Gemeentebreed informatieveiligheidsbeleid

Gemeente Amstelveen

Gemeente Aalsmeer

Versie	: Versie 2.0
Auteurs	: Walter Huith, Nasim Ahmadi, Luella de Regt, Margriet Wiegersma, Erik Schneider, Daniela Wolterson, Erik Kogenhop, Dalila Çakmak, Exsell Rojer, Yoyce Klimsop, Marco Slinger, Madelon Brouwer, Marco Hofman, Annechien Dongen, Margriet Slurink Irma Smak, Aart Los, Timo Vlijm, Karin Wensveen, Ferdy IJsselmuiden, Marie-Louise Radder, Esther Keijzer, Nino Tsjkadoea, Ramona Pakvis, Sander Mastwijk, Erik Kamminga, Milo van der Burgt en Charlotte van den Berg
Datum	: 8 en 15 december 2020

Zaaknummer Amstelveen: Z20-081623/D20-419161

Zaaknummer Aalsmeer: Z20-081624/D20-419173

Versiebeheer

Versie en datum	Wijziging	status
2.0 – 8 december 2020 (Amstelveen), 15 december 2020 (Aalsmeer)	• Geactualiseerd naar de BIO	Vastgesteld college Amstelveen en Aalsmeer
1.05 - 22 december 2017	• Actualisatie namen beheerders	Vastgesteld college Amstelveen en Aalsmeer
1.04 - 24 november 2017	• Toegevoegd beveiligingsbeheerder BGT	
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	
1.02 - 24 september 2017	• Tekst 'Beleid en procedures voor informatie-uitwisseling' verplaatst van 10.4 naar 6.10	
1.01 - 16 december 2016	• CORV beheerder aangepast (in bijlage 1)	
1.0 - 17 november 2016	Eerste oplevering	Vastgesteld college Amstelveen en Aalsmeer

Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van de gemeenten Amstelveen en Aalsmeer. De basis van dit informatieveiligheidsbeleid wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO). De BIO is afgeleid van de internationale informatieveiligheidsnormen NEN-ISO/IEC 27001:2017 en 27002:2017. De eerste standaard (ISO27001) is een norm voor de implementatie en planmatige borging van informatieveiligheid binnen de organisatie. De tweede standaard (ISO27002) bevat een verzameling van beveiligingsmaatregelen voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. In de BIO zijn de methodiek en de terminologie specifiek aangepast voor de situatie bij overheden.

De (landelijke) besluitvorming rondom de BIO heeft samengevat als volgt plaatsgevonden:

- De BIO is na instemming van alle overheidslagen interbestuurlijk bekrachtigd in het Overheidsbrede overleg Digitale Overheid (OBDO). Gemeenten zijn in dit overleg vertegenwoordigd door de VNG. Vervolgens is de BIO in december 2018 vastgesteld door de Ministerraad voor de Rijksoverheid.[1]
- De normen zelf zijn opgenomen in de 'pas-toe-of-leg-uit'-lijst van het Forum Standaardisatie (een bureau vanuit de rijksoverheid dat open standaarden bevordert, komt voort uit de wet digitale overheid) met verplichte standaarden voor de publieke sector. Deze lijst is opgesteld volgens het *comply or explain*-principe, wat betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dit niet te doen.

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

Afspraken die we maken over de rol- en taakverdeling bij de uitvoering van ons informatieveiligheidsbeleid geven uitdrukking aan het leidende principe binnen onze gemeentelijke organisatie, zoals verwoord in SBS (snelheid, bereikbaarheid en samenhang).

Zoals gezegd is de basis van dit informatieveiligheidsbeleid gevormd door de BIO. 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 strategische beleidsuitgangspunten op het gebied van informatieveiligheid[2] en de organisatie daarvan. Hierin staan het verantwoordingsmechanisme en de rollen en verantwoordelijkheden

[1] https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/

[2] Informatieveiligheid is het geheel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie

aangaande informatieveiligheid beschreven. Ook is rekening gehouden met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen 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). Om te voorkomen dat binnen elk van die gebieden separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatieveiligheidsbeleid op te stellen voor alle organisatieonderdelen. 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 BIO. Hierbij kunnen mogelijke alternatieve maatregelen gebaseerd op risico afwegingen worden ingezet om aan de in de BIO vastgestelde normen te voldoen.

Enkele beleidsuitgangspunten hebben betrekking op aandachtsgebieden 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 organisatie de beleidsuitgangspunten in dit document om de veiligheid van informatie bij deze keuze te vergroten.

Met dit document worden tevens de uitgangspunten ten aanzien van de veiligheid van informatieprocessen bepaald. Dit beleid brengt niet de huidige situatie in beeld, maar beschrijft het ambitieniveau aangaande gemeentebrede informatieveiligheid. Waar relevant is in dit document middels voetnoten een verwijzing naar de BIO opgenomen. Dit betekent echter niet dat in alle gevallen de volledige maatregel door de implementatie van dit beleid wordt afgedekt.

I.III Algemene oriëntatie en positionering

Informatieveiligheid maakt deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Het doel van informatieveiligheid is het behoud van:
- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen);
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig);
- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- Controleerbaarheid[3] / auditability (de mogelijkheid om (achteraf) vast te stellen hoe de informatievoorziening en haar componenten is gestructureerd en gebruikt).

I.IV 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 normalisering rechtspositie ambtenaren;

[3] Een regelmatige controle op uitvoering van de beheersmaatregelen is noodzakelijk om vast te stellen of deze goed werken. Daarom is controleerbaarheid (auditability, assurance, audit trail) van groot belang.

- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;
- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie grootschalige topografie (BGT);
- Wet Basisregistratie Ondergrond (BRO);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet Politiegegevens;
- Wet ruimtelijke ordening (Wro)/Omgevingswet.

Op grond van bovenstaande wet- en regelgeving worden er 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 de organisatie bij de sturing op en het beheer van informatieveiligheid. Resultaat: Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

1.1 Strategisch beleidsdocument voor informatieveiligheid

Het college van B en W behoort dit gemeentebreed strategische beleidsdocument voor informatieveiligheid goed te keuren en kenbaar te (laten) maken aan alle medewerkers, alsmede hiernaar te laten handelen.[4] Dit beleidsdocument bevat de onderstaande punten:

- De doelstellingen en strategische uitgangspunten van informatieveiligheid voor de gemeenten Amstelveen en Aalsmeer;
- De beveiligingseisen;
- De organisatie van informatieveiligheid (zie hoofdstuk 2);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatieveiligheidsrollen (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 en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd;
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie hoofdstuk 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. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college. Dit geldt ook voor de Gemeenteraad en de Griffie wanneer zij faciliteiten gebruiken die in beheer zijn bij de ambtelijke organisatie. Alle strategische beleidsuitgangspunten met betrekking tot informatieveiligheid en de organisatie van informatieveiligheid zijn in dit gemeentebrede document samengebracht.
Externe partijen moeten een zelfde beveiligingsniveau hanteren zoals opgenomen in dit beleid. Zij moeten tevens aan kunnen tonen dat zij voldoen aan dit niveau van beveiliging.

Op basis van dit gemeentebrede informatieveiligheidsbeleid worden, onder verantwoordelijkheid van de proceseigenaren, beleidsstukken uitgewerkt. Deze worden vastgesteld per organisatie-onderdeel (MT of hoger). In deze stukken wordt beschreven op welke manier de gemeenten informatieveiligheid borgen op

[4] BIO 5.1.1.1

specifieke onderwerpen, rekening houdend met de risico's. In dit voorliggende document wordt per onderwerp aangegeven welke stukken minimaal nader moeten worden uitgewerkt. De minimaal uit te werken stukken staan in bijlage 2.

1.2.1 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 het UWV [Uitvoeringsinstituut Werknemersverzekeringen] en de SVB [Sociale Verzekeringsbank]), 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 Overheid (BIO), 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.

1.3 Borging van het informatieveiligheidsbeleid

Om de 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 resulterend in een Information Security Management System (ISMS) [5] (zie figuur 1):

1. Informatieveiligheidsbeleid

Bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. 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, dit wordt ook wel het 'pas toe of leg uit' principe genoemd.
Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats.[6]

2. Informatieveiligheidsanalyse

Stap twee is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een informatieveiligheidsanalyse. Hiertoe wordt allereerst een overzicht opgesteld van de gegevensverzamelingen/applicaties in de gemeentelijke organisatie. Deze worden toegewezen aan een eigenaar en geclassifi-

[5] BIO 18.2.1.1

[6] BIO 5.1.2.1

ceerd op de risicoklassen beschikbaarheid, integriteit en vertrouwelijkheid van de informatie (ook wel dataclassificatie genoemd). Tevens wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. Hierbij geldt dat gemeentebreed het BBN2 wordt gehanteerd, hiervan kan bij individuele informatiesystemen slechts voldoende beargumenteerd (vastgelegd) worden afgeweken. Hierna wordt de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatieveiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO, middels het uitvoeren van een risico inventarisatie en evaluatie (RI&E), GAP-analyse, rondgang van het gebouw en een (eventuele) evaluatie van het vorige jaarplan. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar.

3. Jaarplan Informatieveiligheid

Op basis van de informatieveiligheidsanalyse wordt in stap drie een jaarplan opgesteld. De in de analyse geconstateerde risico's worden gewogen en waar nodig van maatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die vanuit de RI&E zijn geconstateerd, de beschikbare tijd en de beschikbare middelen. Hierdoor ontstaat een compact jaarplan waarmee de gemeente vaststelt welke verbeteracties gedurende een periode van 1 of 2 jaar worden uitgevoerd. Dit jaarplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid in de organisatie. De informatieveiligheidsorganisatie komt bij elkaar om de implementatie van het jaarplan informatieveiligheid te evalueren te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het informatieveiligheidsoverleg (zie paragraaf 2.2) minimaal tweemaal per jaar plaats.

4. Technische en organisatorische maatregelen

Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht is op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om applicaties zoals de BRP, SUWI, de BAG, het financiële systeem, of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen. Dit betreft met name het opstellen van procedures en werkinstructies.

