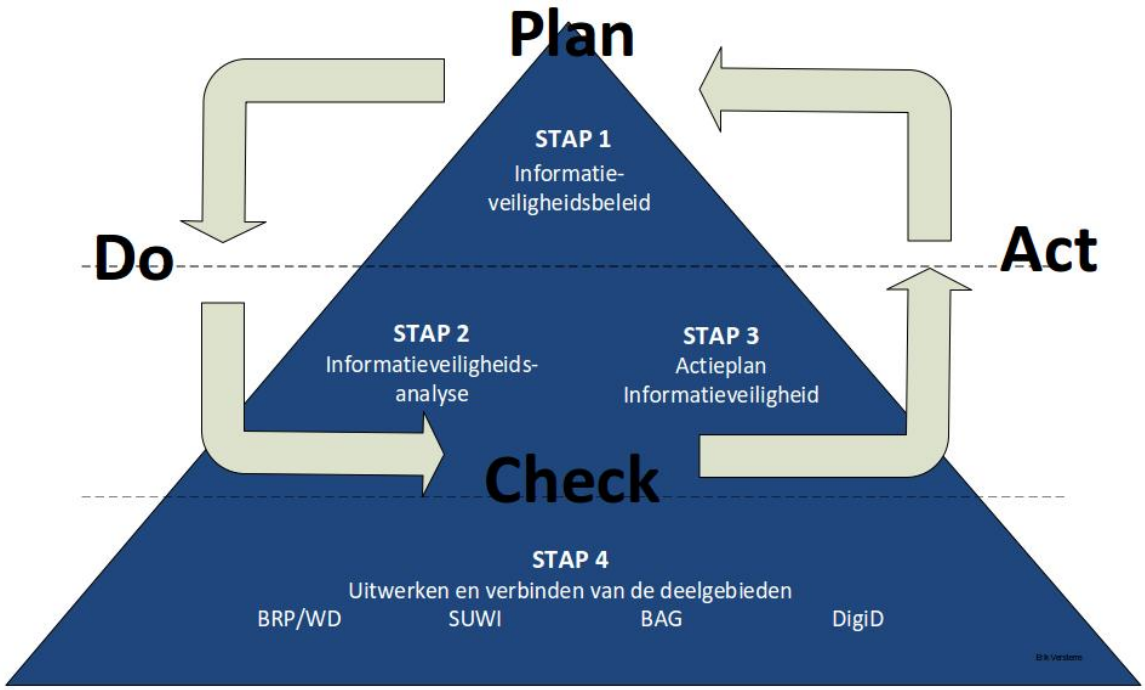
De Gezamenlijke elektronische Voorziening Suwinet (GeVS) wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. Binnen de Suwiketen participeren bronhouders (waaronder UWV en SVB), de beheerder van de centrale omgeving (BKWI) en de afnemers. De Afnemers, waaronder de AA gemeenten hebben deze gegevens nodig voor de uitvoering van hun wettelijke taken binnen het sociaal domein. Deze GeVS keten en de informatie die via GeVS wordt uitgewisseld moeten voldoen aan specifieke beveiligingseisen en aan de AVG (Algemene Verordening Gegevensbescherming). De

beveiligingseisen staan in het teken van de aspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Deze SUWI beveiligingseisen zijn vastgelegd in het Specifieke Suwinet-normenkader voor Afnemers. Dit is, naast de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de specifieke informatiebeveiligingsstandaard die de AA gemeenten hanteren ten aanzien van SUWI.
In dit voorliggende gemeentebrede informatiebeveiligingsbeleid zijn de gemeentebrede en SUWI specifieke beleidsuitgangspunten vastgelegd ten aanzien van onder meer procedures, controles, rollen, taken, verantwoordelijkheden, functiescheiding en toegang, die nodig zijn om de in het Specifieke Suwinet-normenkader voor Afnemers vastgelegde veiligheidsniveau te realiseren.

1.5 Borging van het informatieveiligheidsbeleid
Om borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 2), onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA cyclus (zie figuur 2):

1. Informatieveiligheidsbeleid: bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid vindt plaats in een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats.
2. Informatieveiligheidsanalyse: bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar.
3. Actieplan Informatieveiligheid: bevat de concrete, geprioriteerde acties volgend uit de informatieveiligheidsanalyse. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het actieplan Informatieveiligheid vindt (conform de bespreking in het informatieveiligheidsoverleg zie paragraaf 2.3) twee tot vier maal per jaar plaats.

In de reguliere P&C cyclus wordt gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid.



Figuur 2: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

Doelstelling:
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.

Resultaat:
Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

2.1 Verantwoordelijkheidsniveaus binnen de gemeenten Amstelveen en Aalsmeer
Binnen de gemeenten Amstelveen en Aalsmeer worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
De Colleges van B&W van de gemeenten Amstelveen en Aalsmeer dragen als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Het college stelt de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden op het gebied van beveiliging gemandateerd aan de algemeen directeur.

2.1.2 Gemandateerde verantwoordelijkhede n en taken op organisatieniveau
De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt bij de algemeen directeur. Deze stelt met het managementteam het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De algemeen directeur is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan.

De algemeen directeur heeft in ieder geval de volgende verantwoordelijkheden:
- Het aanwijzen van een CISO en een controller informatieveiligheid.
- Het stellen van operationele kaders en het geven van sturing ten aanzien van de veiligheid van informatie.
- Het sturen op concernrisico's.
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig.
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden.
- Het beleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en -systemen.
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid.

2.1.3 Verantwoordelijkheden en taken op afdelingsniveau en teamniveau
De afdelingshoofden zijn verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun afdeling.

De afdelingshoofden hebben in ieder geval de volgende verantwoordelijkheden:
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn.
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen.
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn).
- Het rapporteren, via de CISO, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C rapportages.

2.1.4 Chief Information Security Officer (CISO)
Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages.

De CISO heeft in ieder geval de volgende verantwoordelijkheden:
- Rapporteert rechtstreeks aan de directie.
- Coördineert het formuleren van informatieveiligheidsbeleid.
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan.

- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid.
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid.
- Ondersteunt de directie en de afdelingshoofden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen.
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid.
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Bevordert het beveiligingsbewustzijn in de organisatie.
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten.
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages. Hierbij bundelt de CISO de deelbijdragen van het afdelingsmanagement.

2.1.5 De controller informatieveiligheid
Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.

De controller informatieveiligheid heeft in ieder geval de volgende verantwoordelijkheden:
- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid. De controller informatieveiligheid is hiervoor verantwoordelijk, maar organiseert dit proces waar mogelijk met de inzet van beveiligingsbeheerders. Het principe hierbij is dat de toetsing binnen een bepaald domein plaatsvindt door een beveiligingsbeheerder van een ander domein en visa versa.
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid.
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Toetsen/bewaken van het niveau van informatieveiligheid.
- Toetsing van evaluatieproces van beveiligingsincidenten.

De rol van controller informatiebeveiliging heeft op twee specifieke deelgebieden een voorgeschreven officiële benaming. Dit betreft het gebied van reisdocumenten en van rijbewijzen. Het betreft de volgende benamingen:

Beveiligingsfunctionaris reisdocumenten
Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.

Beveiligingsfunctionaris rijbewijzen
Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

2.1.6 De beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations), Rijbewijzen (Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI), BAG (BAG beheerder) en DigiD. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken, ICT, DIV en P&O.
D e beveiligingsbeheerder
Is - voor het toegewezen deelgebied - verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden. Hieronder vallen:
- de voorbereiding en coördinatie van audits en (zelf)evaluaties;
- de preventie en detectie van beveiligingsincidenten en het geven van een adequate respons;
- coördineren de toepassen van specifieke wet- en regelgeving;

- rapporteert aan de CISO en de controller informatieveiligheid.

Uitleg over enkele specifieke beveiligingsbeheerdersrollen:

Autorisatiebevoegde Reisdocumenten/Aanvraagstations
Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).

Autorisatiebevoegde Rijbewijzen
Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

Security Officer SUWI
De Security Officer SUWI (beveiligingsbeheerder SUWI) beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. Dit laatste impliceert eveneens de kwaliteitszorg, de kwaliteitsborging en de controle op het toegang en gebruik van Suwinet.

De specifieke SUWI doelstellingen en taken vloeien voort uit de Regeling SUWI. Dit betreft de processen binnen het sociaal domein. Met deze processen worden persoonsgegevens geadministreerd en verwerkt. Ook vindt gegevensuitwisseling plaats met de SUWI-partners, zoals het UWV en SVB. Op grond van artikel 6.4 lid 1 uit de Regeling SUWI is de burgemeester verplicht zorg te dragen voor beveiliging van de gegevensuitwisseling. In dit document wordt daarvan uitwerking gegeven.

De Security Officer SUWI heeft in ieder geval de volgende verantwoordelijkheden:
- Bevordert de beveiliging van Suwinet.
- Ziet er op toe dat de beveiligingsmaatregelen worden nageleefd.
- Adviseert en informeert medewerkers en management.
- Doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet en
- Evalueert de uitkomsten van verbetermaatregelen.
- De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het verantwoordelijk management.
- De Security Officer SUWI vraagt minimaal vier keer per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

Rol- en functiescheiding en autorisatie tot Suwinet
Onderdeel van een rechtmatig en veilig gebruik van Suwinet is het gescheiden beleggen van taken en verantwoordelijkheden. Hiervoor zijn de volgende functiescheidingen aangebracht:
- De gebruikers van Suwinet.
- De lijnmanager.
- De technisch ICT beheerder.
- De applicatiebeheerder Suwinet.
- Security Officer SUWI.

Technisch ICT beheer zorgt voor de technische aansluiting-, werking- en beveiliging- van Suwinet. De lijnmanager is verantwoordelijk voor de aanvraag van mutaties in geval van instroom, doorstroom en uitstroom. Deze aanvraag wordt door de Security officer SUWI beoordeeld en gecontroleerd. De Security Officer SUWI gaat hierbij na of de gevraagde autorisatie overeenkomt met de uit te voeren functie/rol. Indien de Security Officer SUWI akkoord is, wordt het formulier door de Security Officer aangeleverd bij de applicatiebeheerder SUWI, die de autorisaties en toegang inclusief wachtwoorden in orde maakt.

