BEEKDAELEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Beekdaelen

Nr. 36948

23 januari

2024

Informatiebeveiligingsbeleid Gemeente Beekdaelen 2023-2025

Informatieveiligheidsbeleid gemeente Beekdaelen 2023-2025

Inleiding

Dit informatieveiligheidsbeleid legt de basis voor informatiebeveiliging voor de gemeente Beekdaelen. Dit document beschrijft de strategische en tactische uitgangspunten voor de jaren 2023 tot en met 2025 op het gebied van informatiebeveiliging.
Naast dit document zullen in nadere richtlijnen en operationele werkprocessen de uitgangspunten verder worden uitgewerkt per onderwerp.

Introductie in informatieveiligheid

Informatieveiligheid richt zich op de kwaliteit van de informatievoorziening. Daar waar we eerst op een "stand alone" computer werkten, hebben we nu contact met de hele wereld en diverse apparatuur om ons heen. Om dit mogelijk te maken heeft informatieveiligheid zich mee ontwikkeld. Door de grote afhankelijkheid van informatiesystemen en de snelle ontwikkelingen in de informatievoorziening is ook de bedreiging groter geworden.

Dankzij beveiliging kunnen we onze mail ook op de telefoon bekijken, informatie uitwisselen met maatschappelijke partners en vroegtijdig zaken als fraude signaleren. Daarnaast kunnen we incidenten voorkomen. Hieronder staat een top 5 van actuele bedreigingen die te maken hebben met informatieveiligheid. Deze top 5 gaat over bedreigingen die een landelijke bekendheid hebben gekregen en waarvan de impact met weinig woorden duidelijk wordt. Met weinig moeite kunnen deze voorbeelden geprojecteerd worden op alle organisaties, zowel klein als groot.

Inmiddels is de elektronische informatievoorziening verweven met het dagelijks leven van personen en processen van overheden, bedrijven en andere organisaties (informatiesamenleving). Organisaties zijn in hoge mate bezig met het verwerken van informatie. Dit zorgt voor efficiency. Echter is de keerzijde dat een incident (verstoring, corruptie of het stilleggen) van de informatievoorziening grote maatschappelijke impact kan hebben en negatieve impact heeft op het imago van de organisatie en haar bestuurders.

Actuele bedreigingen

Er zijn verschillende instituten die jaarlijks inzicht geven in de actuele bedreigingen. Wanneer we kijken naar instituten zoals het National Cyber Security Center (NCSC) en het Europees Agentschap voor netwerk- en informatieveiligheid (ENISA), zien we de onderstaande bedreigingen waarvoor men waarschuwt.

1		Malware in de vorm van virussen, cryptolockers en spyware.
2		Aanvallen op de ICT infrastructuur en de webapplicaties door hackers. Zeker door de toename van nation state hacks is dit een grote bedreiging.
3		Spam en Phishingmails worden in grote hoeveelheid verspreid.
4		Verlies van data. Het naar een verkeerde persoon versturen van mail is de meest voorkomende vorm van een datalek.
5		De oorzaak van veel incidenten komen voort uit het menselijk gedrag.

Een onderzoek naar de oorzaak van 150.000 incidenten laat zien dat 93% van deze incidenten voorkomen had kunnen worden wanneer een organisatie zich had gehouden aan de principes uit de normen voor informatieveiligheid.

Noodzaak van informatieveiligheid
Het is logisch dat de Europese Unie en ook de landelijke overheden regelgeving heeft opgesteld om de weerbaarheid in het digitale domein te vergroten. In eerste instantie ligt de focus op de vitale infrastructuur. In de kamerbrief van 16-10-2018 geeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan dat het op hoger plan tillen van de informatieveiligheid van overheidsorganisaties de komende jaren één van zijn speerpunten is. Uit de brief is af te leiden dat de focus verbreed wordt en er wettelijke eisen komen "waarin de (minimum)eisen ten aanzien van informatieveiligheid worden vastgelegd".

De Algemene Verordening Gegevensbescherming (AVG) kan niet los gezien worden van deze ontwikkeling. De kern van de AVG is gegevensbescherming en is daarmee voor een belangrijk deel ook informatiebeveiliging van persoonsgegevens. In artikel 32 van de AVG zijn de eisen m.b.t. informatiebeveiliging opgenomen.

De eerste stap is het harmoniseren van informatiebeveiliging voor de verschillende overheidslagen tot één baseline, de Baseline Informatiebeveiliging Overheid, BIO.