1.4 Audits en naleving

De proceseigenaar beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.[7] Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus en ondersteund door een In Control Verklaring (ICV) gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld.[8]

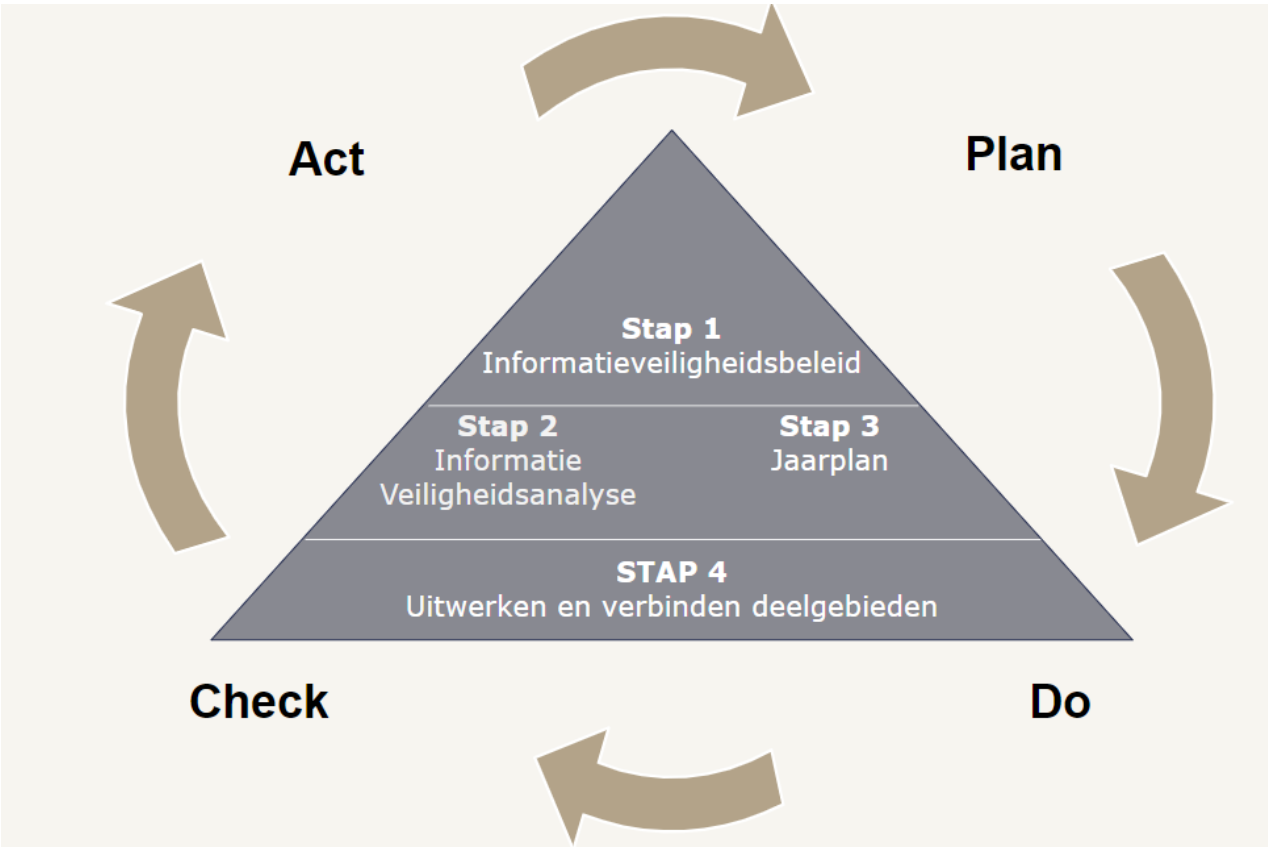
Om te beoordelen of de gemeenten Amstelveen en Aalsmeer hun informatieveiligheidsdoelstellingen behalen, worden periodieke onafhankelijke audits uitgevoerd in opdracht van de proceseigenaar. Hierbij wordt door een onafhankelijke partij een toets uitgevoerd op de opzet, bestaan en werking van beheersmaatregelen. Hiertoe kan een externe (erkende) partij worden ingeschakeld of de eigen afdeling concern control/auditafdeling. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen en organisatieonderdelen deze betrekking hebben.[9] In dit plan wordt tevens een beschrijving van de uit te

[7] BIO 18.2.2

[8] BIO 18.1.4.2, 18.2.2.1

[9] BIO 18.2.1.2

voeren controles opgenomen, evenals de uitvoerders van en verantwoordelijken (lijnniveau) voor de controles gekoppeld aan een tijdsplanning. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel van dit plan.[10] Over de resultaten van de uitgevoerde audits wordt door de lijnverantwoordelijken gerapporteerd aan de CISO en de controller informatieveiligheid. De CISO bundelt deze bijdragen en rapporteert hierover periodiek aan het bestuur.



Figuur 1: De informatieveiligheidspiramide met PDCA cirkel

[10] BIO 18.2.3.1

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.[11] Resultaat: Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

2.1 Verantwoordelijkheidsniveaus binnen de gemeenten Amstelveen en Aalsmeer

Binnen de gemeenten Amstelveen en Aalsmeer worden – waar relevant in lijn met geldende wet- en regelgeving – de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden[12]:

2.1.1 Kaderstellende en controlerende rol van de raad

De raad stelt de algemene beleidskaders vast en bepaalt daarmee de financiële en beleidsmatige grenzen voor de uitvoering door het college. Daarnaast draagt de gemeenteraad een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatieveiligheid. Het college legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring – waarop door een auditor assurance wordt afgegeven – en daarnaast in het jaarverslag met een passage over informatieveiligheid in de paragraaf bedrijfsvoering.[13] Dit alles conform de voorschriften van de landelijke verantwoordingsmethodiek ENSIA (Eenduidige Normatiek Single Information Audit).

2.1.2 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Het college van B en W van de gemeenten Amstelveen en Aalsmeer draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Verder stellen ze met het voorliggende beleidsdocument de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving vast. Het college informeert de Raad over de informatieveiligheid van de gemeente door een aparte paragraaf op te nemen in de jaarrekening van de gemeente. Hierin wordt de Raad op de hoogte gebracht over de stand van zaken, de uitgevoerde plannen van het afgelopen jaar en de planning en plannen van het volgende jaar. Daarnaast worden de Chief Information Security Officer (CISO) en de controller informatieveiligheid op basis van een vastgesteld functieprofiel aangesteld door het college van B en W.[14]

2.1.3 Gemandateerde verantwoordelijkheden en taken op organisatieniveau

De algemeen directeur voert onder mandaat van het college-activiteiten uit voor informatieveiligheid. Dit wordt in een mandaatbesluit vastgelegd. Deze stelt in overleg met het Management Team en de CISO het

[11] BIO 8.1.2

[12] BIO 6.1.1.2

[13] BIO 18.2.2.1

[14] BIO 6.1.1.2, 6.1.1.3, 6.1.1.4

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 proceseigenaar of systeemeigenaar aan (deze is verantwoordelijk voor het stellen van eisen aan een systeem en de inrichting van de controle hierop), zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen.[15]

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 informatieveiligheid;
- Het sturen op risico's omtrent informatieveiligheid;
- 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 om fraude en/of fouten te voorkomen.

2.1.4 Verantwoordelijkheden en taken op afdelingsniveau en teamniveau

De afdelingshoofden (ook wel proceseigenaren) zijn eigenaar van en integraal verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun afdeling.

De *afdelingshoofden* hebben in ieder geval de volgende verantwoordelijkheden:
- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen;
- Medewerkers attenderen op hun verantwoordelijkheid ten aanzien van informatieveiligheid in hun dagelijkse werkprocessen;
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn;
- Het (mede) bepalen van de betrouwbaarheidseisen per informatiesysteem op basis van expliciete risicoafwegingen.
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- Het oplossen van informatieveiligheidsincidenten;[16]
- Het expliciet vaststellen van relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen. Deze eisen moeten vastliggen voor elk informatiesysteem én voor de organisatie;[17]
- Het waarborgen van privacy en bescherming van persoonsgegevens conform relevante wet- en regelgeving;[18]
- Opdrachtgeven tot en toezien op het uitvoeren van periodieke beveiligingsaudits;
- Het rapporteren, via de CISO, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C-rapportages.

[15] BIO 8.1.2

[16] BIO 16.1.2.5

[17] BIO 18.1.1

[18] BIO 18.1.4

2.1.5 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 toezien of adequate risico-afweging plaatsvindt en of daarop vervolgens de juiste maatregelen genomen worden, evenals voor het opstellen van rapportages. Daarnaast coördineert de CISO het privacyteam.

De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:

- Rapporteert rechtstreeks aan de directie en het college van B&W;
- Coördineert het informatieveiligheids- en privacyteam;
- Coördineert het formuleren van informatieveiligheidsbeleid en het privacybeleid;
- Coördineert de uitvoering van de informatieveiligheidsanalyse en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het jaarplan informatieveiligheid;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt het college van B&W, de directie en de afdelingshoofden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid en privacy;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Geeft gevraagd én ongevraagd advies over informatieveiligheid en privacy aan de gehele organisatie;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Zorgt voor de registratie van informatieveiligheidsincidenten in een incidentenregister en is medeverantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatieveiligheid van de gemeente in het jaarverslag.
- Onderhoudt contact met de Informatiebeveiligingsdienst;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C-managementrapportages vergezeld van een in control statement. Hierbij bundelt de CISO de deelbijdragen van het afdelingsmanagement.

2.1.6 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 veiligheidsincidenten.

De *controller informatieveiligheid* is in ieder geval verantwoordelijk voor:

- 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 vice versa;
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en jaarplan informatieveiligheid;
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- De bewaking van het niveau van informatieveiligheid;
- De toetsing van evaluatieproces van veiligheidsincidenten;

- De rapportage van bevindingen aan de directie en aan het college van B en W.

De rol van controller informatieveiligheid heeft op twee specifieke deelgebieden een voorgeschreven benaming. Dit betreft het gebied van reisdocumenten en 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.

2.1.7 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid binnen een specifiek deelgebied. 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: DigiD, BRP, Waardedocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI) en de BAG. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals Facilitaire Zaken, ICT, IV [Archivering] en HRM) en de primaire processen (bijvoorbeeld Sociaal Domein, Financiën, Veiligheid & Handhaving, publieksdiensten [eventueel gecombineerd met BRP en Waardedocumenten], Ruimte/omgeving).

De *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 informatieveiligheidsincidenten en het geven van een adequate respons;
  - coördineren en toepassen van specifieke wet- en regelgeving;
  - rapporteren aan de CISO en de controller informatieveiligheid.

In bijlage 1 “Rollen en namen informatieveiligheidsorganisatie van de gemeente Amstelveen en Aalsmeer” zijn de beveiligingsbeheerders opgenomen en vastgesteld.

Specifiek (wettelijk) verplichte beveiligingsbeheerdersrollen:
- *Autorisatiebevoegde Reisdocumenten/Aanvraagstations:* Verantwoordelijk voor het beheer van de autorisaties (het toekennen van rechten in informatiesystemen aan personen of groepen) 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 (beveiligingsbeheerder SUWI):* verantwoordelijk voor het beheer van 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;
- 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.

