Heemstede

GEMEENTEBLAD

Officiële uitgave van de gemeente Heemstede

Nr. 210533

29 november 2017

Strategisch gemeentebreed informatieveiligheidsbeleid

Versie	: definitief 1.0
Auteurs	: Wineke de Porto, Ugur Balci
Begeleiding	: Ugur Balci (BMC)
Datum	: 4 augustus 2017
Corsanummer	: 2017016133

I Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van de gemeenten Bloemendaal en Heemstede.

Het informatieveiligheidsbeleid is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgeleverd. Tijdens het buitengewone VNG ledencongres op 29 november 2013, is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Hierin is opgenomen dat de Nederlandse gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt nemen om de informatiebeveiliging binnen de gemeentelijke organisaties te waarborgen.

Het beleid is zodanig opgezet dat het een visie geeft in hoe de gestelde inzichten en doelstellingen bereikt gaan worden en geeft een samenhangende reeks stappen aan voor de continuïteit van informatieveiligheid.

De basis van dit informatieveiligheidsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG - VNG/IBD).

I.II Leeswijzer en ambitieniveau

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatieveiligheid en de organisatie van informatieveiligheid waarbij de rollen en verantwoordelijkheden aangaande informatieveiligheid en het verantwoordingsmechanisme staan beschreven. Dit document dient als kapstok voor de verdere inbedding van het informatiebeveiligingsbeleid, de standaarden, de procedures en de processen.

In een separaat document "Tactisch gemeentebreed informatieveiligheidsbeleid", wordt volgens de Baseline Informatiebeveiliging Gemeenten (BIG) het inhoudelijke normenkader beschreven. Hierin worden alle normen en maatregelen vanuit de BIG verder uitgewerkt, die leidend zullen zijn voor alle organisatieonderdelen van de gemeenten Bloemendaal en Heemstede. Met instemming van voorliggende document wordt direct ingestemd met de verdere uitwerking, die beschreven zal worden in het "Tactisch gemeentebreed informatieveiligheidsbeleid".

Met dit document wordt daarnaast bepaald dat de gemeente bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt hanteert. Hierbij is het goed om te vermelden dat hetgeen dat is opgenomen in dit voorliggende document niet de huidige situatie in beeld brengt, maar het ambitieniveau van de gemeenten Bloemendaal en Heemstede aangaande gemeentebrede informatieveiligheid.

II. Waarom informatieveiligheid?

II.I Inleiding

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

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

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

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

De veiligheid van informatie is binnen een groot en toenemend aantal gebieden van de gemeente van belang. Om te voorkomen dat binnen elk van die gebieden - bijvoorbeeld rondom Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD) of Basisregistratie Adressen en Gebouwen (BAG) - separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatieveiligheidsbeleid op te stellen voor alle organisatie onderdelen.

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

II.II De informatieveiligheidspiramide

Ook de centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet- en regelgeving op dit gebied uit zich deze

aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De ontwikkeling door VNG/IBD van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatieveiligheid NEN/ISO 27001 en 27002, bieden een meetlat voor gemeenten om hun informatieveiligheid op orde te brengen en te houden.