2.1.7 Privacybeheerder
Deze rol is gericht op de uitvoering en de naleving van de privacywetgeving. Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De privacybeheerder heeft in ieder geval de volgende verantwoordelijkheden:
- Beheren van het register van persoonsverwerkingen tegen de achtergrond van de kaders van de privacywetgeving en adviseert directie, afdelings- en teamhoofden bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een privacy impact assessment.
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- De privacybeheerder heeft verder als taak:

a. de uitleg van de privacyvoorschriften uit de privacywetgeving;
b. coördineren van de privacywerkzaamheden;
c. coördineren, samenvoegen en beheren van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeenten Amstelveen en Aalsmeer;
d. verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) respectievelijk Functionaris voor de gegevensbescherming (FG);
e. coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
f. inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
g. beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
h. advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

2.1.8 Functionaris voor de gegevensbescherming
De functionaris voor de gegevensbescherming (FG, ook wel Data Protection Officer (DPO) genoemd, is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacy wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.
Naast deze toezichthoudende taken is de functionaris voor de gegevensbescherming verantwoordelijk voor de uitvoer van de klachtafhandelingsprocedure. Dit betekent het initiëren, doorlopen, verzorgen van interne en externe communicatie en afsluiten van de klachtafhandelingsprocedure.

2.1.9 Afdeling Informatiebeheer
Afdeling informatiebeheer, waarvan systeembeheer deel uitmaakt, beheert de werkplekken, serverplatformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

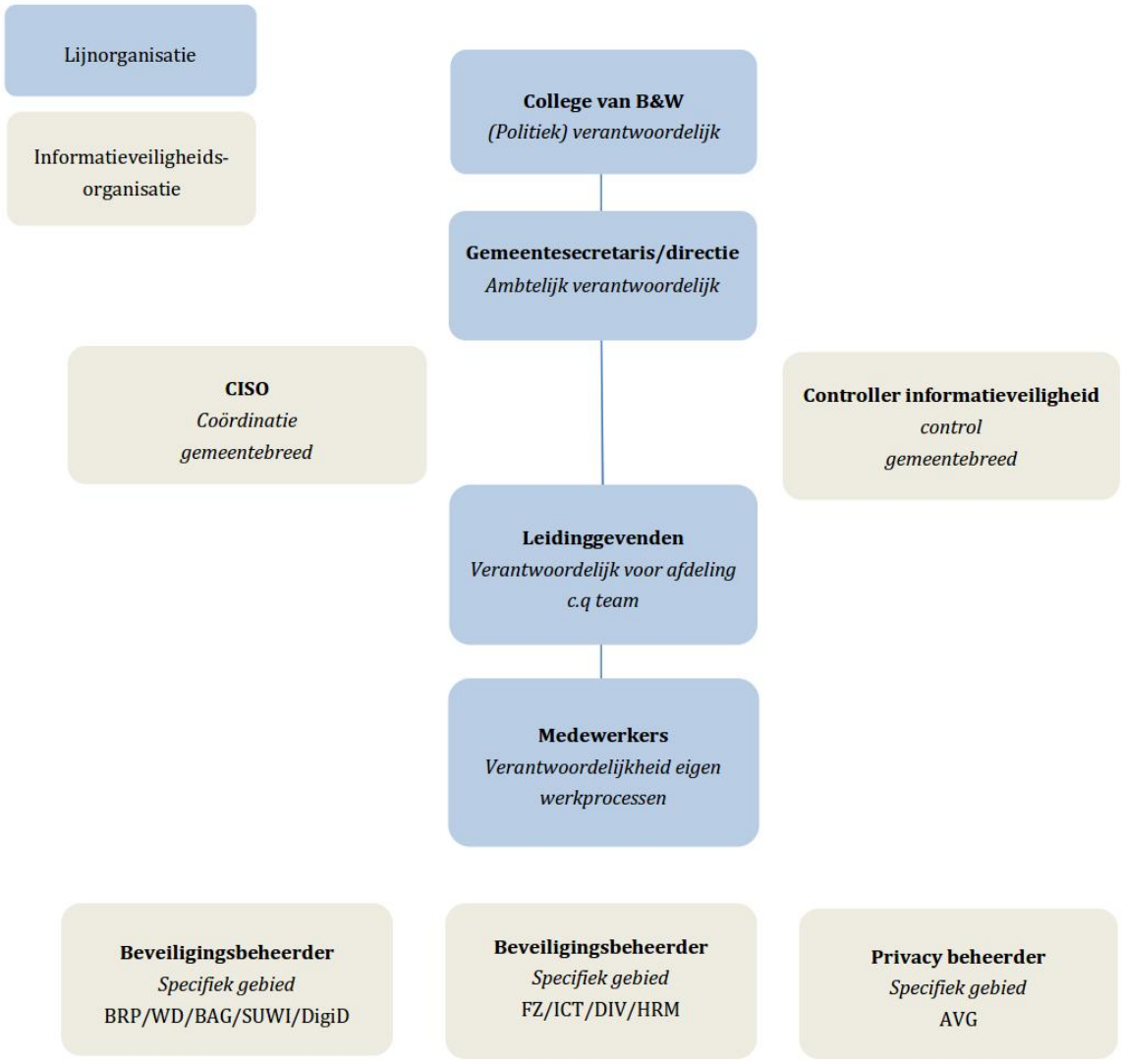
2.1.10 Het team facilitaire zaken
Het team facilitaire zaken is verantwoordelijk voor de fysieke veiligheid in en rond het gebouw, fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging. De beveiligingsbeheerder FZ neemt namens het team deel aan het informatieveiligheidsoverleg.

2.1.11 Het team HRM
Het team HRM is verantwoordelijk voor het beheer en de advisering ten aanzien personele en de organieke veiligheidsaspecten binnen de organisatie. De beveiligingsbeheerder HRM neemt deel aan het informatieveiligheidsoverleg namens team HRM.

2.1.12 F unctioneel en gegevensbeheerder
Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening en voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.1.13 De medewerkers
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit, de beschikbaarheid en de controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken.

In bijlage 1 staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie.



Figuur 3: Functies en rollen in informatieveiligheidsorganisatie

2.3 Overleg en afstemmingsorganen

De CISO is voorzitter van het overleg informatieveiligheid dat 2 tot 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De CISO.
- De controller Informatieveiligheid.
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, SUWI en DigiD.
- Beveiligingsbeheerders t.a.v.: FZ, ICT, HRM en INF.
- De privacybeheerder.
- Agendaleden: directielid, afdelingshoofd, teamleider of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid.
- Beveiligingsincidenten.
- Planning en voorbereiding van Audits, controles en zelfevaluaties.
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Controle of de invulling van de rollen in de Governance structuur nog actueel is.

2.4 ICT crisisbeheersing
Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat in ieder geval uit:
- De coördinator informatieveiligheid / CISO (voorzitter).
- De controller informatiebeveiliging.
- De beveiligingsbeheerder ICT.
- Het afdelingshoofd verantwoordelijk voor de afdeling waar het incident heeft plaatsgevonden.
- Indien nodig: relevante experts, medewerkers en directielid.
- De teamleider communicatie.

2.5 Rapporteren beveiligingsincidenten
De CISO wordt door de medewerkers geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd. Zie hoofdstuk 9 voor meer informatie over de definitie en de procedure met betrekking tot beveiligingsincidenten.
Afspraken moeten worden gemaakt over:
- doel van de registratie;
- inhoud van de registratie;
- mate van detaillering;
- wijze van handelen;
- wijze van rapporteren.

De CISO en de controller informatieveiligheid rapporteren minimaal eenmaal per jaar aan de eindverantwoordelijke (de directie).

2.6 Verantwoordelijkheden afdelingsoverstijgende (informatie)systemen
Afdelingsoverstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van team informatiebeheer gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdelingsoverstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem. Indien de directie hier niet expliciet toe besluit behoort deze verantwoordelijkheid aan het team informatiebeheer.
De procesverantwoordelijke van een afdelingsoverstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

2.7 Externe partijen

2.7.1 Service level agreement (niveau van dienstverlening)
Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen een afdeling en de externe partij een Service Level Agreement (SLA) (hiervoor wordt ook de term DVO (DienstVerleningsOvereenkomst) gebruikt) afgesloten. Hierin staan afspraken over het niveau van informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.

2.7.2 Inhuur derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk leidinggevende van de gemeenten Amstelveen en Aalsmeer. Dit afdelingshoofd waarborgt dat de activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

2.7.3 Toegang derde partijen tot ICT-voorzieningen
Bij toegang van derden tot de gemeentelijke ICT-voorzieningen gelden de onderstaande uitgangspunten:
- Informatieveiligheid is (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in

het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een verwerkersovereenkomst (conform Algemene Verordening Gegevensbescherming) afgesloten.

2.7.4 Overeenkomsten met een derde partij en met betrekking tot ICT voorzieningen
Bij het aangaan van overeenkomsten met derde partijen gelden de volgende beveiligingseisen:
1. De maatregelen behorend bij 2.7.3 zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd.
2. Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
3. In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
4. In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
5. Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.
6. In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
7. Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
8. De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

2.7.4.1 Verwerkers van persoonsgegevens
De Algemene Verordening Gegevensbescherming (AVG) stelt regels voor het opslaan, verzamelen, vernietigen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Wanneer een partij het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij "een verwerker". De gemeenten Amstelveen en Aalsmeer leggen in een register vast welke derden persoonsgegevens bewerken. Ook wordt vastgelegd of een verwerkersovereenkomst nodig is in de relatie tot die andere partij. In een verwerkersovereenkomst leggen de partijen onder andere vast voor welke doeleinden de gegevens mogen worden verwerkt, welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen, welke beveiligingsmaatregelen moeten worden genomen en hoe het zit met de onderlinge aansprakelijkheid.

3. Classificatie en beheer van informatie en bedrijfsmiddelen

Doelstelling:
Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, (informatie) systemen en bedrijfsmiddelen.

Resultaat:
Een goed overzicht van alle ICT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

3.1 Inventarisatie van informatie en (informatie) bedrijfsmiddelen
Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden vastgelegd.