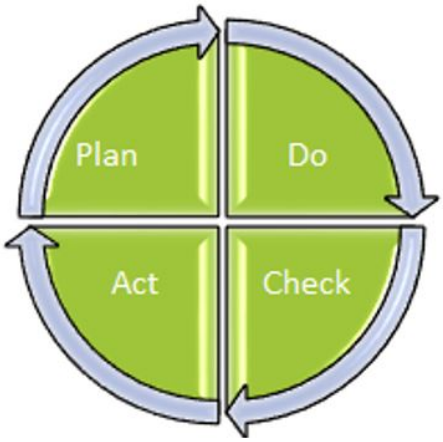
Baseline Informatiebeveiliging Overheid
De Baseline Informatiebeveiliging Overheid (BIO) is per 1 januari 2020 het nieuwe normenkader voor alle overheidsorganisaties. Deze baseline is een vertaling van de internationale informatieveiligheidsnormen NEN-EN-ISO/IEC 27001:2017 (verder ISO27001) en NEN-EN-ISO/IEC 27002:2017 (verder ISO27002). Of anders gezegd, de BIO is gebouwd rondom de ISO27001 met verwijzingen naar maatregelen uit de ISO27002. Implementatie van de BIO impliceert dat ook voldaan moet worden aan (delen van) de informatieveiligheidsstandaard ISO270002. (In de tactische uitgangspunten geven we aan wat de implementatie van de BIO inhoudt voor de organisatie).

De overheid ziet de BIO als belangrijke stap. In een passage uit eerder genoemde kamerbrief blijkt dat informatieveiligheid niet meer als vrijblijvend wordt gezien: "… is het van belang dat bestuurders, ambtelijke top, middenmanagement, (ICT-)professionals en stakeholders op adequate wijze invulling geven aan de gestelde eisen en principes uit de BIO." Een andere aanwijzing dat de vrijblijvendheid met betrekking tot informatieveiligheid gaat verdwijnen is deze passage: "Verkend wordt of de systematiek van de BIO in een Algemene Maatregel van Bestuur (AmvB), horende bij de aanstaande Wet Digitale Overheid, kan worden opgenomen." Hiervoor is een onderzoek gestart of en hoe meer generiek informatieveiligheidsbeleid een plaats krijgt in de volgende tranche van de Wet Digitale Overheid: verankering van informatieveiligheid in wet- en regelgeving. Dit onderzoek loopt tot het tweede kwartaal van 2020. Inmiddels is de BIO als de geldende norm voor de hele overheid geaccepteerd.

We gaan naast dit beleid op strategisch niveau een nadere uitwerking maken op tactisch / operationeel niveau. In deze nadere richtlijnen wordt per aandachtsgebied een uitwerking beschreven die invulling geeft aan het informatieveiligheidsbeleid. Het beleid, met daarbij de richtlijnen, is zodanig opgezet dat het een naslagwerk vormt voor medewerkers en het management, die in het kader van werkzaamheden of projecten moeten weten aan welke kwaliteitsaspecten op het gebied van informatieveiligheid, aandacht moet worden besteed. De gehele organisatie dient kennis te nemen van het informatieveiligheidsbeleid, hoe deze moet worden toegepast en wat de belangrijkste beleidsuitgangspunten zijn.

Ambitieniveau
Onze organisatie heeft zich akkoord verklaard met het implementeren van de BIO. Dit heeft als doel de gegevens van de burger en de organisatie conform de kwaliteitseisen te beschermen.

Om informatieveiligheid te realiseren hebben we een systeem nodig wat ons helpt om op een adequaat niveau te komen. We gaan hier uit van een plan-do-check-act cyclus. Hierdoor krijgen we een systeem wat gericht is op het continue verbeteren. In het vakgebied informatiebeveiliging noemen we dat ook wel een Information Security Management System (ISMS).



Een belangrijke fase in dit model is de fase van risicomanagement waarin verbetermogelijkheden worden gesignaleerd. Deze verbetermogelijkheden zijn een kans voor de organisatie om zich verder te ontwikkelen. Ook in de check fase kunnen controles en audits gezien worden als een belangrijke kans om verdere verbeteringen door te voeren.

In de strategische richtlijn van dit informatieveiligheidsbeleid worden een aantal beleids-uitgangspunten beschreven welke betrekking hebben op aandachtsgebieden. Deze worden pas actueel op het moment dat de organisatie voor een dergelijke keuze of gelijksoortig vraagstuk staat. Hierbij valt te denken aan het al dan niet inzetten van cloud computing, gezamenlijke uitbesteding van softwareontwikkeling of de aanschaf van een nieuw informatiesysteem. In deze specifieke gevallen hanteert de organisatie de beleidsuitgangspunten uit dit document of de nadere richtlijnen, om de veiligheid van informatie bij deze keuze te vergroten.