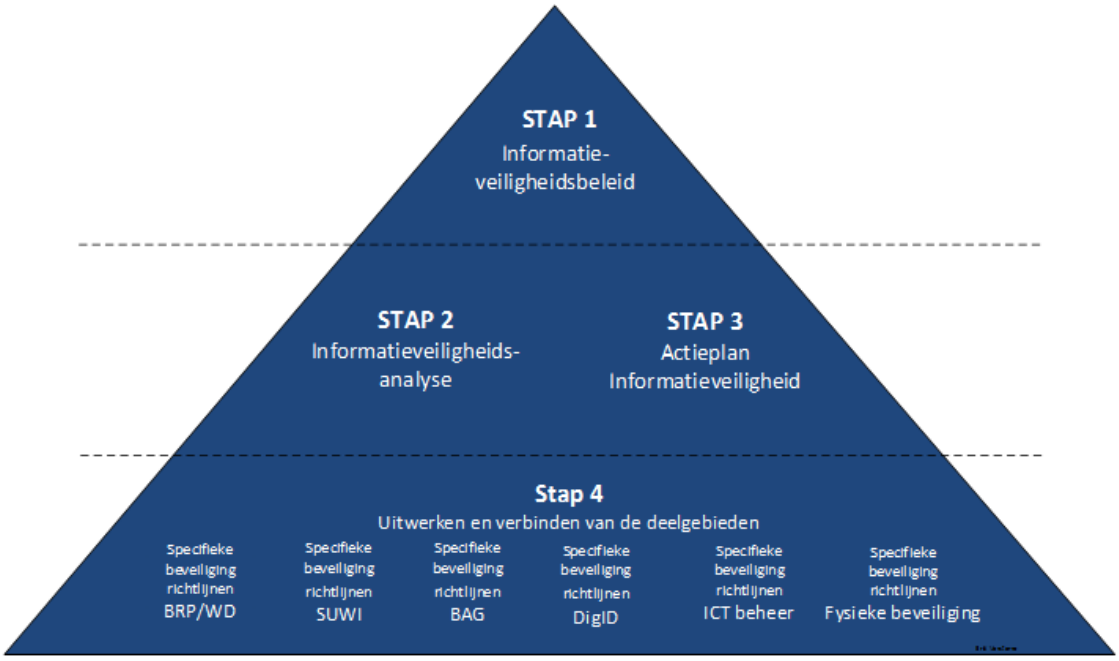
Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/IBD) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking worden gesteld, zoals de Wet basisregistratie personen (Wet Brp), Wet bescherming persoonsgegevens (Wbp), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet openbaarheid bestuur (Wob).
Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet Basisregistratie Adressen en Gebouwen (BAG), Wet Kenbaarheid Publiekrechtelijke Beperkingen (Wkpb), de Wet Ruimtelijke Ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

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

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

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

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



Figuur 1: De informatieveiligheidspiramide

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

II.IV Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid
De gemeenteraad controleert de uitvoering van het beleid inclusief de uitwerking daarvan binnen de gemeente[1] , zo ook voor informatieveiligheid. De verantwoordelijkheid voor informatieveiligheid ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.

De vaststelling en implementatie van de informatieveiligheidsstructuur[2] en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeenten Bloemendaal en Heemstede. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij cluster overstijgende (informatie)systemen.

De gemeentesecretaris is verantwoordelijk voor de informatiesystemen van de gemeente. Deze systemen dienen te worden geclassificeerd en te worden ingericht zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

[1] In hoofdstuk 2 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatieveiligheid uitgebreider beschreven.
[2] Onder het begrip informatieveiligheidsstructuur wordt in dit verband de complete beheercyclus van het informatieveiligheidsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatieveiligheid wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

II.V Algemene oriëntatie en positionering
Informatieveiligheid maakt onlosmakelijk 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.

II.VI Wettelijke basis en controle beveiligingsnormen
De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Wet bescherming persoonsgegevens (Wbp);
- 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 Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet Ruimtelijke Ordening (WRO).

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 organisatie bij de sturing op en het beheer van informatieveiligheid.

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

1.1 Beleidsdocument voor informatieveiligheid
Het college van burgemeester en wethouders behoort een gemeentebreed beleidsdocument voor informatieveiligheid goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen.

Minimaal zijn de volgende aspecten in dit beleidsdocument aanwezig:
- De doelstellingen van informatieveiligheid voor de gemeente;
- De beveiligingseisen en -prioriteiten;
- De organisatie van de informatieveiligheidsfunctie (zie hoofdstuk 2);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatiebeveiligingsrollen (zie hoofdstuk 2);
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie II.II) en de wijze

waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie II.VI);
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie 1.5).

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

1.3 Informatieveiligheidsanalyse
Op basis van dit strategische beleidsdocument, dat door het college van B en W wordt vastgesteld, wordt door het Directie Team (Heemstede) / Management Team (Bloemendaal) een "Tactisch gemeentebreed informatieveiligheidsbeleid", een "Informatieveiligheidsanalyse" en een "Actieplan informatieveiligheid" vastgesteld waarin wordt aangegeven op welke wijze het beleid uitgevoerd wordt.