Het team ICT beheer houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):
- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen).
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer).
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten).
- Diensten (bijvoorbeeld communicatiediensten, PKI diensten, energievoorziening ten behoeve van de informatievoorziening).

Het team Facilitaire Zaken houdt een registratie bij van alle fysieke voorzieningen die verband houden met (informatie) veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

Het team HRM houdt een registratie bij van alle medewerkers en extern personeel dat vanwege uitoefening van de opgedragen werkzaamheden gebruik moet kunnen maken van gemeentelijke ICT voorzieningen.

3.2 Eigendom van informatie en bedrijfsmiddelen
Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijk leidinggevende benoemd.

3.3 Aanvaardbaar gebruik van bedrijfsmiddelen
Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen. Hieronder volgen de geldende uitgangspunten:
- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en gemeentelijke informatie zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie primair voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
  - Illegale software, of niet goedgekeurde software mag niet worden gebruikt voor de uitvoering van het werk.
  - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel.
  - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.

- De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
  - de beveiligingsclassificatie van de informatie;
  - de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatieveiligheidsbeleid);
  - aan de werkplek verbonden risico's;
  - het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

3.4 Classificatie van informatie en bedrijfsmiddelen
Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. De gemeentelijke informatiesystemen worden geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke gemeentelijke infor-

matie als vertrouwelijk wordt geclassificeerd. Na dit inzicht is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen / 0	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*
Laag / I	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: interne rapportages)*	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet en concept college/raad voorstellen)*
Midden / II	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, bijzondere financiële gegevens, zoals aanbestedingscalculaties)*
Hoog / III	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistratie BRP)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie waaraan rechten zijn te ontlenen in b.v in basisregistratie of op de website)*	**Geheim** informatie is alleen toegankelijk voor direct aan de taak toegewezen persoon *(bv: zorggegevens, strafrechtelijke informatie)*

4. Beveiligingsaspecten ten aanzien van personeel

Doelstelling:
Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen.

Resultaat:
Werknemers, ingehuurd personeel en externe gebruikers kennen en begrijpen hun verantwoordelijkheden en zijn geschikt voor de rollen waarvoor zij (beoogd) worden benoemd.

4.1 Algemene uitgangspunten ten aanzien van personele beveiligingsaspecten

Hieronder volgen de geldende algemene uitgangspunten:

- De leidinggevende is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. Het team HRM houdt toezicht op dit proces.
- De leidinggevende bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden verstrekt.
- Bij inbreuk op de beveiliging gelden voor medewerkers de gebruikelijke disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en gemeentelijke regelingen.
- Regels die volgen uit dit beleid en andere gemeentelijke regelingen gelden ook voor externen, die in opdracht van de gemeente werkzaamheden uitvoeren.

4.2 Voorwaarden tewerkstelling vast personeel

Alle medewerkers in dienst van de gemeente:

- Leggen (vanaf 01-03-2006 in dienst) de eed/belofte af.
- Worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol dat ter ondertekening wordt voorgelegd.
- Overleggen eenmalig een Verklaring Omtrent Gedrag (VOG).
- Worden gewezen op de aanwezigheid van een gedragsprotocol.

- Krijgen bij indiensttreding eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling ter ondertekening voorgelegd door de leidinggevende. Dit gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI.

4.3 Voorwaarden tewerkstelling externen
Externen die tewerkgesteld worden bij de gemeenten Amstelveen en Aalsmeer, zoals uitzendkrachten, stagiaires en ingehuurde externe personen (zoals leveranciers) die toegang hebben tot vertrouwelijke gemeentelijk informatie:
- Tekenen een geheimhoudingsverklaring.
- Worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol dat ter inzage wordt voorgelegd.
- Worden gewezen op de aanwezigheid van een gedragsprotocol.
- Krijgen bij indiensttreding eventueel aanvullende, specifieke gedragsregels ten aanzien van een informatiesysteem of afdeling ter ondertekening voorgelegd door de leidinggevende. Dit gebeurt in ieder geval bij de Basisregistratie Personen (BRP), Waardedocumenten en SUWI.
- Overleggen eenmalig) een Verklaring Omtrent Gedrag (VOG).

4.4 Kwetsbare functies
De gemeente kiest voor een zorgvuldige selectieprocedure ter waarborging van een betrouwbaar personeelsbestand. Er wordt geen onderscheid gemaakt tussen functies. Van elke medewerker wordt verwacht dat hij/zij integer handelt.

4.5 Toegang en bevoegdheden personeel
Bij indiensttreding worden de fysieke en logische toegangsbevoegdheden volgens een vastgestelde procedure toegekend. De beslissing hierover moet door geautoriseerde personen worden genomen. Bij dienstbeëindiging of bij wijziging van functie worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van het lijnmanagement met onmiddellijke ingang en volgens een vastgestelde procedure verwijderd of aangepast aan de nieuwe status (zie hoofdstukken 5 en 7).

4.6 Opleiding en communicatie
Alle medewerkers (en voor zover van toepassing externe gebruikers van de gemeentelijke systemen) krijgen training in procedures die binnen de gemeente of afdeling gelden voor informatieveiligheid. Deze training dient regelmatig te worden herhaald om het beveiligingsbewustzijn op peil te houden. Ten aanzien van communicatie en bewustwording geldt dat:
- Alle medewerkers binnen de organisatie worden ingelicht over het informatieveiligheidsbeleid en de (beveiligings)procedures van de gemeente en informatie krijgen over het correcte gebruik van de ICT- en toegangsvoorzieningen. Dit geldt eventueel ook voor externe gebruikers.
- De algemeen directie en de leidinggevenden de algehele communicatie en bewustwording rondom informatieveiligheid bevorderen.
- De leidinggevenden bevorderen dat medewerkers (en externe gebruikers van onze systemen) zich houden aan beveiligingsrichtlijnen.
- In werkoverleggen periodiek aandacht wordt geschonken aan informatieveiligheid. Voor zover relevant worden hierover afspraken vastgelegd in planningsgesprekken.

4.7 Bijzondere situaties
In het geval van ernstige verdenkingen tegen een medewerker op het gebied van verduistering, fraude of ander gedrag dat in strijd is met de interne regels, is het mogelijk dat de AA organisatie gebruik maakt van opsporingsmiddelen zoals camerabeelden en loggegevens. Het betreft hier de bekende en reeds aanwezige middelen: logging ten aanzien van netwerk, applicaties, internet en email, elektronische deursloten en camera's. Voorwaarde voor de inzet van deze middelen, is naast een ernstige verdenking, de schriftelijke toestemming van de algemeen directeur. Indien nieuwe opsporingsmiddelen worden ingezet, zoals verborgen camera's en microfoons, dient een zogeheten "voorafgaand onderzoek" bij de Autoriteit Persoonsgegevens te worden aangevraagd. Deze heimelijke controle mag pas plaatsvinden nadat de Autoriteit Persoonsgegevens op basis van het voorafgaand onderzoek hiervoor toestemming heeft afgegeven.

5. Fysieke beveiliging

Doelstelling:
De fysieke bescherming van gebouwen, terreinen, informatie en (informatie)systemen tegen onbevoegde fysieke toegang, schade of verstoring van continuïteit.

Resultaat:
Maatregelen en procedures waarmee gebouwen, informatie- en ICT-voorzieningen adequaat worden beschermd tegen ongeautoriseerde toegang, kennisneming, verminking of diefstal, waardoor schade en verstoringen worden voorkomen.

5.1 Algemene uitgangspunten ten aanzien van fysieke beveiliging
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- De kwaliteit van toegangsmiddelen (deuren, sleutels, sloten, toegangspassen) is afgestemd op de zonering (en het risicoprofiel).
- Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de Wet Bescherming Persoonsgegevens en nadere regels.
- De fysieke toegang tot ruimten waar zich informatie en ICT-voorzieningen bevinden is voorbehouden aan bevoegd personeel.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht in lijn met geldende "best practices".

5.2 Inventarisatie van bedrijfsmiddelen
Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden onderkend. Het Team Facilitaire Zaken houdt een registratie bij van alle bedrijfsmiddelen die verband houden met veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen:
- De preventieve, detectieve, correctieve en repressieve systemen met betrekking tot inbraak, ontruiming, brand en toegang.
- Overzicht van toegangsrechten van personen tot ruimten, gebouwen en directe omgeving van het gebouw, zoals parkeerplaatsen.

5.3 Servicetaken
Indien voor de bewaking van de gebouwen, personen en goederen een externe bewakingsdienst wordt ingehuurd, voldoet deze bewakingsdienst aan de eisen volgens de Wet Particuliere Beveiligingsorganisaties en Recherchebureaus, beschikt deze over een vergunning van het Ministerie van Justitie en is deze aangesloten bij een brancheorganisatie. Er zijn afspraken gemaakt bij wie de bewakingsdienst verantwoording moet afleggen.

5.4 Verwijderen apparatuur en gegevensdragers
Afdeling ICT heeft een procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen.
Denk hierbij aan de harde schijven van pc's en netwerkservers, cd's/dvd's, back-up tapes, USB sticks en overige gegevensdragers. In deze procedure staan voorschriften voor het verwijderen en zo nodig onbruikbaar maken of vernietigen van die informatie.

5.5 Datakluizen en reserve apparatuur
- De datakluizen voldoen aan de eisen die gesteld worden om opgeslagen gegevensdragers in voldoende mate te beschermen tegen stof, brand, water, beschadiging en diefstal.
- Reserve apparatuur en back-ups worden gescheiden bewaard op een andere locatie of een datacenter om de gevolgen van een calamiteit te minimaliseren.

5.6 Clean desk en clear screen beleid
De gemeenten Amstelveen en Aalsmeer hebben een "clean desk"-beleid vastgesteld voor papieren en verwijderbare opslagmedia, zodat deze materialen niet onbeheerd op het bureau liggen. Daarnaast is er een "clear screen" beleid voor ICT-voorzieningen. Dit betekent dat alle medewerkers bij het verlaten van de werkplek het scherm zelf "locken". Eveneens gaat na een bepaald tijdsverloop het beeldscherm "op zwart" en wordt de toegang tot het werkstation geblokkeerd middels een toegangscode. Dit om het risico van onbevoegde toegang tot, verlies van of schade aan informatie, informatiedragers en ICT-voorzieningen tijdens en buiten normale werktijden te beperken.