2.1.8 Functionaris Gegevensbescherming

De FG (ook wel Data Protection Officer [DPO]) is conform de Algemene Verordening Gegevensbescherming (AVG) de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente.[19] De FG heeft de volgende wettelijke taken (AVG Art. 39), vertaald naar de situatie bij de gemeente:

Het takenpakket van de FG bestaat uit de volgende punten (art. 39 lid 1 AVG):
- Informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen volgens de AVG;
- Toezien op naleving van AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Toezien op naleving van het gemeentelijke beleid of de verwerker met betrekking tot de bescherming van persoonsgegevens;
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Adviseren met betrekking tot vraagstukken over de verwerking van persoonsgegevens;
- Adviseren met betrekking tot veiligheidsincidenten met persoonsgegevens;
- Adviseren met betrekking tot de Data Protection Impact Assessment (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Toezien op en adviseren over de afhandeling van vragen en klachten over het gebruik van persoonsgegevens;
- Adviseren en ondersteunen bij het opstellen van privacynormen, -procedure, -beleid, -regelingen of -gedragscodes;
- Rapporteert rechtstreeks aan directie en het college van B&W;
- Afstemming met de AP;
- Optreden als contactpunt voor de AP.

[19] BIO 18.1.4.1

De FG heeft voor privacy een toezichthoudende taak, vergelijkbaar met de taak van controller informatieveiligheid voor informatieveiligheid. De uitvoering en implementatie van het beleid is belegd bij de proceseigenaren.

2.1.9 De privacybeheerder

Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de privacybeheerder over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De *privacybeheerder* heeft in ieder geval de volgende verantwoordelijkheden:

- Het beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de (Europese) privacywetgeving. De privacybeheerder adviseert directie, afdelings- en teamhoofden bij wijzigingen in procesuitvoering en bedrijfsvoering en de toepassing van een Data Protection Impact Assessment (DPIA).
- 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 (Europese) privacywetgeving en in de sectorale wetgeving;
    b) coördineren van de privacyadvieswerkzaamheden;
    c) coördineren, samenvoegen en openbaar maken 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 FG en Autoriteit Persoonsgegevens (AP);
    e) coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
    f) richt procedures in voor het afhandelen van datalekken en draagt zorg voor de afhandeling van ingekomen veiligheidsincidenten;
    g) beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
    h) advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten, convenanten en de vaststelling van reglementen;
    i) bijdragen aan privacybewustzijn.

2.1.9.1 Privacybeheerder BRP

De privacybeheerder BRP komt voort uit de Wet BRP. Deze adviseert de informatiebeheerder, het College van Burgemeester en Wethouders en de medewerkers van afdeling Burgerzaken en andere gebruikers van de BRP over de privacyaspecten die voortvloeien uit de uitvoering van de Wet BRP en Verordening BRP. Tevens coördineert deze de eventuele BRP/reisdocumenten-audit en zorgt voor het inleveren van deze stukken in de Kwaliteitsmonitor.

2.1.10 Coördinator ENSIA

De coördinator ENSIA coördineert het ENSIA-proces. Hier valt het invullen en inleveren van de jaarlijkse vragenlijst onder, evenals het coördineren van de ENSIA-audits en het inleveren van de benodigde stukken in ENSIA. De eventuele BRP/reisdocumenten-audit en het inleveren van deze stukken in de Kwaliteitsmonitor valt hier niet onder, maar is een taak van de Privacybeheerder BRP. Deze coördinator is eveneens ENSIA-contactpersoon en heeft alle rechten in ENSIA.

2.1.11 I-adviseur

De I-adviseur is het I-aanspreekpunt voor de vakafdelingen en fungeert daarbij als een soort accountmanager; hij spreekt zowel de taal van ICT als van vakafdelingen. Vanuit informatieveiligheid helpt de i-adviseur met de communicatie van de eisen en wensen naar de vakafdeling. Hij wijst de vakafdelingen op hun verantwoordelijkheden en begeleidt hen hierbij. Voorbeelden hiervan zijn DPIA's, risicoanalyses en andere veiligheidsaspecten.

2.1.12 Contactpersonen Informatieveiligheid & Privacy

Er zijn wettelijke aspecten rond informatieveiligheid en privacy die alleen binnen de afdelingen spelen. Daarom hebben de proceseigenaren één of meerdere personen per afdeling/team aangewezen die contactpersoon zijn op het gebied van informatieveiligheid en privacy. Tot de taken van de contactpersoon behoren bijvoorbeeld:

- Actueel houden van het register van verwerkingsactiviteiten met alle verwerkingen die binnen de afdeling zijn geïnventariseerd;
- Het creëren van bewustwording binnen de afdeling;
- Betrokkenen de mogelijkheid bieden om hun rechten uit te oefenen;
- Onderhouden en beheren van verwerkersovereenkomsten.

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 het tactisch informatieveiligheidsbeleid zijn gedragsregels in het kader van informatieveiligheid uitgewerkt. Iedere medewerker wordt geacht deze gedragsregels te kennen en uit te dragen bij het uitoefenen van zijn of haar functie.

2.2 Overleg en afstemmingsorganen

De CISO is voorzitter van het overleg informatieveiligheid dat minimaal tweemaal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De CISO;
- De controller Informatieveiligheid;
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, BGT, BRO, CORV, Suwinet en DigiD;
- Beveiligingsbeheerders t.a.v.: FZ, ICT, IV en HRM;
- Privacybeheerder en Functionaris Gegevensbescherming;
- Agendaleden: directielid, afdelingshoofd, teamleider of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het jaarplan Informatieveiligheid;
- Evaluatie van veiligheidsincidenten;
- 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.

Daarnaast vindt afstemming plaats tussen de CISO en de functioneel-, applicatie- en gegevensbeheerder(s) en de proceseigenaar van (informatie)systemen.

2.3 Afdelingsoverstijgende (informatie)systemen

Afdelingsoverstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van het afdeling A&I 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 de bevoegdheid 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 de afdeling A&I.
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.

De gemandateerd eigenaar maakt minimaal de volgende schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt:

- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatieveiligheid;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van afspraken en oplossen van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

2.4 Informatiebeveiligingscrisisbeheersing

Voor interne crisisbeheersing maken we onderscheid tussen twee soorten crises: enkel ICT of gemeentebreed. In beide gevallen is vastgesteld wie bepaalt of er sprake is van een crisis, wie er contact houdt met de autoriteiten (brandweer, IBD e.d.) en is er een procedure vastgesteld. Voor beide soorten crisis dient er een kernteam geïnstalleerd te zijn. Deze teams komen uitsluitend bij elkaar in geval van grote incidenten of calamiteiten.

Het ICT-crisisteam bestaat in ieder geval uit:

- De coördinator Informatieveiligheid/CISO (voorzitter);
- De controller Informatiebeveiliging;
- De beveiligingsbeheerder ICT;
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts, medewerkers en directielid (indien nodig);
- De teamleider communicatie.

De gemeente voert veel taken uit die van belang zijn voor haar inwoners en/of die zijn verbonden aan wet- en regelgeving. Om deze taken uit te kunnen voeren, worden bedrijfsprocessen uitgevoerd die als ‘kritisch’ kunnen worden aangemerkt. Dit betekent dat langdurige uitval van deze processen onacceptabel is. Om langdurige stagnatie van deze processen te voorkomen, dient een proces voor continuïteitsbeheer te worden ingericht. Hierin is een inventarisatie gemaakt van bedrijfskritische processen. Verder staat er

minimaal beschreven wat er nodig is om de processen uit te voeren, wat de rollen zijn en in welke structuur dit past. Hierbij is het belangrijk dat er gemeentebreed wordt gekeken.

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 voor informatieveiligheid relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

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.

- Afdeling A&I houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (dit heet configuratiemanagement, zie ook 6.3).
- 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.
- De afdeling 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.
- Elke afdeling houdt een registratie bij van alle data, applicaties en overige assets die zij hebben.

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 Classificatie van informatie en bedrijfsmiddelen (en BBN)

Ten aanzien van classificatie van informatie, applicaties en bedrijfsmiddelen geldt het volgende:

- De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.[20]
- De informatie in papieren bestanden en archieven wordt geclassificeerd.[21]
- De classificatie van informatiesystemen wordt vastgelegd in een tabel of een CMDB, op documenten wordt de classificatie aangegeven, zoals nader in gedragsregels wordt uitgewerkt.
- De opsteller van de informatie doet een voorstel tot rubricering en brengt deze aan op de informatie. De vaststeller van de inhoud van de informatie stelt tevens de rubricering vast.

[20] BIO 8.2.1, 8.2.1.1

[21] BIO 11.1.4.1

De proceseigenaren zijn hiervoor verantwoordelijk.

De volgende classificaties en schadecategorieën worden gebruikt:

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0 **(geen schade)**	**Openbaar** Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.	**Niet zeker** Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.	**Niet nodig** De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
Laag / I **(enige schade)**	**Bedrijfsvertrouwelijk** Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.	**Beschermd** Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-) fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen	**Belangrijk** De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen
Midden / II **(serieuze schade)**	**Vertrouwelijk** Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.	**Hoog** Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen.	**Noodzakelijk** De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schade toebrengen.
Hoog / III **(zeer grote schade)**	**Geheim** Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. Weerstand tegen statelijke actoren noodzakelijk. Let wel: statelijke actoren kan binnen de gemeentelijke context vertaald worden naar georganiseerde misdaad en ondermijning.	**Absoluut** Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen	**Essentieel** De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.

Bron: Handreiking Dataclassificatie v.2.1, IBD, 2019

Basisbeveiligingsniveaus

BBN	Beschikbaarheid	Integriteit	Vertrouwelijkheid
BBN 1	Laag	Laag	Laag
BBN 2	Midden	Midden	Midden
BBN 3	Midden	Midden	Hoog

Voor de toepasselijkheid van BasisBeveiligingsNiveaus (BBN), zoals die in de BIO worden gebruikt, geldt het volgende:

- In het algemeen moeten bij overheden maatregelen van BBN2 worden toegepast;
- Voor informatie, applicaties en bedrijfsmiddelen met een classificatie 0 of 1 op zowel vertrouwelijkheid, integriteit als beschikbaarheid kan worden volstaan met maatregelen volgens BBN1;
- Voor informatie, applicaties en bedrijfsmiddelen met een classificatie 3 op een of meer van de aspecten vertrouwelijkheid, integriteit of beschikbaarheid, wordt met een gedocumenteerde risicoanalyse onderzocht of en welke additionele maatregelen ten aanzien van deze aspecten nodig zijn.

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. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

4.1 Verantwoordelijkheden en uitgangspunten

Verantwoordelijkheden

Het lijnmanagement is verantwoordelijk voor de personele beveiliging binnen de gemeentelijke organisatie. Daarbij is het afdelingshoofd verantwoordelijk voor een juiste afhandeling van het aangaan, wijzigen of beëindigen van een dienstverband of overeenkomst met interne en externe partijen. De afdeling HRM ziet toe op en ondersteunt in een correct in-, door- en uitstroomproces van medewerkers en ingehuurd personeel en voorziet in aansluiting bij een klokkenluidersregeling.[22]

Van iedere medewerker ligt vast wat de taken en verantwoordelijkheden zijn ten aanzien van informatieveiligheid, met minimaal aandacht voor:[23]

- de uitvoering en naleving van de uitgangspunten uit het informatieveiligheidsbeleid;
- de bescherming van en juiste omgang met bedrijfsmiddelen;
- het melden van informatieveiligheidsincidenten;
- de bescherming en beveiliging van en juiste omgang met persoonsgegevens.