De kernelementen in het tactische gemeentebrede informatieveiligheidsbeleid zijn de uitwerkingen van de volgende onderwerpen:
- Beveiligingsaspecten ten aanzien van personeel;
- Fysieke beveiliging;
- Beheer van communicatie- en bedieningsprocessen;
- Logische toegangsbeveiliging;
- Verwerving, ontwikkeling en onderhoud van systemen;
- Beveiligingsincidenten;
- Continuïteitsbeheer;
- Naleving.

De kernelementen in de informatieveiligheidsanalyse zijn:
- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van de informatieveiligheidsanalyse wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau;
- Het uitvoeren van een risico analyse waarin de verschillende risico's worden onderscheiden:
  - Risico's die onvoldoende af te dekken zijn door maatregelen;
  - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen;

Voor het uitvoeren van de informatieveiligheidsanalyse is een overzicht van de aanwezige (informatie)systemen een voorwaarde waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.
Voor het bepalen van afhankelijkheden en risico's wordt de analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse ontstaat een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden.

1.4 Aanvullende maatregelen
Afwijkend beveiligingsniveau
Als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist dan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden daarvoor aanvullende maatregelen getroffen. Dit zijn aanvullende maatregelen boven op de maatregelen die zorgen voor een veiligheidsniveau op basis van de BIG normen. In bepaalde gevallen zal hier voor toestemming gevraagd worden aan het college van B en W. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen.

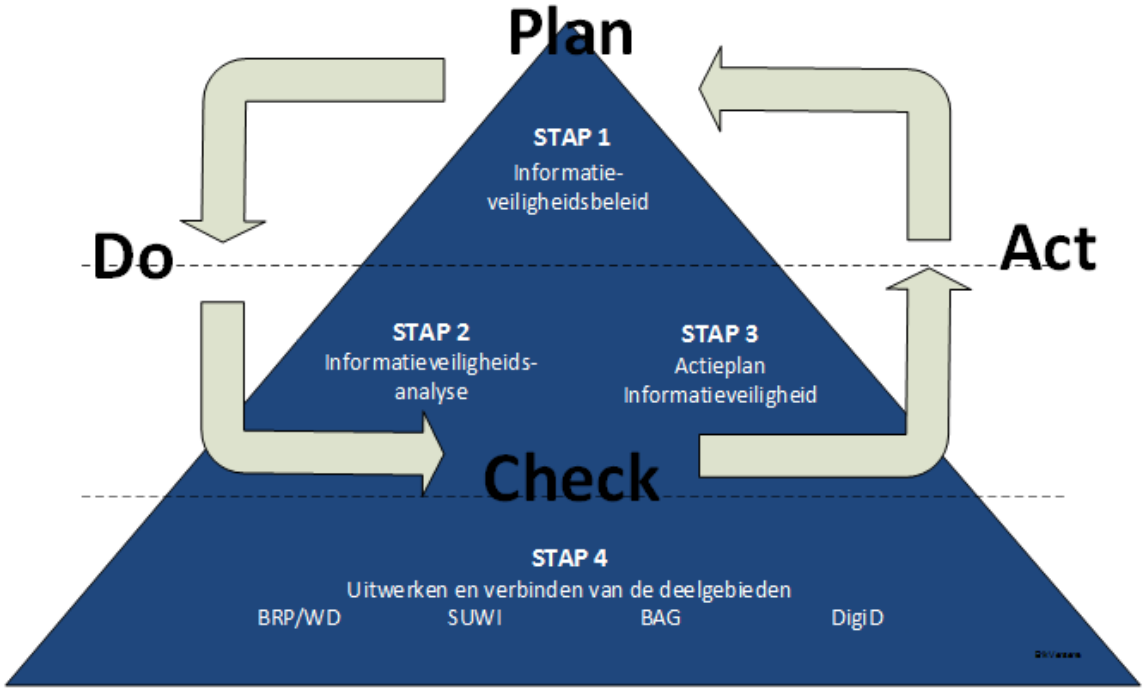
Persoonsgegevens
Bij de verwerking van persoonsgegevens zijn aanvullende maatregelen vereist, afhankelijk van de klassenindeling van de Wet bescherming persoonsgegevens (Wbp).