5.7 Beveiliging van (mobiele) apparatuur

Informatieverwerkende mobiele apparatuur moet zowel binnen als buiten het gebouw zo mogelijk fysiek beschermd worden. Dit betreft laptops, PDA's, tablets (bijvoorbeeld iPad's), memorysticks en mobiele telefoons (smartphones). Voor het gebruik van deze apparatuur worden richtlijnen vastgesteld:

- Apparatuur en bijbehorende media mogen buiten de locatie niet onbeheerd worden achtergelaten.
- Bij het verwerken van vertrouwelijke, privacygevoelige en/of kritische gegevens zijn aanvullende maatregelen getroffen passend bij het classificatieniveau, zoals encryptie, wachtwoordbeveiliging, antivirusscanners enzovoort.
- Het uitwisselen van persoonsinformatie vindt altijd versleuteld plaats.

6. Beheer van communicatie- en bedieningsprocessen

Doelstelling:
Het garanderen van correcte en veilige bediening en beheer van de ICT-voorzieningen.

Resultaat:
Maatregelen en procedures voor het beheer en de bediening van de ICT-voorzieningen en het adequaat reageren op incidenten.

6.1 Organisatorische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.
- In beginsel is er een scheiding tussen beheertaken en overige gebruikstaken. Hierbij worden beheerwerkzaamheden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker. Er wordt echter per specifieke situatie bezien of deze scheiding een werkbare situatie oplevert en of de veiligheid hierdoor in dit specifieke geval wordt verhoogd.

6.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- Bij het openen of wegschrijven van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. Ook inkomende en uitgaande e-mails worden hierop gecontroleerd. De update voor de detectiedefinities vindt in beginsel dagelijks plaats.
- Op verschillende niveaus binnen de ICT-infrastructuur (netwerkcomponenten, servers, pc's) wordt antivirus software toegepast.
- Het is niet toegestaan niet-geautoriseerde (pc)programmatuur te gebruiken of te installeren op gemeentelijke ICT voorzieningen.
- Alle apparatuur die is verbonden met het netwerk van de gemeente moet kunnen worden geïdentificeerd.
- Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.
- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.
- Updates die ten behoeve van het verhogen van de veiligheid worden vrijgegeven door de leverancier worden zo spoedig mogelijk via de geëigende wijzigingsprocedure doorgevoerd. Dit geldt zowel voor besturingssoftware, informatiesystemen, als voor ondersteunende software (Java, Java applets, ActiveX, Flash en Adobe) en besturingssystemen voor mobiele apparatuur en actieve componenten.
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.
- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.

6.3 Beheerprocedures en verantwoordelijkheden

De verantwoordelijkheden en procedures voor het beheer van de bediening van de ICT-voorzieningen zijn beschreven en vastgesteld. Procedures zijn voor zover mogelijk in lijn gebracht met de ISO 20000-1 en ISO 20000-2 (ITIL 3).

Documentatie van beheerprocedures
De beheerprocedures zijn gedocumenteerd en worden bijgehouden. Deze procedures bevatten instructies voor de planmatige uitvoering van de activiteiten met betrekking tot ICT-voorzieningen. Het gaat om de volgende processen:

Change management / release management - doorvoeren van vernieuwingen en wijzigingen
Het aanbrengen van wijzigingen in de informatie-infrastructuur of het installeren van nieuwe versies vindt plaats volgens een vastgestelde wijzigingsprocedure waarin de formele goedkeuring geregeld is. Dit geldt voor apparatuur, programmatuur, productiesystemen en procedures. Voornaamste aspect bij dit proces is het garanderen van de continuïteit van het productiesysteem. Uitgangspunten hierbij zijn:

- Nieuwe systemen, upgrades en nieuwe versies worden getest op impact en gevolgen en pas geïmplementeerd na formele acceptatie en goedkeuring door de opdrachtgever en ICT (veelal de proceseigenaar). De test en de testresultaten worden gedocumenteerd.
- Systemen voor Test en/of Acceptatie (TA) zijn logisch gescheiden van Productie (P).
- Faciliteiten voor Testen, Acceptatie en Productie (TAP) zijn gescheiden om onbevoegde toegang tot of wijziging in het productiesysteem te voorkomen.
- In de TA worden testaccounts gebruikt. Er wordt in beginsel niet getest met productie accounts, mits voor de test absoluut noodzakelijk.
- Vertrouwelijke data uit de productieomgeving mag niet worden gebruikt in de ontwikkel-, test-, opleidings-, en acceptatieomgeving tenzij de gegevens zijn geanonimiseerd. Indien het toch noodzakelijk is om data uit productie te gebruiken, is uitdrukkelijke toestemming van de eigenaar van de gegevens vereist en dienen er procedures te worden gevolgd om data te vernietigen na ontwikkelen en testen.
- Het gebruik van ICT-middelen wordt gemonitord ten behoeve van een tijdige aanpassing van de beschikbare capaciteit aan de vraag.

Incident management - afhandeling van incidenten in de ICT infrastructuur
Om te waarborgen dat incidenten snel, effectief en ordelijk worden afgehandeld, zijn verantwoordelijkheden en procedures voor beheer vastgesteld. Hierbij worden verschillende typen incidenten onderscheiden en wordt gezorgd voor registratie en gedocumenteerde afhandeling van de incidenten.

Capaciteitsmanagement - omgang met de capaciteit van ICT voorzieningen
Om te waarborgen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken stelt afdeling ICT verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit.

Problemmanagement - identificeren en afhandelen van fouten in de ICT infrastructuur
Afdeling ICT richt een organisatie in en stelt procedures op ten aanzien van het achterhalen en wegnemen van fouten in de infrastructuur.

IT service continuity management - waarborgen van de continuïteit van de ICT-dienstverlening in geval van calamiteiten
Afdeling ICT stelt procedures op ten aanzien van voldoende technische, financiële en organisatorische voorzieningen ten behoeve van het waarborgen van de overeengekomen continuïteit van de ICT-dienstverlening in geval van calamiteiten. Uitgangspunten hierbij zijn:

- In opdracht van de eigenaar van data maakt ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd.
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens.
- De back-up wordt iedere dag buiten het gebouw opgeslagen.
- De back-up- en recovery-maatregelen worden regelmatig, doch minimaal één maal per jaar op een uitwijkcentrum en één keer per jaar in de eigen ICT-omgeving, getest.
- Over het resultaat van de test wordt aan de procesverantwoordelijken, de CISO en de controller informatieveiligheid gerapporteerd.

Configuratie management - registratie van ICT voorzieningen
Afdeling ICT stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.

Information security management - omgang met de v eiligheid van ICT voorzieningen
De CISO richt een organisatie in, stelt procedures op en traint personeel zodanig dat aan de eisen van het Informatieveiligheidsbeleid wordt voldaan.

6.4 Uitgangspunten voor controle en logging

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico, en zodanig dat tenminste wordt voldaan aan alle relevante wettelijke eisen, met name ten aanzien van de wet BRP en SUWI. Bij systemen waarin persoonsgegevens zijn ondergebracht, wordt logging ingezet om, in het kader van de Wet Bescherming Persoonsgegevens, c.q. meldplicht datalekken, inzichtelijk te kunnen maken of onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden. Deze loggings kunnen worden betrokken bij het doorlopen van de procedure veiligheidsincidenten - datalekken.

Relevante zaken om te loggen zijn:
Een log-regel bevat minimaal: een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; de gebeurtenis, waar mogelijk de identiteit van het werkstation of de locatie, het object waarop de handeling werd uitgevoerd, het resultaat van de handeling, de datum en het tijdstip van de gebeurtenis.

In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen.
Er worden maatregelen getroffen om te verzekeren dat gegevens over logging beschikbaar blijven en niet gewijzigd kunnen worden door een gebruiker of systeembeheerder. De bewaartermijnen zijn in overeenstemming met wettelijke eisen.
Ten aanzien van SUWI vraagt de Security Officer SUWI meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van SUWInet door de gemeente. Ten aanzien van de BRP worden logging rapportages minimaal maandelijks beoordeeld door de BRP beheerder.

6.5 Beheer van de dienstverlening door een derde partij

Bij externe hosting van data en/of services (uitbesteding, cloud computing) blijft de gemeente eindverantwoordelijk voor de betrouwbaarheid van uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.
Uitgangspunten bij externe hosting van data en/of services zijn:

- Goedgekeurd door de verantwoordelijke leidinggevende van de gemeenten Amstelveen en Aalsmeer.
- Voldoet aan de criteria voor leveranciers van webapplicaties en webservices opgenomen in de norm ICT-beveiligingsassessments DigiD.
- In overeenstemming met informatieveiligheidsbeleid en algemeen gemeentelijk beleid.
- Vooraf gemeld bij ICT ten behoeve van toetsing op beheeraspecten.
- De beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de (verwerkers)overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd.
- De diensten, rapporten en registraties, die door de derde partij worden geleverd, worden gecontroleerd en er bestaat de mogelijkheid voor het uitvoeren van (periodieke) audits.
- In de basis-SLA voor dienstverlening is aandacht besteed aan informatieveiligheid.
- Er is een basiscontract voor de toegang tot de ICT-voorzieningen en/of de informatievoorziening (bestanden, gegevens) door derden waarin de kaders staan voor de toegang tot ICT-voorzieningen door derden.

6.6 Telewerken

De gemeenten Amstelveen en Aalsmeer staan telewerken toe (op afstand werken op het netwerk van de gemeente, bijvoorbeeld thuiswerken) na toestemming van de verantwoordelijke leidinggevende. Hiervoor worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet en regelgeving (vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan).