Uitgangspunten

Alles wat in dit document of in de documenten van HRM m.b.t. informatieveiligheid wordt opgeschreven, is (tenzij anders aangegeven) van toepassing op alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen van de gemeenten Amstelveen en Aalsmeer (hierna: medewerker). Iedere medewerker die werkzaam is voor de gemeenten dient bekend te zijn met en aandacht te besteden aan de uitgangspunten zoals beschreven in dit document.

Er worden door afdeling HRM voorschriften en gedragsregels opgesteld. Deze zijn eenvoudig toegankelijk en gecommuniceerd. Het niet naleven van regelingen, voorschriften of beleid kan leiden tot disciplinaire maatregelen jegens de medewerker.

Iedere medewerker heeft de juiste (minimale) autorisaties voor informatiesystemen om zijn werk te kunnen doen. Zie voor nadere eisen hoofdstuk 6**.**

[22] BIO 7.2.1.1

[23] BIO 6.1.1.1

Toegang tot persoonlijke mailbox of account
Het is mogelijk dat een afdelingshoofd een verzoek doet (bij de Servicedesk ICT) voor toegang tot de persoonlijke mailbox of persoonlijke account van een medewerker. Deze medewerker is vaak langdurig ziek, ontslagen of om andere redenen (niet meer) aanwezig. Er kunnen echter goede (continuïteits)redenen zijn van de afdeling om deze toegang te verlenen. Tegelijkertijd moet de bescherming van de levenssfeer van de medewerker geborgd zijn. Om deze reden kan een dergelijk verzoek pas gehonoreerd worden na schriftelijke opdracht van de gemeentesecretaris, die zich kan laten adviseren door de CISO en de FG.

Verdenking
In gevallen 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 gemeenten Amstelveen en Aalsmeer gebruik maken van heimelijke waarneming en toegang tot informatie waartoe normaal gesproken alleen de medewerker is geautoriseerd (zoals de persoonlijke mailbox). Ook bedrijfsmiddelen, zoals telefoons en gegevensdragers, en netwerkgebruik kunnen in deze gevallen worden onderzocht. Er kan gebruik worden gemaakt van opsporingsmiddelen zoals camerabeelden, loggegevens en bestandsinspecties. Het betreft hier de bekende en reeds aanwezige middelen: logging ten aanzien van netwerk, applicaties, internet en email, elektronische deursloten en camera's. Voorwaarde van de inzet van deze middelen is, naast een ernstige verdenking, een schriftelijke opdracht van de gemeentesecretaris of de burgemeester en op basis van een regeling waarmee de ondernemingsraad heeft ingestemd (Art. 27 WOR).[24] 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.

4.2 Gedragseisen

Er zijn gedragsregels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen. Hier worden nadere regels voor opgesteld, minimaal:

- het werken op afstand;
- het gebruik van privémiddelen;
- gedragscode t.a.v. het gebruik van e-mail en internet.

4.2.1 10 gouden regels
In deze bovenstaande regels worden minimaal de tien gouden regels voor informatieveiligheid en privacy uitgewerkt:

1. Ga vertrouwelijk om met informatie
    a. Houd je aan de geheimhoudingsplicht die je met je werkgever hebt afgesproken
    b. Praat met je collega's niet over vertrouwelijke informatie van collega's, burgers en bedrijven
2. Houd je aan clean desk en clear screen
    a. Vergrendel je beeldscherm. Herinner je collega's hier ook aan wanneer zij dit vergeten.
    b. Laat vertrouwelijke informatie niet onbeheerd op je bureau liggen.
    c. Zorg dat je bureau leeg is als je langdurig van je plek af bent én aan het einde van de dag.
3. Laat geen onbevoegden toe op onze werkplekken

[24] BIO 7.2.3

   a. Begeleid je bezoeker het gebouw in en laat ze ook weer uit.
   b. Spreek onbekende personen aan indien je vermoedt dat zij onbegeleid door het gebouw zwerven.
4. Houd je wachtwoorden altijd geheim
   a. Deel je wachtwoorden niet met derden of collega's
   b. Wijzig je wachtwoorden regelmatig en schrijf wachtwoorden niet op
   c. Lengte wint het van complexiteit, gebruik eventueel een zin als wachtwoord
5. Meld veiligheidsincidenten en datalekken direct via TOPdesk Selfservice Portal (via Atlas)
   a. Wees niet terughoudend met het melden van incidenten. Er zijn geen consequenties verbonden aan het doen van een melding. Er wordt geen informatie vrijgegeven over de melder.
   b. De procedure is zo laagdrempelig mogelijk ingericht, zodat meldingen snel kunnen worden opgepakt en er beheersmaatregelen kunnen worden getroffen.
   c. Twijfel je? Je kunt ook eerst bellen met het privacyteam.
6. Werk veilig met digitale gegevensdragers en mobiele apparatuur
   a. Laat laptops, tablets en telefoons nooit onbeheerd achter.
   b. Zorg voor goede beveiliging zoals pincodes en gebruik enkel goedgekeurde apps.
   c. Werk altijd via de beveiligde thuiswerkfaciliteit en plaats geen vertrouwelijke bestanden op je mobiele apparatuur.
   d. Maak gebruik van veilige en met een wachtwoord beveiligde Wifi-verbindingen. Bij gebruik van open en onbeveiligde Wifi-verbindingen kan iedereen kinderlijk eenvoudig meekijken.
7. Werk zo min mogelijk met papieren dossiers
   a. De gemeente heeft als uitgangspunt zoveel mogelijk digitaal te werken.
   b. De bestanden worden op ons netwerk goed beveiligd.
   c. Neem informatie alleen in fysieke vorm mee als dit strikt noodzakelijk is.
8. Wees alert op verdachte websites, e-mails en telefoontjes
   a. Wees alert op verdachte telefoontjes. Verstrek geen vertrouwelijke gegevens als je niet 100% zeker bent of je de juiste persoon aan de lijn hebt.
   b. Open geen verdachte bestanden en klik niet op links die je niet vertrouwt.
   c. Neem bij twijfel contact op met de Servicedesk ICT.
9. Mail persoonsgegevens naar externen altijd via ZIVVER
   a. Verstuur persoonsgegevens naar externen altijd via de beveiligde mailfunctie. Accepteert de ontvangende partij dit niet, doe hier dan melding van bij de CISO en/of FG.
   b. Wend je bij vragen over het gebruik van ZIVVER tot de applicatiebeheerder ZIVVER via TOPdesk Selfservice Portal (via Atlas)
10. Gebruik je gezonde verstand!
   a. Informatieveiligheid en privacy is vaak ook een kwestie van je gezonde verstand gebruiken.
   b. Schiet niet in de kramp.
   c. Bij twijfel: raadpleeg de CISO, FG of privacybeheerder, zij staan je graag te woord!

4.2.2 Andere generieke eisen

Andere eisen zijn:

- 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.

- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan. 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 IT apparatuur is in beperkte mate toegestaan. De IT apparatuur die aan medewerkers van gemeente beschikbaar wordt gesteld, dient in principe voor zakelijke doeleinden gebruikt te worden. In beperkte mate is het gebruik voor privé-doeleinden echter toegestaan.
- E-mails naar buiten met gevoelige gegevens (zoals persoonsgegevens) worden altijd beveiligd verstuurd.
- Vertrouwelijke informatie (zoals persoonsgegevens) worden niet gedeeld via Sociale Netwerken (Facebook, LinkedIn etc.) en openbare clouddiensten (Dropbox, Google Docs, Gmail, WeTransfer etc.). Deze hebben een te laag beschermingsniveau, er spelen commerciële belangen en zijn vaak buiten Europa gevestigd, waardoor internationale regelgeving geldt (lees: mogelijke beschikbaarheid voor buitenlandse onderzoekdiensten).
- Enkel applicaties en diensten die worden aangeboden door de gemeente worden gebruikt voor het delen van vertrouwelijke informatie.
- Het uitwisselen van persoonsinformatie vindt altijd versleuteld plaats.
- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- 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 mobiele apparatuur, verwijderbare media, (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 geen vertrouwelijke documenten bij de printer en dergelijke te laten liggen.

4.2.3 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 en voor zover niet wordt verboden door wet en regelgeving.[25] Hiervoor worden in een thuiswerkbeleid en gedragsregels beveiligingsmaatregelen vastgesteld en getroffen die in overeenstemming zijn met het gemeentelijk informatieveiligheidsbeleid.

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;
- Het inloggen met bijzondere systeembeheer bevoegdheden (administrator en root) via de telewerkplek is niet toegestaan tenzij er aanvullende maatregelen zijn getroffen;
- De medewerker is verplicht om de eigen computer te beveiligen;

[25] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

- 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.

4.2.4 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.[26] Gebruikers met eigen of ongeauthenticeerde apparatuur (BYOD) krijgen alleen toegang tot een onvertrouwde zone.[27]

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 voor werk 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 MDM-software [MDM staat voor mobile device management]). Deze beveiligingsinstellingen 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.

4.2.5 Sociale media

Niet iedereen mag op sociale media over of namens de gemeenten communiceren. Dit mag alleen door de directie van de gemeenten Amstelveen/Aalsmeer én door hen aangewezen medewerkers. Andere medewerkers is dit niet toegestaan, ook niet met een privéaccount. Dit geldt zowel voor teksten als voor foto’s, video- en geluidsopnamen. Bij sociale media valt te denken aan: Facebook, LinkedIn, Twitter, Snapchat, Instagram etc.[28]

Het privégebruik 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

[26] Vanuit de SUWI regelgeving en de BRP regelgeving wordt thuisgebruik niet zondermeer toegestaan.

[27] BIO 9.1.2.2

[28] BIO 10.8.1.2

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.

4.3 Voorwaarden tewerkstelling personeel

Er wordt een indiensttredingsprocedure opgesteld, voor alle medewerkers. Hierin staat vermeld welke activiteiten in het proces worden uitgevoerd en waar de verantwoordelijkheid voor de verschillende activiteiten is belegd. De eisen van de BIO worden hierin meegenomen.

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.