1.5 Borging van het informatieveiligheidsbeleid

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

1. **Informatieveiligheidsbeleid (zowel strategisch als tactisch):** bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 4 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats;
2. **Informatieveiligheidsanalyse:** bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;
3. **Actieplan Informatieveiligheid:** bevat de concrete geprioriteerde acties volgend uit de informatieveiligheidsanalyse. De governance komt bij elkaar om de implementatie van het actieplan informatieveiligheid te monitoren, dit vindt conform de bespreking in het informatieveiligheidsoverleg (zie paragraaf 2.2) twee maal per jaar plaats.

In de jaarrekening wordt gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid.



Figuur 2: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

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

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

2.1 Verantwoordelijkheidsniveaus binnen de gemeenten Bloemendaal en Heemstede

Binnen de gemeenten Bloemendaal en Heemstede worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.1.1 Controlerende rol door de gemeenteraad op de uitvoering van het informatieveiligheidsbeleid

De gemeenteraad heeft een controlerende rol op de uitvoering van het beleid door de gemeente.

2.1.2 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het college van B en W van de gemeenten Bloemendaal en Heemstede dragen, ieder voor zich, als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Het college van B en W stelt de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Daarnaast wordt de CISO en de controller informatieveiligheid vastgesteld door het college van B en W. Het college van B en W is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden op het gebied van beveiliging gemandateerd aan de gemeentesecretaris.

2.1.3 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt bij de gemeentesecretaris. Deze stelt in overleg met het Directie Team (Heemstede) / Management Team (Bloemendaal) en de CISO het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan.

De gemeentesecretaris heeft in ieder geval de volgende verantwoordelijkheden:
- Het stellen van operationele kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- 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.

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

De *afdelingshoofden* hebben in ieder geval de volgende verantwoordelijkheden:
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);

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 beheersen van risico's, evenals het opstellen van rapportages.

De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:
- Rapporteert rechtstreeks aan de gemeentesecretaris en het bestuur;
- Coördineert het formuleren van informatieveiligheidsbeleid;
- Stelt de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de gemeentesecretaris en het Directie Team (Heemstede) / Management Team (Bloemendaal) met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van beide gemeenten over het onderwerp informatieveiligheid;

- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Rapporteert over de informatieveiligheid van de gemeente in de jaarrekening.

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 beveiligingsincidenten.

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

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

2.1.7 De beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: DigiD, BRP, Waardedocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI), BAG (BAG beheerder). Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken, GRIT (Automatisering), DIV (Archivering) en P&O.

Specifieke verplichte beveiligingsbeheerdersrollen:
Autorisatiebevoegde Reisdocumenten/Aanvraagstations
Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).
Autorisatiebevoegde Rijbewijzen
Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

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

2.1.8 Security Officer SUWI

De Security Officer SUWI (de beveiligingsbeheerder SUWI) beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet en ziet er daarnaast op toe dat de maatregelen worden nageleefd. Ook adviseert de Security Officer medewerkers en management, doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet en evalueert de uitkomsten van verbetermaatregelen. De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het hoogste management en/of college. De Security Officer SUWI vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

2.1.9 Privacybeheerder
Deze rol is gericht op de uitvoering en de naleving van de Wet bescherming van persoonsgegevens (Wbp). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De *privacybeheerder* heeft in ieder geval de volgende verantwoordelijkheden:
- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van de privacywetgeving en adviseert het Directie Team (Heemstede) / Management Team (Bloemendaal) en afdelingshoofden bij wijzigingen in proces uitvoering, bedrijfsvoering en de toepassing van een privacy impact assessment.
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- De privacybeheerder heeft verder als taak:
  a. de uitleg van de privacyvoorschriften in de Wet bescherming persoonsgegevens (Wbp), vanaf 25 mei 2018 van de AVG, en daarnaast in de sectorale wetgeving;
  b. coördineren van de privacywerkzaamheden;
  c. de privacybescherming in de organisatie onder de aandacht te brengen zowel op verzoek als ook pro-actief uit eigen beweging;
  d. coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
  e. verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) tot de inwerkingtreding van de AVG;
  f. te fungeren als aanspreekpunt voor de AP tot de inwerkingtreding van de AVG;
  g. coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
  h. rapporteren aan het Directie Team (Heemstede) / Management Team (Bloemendaal);
  i. richt procedures in voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
  j. beheer en onderhoud van de standaarddocumenten voor bewerkersovereenkomsten, convenanten en reglementen;
  k. advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van bewerkersovereenkomsten en convenanten en de vaststelling van reglementen;