Waar binnen de organisatie persoonsgegevens verwerkt worden, is wetgeving over gegevensbescherming van toepassing. In het gegevensbeschermingsbeleid worden aanvullende bepalingen nader uitgewerkt om te voldoen aan de vereisten van gegevensbeschermingswetgeving via een Privacy Management Systeem (PMS). Daar waar gevraagd wordt om beveiligingsmaatregelen wordt ook hier geput uit het informatiebeveiligingsbeleid en de nadere richtlijnen.

Met de opstelling van dit document is bepaald dat de organisatie bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen, de beleidsregels uit dit document en de aanvullende richtlijnen als uitgangspunt hanteert.

Principes, doelen en scope

Bestuurlijke principes

Informatieveiligheid is een organisatiebreed aandachtspunt. Het is in feite een kwaliteitsaspect dat in alle processen van de organisatie terugkomt. Dit is de reden dat we informatieveiligheid niet als een geïsoleerd onderwerp kunnen benaderen.

Om dit te borgen is in VNG verband besloten om de volgende 10 bestuurlijke principes te hanteren:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatieveiligheid is van iedereen.
3. Informatieveiligheid is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatieveiligheid behoeft ook aandacht in (keten)samenwerking.
6. Informatieveiligheid is een proces.
7. Informatieveiligheid kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

In het kort kunnen we stellen dat het gemeentebestuur de rol heeft om de organisatie te faciliteren in het goed op orde brengen van de informatieveiligheid. Het proces richt zich vooral op het in beeld brengen van de risico's en de aandachtspunten uit deze analyses te gebruiken om verdere verbeteringen door te voeren. Een goede risicoanalyse komt voort uit een samenwerking tussen het management, vakspecialisten en een CISO/FG.

Doel van het beleid
Het beleid dient ondersteuning te bieden aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid. Om dit doel te kunnen realiseren dienen we in het informatieveiligheidsbeleid in ieder geval de volgende aspecten te beschrijven:

- de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatieveiligheid en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
- de organisatie van de informatieveiligheidsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
- de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan afdelingsmanagers;
- de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn;
- de frequentie waarmee het informatieveiligheidsbeleid wordt geëvalueerd;
- de bevordering van het beveiligingsbewustzijn.

Scope
De scope van dit beleid omvat alle informatieprocessen en –systemen van de gemeente en die ten behoeve van de gemeente ingezet worden. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook op de informatie in fysieke c.q. analoge vorm, ongeacht de locatie, het tijdstip of de gebruikte apparatuur.

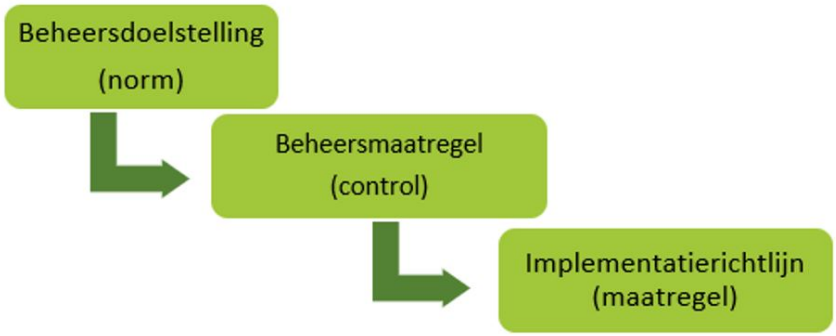
Actualiteit van beleid
Dit beleid wordt minimaal één keer per drie jaar beoordeeld op actualiteit (BIO 5.1.2.1). Dit daar het onderwerp informatieveiligheid door snelle ontwikkelingen in de techniek, maar ook binnen de diverse vakgebieden snel kan verouderen. Het beleid is echter meer toegespitst op de feitelijke situatie binnen de organisatie en zal hierdoor periodiek of als zich significante wijzigingen voordoen worden geëvalueerd en indien nodig worden bijgesteld (BIO 5.1.2).