Minimaal gelden hierbij de volgende uitgangspunten:

- Afspraken tussen de procesverantwoordelijke en "de telewerker", bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke of hoger geclassificeerde informatie.
- Richtlijnen op basis van risico's en wetgeving voor identificatie, authenticatie en wachtwoordgebruik.
- Richtlijnen op basis van risico's en wetgeving voor de technische inrichting van de telewerkplek (firewall, virusscanner, softwareversies, enz.).
- Afspraken omtrent de telewerkplek (de gemeente ondersteunt telewerken, maar faciliteert geen thuiswerkplek).
- Het inloggen met bijzondere systeembeheer bevoegdheden (administrator en root) via de telewerkplek is niet toegestaan tenzij er aanvullende maatregelen zijn getroffen.

6.7 Mobiele (privé-)apparatuur
Ten aanzien van "Bring Your Own Device/ Choose Your Own Device" (BYOD/CYOD) wordt beleid opgesteld en worden beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid en voor zover niet wordt verboden door wet- en regelgeving (Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan). Minimaal wordt aan onderstaande punten aandacht besteed:

- Afspraken tussen de procesverantwoordelijke en "de gebruiker van mobiele en/of privé apparatuur", bij voorkeur in de vorm van een overeenkomst, over het omgaan met vertrouwelijke en/of kritische informatie en/of documenten.
- Alle getroffen beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als op privé-apparatuur.
- Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, antivirusprogrammatuur en de instellingen van deze programmatuur, etc..
- Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ("jail break", "rooted device") is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan "mobile device management software").
- 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. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, ook betrekking hebben op privémiddelen en privébestanden.

6.8 Gebruik internet en email
E-mail- en internetprotocol
De gemeenten Amstelveen en Aalsmeer hebben een protocol (gedragscode) ten aanzien van het gebruik van e-mail en het gebruik van internet. In deze protocollen zijn maatregelen opgenomen om beveiligingsrisico's, verbonden aan het gebruik van e-mail en internet, te beperken.

6.9 Sociale media
Het gebruik van sociale media door medewerkers van de gemeenten Amstelveen en Aalsmeer is toegestaan. De medewerkers dienen zich ervan bewust te zijn dat ze online gezien worden als vertegenwoordigers van de organisatie. Uitingen op het internet worden permanent opgeslagen en kunnen eventueel via andere media opnieuw worden gepubliceerd. Voor het gebruik van sociale media wordt een protocol opgesteld. Hierin worden in ieder geval de volgende - middels dit document vastgestelde beleidsuitgangspunten - verder uitgewerkt:

- Geef nooit persoonlijke gegevens van jezelf of collega's zoals adressen en telefoonnummers. Dit om identiteitsfraude te voorkomen.
- Ook op internet is het wettelijk kader van toepassing en besef dat smaad, laster, auteursrecht en wetgeving op het gebied van gegevensbescherming van toepassing is.
- Bij de uitingen op het internet dient rekening gehouden te worden met het effect op het imago van de gemeenten Amstelveen en Aalsmeer.
- Uitingen op het internet mogen geen uitingen inzake klanten of zaken bevatten.

6.10 Beleid en procedures voor informatie-uitwisseling
Buiten onderstaande uitgangspunten worden beleid, formele procedures en formele beheersmaatregelen vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

- Het meenemen van vertrouwelijke of hogere geclassificeerde informatie buiten de gemeente vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is en uitsluitend indien maatregelen zijn getroffen die afgestemd zijn op de risico's en wetgeving (onder andere AVG, BRP en SUWI).
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met (telefoon)gesprekken, e-mail, faxen, ingesproken berichten op antwoordapparaten en het gebruik van de diverse digitale berichtendiensten dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt.
- Medewerkers zijn geïnstrueerd om zodanig om te gaan met mobiele apparatuur en verwijderbare media dat de kans op uitlekken van vertrouwelijke informatie geminimaliseerd wordt. Hierbij wordt ten minste aandacht besteed aan het risico van adreslijsten en opgeslagen boodschappen in mobiele telefoons.

- Medewerkers zijn geïnstrueerd om geen vertrouwelijke documenten bij de printer en dergelijke te laten liggen.
- Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.

7. Logische toegangsbeveiliging

Doelstelling:
Het beheersen van de toegang tot informatie en (informatie)systemen.

Resultaat:
Gedocumenteerd beleid en daarvan afgeleide maatregelen en procedures voor effectieve toegangsbeveiliging tot de informatie-infrastructuur en gegevens en het voorkomen van ongeautoriseerde toegang.

7.1 Beleid voor logische toegangsbeveiliging

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen implementeren en onderhouden is er een gemeentebreed toegangsbeleid. Naast dit gemeentebrede toegangsbeleid heeft ieder informatiesysteem nog een specifiek gedefinieerd toegangsbeleid, dat is afgestemd op de classificatie van de informatie.
Het toegangsbeleid is vastgesteld en bekend gemaakt aan de organisatie. Hierin worden in ieder geval de volgende - middels dit document vastgestelde beleidsuitgangspunten - verder uitgewerkt:

- Wachtwoorden bestaan uit minimaal 8 vrij te kiezen karakters, waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken. Daarnaast zijn wachtwoorden maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.
- Aanvragen voor toegang worden geautoriseerd door de procesverantwoordelijke (eigenaar van de data/applicatie).
- Er worden in de regel geen "algemene" identiteiten gebruikt. Voor herleidbaarheid en transparantie is het namelijk nodig om te weten wie een bepaalde actie heeft uitgevoerd.
- De gemeente maakt, waar mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie, autorisatie en informatieveiligheid (zoals: DigiD en eHerkenning).
- Alle toegekende bevoegdheden worden geregistreerd en beheerd, bijvoorbeeld in een autorisatiematrix.
- Het gebruik van speciale bevoegdheden wordt beperkt en beheerd.

7.2 Beheer van toegangsrechten

Voor de beheersing van toewijzing van toegangsrechten is een procedure vastgesteld, waarin de gehele cyclus is opgenomen van het registreren tot het afmelden van gebruikers. Naast wachtwoorden kunnen ook andere technologieën worden toegepast voor gebruikersidentificatie en authenticatie, zoals biometrie, handtekeningverificatie, hardware (bijvoorbeeld token), SMS authenticatie en cryptografische sleutels.
Bij het beheer van gebruikerswachtwoorden is vastgelegd op welke wijze het initiële wachtwoord aan de gebruiker kenbaar wordt gemaakt en hoe gehandeld wordt bij het vergeten van het wachtwoord.
Verstrekte wachtwoorden moeten onmiddellijk na het eerste gebruik door de gebruiker worden gewijzigd.

7.3 Externe toegang

De gemeente kan een externe partij toegang verlenen tot het gemeentelijke netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente, tenzij uitdrukkelijk overeengekomen.
De externe partij is verantwoordelijk voor authenticatie en autorisatie van haar eigen medewerkers. De gemeente heeft het recht hierop te controleren en doet dat aan de hand van de audit trail en interne logging.

7.4 Mobiel werken, thuiswerken en internetfaciliteiten

Uitgangspunten voor beleid ten aanzien van mobiel werken, thuiswerken en internetfaciliteiten:

- Voor werken op afstand is een thuiswerk- c.q. mobiele werkplekomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- Onbeheerde apparatuur (privé-apparaten of de "open laptop") kan gebruik maken van draadloze toegangspunten (WiFi). Deze zijn logisch gescheiden van het gemeentelijke bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat ("zero footprint"). Gemeentelijke informatie dient te worden versleuteld bij transport en opslag conform classificatie eisen.

- Sociale netwerken (Linkedin, Twitter, Google+, Pinterest, Instagram, Facebook, enz.) en openbare clouddiensten (Google docs, Dropbox, Gmail, OneDrive, WeTransfer, GoogleDrive, ICloud, etc.) worden door het lage beschermingsniveau (veelal alleen naam, wachtwoord en het ontbreken van versleuteling), commerciële belangen (verzamelen, verrijken en koppelen van informatie) en internationale regelgeving (mogelijk beschikbaar voor buitenlandse onderzoekdiensten), niet gebruikt voor het delen van vertrouwelijke informatie. Onder vertrouwelijke informatie valt in ieder geval persoonsinformatie.

7.5 Controle op toegangsrechten
Alle medewerkers die van het netwerk of applicaties gebruikmaken, moeten door het systeem of applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de Informatiearchitectuur effectief te beheren, wordt periodiek een uitdraai gemaakt van de verstrekte toegangsmachtigingen. Deze uitdraai wordt gecontroleerd op juistheid en volledigheid door de controller informatieveiligheid.

7.6 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten
Aanbrengen van scheidingen
Daar waar de risico's dit noodzakelijk maken, is scheiding in de netwerken aangebracht. De toegang tussen deze gescheiden "netwerkdomeinen" zijn beveiligd via bijvoorbeeld gateways, firewalls en routers. Afhankelijk van de toegangseisen voor de betreffende ICT-voorziening is het gebruik van de verbindingsmogelijkheden beperkt.

Demilitarized Zone (DMZ)
Voor wat betreft de internetfacing systemen moet gebruik worden gemaakt van een Demilitarized Zone (DMZ), waarbij compartimentering wordt toegepast en de verkeersstromen tussen deze compartimenten wordt beperkt tot alleen de hoogst noodzakelijke. O.a. de webapplicaties die gebruik maken van DigiD bevinden zich in deze DMZ. Door middel van minimaal 2 (virtuele) firewalls worden verkeersstromen tussen het internet, de (web)applicaties in het DMZ en het interne netwerk waar de backoffice applicaties en de gemeentelijke basisregistraties zich bevinden, tot een minimum beperkt.

Intrusion Detection Systeem
De gemeente maakt gebruik van een intrusion detection systeem zodat tijdig wordt gedetecteerd dat kwaadwillende misbruik willen maken van de webapplicatie. Intrusion Detection Systemen (IDS) helpen bij het detecteren van aanvallen op webapplicaties. Een IDS monitort continu het netwerk verkeer dat zich door de DMZ compartimenten verplaatst en kan, veelal op basis van aanvalspatronen, misbruik van webapplicaties en andere infrastructuurcomponenten detecteren.

Draadloze en openbare netwerken
Gebruik van draadloze netwerken vraagt om specifieke beveiligingsmaatregelen. Voor transport van vertrouwelijke en privacygevoelige gegevens via openbare netwerken zijn eveneens extra maatregelen nodig. Wettelijk is ten aanzien van persoonsgegevens minimaal encryptie vereist.