2.1.10 Functionaris gegevensbescherming
Op 25 mei 2018 treedt de algemene verordening gegevensbescherming (AVG) in werking. Voor overheidsinstanties zoals de gemeenten Bloemendaal en Heemstede zal het aanwijzen van een functionaris gegevensbescherming (FG) dan verplicht zijn (artikel 37 lid 1 AVG). Momenteel is er een privacybeheerder BRP, maar nog geen FG en ook geen gemeentebrede privacybeheerder binnen de gemeenten Bloemendaal en Heemstede. De FG zal een centraal punt zijn binnen de gemeente wat betreft de gegevensbescherming binnen de organisatie.

Het takenpakket van de FG zal uit de volgende punten bestaan (art. 39 lid 1 AVG):
- informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken over hun verplichtingen die voortvloeien uit de AVG en andere wetten met betrekking tot gegevensbescherming;
- toezien op naleving van zowel de AVG en andere wetten met betrekking tot gegevensbescherming als het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking betrokken personeel en de betreffende audits;
- desgevraagd adviseren omtrent gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan;
- samenwerken met en als contactpunt optreden voor de AP.

2.1.11 De afdeling Informatisering en Automatisering
De afdelingen Dienstverlening zijn belast met de informatisering van de gemeenten Bloemendaal en Heemstede en zijn tevens direct aanspreekpunt voor de automatisering van de uitvoeringsorganisatie Gemeenschappelijke Regeling Informatie Technologie (GRIT). De gemeenten Bloemendaal en Heemstede voeren de informatisering uit en hebben de coördinatie van de automatisering samengebracht in de uitvoeringsorganisatie GRIT. De uitvoeringsorganisatie GRIT beheert de werkplekken, serverplatformen, lokale netwerken, straalverbindingen, externe netwerkverbindingen (zoals Gemnet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast is zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de verantwoordelijken voor (informatie)systemen afgelegd.

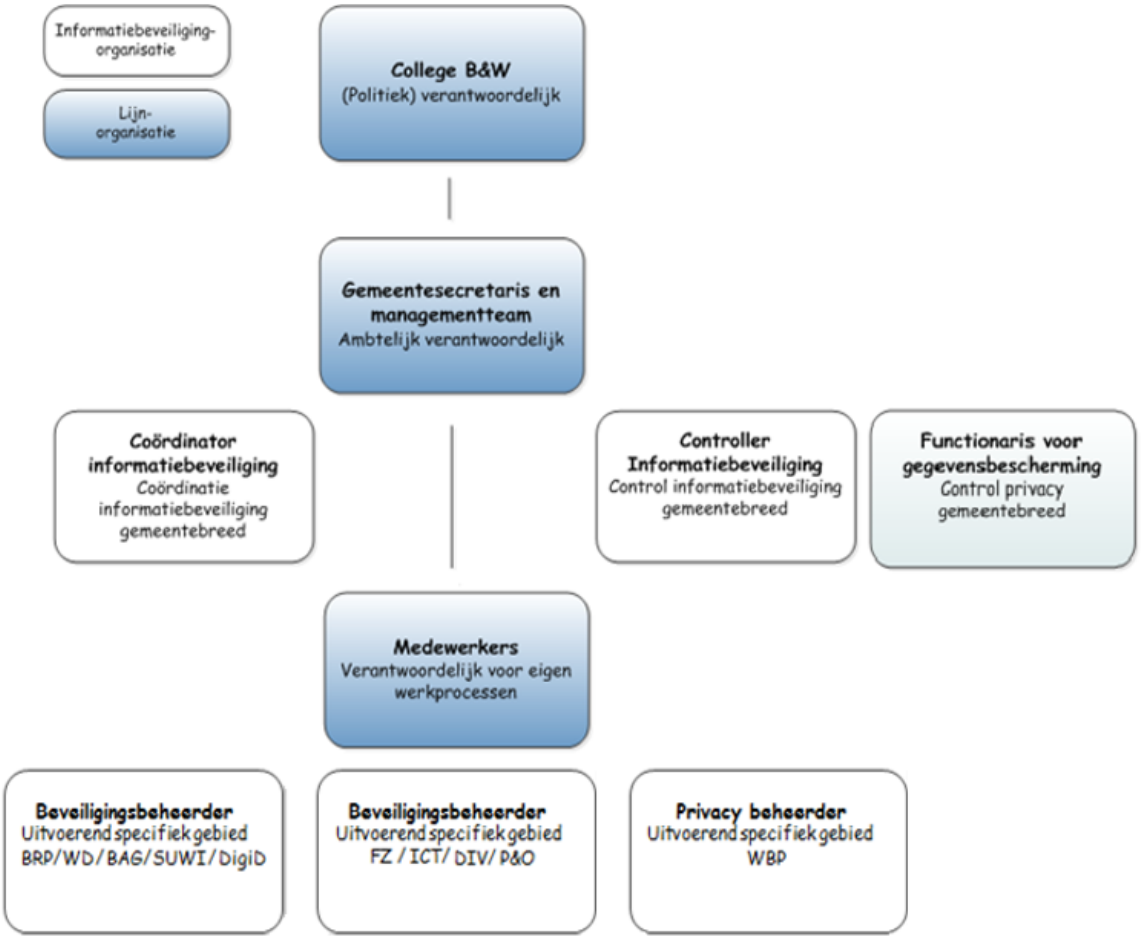
2.1.12 De afdeling Facilitaire Zaken en Bouwkunde
Het afdelingshoofd Facilitaire Zaken en het afdelingshoofd Bouwkunde zijn verantwoordelijk voor de fysieke veiligheid in en rond het gebouw, fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging.