Alle medewerkers in dienst van de gemeente:

- Indien in dienst: leggen de eed/belofte af. Onderdeel daarvan is de verplichting tot geheimhouding.
- Indien extern: tekenen een geheimhoudingsverklaring.
- Doen mee met een onboardingsbijeenkomst waarin o.a. aandacht wordt gevestigd op informatieveiligheid & privacy. Daarnaast volgen ze een verdiepingscursus over dit onderwerp.
- Volgen een e-learningscursus ten aanzien van Informatieveiligheid & privacy
- Worden geacht te handelen conform de voorschriften zoals vermeld in het integriteitsprotocol dat ter ondertekening wordt voorgelegd.
- Overleggen eenmalig een Verklaring Omtrent Gedrag (VOG).
- Ontvangen schriftelijk de algemene en functiegebonden gedragsregels en verantwoordelijkheden op het gebied van informatieveiligheid. Voorbeeld: integriteitsprotocol.
- 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.

4.4 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 hoofdstuk 6).

4.5 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 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.

Door de gemeente wordt een opleidingsplan vastgesteld. Onderdeel hiervan is dat elke medewerker binnen drie maanden na indiensttreding een training I-bewustzijn succesvol moet hebben gevolgd.[29] Hiermee wordt geborgd dat medewerkers over adequate kennis en vaardigheden beschikken om hun functie juist en veilig uit te voeren. Hiermee wordt tevens geborgd dat er voldoende kennis en vaardigheid in de organisatie aanwezig is om het gewenste niveau van informatieveiligheid te bereiken en te behouden.[30]

[29] BIO 7.2.2.2

[30] BIO 7.2.2

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 verstoring wordt voorkomen.

Implementatie:
Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

5.1 Algemene uitgangspunten ten aanzien van fysieke beveiliging

- Reikwijdte: Dit beleid is van toepassing op alle terreinen en gebouwen die door de gemeenten Amstelveen en Aalsmeer worden gebruikt voor haar wettelijke taken, ook wanneer deze geheel of gedeeltelijk door een derde worden beheerd of mede gebruikt worden door andere organisaties. Gebouwen die uitsluitend als sporthal, zwembad of buurthuis worden gebruikt vallen niet onder dit beleid.
- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen;
- In en rond de gebouwen zijn beveiligingszones gedefinieerd.[31] Bijzondere aandacht is er daarbij voor decentrale ICT- en technische ruimtes (zoals patch- en zekeringskasten). Per zone gelden eigen, beschreven, beveiligingsmaatregelen. De overgangen tussen deze zones zijn fysiek gescheiden.[32] Toegang tot niet-openbare zones is alleen mogelijk na autorisatie daartoe. De autorisaties worden verleend op basis van het principe least privilege: medewerkers krijgen alleen toegang tot ruimtes voor zover dit voor hun werk nodig is.
- De uitgifte van toegangsmiddelen wordt geregistreerd en de identiteit van de ontvanger wordt vastgesteld d.m.v. een legitimatiebewijs. Niet-uitgegeven toegangsmiddelen worden beveiligd opgeborgen. Indien gebruik gemaakt wordt van beeldmateriaal wordt dit beperkt door de AVG en nadere regels.
- Bij de keuze van locaties en bij de nieuwbouw, verbouw en renovaties wordt rekening gehouden met misdaadpreventie en veiligheid, dit wordt gedocumenteerd op basis van een risico-analyse waarbij de systematiek van de VRKI uitgegeven door het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) wordt gebruikt. Bij het ontwerp, de omgeving en de inrichting van gebouwen worden de principes van CPTED (Crime Prevention Through Environmental Design) toegepast.
- Serverruimtes, datacenters en daaraan gekoppelde bekabelingsystemen zijn ingericht volgens Telecommunication Infrastructure Standard for Data Centers (TIA-942).[33]
- Er is door de brandweer goedgekeurde en voor de situatie geschikte brandblusapparatuur geplaatst en aangesloten. Dit wordt jaarlijks gecontroleerd.

[31] BIO 11.1.1
[32] BIO 11.1.2
[33] BIO 11.2.3

- Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010 (de norm voor elektrotechnische laagspanningsinstallaties in woningen, gebouwen en infrastructuur).[34] In het bijzonder wordt vermeden dat van buitenaf herkenbaar is waar deze kabels het pand binnenkomen.
- Gebouwen zijn beveiligd tegen blikseminslag.
- Voor fysieke toegangssystemen, alarmeringssystemen, noodstroomvoorzieningen en klimaatvoorziening voor serverruimtes/datacenters is een onderhoudsplan dat voorziet in periodieke controles, preventief onderhoud en tijdige vervanging.[35]

5.2 Inventarisatie van bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten zowel de informatie als de bedrijfsmiddelen worden geïnventariseerd en vervolgens moet 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. Er wordt minimaal jaarlijks geverifieerd of de bewakingsdienst aan deze eisen voldoet.

5.4 Verwijderen apparatuur en gegevensdragers

Afdeling A&I 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.[36]

Bij uitbesteding van de vernietiging of wanneer apparatuur eigendom is van een externe partij (bijv. lease), overlegt de externe partij na verwijdering van apparatuur een certificaat waaruit blijkt dat de gegevens op de apparatuur door een CA+-gecertificeerd bedrijf zijn vernietigd volgens DIN 66399 veiligheidsniveau 3 of hoger.

[34] BIO 11.2.3

[35] BIO 11.2.4

[36] BIO 8.3.1.1, 8.3.2, 8.3.2.1, 11.2.7

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 dat minimaal 1 kilometer is verwijderd van de oorspronkelijke omgeving 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 wachtwoord. 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 o.a. laptops, tablets (bijvoorbeeld iPad's), memorysticks en mobiele telefoons (smartphones). Voor het gebruik van deze apparatuur worden richtlijnen vastgesteld, waaronder:

- Apparatuur en bijbehorende media mogen buiten de locatie niet onbeheerd worden achtergelaten[37];
- Bij het verwerken van vertrouwelijke, privacygevoelige en/of kritische gegevens zijn aanvullende maatregelen getroffen passend bij het classificatieniveau, zoals encryptie, wachtwoordbeveiliging, antivirusscanners enzovoort;

5.8 Beveiliging van fysieke documenten

- Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten.

[37] BIO 8.3.2.1, 8.3.3

6. Logische toegangsbeveiliging (Autorisaties)

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. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

6.1 Beleid voor logische toegangsbeveiliging

Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen implementeren en onderhouden is er een gemeentebreed autorisatie- en authenticatiebeleid. Dit houdt rekening met de classificatie van de informatie. Het autorisatiebeleid dient te zijn vastgesteld en bekend gemaakt aan de organisatie. Hierin worden in ieder geval de volgende – middels dit document vastgestelde beleidsuitgangspunten – verder uitgewerkt:

- Authenticatiemiddelen zijn voldoende veilig. Dit is gebaseerd op de classificatie, met minimale eisen. Wachtwoorden voldoen aan de BIO-eisen.[38]
- Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordkluis.[39]
- 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 (terminologie: functiescheiding). Benodigde functiescheiding wordt in een conflictmatrix per applicatie vastgelegd, op basis van een risicoafweging.[40] In de conflictmatrix wordt beschreven welke rollen of rechten niet gezamenlijk aan een medewerker mogen worden toegekend, zoals het aanmaken van een leverancier en het boeken van een factuur.[41] Indien functiescheiding niet mogelijk is, worden er passende beheersmaatregelen genomen, bijvoorbeeld een audit trail.
- Aanvragen voor toegang worden geautoriseerd door de proceseigenaar (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. [42]
- 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.

[38] BIO 9.2.2
[39] BIO 9.3.1.1
[40] BIO 9.2.2.2, 6.1.2
[41] BIO 6.1.2.1
[42] BIO 9.2.1.2

- Het gebruik van bevoegdheden wordt beperkt en beheerst.[43] Maatregelen worden afgestemd n.a.v. een risicoanalyse.
- Voor werken op afstand is een thuiswerk- c.q. mobiele werkplekomgeving beschikbaar. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- 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 die vertrouwelijke of privacygevoelige gegevens verwerken, vereisen speciale maatregelen, zoals het plaatsen in een aparte beveiligde omgeving of domein. De proceseigenaar stelt expliciet de gevoeligheid van een (informatie)systeem vast en de noodzaak voor aanvullende maatregelen.
- 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.
- 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.

6.2 Externe toegang

De gemeente kan een externe partij toegang verlenen tot het gemeentelijke netwerk. Hiervoor dient een procedure gemaakt en gevolgd te worden, waarbij er rekening gehouden wordt met een risico-analyse. 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 bijvoorbeeld aan de hand van een audit trail en interne logging.

6.3 Controle op toegangsrechten

Alle medewerkers die van het besloten gemeentenetwerk of applicaties gebruikmaken, moeten door het systeem of applicatie op unieke wijze geïdentificeerd kunnen worden. Om de toegang tot de Informatiearchitectuur effectief te beheren, worden de toegangsrechten regelmatig beoordeeld: halfjaarlijks (BBN2), jaarlijks (BBN1) en indien er sprake is van speciale bevoegdheden éénmaal per kwartaal. Er wordt dan een uitdraai gemaakt van de verstrekte toegangsmachtigingen. Deze uitdraai wordt gecontroleerd op juistheid en volledigheid door de proceseigenaar. De opvolging van de bevindingen wordt gedocumenteerd. Bij een vermoeden van misbruik/onbevoegde toegang wordt de bevinding behandeld als een informatieveiligheidsincident.

6.4 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.

[43] BIO 9.2.3

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. Er is een proces voor het toewijzen van geheime authenticatie-informatie. Er is een beleid opgesteld rondom het gebruik van single sign on en centrale authenticatie via Active Directory, i.c.m. MFA.

Schermbeveiliging (clear screen)[44]
Medewerkers moeten bij het verlaten van de werkplek het scherm zelf 'locken' en na een vaste periode van inactiviteit van maximaal 15 minuten wordt een werkstation automatisch geblokkeerd. Bij werkstations (op locaties) met verhoogd risico kunnen aanvullende maatregelen genomen worden.

[44] BIO 11.2.9

7. Beheer van ICT-voorzieningen

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. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

7.1 Organisatorische uitgangspunten ten aanzien van beheer van ICT-voorzieningen

- In beginsel is er een scheiding tussen beheertaken en overige gebruikstaken. Hierbij voert de medewerker beheerwerkzaamheden alleen uit wanneer deze ingelogd is als beheerder; de medewerker voert normale gebruikstaken alleen uit wanneer deze ingelogd is 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.
- Systeemaccounts zijn accounts met beheerrechten die niet zijn gekoppeld aan één persoon, zoals DomainAdmin voor Windows of root in Unix-systemen. Het gebruik van deze accounts wordt geminimaliseerd door rechten toe te wijzen aan beheeraccounts. Deze accounts worden alleen gebruikt vanaf speciale werkstations die gehardend zijn. Indien mogelijk worden deze accounts gedeactiveerd.