Strategische uitgangspunten

Hoofdstuk 1 De Baseline Informatiebeveiliging Overheid

De Baseline Informatiebeveiliging Overheid (BIO) is per 2020 het nieuwe normenkader voor alle overheidsorganisaties en daarmee ook voor de gemeente Beekdaelen. De BIO is gebaseerd op de NEN-EN-ISO/IEC 27001:2017 (verder ISO27001) en kent daarmee een vergelijkbare indeling. Uitwerking van de BIO vindt plaats op basis van NEN-ISO/IEC 27002 (verder ISO 27002). Onderstaand treft u een uitwerking van de opzet en de implementatiemaatregelen van de BIO.

Opzet BIO
De BIO kent dezelfde opbouw als de ISO27001. De niveaus beheersdoelstellingen, beheersmaatregelen en implementatierichtlijnen zijn identiek aan de ISO27002 (zie figuur 1). De beheersdoelstellingen (ook wel normen genoemd) kennen beheersmaatregelen (ook wel controls genoemd) die op hun beurt zijn uitgewerkt in implementatierichtlijnen (ook wel maatregelen genoemd). In de BIO is een deel van de beheersmaatregelen op voorhand gekoppeld aan implementatierichtlijnen en worden daarom ook wel aangeduid als overheidsmaatregelen.



Implementatierichtlijnen (maatregelen)
Iedere control van de BIO is in de ISO27002 uitgewerkt in implementatierichtlijnen. Deze implementatierichtlijnen moeten worden gebruikt om te bepalen hoe de controls uitgewerkt kunnen worden in maatregelen. De implementatierichtlijnen zijn niet allemaal in de BIO opgenomen, hiervoor wordt verwezen naar de ISO27002.

Een deel van de controls is wel uitgewerkt in verplichte implementatierichtlijnen, omdat zij:

- voortvloeien uit wet- en regelgeving. Het niet treffen van een dergelijke maatregel is dan in strijd met wet- en regelgeving;
- zo basaal zijn dat zij het fundament vormen van een betrouwbare informatievoorziening;
- dienstbaar zijn aan de beveiliging in een procesketen of netwerk; niet-naleving door een enkele organisatie is per saldo niet effectief voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit niet efficiënt. Voor een generieke dienst geldt een afweging die analoog is aan het ketenvraagstuk.

De BIO noemt deze verplichte maatregelen 'overheidsmaatregelen'. De overheidsmaatregelen dekken niet de gehele beveiligingsdoelstellingen van de control af. Net als bij de controls, geldt hier een hardheidsbepaling: in het geval een maatregel voor een specifiek geval niet van toepassing kan zijn, vervalt de verplichting.

Bij een aantal overheidsmaatregelen zijn binnen de BIO verwijzingen toegevoegd naar relevante wet- en regelgeving. Deze overheidsmaatregelen hebben een verplichtend karakter.

Hoofdstuk 2 Risicomanagement

Risicomanagement
Binnen de Baseline Informatiebeveiliging Overheid wordt uitgegaan van een risicogerichte benadering van informatieveiligheid. Deze benadering is gericht op het in kaart brengen van invloeden waar we geen of onvoldoende invloed op hebben. Daar waar onvoldoende maatregelen zijn getroffen kan de organisatie kwetsbaar zijn. Een kwetsbaarheid levert automatisch ook een mate van onzekerheid op voor de bedrijfsprocessen en daarmee de doelstellingen van de organisatie.

Hoewel overheidsorganisaties in hoge mate dezelfde diensten leveren, wil dat niet zeggen dat de omstandigheden ook overal hetzelfde zijn. De wijze van organiseren, de gebruikte techniek en de kennis en vaardigheden van het personeel kunnen per organisatie verschillen. De BIO gaat uit van een basisbeveiligingsniveau (BBN). Bovenop de basis zijn aanvullende maatregelen nodig. Er kunnen ondanks de implementatie van de BIO nog kwetsbaarheden bestaan. Door organisatorische en technische veranderingen kunnen daarnaast steeds weer nieuwe kwetsbaarheden ontstaan.

GAP-analyse
De overheidsmaatregelen hebben een verplicht karakter en dienen daardoor geïmplementeerd te worden. Voor het deel van de controls met overheidsmaatregelen zullen we een GAP-analyse uitvoeren. Op deze manier kunnen we bepalen in welke mate we wel of niet voldoen aan deze verplichte overheidsmaatregelen.

Risicoanalyse
De risicoanalyse bestaat, onafhankelijk van de methode die wordt gekozen, uit een aantal stappen:

1. Het bepalen van de scope van het onderzoek;
2. Het in kaart brengen van bedreigingen (dreigingsanalyse);
3. Het in kaart brengen van de maatregelen (maatregelanalyse / GAP-analyse);
4. Het in kaart brengen van de kwetsbaarheden;
5. Het inschatten van de kans van optreden en de schade;
6. Het identificeren van aanvullende maatregelen.