Actieve componenten
Voor logische toegang tot actieve componenten als routers, switches en firewalls gelden als basis dezelfde toegangsprocedures als voor de overige ICT voorzieningen. Daarbij voldoet de procedure aan de normen zoals gesteld in Norm ICT-beveiligingsassessments DigiD.

7.7 Toegangsbeveiliging met betrekking tot werkstations
Inlogprocedure werkstations
De toegang tot een informatiesysteem verloopt via een inlogprocedure, bedoeld om het risico van ongeautoriseerde toegang te beperken. In de procedure is onder meer het maximale aantal toegestane inlogpogingen, wachtwoordlengte en frequentie van wijziging vastgelegd.

Gebruikersidentificatie en -authenticatie
Identificatie en authenticatie van de gebruiker vindt altijd plaats. Hierdoor zijn activiteiten in het (informatie)systeem herleidbaar tot een natuurlijk persoon. Identificatie en authenticatie kunnen plaatsvinden door middel van gebruikersnamen in combinatie met wachtwoorden, smartcards, tokens of SMS authenticatie.

Schermbeveiliging (clear screen)
Medewerkers moeten bij het verlaten van de werkplek het scherm zelf "locken" en na een vaste periode van inactiviteit wordt een werkstation automatisch geblokkeerd. Bij werkstations op locaties met verhoogd risico kunnen aanvullende maatregelen genomen worden.

7.8 Toegangsbeveiliging met betrekking tot (informatie)systemen
Toegang tot (informatie)systemen

Autorisatie voor (informatie)systemen wordt verleend op grond van de rol van de medewerker. Binnen het (informatie)systeem krijgt de medewerker alleen toegang tot de functionaliteit en gegevens die nodig zijn voor de uitvoering van zijn of haar rol/taken. Alle medewerkers hebben een individueel gebruikersprofiel zowel op netwerk als op applicatieniveau waardoor mutaties en zo mogelijk ook raadplegingen altijd zijn terug te herleiden tot een individu.

(Informatie)systemen met vertrouwelijke of privacygevoelige gegevens
(Informatie)systemen die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciale maatregelen, zoals het plaatsen in een aparte beveiligde omgeving of domein. De procesverantwoordelijke stelt expliciet de gevoeligheid van een (informatie)systeem vast en de noodzaak voor aanvullende maatregelen.

8. Verwerving, ontwikkeling en onderhoud van systemen

Doelstelling:
Het waarborgen dat beveiliging wordt ingebouwd in (informatie)systemen en dat beveiligingseisen worden meegenomen in het proces van systeemontwikkeling en -onderhoud.

Resultaat:
(Informatie)systemen waarin zoveel mogelijk geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Maatregelen en procedures waarmee de beveiliging tijdens de ontwikkeling en het onderhoud van (informatie)systemen wordt gegarandeerd.

8.1 Beveiligingseisen voor (informatie)systemen

Bij de ontwikkeling van (informatie)systemen moeten beveiligingseisen vanaf aanvang in het ontwerpproces worden meegenomen. Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn. De volgende aspecten moeten bij ontwikkeling en onderhoud aan de orde komen:

- Beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd voordat een (informatie)systeem wordt ontwikkeld of aangekocht.
- Benodigde beveiligingsmaatregelen met betrekking tot audittrails en validatie van invoergegevens, interne verwerking en uitvoergegevens zijn, waar mogelijk, ingebouwd.
- Voor (informatie)systemen die vertrouwelijke of privacygevoelige gegevens bevatten, kunnen aanvullende beveiligingsmaatregelen nodig zijn die, op basis van classificatie en risicoanalyse, zijn vastgesteld.
- Bij extern toegankelijke applicaties, bijvoorbeeld webapplicaties, wordt extra aandacht besteed aan het voorkomen van ongeautoriseerde toegang.

8.2 Cryptografische beveiliging

Cryptografische systemen en technieken moeten worden toegepast in (informatie)systemen die vertrouwelijke en/of privacygevoelige gegevens verwerken en die onvoldoende kunnen worden beveiligd door andere maatregelen. Dit geldt met name voor gegevens die via openbare, grensoverschrijdende en draadloze netwerken worden getransporteerd (ook USB-sticks) en voor systemen die als standalone toepassing gebruikt worden, bijvoorbeeld op laptops, PDA's, tablets en smartphones.

PKI-certificaten worden herkend in veel standaardtoepassingen, zoals webbrowsers en e-mailpakketten. Met behulp van algemene PKI-certificaten is de informatie die personen en organisaties over het internet sturen, op een hoog niveau beveiligd.
PKIoverheidcertificaten bieden aanvullende zekerheden. Een digitaal certificaat van PKIoverheid (Public Key Infrastructure voor de overheid) waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling.
PKIoverheidcertificaten worden gebruikt bij:

- het zetten van een rechtsgeldige elektronische handtekening;
- het beveiligen van websites;
- het op afstand authenticeren van personen of services;
- het versleutelen van berichten.

Wanneer er gebruik gemaakt wordt van cryptografische sleutels dan dient het sleutelbeheer te zijn georganiseerd. Het gaat dan met name om de bescherming van de sleutels, het inrichten van de beheersrollen en de recoverymogelijkheden. Een sleutelbeheersysteem moet er minimaal voor zorgen dat sleutels niet onversleuteld op de servers te vinden zijn.

8.3 Digitale handtekening

Bij gebruik van digitale handtekeningen als middel om de authenticiteit en integriteit van elektronische documenten te waarborgen, worden alle sleutels afdoende beveiligd tegen wijziging en vernietiging. Ook worden persoonlijke sleutels (private keys) beschermd tegen onbevoegde openbaarmaking.

8.4 Uitbesteding ontwikkeling van (informatie)systemen

In deze situatie ontwikkelt de gemeente niet zelf een (informatie) systeem, maar besteedt het ontwikkel- en productiewerk uit. De gemeente gaat vervolgens over tot aanschaf van het (informatie) systeem of afname van een dienst. Bij uitbesteding van de ontwikkeling van (informatie)systemen wordt rekening gehouden met:

- Aangaan van een formele overeenkomst op basis van de algemene leveringsvoorwaarden van de gemeenten Amstelveen en Aalsmeer.
- Licentieovereenkomsten, eigendom van de broncode en intellectuele eigendomsrechten.
- Beoordeling en controle van de kwaliteit en nauwkeurigheid van het uitgevoerde werk.
- Privacygevoeligheid en bedrijfsvertrouwelijkheid van testgegevens, bijvoorbeeld door het gebruik van anonieme of fictieve gegevens en ingeval door de leverancier persoonsgegevens worden bewerkt. Daarnaast of deze leverancier meewerkt aan de totstandkoming van een verwerkersovereenkomst met de gemeente in de zin van de Wet Bescherming Persoonsgegevens.
- Mogelijkheid tot uitvoeren van IT audits bij de leverancier op de interne beheersingsmaatregelen of bij de door de leverancier ingeschakelde derden namens de gemeente.
- Zorgen voor een borg in geval de externe partij in gebreke blijft (b.v. Escrow).
- De leverancier een Third Party Memorandum (TPM) of ISAE3402 verklaring verzorgt, of vergelijkbare verklaring van een onafhankelijke partij (Register EDP auditor) over de relevante interne beheersing van processen en in het bijzonder de beveiligingsprocessen en aan de gemeente verstrekt indien deze daarom verzoekt.
- De beschrijving van de dienst is opgenomen in de overeenkomst. Verwijzing per geleverde dienst naar de betreffende service level specificaties. Denk hierbij aan een concrete beschrijving van diensten, servicetijden (normale servicetijden, weekends, feestdagen en vakantiedagen), service beschikbaarheid, responsetijden, oplostijden et cetera.
- De beschrijving van de overlegstructuren, de contactpersonen en de onderlinge communicatie is opgenomen in de overeenkomst. Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix).
- De beschrijving van de geschillenregeling is opgenomen in de overeenkomst. Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener (-aanbieder).
- De beschrijving van prestatie indicatoren, de manier van meten en de rapportagestructuur is opgenomen in de overeenkomst. Beschrijving van de prestatie indicatoren (Key Performance Indicators (KPI's)), hoe deze worden gemeten en hoe hierover wordt gerapporteerd.
- Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage.
- De leverancier toereikende technische en organisatorische maatregelen heeft genomen om de webapplicatie en gerelateerde gegevens te beveiligen tegen verlies, diefstal en inzage door daartoe niet bevoegde personen.
- De leverancier in de overeenkomst aangeeft dat de gehanteerde beveiligingsmaatregelen, zowel technisch als organisatorisch up to date worden gehouden en voldoen aan de laatst bekende beveiligingsinzichten, beveiligingsnormen en -richtlijnen.
- Of ingeval van een webapplicatie tenminste jaarlijks penetratietesten worden uitgevoerd waarbij uitgangspunt is dat de leverancier de gemeente in staat stelt om aan haar verplichtingen als verantwoordelijke, voortvloeiend uit de aan de DigiD gekoppelde wet- en regelgeving en de Algemene Verordening Gegevensbescherming (AVG) te voldoen.

8.5 Hardening van systemen

De hardening van alle systemen maar met name de internet facing systemen dient strak te zijn geregeld. Voor de webapplicaties en systemen geldt: alles dat open staat moet een reden hebben en alles dat open staat moet veilig worden aangeboden.

De hardening van interne systemen mag minder stringent. Voor interne systemen moeten de management functies secure zijn, er geen onveilige protocollen worden gebruikt, de default wachtwoorden zijn gewijzigd, en ongebruikte applicaties worden verwijderd.
Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het

standaard (default) installatie proces. Alle componenten van de ICT-infrastructuur moeten deel uitmaken van het hardeningsproces.

Voorbeelden van risico's die door hardening teniet worden gedaan zijn:
- Indien (externe) systemen, zoals webservers en mailservers "reclame" maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren.
- Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

8.6 Hardening van websites
Speciale aandacht krijgen hierbij de websites van de gemeente. Aangezien niet langer gebruikte websites of verouderde informatie die toegankelijk is via het internet een beveiligingsrisico opleveren dient de gemeente deze informatie te (laten) verwijderen. De gemeente en meer in het bijzonder de eigenaar van de specifieke website is hiervoor verantwoordelijk.