2.1.13 De afdeling P&O
De afdeling P&O is verantwoordelijk voor de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.

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

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

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



Figuur 3: Functies en rollen in informatieveiligheidsorganisatie

2.2 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, SUWI en DigiD;
- Beveiligingsbeheerders t.a.v.: FZ, ICT (GRIT), DIV en P&O;
- Privacybeheerder;
- Agendaleden: MT lid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid;
- Beveiligingsincidenten;
- Planning en voorbereiding van Audits, controles en zelfevaluaties;
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.

Van het overleg informatieveiligheid over de genoemde onderwerpen zal een vertrouwelijke rapportage worden gemaakt. Deze rapportage zal ook worden verstuurd aan de portefeuillehouder.

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

2.3 ICT crisisbeheersing
Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat in ieder geval uit:

- Gemeentesecretaris (voorzitter);
- CISO;
- De beveiligingsbeheerder ICT (GRIT);
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts (indien nodig);
- Een lid van de afdeling communicatie.

De bovenstaande personen zullen eerst zelf bepalen wat de impact is van het incident of de calamiteit.

Op basis van de mogelijke politieke gevolgen van het incident licht de gemeentesecretaris de verantwoordelijke portefeuillehouder in.

2.4 Rapporteren beveiligingsincidenten
De CISO wordt door de medewerkers geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd.
Afspraken moeten worden gemaakt over:

- doel van de registratie;
- inhoud van de registratie;
- mate van detaillering;
- wijze van handelen;
- wijze van rapporteren.

De CISO rapporteert eenmaal per jaar aan de gemeentesecretaris en stuurt een kopie naar de portefeuillehouder.

2.5 Verantwoordelijkheden afdeling overstijgende (informatie)systemen
Afdeling overstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van de uitvoeringsorganisatie GRIT gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie / het management het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.

De procesverantwoordelijke van een afdeling overstijgend (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 schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:

- 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 de afspraken en oplossing 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.

2.6 Contracten met derden

2.6.1 Service level agreement (niveau van dienstverlening)

Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van de website(s) wordt tussen de afdelingen van de gemeenten Bloemendaal en Heemstede en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.

2.6.2 Inhuren van derden

Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk leidinggevende van de gemeenten Heemstede of Bloemendaal. Deze leidinggevende dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

2.6.3 Toegang

Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatieveiligheid is (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald wat de duur is van het contract.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform Wbp artikel 14) afgesloten.
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd aan het verantwoordelijke afdelingshoofd.