Vervolgens kunnen de risico's gemanaged worden doordat voor de aanvullende maatregelen een planning wordt opgesteld.

De jaarplanning
De BIO kan niet in één keer volledig worden geïmplementeerd. Een dergelijke implementatie zou een onevenredige inspanning van de organisatie verlangen. Daarnaast zijn er voor toekomstige technische en organisatorische veranderingen aanpassingen nodig.

Om deze redenen gaat het jaarplan informatieveiligheid dan ook (zoals beschreven bij het ambitieniveau) uit van een systeem van continue plannen, uitvoeren, monitoren en verbeteren. We sluiten hiermee aan op de planning en control cyclus die is ingericht conform het plan-do-check-act principe van Deming (hierna PDCA cyclus).

De cyclus komt terug in het jaarplan en begint met het richting geven aan de organisatie. Met het accorderen van de BIO als normenkader en het instemmen met de bestuurlijke principes van de VNG, is

op bestuurlijk niveau commitment gegeven aan de BIO. Het is van belang om dit ook uit te spreken binnen de eigen organisatie en dit te verankeren in het informatiebeveiligingsbeleid.

Aan de hand van het beleid kunnen maatregelen worden geïmplementeerd en gemonitord worden op de naleving van de maatregelen. Met het bijstellen van de maatregelen of het corrigeren van de uitvoering worden verbeteringen doorgevoerd.

Voor een efficiënte en effectieve benadering gaat een jaarplanning minimaal uit van:

- Het inventariseren van veranderingen in de organisatie (nieuwe taken, veranderingen in wetgeving etc..);
- Het periodiek uitvoeren van controles;
- Het periodiek uitvoeren van risicoanalyses (nieuwe of bij veranderingen);
- Het periodiek communiceren over beveiliging;
- Het periodiek opstellen van rapportages;
- Het voorbereiden van audits.

Hoofdstuk 3 Informatieveiligheidsorganisatie

Doelstelling
Informatiebeveiliging heeft ook een kwaliteitsaspect. Om de kwaliteit te borgen binnen de organisatie zijn een aantal sleutelpersonen nodig die het management ondersteunt bij de implementatie en het op orde houden van informatieveiligheid. Het geheel aan taken, bevoegdheden en verantwoordelijkheden noemen we de governance. In dit hoofdstuk gaan we in op de wijze waarop de governance is ingericht.

Verantwoordelijkheden
Het beleggen van verantwoordelijkheden bij de implementatie en uitvoering van informatieveiligheid is een randvoorwaarde voor het structureel doorlopen van het Information Security Management System (ISMS) / PDCA cyclus. Naast het structureel doorlopen van het ISMS is het van essentieel belang om passende contacten met overheidsinstanties te onderhouden en het onderwerp informatieveiligheid structureel in projecten mee te wegen.

Uitgangspunten ten aanzien van de informatieveiligheidsorganisatie zijn als volgt gedefinieerd:

- De gemeenteraad heeft een toezichthoudende rol op basis van de controlerende taak die de Gemeentewet aan de gemeente raad toekent;
- Het college van B en W van de gemeente draagt als eindverantwoordelijke van de informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor het bewerkstelligen van een passend niveau van informatieveiligheid;
- Het college stelt de kaders ten aanzien van informatieveiligheid vast, op basis van wet- en regelgeving en landelijke normenkaders;
- Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatie om beveiligingsmaatregelen te nemen;
- Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van informatieveiligheid, gemandateerd aan de gemeentesecretaris;
- De gemeentesecretaris is ambtelijk eindverantwoordelijk voor de informatieveiligheid en de inrichting en werking van de beveiligingsorganisatie en stelt hiervoor richtlijnen en procedures op;
- Het lijnmanagement is verantwoordelijk voor hun eigen processen en stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;
- Op grond van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit;
- Informatieveiligheid is een cyclisch proces en is volgens de PDCA cyclus ingericht.

Het management wordt intern ondersteund door diverse vakspecialisten. De volgende rollen dienen minimaal te worden ingevuld:

Chief Information Security Officer (CISO)
De CISO is de interne adviseur op het gebied van informatieveiligheid binnen de organisatie. Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren van het management, het adviseren bij projecten evenals het opstellen van rapportages.