9. Beveiligingsincidenten

Doelstelling:
Bewerkstelligen dat informatieveiligheidsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Resultaat:
Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

9.1 Definitie beveiligingsincident
Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de beschikbaarheid, de integriteit of de vertrouwelijkheid van informatie of informatiesystemen in gevaar is of kan komen. Ook een mogelijk datalek valt onder de categorie beveiligingsincident.

Hierbij staat beschikbaarheid voor de garanties over het afgesproken niveau van dienstverlening en over de toegankelijkheid en bruikbaarheid van informatie(systemen) op de afgesproken momenten. Integriteit staat voor de juistheid, volledigheid en tijdigheid van informatie(systemen). Vertrouwelijkheid heeft betrekking op exclusiviteit van informatie en de privacybescherming. Hiermee wordt bedoeld dat uitsluitend gemachtigden toegang mogen hebben tot informatie(systemen).

Voorbeelden van beveiligingsincidenten zijn: besmettingen met virussen en/of malware, pogingen om ongeautoriseerd toegang te krijgen tot informatie of systemen (hacken), niet beschikbaar zijn van de website met dienstverleningsportaal, verlies van usb-stick met gevoelige informatie, diefstal van data of hardware of een gecompromitteerde mailbox.

9.2 Procedure melding en omgang beveiligingsincidenten
Er is een procedure voor het rapporteren van beveiligingsincident vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident. Hiervoor gelden de volgende uitgangspunten:
- Een medewerker meldt geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten bij de helpdesk.
- De beveiligingsincidenten worden door de helpdesk als geregistreerd.
- Vermissing of diefstal van apparatuur of informatie gerelateerd aan de gemeente of een veiligheidsincident waarbij persoonsgegevens zijn betrokken (mogelijk datalek) wordt ook aangemerkt als informatiebeveiligingsincident.
- Wanneer bij het incident persoonsgegevens zijn betrokken wordt direct de privacybeheerder hierbij betrokken.
- Afhankelijk van de ernst van een incident is er een meldplicht bij de Autoriteit Persoonsgegevens (AP) en betrokkenen.
- In de procedure worden eveneens de contact met de Informatieveiligheidsdienst (IBD) opgenomen.

- De informatie verkregen uit het beoordelen van beveiligingsmeldingen wordt geëvalueerd met als doel beheersmaatregelen te verbeteren (PDCA Cyclus).

Onderdeel van deze procedure of naast deze veiligheidsincidenten procedure stelt de gemeente een procedure vast voor het melden van datalekken inclusief een beslisboom inzake de meldplicht en zorgt de gemeente dat deze bekend is gemaakt binnen de organisatie. Van Algemene Verordening Gegevensbescherming (AVG) is er sprake van een datalek als de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Hier kan het ook gaan over een hack, diefstal van een laptop, een verkeerd geadresseerd mailbericht, etc. Ook indien er wel sprake is van een voldoende beveiligingsniveau kan er dus sprake zijn van een meldplicht datalek.

10. Continuïteitsbeheer

Doelstelling:
Het voorkomen van onderbreking van activiteiten van de gemeentelijke ICT-infrastructuur en het beschermen van de kritische bedrijfsprocessen tegen de effecten van ingrijpende storingen of calamiteiten.

Resultaat:
Een beheerst proces voor het waarborgen van de bedrijfscontinuïteit, waarmee de gebruikers, binnen een vastgestelde periode na het optreden van een beveiligingsincident of calamiteit, op aanvaardbaar niveau hun taken kunnen hervatten.

10.1 Proces van continuïteitsmanagement

Er is een beheerst proces vastgesteld om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen. Het proces kent de volgende onderdelen:

- Elke gemeentelijke afdeling voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland.
- Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In het continuïteitsplan worden de maatregelen beschreven waarmee de kritische bedrijfsprocessen van een afdeling na een onderbreking of verstoring voortgezet of tijdig hersteld kunnen worden. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - De risico's van bedreigingen worden beoordeeld naar de waarschijnlijkheid dat zij zich voordoen, de eventuele schade als gevolg daarvan en het herstel.
  - Identificatie van essentiële procedures voor bedrijfscontinuïteit.
  - Wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan.
  - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie).
  - Prioriteiten en volgorde van herstel en reconstructie.
  - Documentatie van systemen en processen m.b.t de noodprocedures.
  - Kennis en kundigheid van personeel om de processen weer op te starten.
  - Wijze en frequentie van testen van het plan.
- Indien interne of externe uitwijk is gerealiseerd, wordt minimaal jaarlijks een uitwijktest uitgevoerd. De uitwijkprocedures zijn ondergebracht in het draaiboek uitwijk.

10.2 Relatie met nood- en ontruimingsplan

De afdeling informatiebeheer zorgt voor het vaststellen van een ontruimingsregeling voor de computerruimte(n). Dit in aansluiting op het algemene noodplan en ontruimingsplan. Hierin is aangegeven op welke wijze de computerfaciliteiten worden uitgeschakeld bij calamiteiten, eventueel van buitenaf op afstand te regelen. Voorts is vastgesteld hoe afdeling ICT de afgesproken regeling zal testen en met welke frequentie.

10.3 Veiligstelling programmatuur

Voor alle systeemsoftware en informatiesystemen moet een afweging gemaakt worden of de broncodes door middel van bijvoorbeeld een Escrow-contract bij derden moeten worden ondergebracht.

10.4 Monitoring capaciteit

Voor alle relevante ICT-middelen wordt het capaciteitsbeslag dusdanig gepland dat continu wordt voldaan aan de eisen die gesteld worden vanuit de afspraken met de afnemers van het systeem. Performanceproblemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.

11. Naleving

Doelstelling:
Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen en waarborgen dat systemen en processen voldoen aan het beveiligingsbeleid van de gemeenten Amstelveen en Aalsmeer.

Resultaat:
Maatregelen en procedures waarmee naleving van wetten, verplichtingen en beveiligingseisen uit het beleid van de gemeente bewaakt wordt.

11.1 Organisatorische uitgangspunten

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin de informatieveiligheid het bereiken van de strategische doelstellingen ondersteunt.

- De CISO coördineert namens de algemeen directeur de uitvoering van het informatieveiligheidsbeleid.
- Afdeling informatiebeheer en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het informatieveiligheidsbeleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI, BRP en waardedocumenten. Aanvullend op dit informatieveiligheidsbeleid kunnen daarom specifieke normen gelden.
- Periodiek wordt de kwaliteit van informatieveiligheid onderzocht. Bijvoorbeeld door gemeentelijke auditors, onafhankelijke externen, audits, onderzoeken of zelfevaluaties. Jaarlijks worden meerdere audits/onderzoeken/zelfevaluaties uitgevoerd. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het "in control" statement.
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

11.2 Naleving van informatieveiligheidsbeleid en -plan

Om de naleving van de beveiligingseisen uit het informatieveiligheidsbeleid en -plan te bewaken, legt de procesverantwoordelijke adequate organisatorische en procedurele afspraken vast. Kernelementen in het controle- en evaluatieproces zijn:

- Zelfevaluatie en/of een audit, tenminste eenmaal per jaar, door de procesverantwoordelijke.
- Managementrapportages, tenminste eenmaal per jaar, getoetst door de controller informatieveiligheid op inhoud en vorm en ingebed in bestaande P&C-cyclus.

11.3 Naleving van wettelijke voorschriften

Relevante eisen uit wet- en regelgeving en contractuele eisen moeten voor ieder (informatie)systeem zijn vastgelegd. Er wordt deskundig advies over specifieke juridische eisen ingewonnen bij de juridische adviseur(s) van de gemeente. Conform de Archiefwet (de wettelijke plicht voor een gemeentelijk documentair structuurplan (DSP) is afgeschaft, maar het blijft verplicht om als gemeente de archiefbescheiden (document-, proces- of zaakgericht) te ordenen) beschikken de gemeenten Amstelveen en Aalsmeer over een systeem waarin opslag, bewaartermijn en vernietiging van gegevens en informatie in analoge en digitale vorm is geregeld.

Aan de bescherming van persoonsgegevens stelt de Algemene Verordening Gegevensbescherming (AVG) duidelijke eisen. De gemeenten Amstelveen en Aalsmeer stellen een privacybeheerder en een Functionaris Gegevensbescherming aan, die de uitvoering en de naleving van de AVG bewaken.

11.4 Beoordeling van de naleving
De procesverantwoordelijke leidinggevenden zorgen voor de controle en evaluatie op de naleving van wettelijke voorschriften van het informatieveiligheidsbeleid. Zij beoordelen of alle beveiligingsprocedures binnen hun verantwoordelijkheidsgebied correct worden uitgevoerd en of hun processen en (informatie)systemen voldoen aan relevante wet- en regelgeving, beveiligingsbeleid, normen en andere beveiligingseisen. Zij controleren de naleving van technische normen door productiesystemen te onderzoeken op de effectiviteit van de geïmplementeerde beveiligingsmaatregelen, bijvoorbeeld door het uitvoeren van een security scan. Daarnaast worden controles uitgevoerd door externe auditors (bv DigiD, BRP-, SUWI- en BAG-audit en de externe accountant) of door middel van zelfevaluaties.

Aldus vastgesteld in de vergadering van 30 januari 2018.
de secretaris,
mr. F.L. Romkema
de burgemeester,
J.J. Nobel

Begrippenlijst

Acceptatieprocedure
Procedure om vast te stellen of een nieuw (informatie)systeem voldoet aan de gestelde eisen Applicatiebeheer Onderhoud en exploitatie van de geautomatiseerde gedeeltes (software) van een informatiesysteem.

Afdelingsoverstijgend informatiesysteem (AIS)
Systeem dat door meer dan één afdeling wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd.

Application controls
Geprogrammeerde maatregelen binnen een applicatie ter waarborging van de vertrouwelijkheid, juistheid en volledigheid van de data. We kunnen hierbij denken aan het afschermen van menukeuzes, waardoor informatie niet oproepbaar is of het controleren van input op juistheid (postcode check) of volledigheid.