2.6.4 Overeenkomsten met een derde partij en met betrekking tot ICT voorzieningen

Bij het aangaan van overeenkomsten met derde partijen gelden de volgende beveiligingseisen:

- De maatregelen behorend bij 2.6.3 zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd.
- Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
- In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
- In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
- Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.
- In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
- Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
- De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

2.6.4.1 Bewerkers van persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) stelt regels voor het opslaan, verzamelen, vernietigen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Wanneer een partij het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij 'een bewerker'. De gemeenten Bloemendaal en Heemstede leggen in een register vast welke derden persoonsgegevens bewerken. Ook wordt vastgelegd of een bewerkersovereenkomst nodig is in de relatie tot die andere partij. In een bewerkersovereenkomst leggen de partijen onder andere vast voor welke doeleinden de gegevens verwerkt mogen worden, welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen en hoe het zit met de onderlinge aansprakelijkheid. Het gemeentebestuur van de gemeenten Bloemendaal en Heemstede blijven ieder voor zich de verantwoordelijke voor de verwerking van persoonsgegevens.

3. Classificatie en beheer van informatie en bedrijfsmiddelen

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

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

3.1 Inventarisatie van informatie en (informatie) bedrijfsmiddelen

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

De uitvoeringsorganisatie GRIT houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):

- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen);
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer);
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten);
- Diensten (bijvoorbeeld communicatiediensten, PKI diensten, energievoorziening ten behoeve van de informatievoorziening).

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de proces-verantwoordelijken en beheerders zijn.

De afdeling Facilitaire Zaken en de afdeling Bouwkunde 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.

3.2 Eigendom van informatie en bedrijfsmiddelen

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

3.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen. Hieronder volgen de geldende uitgangspunten:

- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen;
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen;
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen;

- Medewerkers gebruiken gemeentelijke informatie uitsluitend voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt;
- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan;
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
    - Illegale software, of niet goedgekeurde software mag niet worden gebruikt voor de uitvoering van het werk;
    - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel;
    - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.
        - De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
            - de beveiligingsclassificatie van de informatie;
            - de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatieveiligheidsbeleid)
            - aan de werkplek verbonden risico's;
            - het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

3.4 Classificatie van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. De gemeentelijke informatiesystemen worden geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke gemeentelijke informatie als vertrouwelijk wordt geclassificeerd. Na dit inzicht is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Daar waar de maatregelen op de punten beschikbaarheid (niveau 'noodzakelijk'), integriteit (niveau 'hoog') en vertrouwelijkheid (niveau 'vertrouwelijk'), zoals gehanteerd in dit gemeentebreed informatiebeveiligingsbeleid (conform de BIG) als voldoende kunnen worden aangemerkt, is het niet noodzakelijk om aanvullende maatregelen te treffen. Door het implementeren van alle maatregelen, zoals beschreven in dit gemeentebreed informatiebeleid wordt het vereiste beveiligingsniveau voldoende afgedekt.

Classificatietabel

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

Begrippenlijst

Cluster overstijgend informatiesysteem
Systeem dat door meer dan één cluster wordt gebruikt en waarin gegevens van meerdere organisatie-onderdelen worden vastgelegd

Audit
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

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

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen

Beschikbaarheid
zie Continuïteit

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

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

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

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

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

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

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

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

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens

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

Incident
Onverwachte of ongewone gebeurtenis

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

Informatieveiligheidsbeleid
Strategie van een organisatie met betrekking tot informatieveiligheid.

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

Chief Information Security Officer/CISO
Medewerker die gemeentebreed adviseert over informatieveiligheidsvraagstukken in brede zin en activiteiten op het gebied van informatieveiligheid coördineert

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

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

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

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

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

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

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

Programmatuur
Het geprogrammeerde deel van (informatie)systemen

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

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem

BIJLAGE 1 Rollen en namen informatieveiligheidsorganisatie van de gemeenten Bloemendaal en Heemstede

Zie hiervoor de aparte bijlage, in verband met de namen van betrokken medewerkers wordt deze niet gepubliceerd maar alleen intern verstrekt.