Controller informatieveiligheid
Daar waar de CISO als adviseur voor de organisatie een coördinerende en adviserende rol heeft, wordt de interne beheersing en toezicht bij de controller Informatieveiligheid belegd. Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatiebeveili-

gingsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.

Beveiligingsbeheerder
Binnen de diverse vakgebieden is het noodzakelijk dat experts op het vakgebied werken aan de kwaliteit van de processen. De beveiligingsbeheerder richt zich in eerste instantie op het eigen vakgebied en werkt daarnaast samen met de CISO aan organisatie brede onderwerpen.

Functionaris voor de Gegevensbescherming (FG)
Voor de gemeente is het aanstellen van een functionaris voor de gegevensbescherming (FG) verplicht op grond van de Algemene Verordening Gegevensbescherming (AVG). De FG is de interne toezichthouder op de verwerking van persoonsgegevens en naleving van de AVG binnen de organisatie. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Bij organisaties met een FG stelt de Autoriteit Persoonsgegevens (AP) zich terughoudend op als toezichthouder.

Privacy Officer (PO)
De Privacy Officer is verantwoordelijk voor het vormgeven en implementeren van het gegevensbeschermingsbeleid binnen de gemeente. Daarnaast kan de Privacy Officer het management ondersteunen bij het in kaart brengen van de risico's door bijvoorbeeld een Data Protection Impact Assessment (DPIA) uit te voeren. De Privacy Officer is de uitvoerende functionaris op het gebied van gegevensbescherming en ondersteunend aan het management.

Let op!
Binnen diverse vakgebieden kunnen andere specialisten aanwezig zijn die een rol hebben op het gebied van informatieveiligheid of gegevensbescherming. In de bijlage worden die rollen benoemd. Via separate richtlijnen per aandachtsgebied worden de taken, bevoegdheden en verantwoor-delijkheden beschreven.

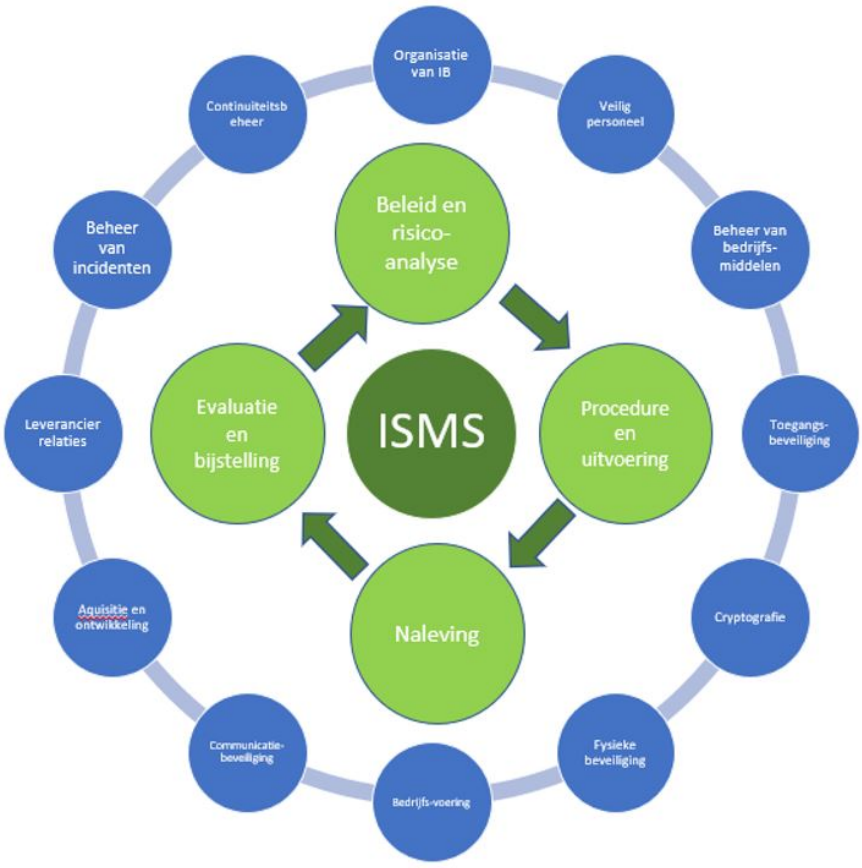
Tactische uitgangspunten BIO

Inleiding

De tactische uitgangspunten van het informatieveiligheidsbeleid gaan in op de beheersdoelstellingen per onderdeel van de BIO.