Audit (informatieveiligheids -)
Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid.

Authenticatie
Verificatie van de geclaimde identiteit, bijvoorbeeld door gebruik van wachtwoord, token, biometrie of een combinatie hiervan.

Autorisatie / autoriseren
Toekenning / toekennen van rechten (aan (groepen van) personen, processen en/of systemen).

Back-up
Reservekopie van een computerbestand of programmatuur.

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen.

Beschikbaarheid
Zie Continuïteit.

Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten.

Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen.

Change management
Beheer en beheersing van alle wijzigingen van componenten van (informatie)systemen en de ICT-infrastructuur.

Classificatie
Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.

Clean desk
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren.

Clear screen
Een uitgeschakeld of afgesloten beeldscherm dat alleen met een inlogprocedure weer actief gemaakt kan worden.

Compliance
Het begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.

Configuratie management

Beheer en beheersing van de samenstelling en de status van de ICT-infrastructuur en de (informatie)systemen die er gebruik van maken.

Configuratieschema
Overzicht van de onderdelen waaruit een (informatie)systeem is opgebouwd.

Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben.

Continuïteitsmanagement
Stelsel van samenhangende activiteiten, mensen en middelen met als doel de continuïteit van de (kritische) bedrijfsprocessen te waarborgen.

Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden.

Datakluis
Brand- en inbraakwerende ruimte voor de opslag van (elektronische) gegevensdragers.

Document Structuurplan (DSP)
Een DSP biedt een overzicht van alle aanwezige informatie- en archiefbestanden van een organisatie in relatie tot het werk dat in die organisatie gedaan wordt.

Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatieveiligheidsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen.

Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de softwareklant indien die zich wil indekken tegen bepaalde risico's in hoofde van de softwareleverancier (het meest gevreesde daarbij wellicht het faillissement van de leverancier).
De softwareleverancier zal de broncode van de software (en de bijhorende documentatie) in bewaring geven bij de escrowagent, en deze broncode regelmatig updaten indien nieuwe versies op de markt gebracht worden. Indien de leverancier dan failliet zou gaan, heeft de klant tenminste de broncode van haar applicatie en kan zij alsnog trachten haar applicatie aan de praat te houden.

Functiescheiding
Het scheiden van gerelateerde taken en bevoegdheden met als doel het voorkomen van fouten en fraude.

Fysieke beveiliging
Beveiliging die met behulp van fysieke (bouwkundige, technische en/of organisatorische) middelen gerealiseerd wordt.

Gateway
Verbinding tussen verschillende netwerken waarop wordt bijgehouden welke computers c.q. protocollen met elkaar verbonden mogen worden.

Gebruiker / gebruikende partij
Degene die geautoriseerd gebruik maakt van een (informatie)systeem.

Gegevensdrager
Een fysiek object waarin/waarop informatie is vastgelegd, bijvoorbeeld een boek, harde schijf, DVD of USB-stick.

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens.

Hardening
Het proces van het beveiligen van een systeem en het verminderen van kwetsbaarheden door middel van het reduceren van bijvoorbeeld (onbenodigde) software, functies, gebruikersnamen, logins of diensten. (Deze zouden namelijk toegang tot het systeem kunnen genereren via achterdeurtjes).

Informatie- en communicatietechnologie (ICT)

Het vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers. Hieronder valt het ontwikkelen en beheren van systemen, netwerken, databanken en websites. Ook het onderhouden van computers en programmatuur en het schrijven van administratieve software valt hieronder. Vaak gebeurt dit in een bedrijfskundige context.

ICT-component
Onderdeel van de informatie- en communicatie infrastructuur, zoals netwerk, bekabeling, servers, werkstations.

Identificatie
Bepaling van de identiteit van een persoon, bijvoorbeeld door een unieke gebruikersnaam of netwerkadres.

Incident
Onverwachte of ongewone gebeurtenis.

Incident management
Beheer en beheersing van de afhandeling van incidenten.

Informatieveiligheid
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.

Informatieveiligheidsbeleid
Strategie van een organisatie met betrekking tot informatieveiligheid.

Informatieveiligheidscontroller
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid en de escalatie van beveiligingsincidenten.

CISO
Medewerker die gemeentebreed adviseert over informatieveiligheidsvraagstukken in brede zin en activiteiten op het gebied van informatieveiligheid coördineert.

Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen.

Informatieveiligheidsanalyse
Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatieveiligheidsbeleid.

Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan.

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer

Information Technology Infrastructure Library (ITIL)
Een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar eerder een reeks van best practices (de beste praktijkoplossingen) en concepten.

Local Area Network (LAN)
Zie Lokaal netwerk.

Logische (toegangs)beveilig ing
(Toegangs)beveiliging die met behulp van programmatuur gerealiseerd wordt.

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellinggebonden netwerk.

Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur.

MARAP

Management Rapportage.

Medium (opslag-)
Fysieke gegevensdrager.

Netwerk
Een verzameling objecten voor communicatie tussen tenminste twee knooppunten van apparatuur en programmatuur, waarbij gebruik gemaakt wordt van voorgeschreven communicatieprotocollen.

Netwerkadres (IP Adres)
Unieke identificatie van een element in een netwerk.

Netwerkconfiguratie
Overzicht van de objecten waaruit het netwerk bestaat en de relaties tussen deze objecten.

Noodplan
Document waarin beschreven staat welke acties een organisatieonderdeel moet ondernemen in een noodsituatie.

Ontruimingsplan
Document waarin beschreven staat op welke wijze een gebouw ontruimd moet worden in een noodsituatie.

OTAP
Een methodiek die wordt gebruikt in de ICT. Dit geeft een pad aan dat wordt doorlopen tijdens onder andere softwareontwikkeling of het implementeren van nieuwe applicaties.
Het pad dat wordt doorlopen is als volgt: Een programma of component wordt eerst ontwikkeld in de ontwikkelomgeving. Als de programmeur denkt klaar te zijn wordt het gekopieerd naar de testomgeving. Daar kan gecontroleerd worden of het programma of component naar behoren werkt en of het goed kan communiceren met zijn omgeving. Als het goed is bevonden wordt het gekopieerd naar de acceptatieomgeving. Dit is een omgeving waar een gebruiker in kan kijken maar waar normaal gesproken geen gebruikers bij kunnen. De gebruiker kan dan beoordelen of aan zijn eisen en specificaties is voldaan. Indien de gebruiker het programma of component goedkeurt wordt het gekopieerd naar de productieomgeving waar het gebruikt kan worden door alle gebruikers van het systeem.

Personal Digital Assistant (PDA)
Kleine computer, formaat "binnenzak".

PKI (Public Key Infrastructure)
Een Public Key Infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd. Een onafhankelijke partij waarborgt de integriteit en authenticiteit van het certificaat. Hiermee wordt gegarandeerd dat de identiteit van de certificaatbezitter klopt ("je bent wie je zegt dat je bent") en dat gegevens veilig kunnen worden uitgewisseld.

Privacybeheerder
Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert.

Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel.

Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces.

Programmatuur
Het geprogrammeerde deel van (informatie)systemen.

Recovery
Herstel van een computerbestand of programmatuur.

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen.

Routering
Het bepalen van de weg die berichten volgen Security scan Gericht onderzoek naar de mate van implementatie van beveiligingsmaatregelen.

Service Level Agreement (SLA)
Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten.

Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet.

SNMP
Simple Network Management Protocol: een protocol voor netwerk management en beheer.

Systeem
Een verzameling van één of meer samenhangende objecten met tezamen een gespecificeerde functionaliteit. Objecten kunnen zowel fysiek (computersysteem) als logisch (besturingssysteem) zijn.

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem.

Systeemhulpmiddel
Hulpprogramma voor beheer en onderhoud van (informatie)systemen en ICT-infrastructuur.

Systeemklok
Interne klok in een computersysteem.

Systeemprivilege
Recht op het gebruik van of toegang tot (een onderdeel van) een (informatie)systeem.

Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem.

Technisch beheer
Opslag en onderhoud van digitale informatie door middel van technische Maatregelen.

Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding.

Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt.

Utility
Zie Systeemhulpmiddel.

Voice over IP (VOIP)
Gebruik van dezelfde netwerkbekabeling voor zowel spraak- als datacommunicatie.

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden.

Wide Area Network (WAN)
Netwerk dat zich niet beperkt tot één fysieke locatie en waaraan meerdere lokale netwerken (LAN's) gekoppeld kunnen zijn.

BIJLAGE 1 Rollen, namen informatieveiligheidsorganisatie

Beveiligingsrollen	Naam	Vervanger
Chief Information Security Officer (CISO)	Erik Versterre	Alfred Vonk
Controller Informatieveiligheid	Marco Slinger	
Functionaris Gegevensbescherming	Vacature	
Privacybeheerder	Nasim Ahmadi	Stephanie Dreyer
Beveiligingsbeheerder BRP	Margriet Wiegersma	Paul Herscheid
Beveiligingsbeheerder Suwinet	Erik Schneider	Vincent Bruinsma
Beveiligingsbeheerder Waardedocumenten	Margriet Wiegersma	Paul Herscheid
Beveiligingsbeheerder BAG	Dolf de Rooij	Irma Smak
Beveiligingsbeheerder BGT	Irma Smak	Dolf de Rooij
Beveiligingsbeheerder CORV	Cheryl Cordery	
Beveiligingsbeheerder DigiD	Erik Kogenhop	Luella de Regt
Beveiligingsbeheerder ICT	Erik Kogenhop	Marco Hofman
Beveiligingsbeheerder HRM	Daniela Wolterson	Yoyce Klimsop
Beveiligingsbeheerder IV	Maarten Schiphorst	Charlotte van den Berg
Beveiligingsbeheerder FZ	Dalila Çakmak	Exsell Rojer
Algemeen Contactpersoon Informatiebeveiliging (ACIB)	Erik Kamminga, Ingeborg Smal, Klaartje van Lakwijk en Raymond van Trirum	Helpdesk(medewerkers)
Vertrouwd Contactpersoon Informatiebeveiliging (VCIB)	Erik Kogenhop	Marco Hofman