7.2 Technische uitgangspunten ten aanzien van communicatie- en bedieningsprocessen

- Er is beleid over de technische bescherming t.a.v communicatie- en bedieningsprocessen
- Op elk apparaat (werkplek, server, netwerkcomponenten e.d.) is een virusscanner en een firewall actief en worden zowel in- en uitgaande communicatie (data in transit) als bestanden op opslagmedia bij het lezen en schrijven gescand. Malware/virusdefinities worden ten minste dagelijks geactualiseerd.[45] Bij detectie van malware volgt een automatische melding aan ICT-beheer en wordt het bestand in quarantaine geplaatst. Het bestand is dan alleen nog toegankelijk met medewerking van ICT-beheer. [46]
- 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.

[45] BIO 12.2.1.3, 12.2.1.3 12.2.1.5

[46] BIO 12.2.1.1

- Het (ongecontroleerd) kopiëren van vertrouwelijke gegevens is niet toegestaan, behalve voor back-up door bevoegd systeembeheer.
- Ten aanzien van patching en de opvolging van kwetsbaarheden geldt het volgende.
    - Er is een proces ingericht voor het beheer van technische kwetsbaarheden;
    - Van softwarematige voorzieningen van de technische infrastructuur wordt periodiek (bij voorkeur geautomatiseerd) gecontroleerd of de laatste updates (patches) daarin zijn doorgevoerd;
    - Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch zo spoedig mogelijk te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid en kwaliteit van het netwerk niet onder het afgesproken minimum niveau (service levels) komt.

7.3 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 best practices en/of beheerframeworks (zoals ITIL).

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 minimaal om de volgende processen:

- Change management / release management – doorvoeren van vernieuwingen en wijzigingen
    - Er is aantoonbaar wijzigingsmanagement ingericht ten aanzien van organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging. In de procedure voor wijzigingenbeheer is ten minste aandacht besteed aan:[47]
        a) het administreren van wijzigingen;
        b) risicoafweging van mogelijke gevolgen van de wijzigingen;
        c) goedkeuringsprocedure voor wijzigingen.
        d) omgang met test- en productieomgevingen. (Deze zijn gescheiden)[48]
        e) 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;
- ICT-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.

[47] BIO 12.1.2.1
[48] BIO 12.1.3

- Monitoring en capaciteitsbeheer – omgang met de capaciteit van ICT voorzieningen
    - Om te waarborgen dat informatiesystemen conform de gestelde eisen van continuïteit en snelheid blijven werken stelt afdeling A&I verantwoordelijkheden en procedures op ten aanzien van de monitoring van de capaciteit. Performanceproblemen worden tijdig gesignaleerd en geanalyseerd op basis van betrouwbare gegevens.
- Problemmanagement – identificeren en afhandelen van fouten in de ICT infrastructuur
    - Afdeling A&I 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 A&I 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 Raadhuis van Amstelveen 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/asset management – registratie van ICT voorzieningen
    - Afdeling A&I stelt procedures op ten aanzien van het registreren en muteren van ICT voorzieningen en de daaraan gerelateerde documentatie.
- Information security management – omgang met de veiligheid 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.

7.4 Toegangsbeveiliging met betrekking tot netwerkdomeinen en componenten

Aanbrengen van scheidingen
Netwerken worden gescheiden op basis van gebruikersgroepen, vereiste vertrouwelijkheid en betrouwbaarheid (integriteit, beschikbaarheid) van de diensten die gebruikmaken van de netwerken.[49] Deze scheiding kan fysiek of logisch (d.m.v. van VLAN's, gateways, firewalls, routers e.d.) worden bereikt. Per netwerksegment is er in kaart gebracht wat de vertrouwelijkheidszone (waaronder DMZ, vertrouwd LAN etc.) en de toegangsbeveiliging is. Afhankelijk van de toegangseisen voor de betreffende ICT-voorziening is het gebruik van de verbindingsmogelijkheden beperkt.

Demilitarized Zone (DMZ)

[49] BIO 13.1.3

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 worden 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.

Draadloze en openbare netwerken
Het 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.

7.5 Uitgangspunten voor controle en logging

De afdeling A&I stelt beleid op t.a.v. logging dat voldoet aan de BIO. Hierin wordt besloten wat er op welke manier wordt gelogd. Voor de analyse van loggegevens wordt gebruikgemaakt van een Security Information and Event Management-Systeem (SIEM) en SOC (Security Operations Center). De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.

Het gebruik van informatiesystemen, alsmede uitzonderingen en informatieinformatieveiligheidsincidenten, worden vastgelegd in logbestanden op een manier die in overeenstemming is met het risico. Dit wordt zodanig gedaan dat er 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 AVG, inzichtelijk te kunnen maken of onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden. Deze loggings kunnen worden betrokken bij het doorlopen van de procedure veiligheidsincidenten en datalekken.

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.

7.6 Beheer van de dienstverlening door een derde partij

Er wordt beleid opgesteld over dienstverlening van externe partijen. 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.

7.7 Beheer van devices

- De devices en maatregelen genoemd onder hoofdstuk 4.2 worden beheerd.
- Er zijn maatregelen getroffen om het automatisch doorsturen van interne e-mail berichten naar externe e-mail adressen te voorkomen.
- 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’).[50] Gemeentelijke informatie dient te worden versleuteld bij transport en opslag conform classificatie-eisen. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur ‘wissen op afstand’ mogelijk zijn.

[50] BIO 6.2.1.1

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. Implementatie: Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

8.1 Beveiligingseisen voor (informatie)systemen

De AA-organisatie ontwikkelt geen systemen. Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen. Deze eisen moeten worden opgenomen bij de aankoop van nieuwe of uitbreiding van bestaande informatiesystemen, hier is een proces voor.[51] Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn. Informatiesystemen worden jaarlijks beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. Ze worden bovendien gecontroleerd op risico's t.a.v. feitelijke veiligheid. Dit kan door kwetsbaarheidsanalyses en pentesten.[52]De volgende aspecten moeten bij inkoop en onderhoud aan de orde komen:

- Beveiligingseisen zijn zoveel mogelijk onderkend, gedocumenteerd en goedgekeurd voordat een (informatie)systeem wordt aangekocht of uitgebreid;
- Benodigde beveiligingsmaatregelen met betrekking tot audit trails 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

Cryptografie houdt zich bezig met het versleutelen van informatie. Er is een beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd.[53] Ze worden toegepast in overeenstemming met alle relevante overeenkomsten en wet- en regelgeving.[54]

Een onderdeel van cryptografie zijn (PKI[55]-)certificaten. Deze worden herkend in veel standaardtoepassingen en zorgen voor een goede beveiliging. Zo een digitaal certificaat is een combinatie van identiteit en een

[51] BIO 14.1

[52] BIO 18.2.3

[53] BIO 10.1

[54] BIO 18.1.5

[55] PKI staat voor Public Key Infrastructure en is een systeem om certificaten uit te geven.

openbare sleutel die gewaarmerkt is door de certificaatautoriteit. Er is beleid ontwikkeld en geïmplementeerd m.b.t. het gebruik, de bescherming en de levensduur van deze cryptografische sleutels.[56]

PKI-overheid-certificaten bieden aanvullende zekerheden. Een digitaal certificaat van PKI-overheid waarborgt op basis van Nederlandse wetgeving de betrouwbaarheid van informatie-uitwisseling via e-mail, websites of andere gegevensuitwisseling. Er is beleid over wanneer een PKI-overheid-certificaat wordt gebruikt.[57] T.a.v. het sleutelbeheer worden de PKI-overheid-eisen gehanteerd.
PKI-overheid-certificaten 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.

Bij gebruik van digitale handtekeningen als middel om de authenticiteit en integriteit van elektronische documenten te waarborgen, wordt gebruik gemaakt van de AdES Baseline Profile standaard.[58] Ook worden persoonlijke sleutels (private keys) beschermd tegen onbevoegde openbaarmaking.

Er wordt voor alle informatiedragers beleid opgesteld t.a.v. cryptografie. Hierbij gaat het minimaal over:

- disks in een NUC;
- disks in een notebook;
- master storage in de serverruimte;
- standalone servers met eigen disks;
- USB-sticks;
- harddisks.

8.3 Uitbesteding ontwikkeling van (informatie)systemen

In deze (standaard)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);

[56] BIO 10.1.2
[57] Zie ook BIO 13.2.3.3
[58] BIO 13.2.3.4

- 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.

8.4 Hardening

Hardening is het proces waarbij maatregelen getroffen worden om de aanvalsmogelijkheden op een systeem te verkleinen. Toegangsbeveiliging (zie h.7) is een onderdeel van hardening, evenals meerdere onderwerpen uit hoofdstuk 6. Er is een hardeningsbaseline opgesteld en geïmplementeerd, waarin duidelijk wordt welke hardeningsmaatregelen zijn getroffen. 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.

Speciale aandacht krijgen hierbij de websites van de gemeente, daarvoor bestaat ook een hardeningsbaseline. Niet langer gebruikte websites of verouderde informatie die toegankelijk is via het internet dient de gemeente te (laten) verwijderen. De gemeente en meer in het bijzonder de eigenaar van de specifieke website is hiervoor verantwoordelijk.

9. Informatieveiligheidsincidenten

Doelstelling:
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheidsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.[59]

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.

Implementatie:
Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

9.1 Definitie informatieveiligheidsincident

Een informatieveiligheidsincident 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 informatieveiligheidsincidenten.

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 informatieveiligheidsincidenten 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 informatieveiligheidsincidenten

Er is een procedure vastgesteld (incl. directieverantwoordelijkheden) om een snelle, doeltreffende en ordelijke respons op informatieveiligheidsincidenten te bewerkstelligen. Informatieveiligheidsgebeurtenissen worden beoordeeld en evt. geclassificeerd als incidenten. Ze worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd. Informatieveiligheidsincidenten die hebben geleid tot een vermoedelijk/mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, worden z.s.m. (binnen 72 uur) gemeld aan de Informatiebeveiligingsdienst (IBD).[60] Er wordt geleerd uit informatieveiligheidsincidenten en bewijsmateriaal wordt correct verzameld en opgeslagen.

[59] BIO 16.1

[60] BIO 16.1.4.1. De IBD is de sectorale CERT van gemeenten.

Onderdeel van deze procedure is een proces voor het melden van datalekken en de gemeente zorgt ervoor dat deze bekend is gemaakt binnen de organisatie. Op grond van de 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 datalek met meldplicht aan de AP.

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 informatieveiligheidsincident of calamiteit, op aanvaardbaar niveau hun taken kunnen hervatten.