De BIO kent naast het ISMS een aantal inhoudelijke onderwerpen. Deze onderwerpen staan veelal niet op zich daar de onderwerp vaak samen zorgen voor een niveau van veiligheid. Zo is er samenhang tussen de HRM processen instroom, doorstroom en uitstroom en het beheer van autorisaties. Op het gebied van communicatie op het internet is er samenhang met het beheer van encryptiesleutels. Wanneer een organisatie excelleert op één gebied kan een ander gebied weer voor onveiligheid zorgen. We zeggen dan ook wel dat de beveiliging zo goed is als de zwakste schakel in de keten.

Per onderwerp zullen we op tactisch niveau aangeven wat het doel is van dit beheeraspect.



Veilig personeel

Doelstelling
Medewerkers dienen geschikt te zijn en geschikt te blijven voor hun functie. De belangrijkste waarborg is het aantrekken van betrouwbaar en geschikt personeel en de zorg dat de medewerkers geschikt blijven voor hun functie, zodat ze op een goede wijze met de informatie van de organisatie om kunnen gaan tijdens en na afloop van hun contract.

Toelichting
Informatieveiligheid valt en staat met de kennis, houding en gedrag van de medewerkers. Om de juiste medewerkers in de organisatie te krijgen, deze gedurende hun loopbaan te trainen en te coachen zodat zij over de kennis en vaardigheden beschikken die nodig zijn om hun functie naar behoren uit te voeren.

Beheer van bedrijfsmiddelen

Doelstelling
De gemeente gebruikt een groot aantal systemen (apparatuur, devices en software) om de informatie-voorziening te faciliteren. Het doel van dit beheer aspect is het identificeren van alle hard en software zodat deze op een adequate wijze beheerd en beveiligd kunnen worden.

Toelichting
Om informatie adequaat te kunnen beheren is het van belang om inzicht te hebben in diverse ICT-componenten die gebruikt worden om informatie te verwerken. Er kan pas adequaat beheer gevoerd worden wanneer je in het zicht hebt wat je moet beheren. De administratie waarin de ICT-componenten worden beschreven (ook wel configuratie management database CMDB) genoemd dient als basis van diverse beheerprocessen zoals patchmanagement, incidentmanagement evenals het informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging door de verantwoordelijke afdelingsmanager kan worden bepaald.

Toegangsbeveiliging

Doelstelling

Toegang tot informatie en informatie op een passende wijze beveiligen zodat onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie wordt voorkomen.

Toelichting
Om effectieve toegangscontrole tot vertrouwelijke en privacygevoelige informatie te kunnen invoeren en onderhouden wordt er een toegangsrichtlijn opgesteld. Naast deze toegangsrichtlijn heeft ieder informatiesysteem nog een specifiek gedefinieerde uitwerking omtrent toegang, dat is afgestemd op het beveiligingsniveau van de informatie.

Cryptografie

Doelstelling
Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Toelichting
Een effectieve manier om informatie te beveiligen tegen onbevoegde inzage is het versleutelen van deze informatie. Dit gebeurt bij voorkeur zowel bij de opslag als het transport. Belangrijk beheeraspect is dat versleuteling wordt toegepast met behulp van sleutels die veilig genoeg zijn conform de actuele standaarden. Om verlies van data te voorkomen is het van belang dat er ten aanzien van het beheer van de sleutels goede maatregelen zijn getroffen.

Fysieke beveiliging

Doelstelling
Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Toelichting
Een belangrijk aspect van informatieveiligheid is het voorkomen dat onbevoegden fysiek toegang hebben tot informatie. Ondanks de snelle ontwikkeling van digitale informatieverwerking is veel informatie ook nog analoog beschikbaar. Daarnaast dienen de informatie verwerkende computers en devices beschermd te worden tegen onbevoegde toegang.

Fysieke beveiliging wordt ingezet om onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

Beveiliging bedrijfsvoering

Doelstelling
Correcte en veilige bediening van informatie verwerkende faciliteiten ter voorkoming van ongewenste aanpassingen, verlies en diefstal van gegevens

Toelichting
Informatie wordt door de gehele organisatie heen gebruikt en daarnaast wordt informatie ook gedeeld met andere organisaties. Doordat informatie wordt hergebruikt is het van belang dat informatie goed wordt beheerd. Uitgangspunt hierbij is dat ieder brok aan informatie wordt beheerd vanuit een aangewezen organisatie onderdeel die daarvoor eenduidige processen en controlemaatregelen heeft ingericht om heeft de kwaliteit van de informatie te kunnen waarborgen.