Implementatie:
Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

10.1 Proces van continuïteitsmanagement

Er zijn documenten om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen.[61]

- Er zijn organisatiebrede eisen t.a.v. informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer rondom calamiteiten.
- Er zijn processen, procedures en beheersmaatregelen vastgesteld, gedocumenteerd, geïmplementeerd en gehandhaafd om de bovengenoemde eisen te waarborgen.
    - Hierbij wordt een expliciete risicoafweging uitgevoerd waardoor bedrijfskritische procesonderdelen en bijbehorende betrouwbaarheidseisen worden geïdentificeerd.
    - De dienstverlening van deze bedrijfskritische onderdelen wordt bij calamiteiten binnen maximaal een week hersteld
- Er zijn continuïteitsplannen, deze worden jaarlijks getest.
- Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er is middels een expliciete risicoafweging bepaald wat het maximaal toegestane dataverlies (BBN2: 28 uur) en de maximale toegestane hersteltijd (BBN2: 16 werkuren in 85% van de gevallen) is. De back-up wordt zodanig ergens opgeslagen, waarbij het incident op de ene locatie niet kan leiden tot schade op de andere. Elke gemeentelijke afdeling voert op haar processen een business impactanalyse uit. Afhankelijk van de bevindingen worden vervolgacties gepland;
- Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In dit 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;

[61] BIO 17.1

- 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 er minimaal jaarlijks een uitwijktest uitgevoerd volgens geïmplementeerde procedures.[62]

10.2 Relatie met nood- en ontruimingsplan

De afdeling A&I 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 A&I 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.

[62] BIO 12.3

11. Naleving

Doelstelling:
Het naleven van strafrechtelijke of civielrechtelijke wetgeving; wettelijke, reglementaire of contractuele verplichtingen en beveiligingseisen én waarborgen dat systemen en processen voldoen aan het informatieveiligheidsbeleid 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.

Implementatie:
Zie voor de op te leveren tactische stukken, inclusief eigenaarschap, bijlage 2

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.
- Afdeling A&I en externe hostingproviders 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 actieplan

Om de naleving van de beveiligingseisen uit het informatieveiligheidsbeleid en actieplan te bewaken, worden deze onafhankelijk en met geplande tussenpozen of bij belangrijke veranderingen beoordeeld.[63] De procesverantwoordelijke legt 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.

In het Information Security Management Systeem (ISMS) wordt de plan-do-check-act op gestructureerde wijze afgedekt (zie ook hoofdstuk 1.4). Daarnaast is er een vastgesteld auditplan waarin jaarlijkse keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.[64] In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, wat resulteert in een In Control Verklaring (ICV) over informatiebeveiliging.

11.3 Naleving van wettelijke voorschriften

Relevante eisen uit wet- en regelgeving, contractuele eisen en beleid vanuit de organisatie moeten voor ieder (informatie)systeem zijn vastgelegd.[65] Daarbij is bekend wat de aanpak is van de organisatie om aan deze eisen te voldoen. Er zijn specifieke procedures voor de naleving van de eisen rondom het intellectuele eigendomsrecht.

Aan de bescherming van persoonsgegevens stellen meerdere wetten, w.o. de Algemene Verordening Gegevensbescherming (AVG), duidelijke eisen.[66] De gemeenten Amstelveen en Aalsmeer stellen een privacybeheerder en een voldoende gemandateerde Functionaris Gegevensbescherming (FG) aan, die de uitvoering en de naleving van de AVG bewaken.

Conform de Archiefwet[67] 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. Registraties behoren (conform wet- en regelgeving, contracten en organisatie-eisen) te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.

11.4 Beoordeling van de naleving

De proceseigenaren 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 geïmple-

[63] BIO 18.2.1

[64] BIO 18.2

[65] BIO 18.1

[66] BIO 18.1.4

[67] 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.

menteerde 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.

Begrippenlijst

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

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

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

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

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

Controller informatieveiligheid
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid en de escalatie van informatieveiligheidsincidenten.

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

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).

(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
*IT-incident: een ongeplande interruptie of kwaliteitsreductie van een IT-service
*Informatieveiligheidsincident: Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten

Incident management
Beheer en beheersing van de afhandeling van incidenten

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

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

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

Informatieveiligheidsbeleid
Strategie van een organisatie met betrekking tot informatieveiligheid.

Informatieveiligheidsincident
Zie Incident

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

ITIL (Information Technology Infrastructure Library)
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.

LAN (Local Area Network/lokaal netwerk)
Fysiek afgegrensd, instellingsgebonden netwerk

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

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

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

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.

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

Proceseigenaar
De lijnmanager die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem (BIO p. 15)

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

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

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

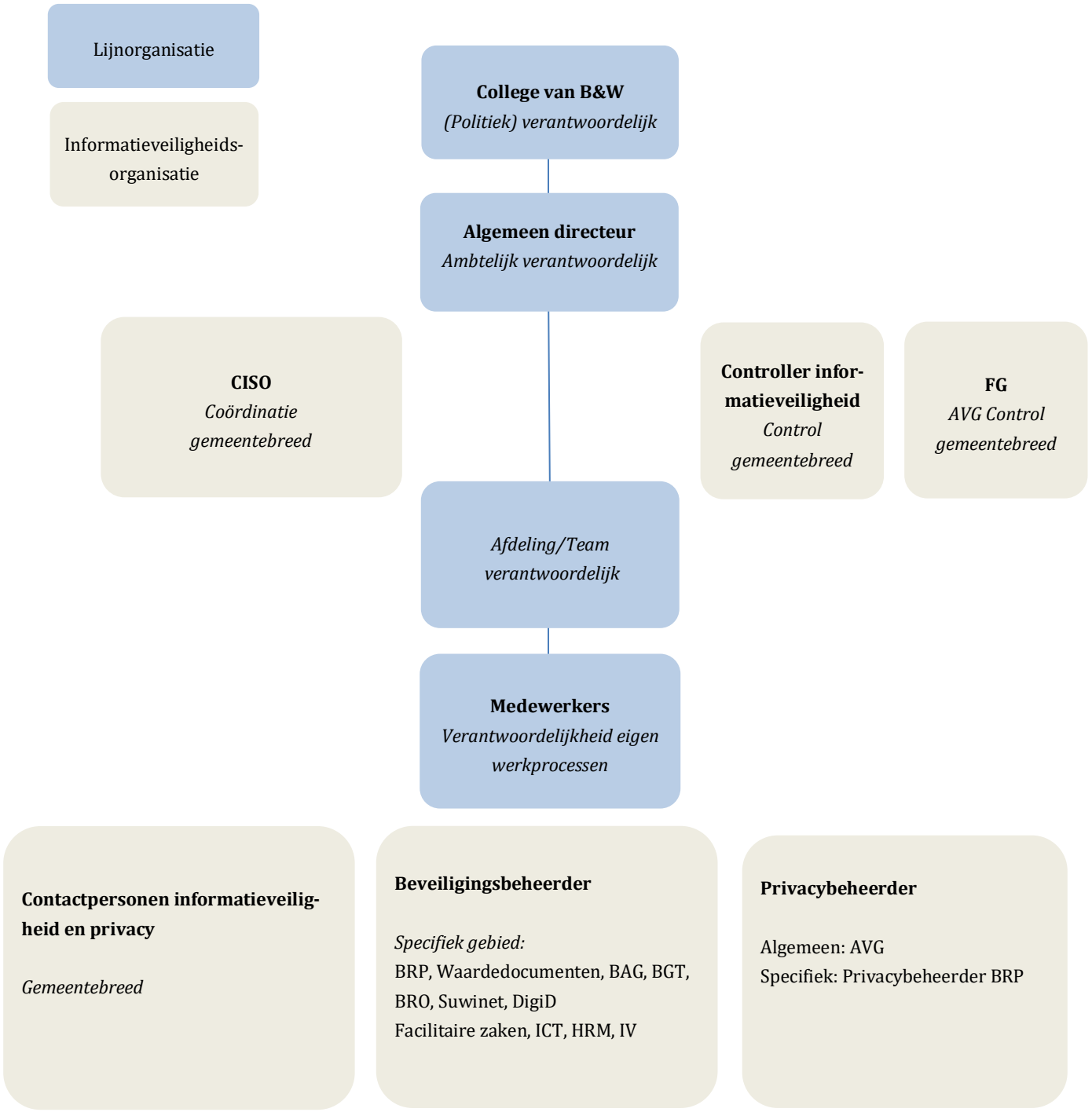
Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding

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

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden

BIJLAGE 1 Rollen, namen informatieveiligheidsorganisatie

Beveiligingsrollen	**Naam**	**Vervanger**
1. Chief Information Security Officer (CISO)	Nasim Ahmadi	Luella de Regt
2. Controller Informatieveiligheid	Marco Slinger	Madelon Brouwer
3. Functionaris Gegevensbescherming	Madelon Brouwer	Marco Slinger
4. Privacybeheerder	Ferdy IJsselmuiden	Nino Tsjkadoea
5. Beveiligingsbeheerder BRP en Waardedocumenten	Margriet Wiegersma	Marie-Louise Radder en Esther Keijzer
6. Beveiligingsbeheerder Suwinet	Margriet Wiegersma	Richard Slagter
7. Beveiligingsbeheerder BAG	Aart Los	Irma Smak
8. Beveiligingsbeheerder BGT	Irma Smak	Aart Los
9. Beveiligingsbeheerder BRO	Karin Wensveen	Timo Vlijm
10. Beveiligingsbeheerder CORV	Annechien Dongen	Margriet Slurink
11. Beveiligingsbeheerder DigiD	Erik Kogenhop	Luella de Regt
12. Beveiligingsbeheerder ICT	Erik Kogenhop	Marco Hofman
13. Beveiligingsbeheerder HRM	Daniela Wolterson	Yoyce Klimsop
14. Beveiligingsbeheerder IV	Milo van der Burgt	Charlotte van den Berg
15. Beveiligingsbeheerder FZ	Dalila Çakmak	Exsell Rojer
16. Vertrouwd Contactpersoon Informatiebeveiliging (VCIB)	CISO Veiligheidsbeheerders ICT Alle systeem- en netwerkbeheerders in vaste dienst	
17. Algemeen Contactpersoon Informatiebeveiliging (ACIB)	Alle VCIB's Servicedesk ICT Afdelingshoofd en teamleiders A&I in vaste dienst	


Lijnorganisatie
Informatieveiligheids-organisatie
College van B&W
(Politiek) verantwoordelijk
Algemeen directeur
Ambtelijk verantwoordelijk
CISO
Coördinatie gemeentebreed
Controller infor-matieveiligheid
Control gemeentebreed
FG
AVG Control gemeentebreed
Afdeling/Team verantwoordelijk
Medewerkers
Verantwoordelijkheid eigen werkprocessen
Contactpersonen informatieveilig-heid en privacy
Gemeentebreed
Beveiligingsbeheerder
Specifiek gebied:
BRP, Waardedocumenten, BAG, BGT, BRO, Suwinet, DigiD
Facilitaire zaken, ICT, HRM, IV
Privacybeheerder
Algemeen: AVG
Specifiek: Privacybeheerder BRP

BIJLAGE 2 Op te leveren tactische stukken

In deze bijlage staan de op te leveren tactische stukken incl. de verantwoordelijke; vaak is dit een afdeling, soms meerdere afdelingen en soms de proceseigenaar. Deze stukken komen rechtstreeks uit dit informatieveiligheidsbeleid. Zie voor meer informatie over de stukken dus het hoofdstuk waar het stuk uitkomt.

Hoofd-stuk	Para-gaaf	Stuk dat moet worden uitgewerkt	Verantwoordelijke
3	1	Registratie bedrijfsmiddelen die verband houden met informatiesystemen (configuratiemanagement), incl. eigenaar	Afdeling A&I
3	1	Registratie van alle fysieke voorzieningen die verband houden met (informatie)veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.	Services, Team FZ
3	1	Registratie van alle medewerkers en extern personeel dat vanwege uitoefening van de opgedragen werkzaamheden gebruik moet kunnen maken van gemeentelijke ICT voorzieningen	Afdeling HRM
3	1	Registratie van alle data, applicaties en overige assets	Elke afdeling
3	2	Overzicht bedrijfsmiddelen die verband houden met ICT-voorzieningen én eigenaren	Elke afdeling
3	2	Overzicht bedrijfsprocessen/applicaties/gegevensverzamelingen/ICT-faciliteiten én verantwoordelijk leidinggevenden	Elke afdeling
3	3	Classificatie informatie en informatiesystemen incl. rubricering	Proceseigenaar
3	3	Classificatie informatie in papieren bestanden en archieven incl. rubricering	Proceseigenaar
4	1	IDU-proces medewerkers en ingehuurd personeel	Afdeling HRM
4	1	Aansluiting bij klokkenluidersregeling	Afdeling HRM
4	1	Taken en verantwoordelijkheid voor medewerker t.a.v. informatieveiligheid	Afdeling HRM
4	1	Voorschriften en gedragsregels – toegankelijk en gecommuniceerd. (4.2: integriteitsprotocol)	Afdeling HRM
4	1	Beleid/procedures/beheersmaatregelen om uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen	Afdeling HRM (Afdeling A&I)
4	1	Regeling i.v.m. heimelijke waarneming/toegang – ingestemd door de OR	Afdeling HRM
4	2	Gedragsregels voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen.	Afdeling HRM
4	2	Thuiswerkbeleid	Afdeling HRM
4	2	Beleid BYOD/CYOD	Afdeling HRM Afdeling A&I
4	2	Protocol Sociale Media	Afdeling HRM

			Services, Team communicatie
4	2	Lijst medewerkers die namens gemeenten mogen communiceren op Sociale Media	Services, Team Communicatie
4	3	Indiensttredingsprocedure	Afdeling HRM
4	3	Aanvullende, specifieke gedragsregels t.a.v. informatiesystemen/afdelingen. In ieder geval BRP, Waardedocumenten en Suwi	o.a. afdeling Publiekszaken en afdeling Werk en Inkomen
4	4	Autorisatieprocedure	Afdeling A&I Proceseigenaren (Afdeling HRM)
4	5	Opleidingsplan, incl. training i-bewustzijn	Afdeling HRM
5	1	Beveiligingszones van alle terreinen en gebouwen die gebruikt worden door wettelijke taken (excl sporthal, zwembad, buurthuis)	Services, Team FZ (Afdeling A&I)
5	1	Beschreven beveiligingsmaatregelen per zone	Services, Team FZ (Afdeling A&I)
5	1	Proces Autorisatie tot ruimtes	Services, Team FZ (Afdeling A&I)
5	1	Registratie uitgifte toegangsmiddelen	Services, Team FZ
5	1	Risico-analyses locatiekeuzes	Services, Team FZ
5	1	Brandblusapparatuur	Services, Team FZ
5	2	Registratie bedrijfsmiddelen die verband houden met veiligheid van ruimten, gebouw(en) en de directe omgeving van de gebouwen	Services, Team FZ
5	3	Afspraken verantwoording bewakingsdienst	Services, Team FZ
5	4	Procedure voor het verwijderen of gereed maken voor hergebruik van overbodige apparatuur en gegevensdragers waarop gemeentelijke informatie en in licentie gebruikte software is opgeslagen	Afdeling A&I
5	5	Eisen datakluizen	Afdeling A&I
5	6	Clean desk en clear screen beleid	Afdeling HRM
5	7	Richtlijnen gebruik (mobiele) apparatuur	Afdeling A&I Afdeling HRM
5	8	Beleid opslag papier	Afdeling A&I
5	8	Regeling toegang archiefruimten	Afdeling A&I
6	1	Gemeentebreed autorisatiebeleid	Afdeling A&I Proceseigenaar
6	1	Conflictmatrix per applicatie i.v.m. functiescheiding	Afdeling A&I Proceseigenaar
6	1	Registratie en beheer toegekende bevoegdheden, bijv. in een autorisatiematrix	Afdeling A&I Proceseigenaar
6	1	Registratie gevoeligheid (informatie)systeen en noodzaak aanvullende maatregelen	Proceseigenaar
6	1	Procedure beheersing en toewijzing van toegangsrechten	Afdeling A&I

6	1	Procedure beheer gebuikerswachtwoorden incl. wijze van toekenning en handelingswijze bij een vergeten wachtwoord	Afdeling A&I
6	2	Procedure toegang externe partijen tot gemeentelijk netwerk	Afdeling A&I
6	3	Proces controle toegangsrechten	Controller informatieveiligheid
6	4	Inlogprocedure werkstations	Afdeling A&I
6	4	Proces toewijzen van geheime authenticatie-informatie	Afdeling A&I
6	4	Beleid rondom gebruik Single Sign On en centrale authenticatie via Active Directory, i.c.m. MFA	Afdeling A&I
7	1	Overzicht beheeraccounts incl. reden	Afdeling A&I Proceseigenaar
7	2	Beleid over technische bescherming t.a.v. communicatie- en bedieningsprocessen	Afdeling A&I
7	2	Proces voor beheer van technische kwetsbaarheden	Afdeling A&I
7	2	Proces patching	Afdeling A&I
7	2	Afgesproken minimum niveau (service levels)	Afdeling A&I
7	3	Beheerprocedure – change management	Afdeling A&I
7	3	Beheerprocedure – release management	Afdeling A&I
7	3	Beheerprocedure – ICT-incident management	Afdeling A&I
7	3	Beheerprocedure – Monitoring en capaciteitsbeheer	Afdeling A&I
7	3	Beheerprocedure – Problemmanagement	Afdeling A&I
7	3	Beheerprocedure – IT service continuity management	Afdeling A&I
7	3	Beheerprocedure – IT- Configuratie/asset management	Afdeling A&I
7	3	Beheerprocedure – information security management	CISO
7	4	Overzicht vertrouwelijkheidszone per netwerksegment incl. toegangsbeveiliging	Afdeling A&I
7	4	Beleid DMZ incl. compartimentering	Afdeling A&I
7	4	Beleid draadloze/openbare netwerken	Afdeling A&I
7	4	Toegangsbeleid actieve componenten	Afdeling A&I
7	5	Loggingsbeleid	Afdeling A&I
7	5	Loggingsbeleid Suwinet	Afdeling Werk & Inkomen Afdeling A&I
7	5	Loggingsbeleid BRP	Afdeling Publiekszaken Afdeling A&I
7	6	Beleid dienstverlening externe partijen	Services, Team I&A Afdeling A&I
7	7	Zero-footprintbeleid	Afdeling A&I
8	1	Risicoafweging nieuwe systemen/grote wijziging	Afdeling A&I Proceseigenaar
8	1	Proces informatieveiligheidseisen opnemen bij aankoop van nieuwe of uitbreiding van bestaande informatiesystemen	Afdeling A&I
8	2	Beleid voor het gebruik van cryptografische beheersmaatregelen	Afdeling A&I

8	2	Beleid voor gebruik, bescherming en levensduur van (PKI-)certificaten	Afdeling A&I
8	2	Beleid over wanneer een PKI-overheid-certificaat wordt gebruikt	Afdeling A&I
8	2	Er wordt voor alle informatiedragers beleid opgesteld t.a.v. cryptografie. Hierbij gaat het minimaal over: • disks in een NUC; • disks in een notebook; • master storage in de serverruimte; • standalone servers met eigen disks; • USB-sticks; • Harddisks.	Afdeling A&I
8	3	Eisen rondom de aanschaf van een (informatie)systeem of de afname van een dienst	Afdeling A&I
8	4	Hardeningsbaseline systemen	Afdeling A&I
8	4	Hardeningsbaseline websites	Afdeling A&I
9	2	Procedure melding en omgang informatieveiligheidsincidenten	CISO
9	2	Proces melden datalekken	CISO
10	1	Documenten om de bedrijfscontinuïteit van de organisatie als geheel te waarborgen:	Services, Team FZ Afdeling A&I Afdeling VVH Proceseigenaren
10	1	Processen, procedures en beheersmaatregelen t.a.v. bedrijfscontinuïteit incl. risico-afweging	Services, Team FZ Afdeling A&I Afdeling VVH Proceseigenaren
10	1	Continuïteitsplannen	Services, Team FZ Afdeling A&I Afdeling VVH Proceseigenaren
10	1	Back-up beleid	Afdeling A&I Proceseigenaren
10	1	Plannen voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer)	Elke afdeling
10	1	Procedures uitwijktest	Afdeling A&I
10	2	Ontruimingsplan voor computerruimte(n) incl. testen	Afdeling A&I
10	2	Algemeen noodplan en ontruimingsplan	Team FZ
10	3	Beleid rondom broncodes onderbrengen	Afdeling A&I
11	1	Verklaring naleving informatieveiligheidsbeleid	Afdeling A&I Externe hostingproviders
11	1	Periodiek onderzoek kwaliteit informatieveiligheid	o.a. controller informatieveiligheid
11	1	In Control Statement	Controller Informatieveiligheid

11	1	Beveiligingsdocumentatiedossier	Informatieveiligheidsorganisatie
11	2	Informatieveiligheidsbeleid	CISO
11	2	Actieplan	CISO
11	2	Zelfevaluatie of audit	Procesverantwoordelijke
11	2	Managementrapportages	Afdelingshoofden, getoetst door Controller Informatieveiligheid
11	2	ISMS	CISO
11	2	Auditplan	Controller Informatieveiligheid CISO
11	3	Vastlegging voor ieder (informatie)systeem: relevante eisen uit wet- en regelgeving, contractuele eisen en beleid vanuit de organisatie	Proceseigenaar Afdeling A&I
11	3	Bewaartermijn per soort informatie	Proceseigenaar
11	4	Controle en evaluatie op naleving van wettelijke voorschriften van het informatieveiligheidsbeleid	Proceseigenaar