Communicatiebeveiliging

Doelstelling
Informatie van de organisatie die via het interne netwerk intern dan wel extern wordt getransporteerd dient afdoende te worden beveiligd om onderschepping en/of ongewenste aanpassing van informatie te voorkomen.

Toelichting
Bij het beheer van netwerken moet onderscheid worden gemaakt tussen het eigen netwerk en netwerken die de grens van de organisatie overschrijden. Voor transport van vertrouwelijke en privacygevoelige gegevens via netwerken dienen extra maatregelen ter waarborging van de veiligheid te worden getroffen om te zorgen dat de data-integriteit en de vertrouwelijkheid bij transport is gewaarborgd. Zeker nu we steeds meer met externe partijen samenwerking is het van groot belang te kunnen vertrouwen op de communicatiekanalen.

Aankoop, ontwikkeling en onderhoud van informatiesystemen

Doelstelling
Waarborgen dat informatieveiligheid integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus en bij het testen van systemen. Dit zowel bij interne systemen als bij gebruik van een cloud leverancier.

Toelichting
Bij de ontwikkeling van (informatie)systemen moeten beveiliging en gegevensbescherming vanaf aanvang in het ontwerpproces of in het pakket aan eisen worden meegenomen (security bij design/default en gegevensbescherming bij design/default). Bij standaardprogrammatuur moet voor aanschaf worden vastgesteld of geautomatiseerde beveiligingsmaatregelen zijn ingebouwd en aan de eisen vanuit de AVG wordt voldaan. Bij het onderhoud van (informatie)systemen moet informatieveiligheid een vast aandachtspunt zijn.

Leveranciers

Doelstelling
Er dienen met leveranciers overeenkomsten te worden gesloten die ervoor zorgen dat de dienstverlening is overeenstemming is met het gemeentelijk informatieveiligheidsbeleid en de wettelijke bepalingen.

Toelichting
Organisatie zijn ten aanzien van de verwerking van informatie sterk afhankelijk van diverse leveranciers. Dit niet alleen vanwege de aanschaf en de primaire werking maar vanwege de dienstverlening die verbonden is aan de primaire dienstverlening. Het is van belang om met de leveranciers goede afspraken te maken over de aard van de dienstverlening. Daarnaast dient periodiek te worden gecontroleerd of ook aan de eisen wordt voldaan.

Incidentenbeheer

Doelstelling
Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatieveiligheid incidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging

Toelichting
Het beheer van incidenten kent twee gezichtspunten. Ten eerste dienen incidenten snel en adequaat te worden afgehandeld maar daarnaast zijn incidenten ook een signaal dat bestaande maatregelen wellicht niet voldoen. Het is dus van belang dat een incident zowel goed en snel wordt afgehandeld en dat daarnaast een analyse plaatsvindt zodat duidelijk is wat de oorzaak is geweest en hoe we er structureel voor kunnen zorgen dat een dergelijk voorval niet meer plaats kan vinden.

Continuïteitsbeheer

Doelstelling
Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

Toelichting
Continuïteitsbeheer heeft als doel om ervoor te zorgen dat de dienstverlening intern en extern ongestoord kan plaatsvinden. Om de dienstverlening ongestoord doorgang te laten vinden dienen we zowel te kijken naar de systemen die nodig zijn als naar de facilitaire voorzieningen.

Naleving

Doelstelling
Verzekeren dat informatieveiligheid wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie ter voorkoming van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatieveiligheid en beveiligingseisen.

Toelichting
Het uitdragen van beleid en het opstellen van procedures moeten een waarborg bieden voor de kwaliteit. Het controleren van het beleid en de naleving van de procedures zijn erop gericht om te beoordelen of beleid en procedures ook werkbaar zijn in de praktijk, maar ook om onrechtmatig-heden te kunnen detecteren. Daarnaast kunnen controles ook gebruikt worden om verdere sturing te geven aan de organisatie en zijn daarmee een essentieel onderdeel van de governance.

BEEKDAELEN

Bijlage 1 Beveiligingsrollen in de gemeente Beekdaelen

Generieke informatiebeveiligingsrollen binnen de gemeente Beekdaelen

Rol	Taken en verantwoordelijkheden informatiebeveiliging
Gemeentesecretaris	• Verantwoordelijk voor de informatiebeveiliging binnen de eigen organisatie. • Stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. • Wijst een coördinator informatieveiligheid (CISO) aan. • Stelt operationele kaders en geeft sturing ten aanzien van de veiligheid van informatie. • Stuurt op de beheersing van risico's. • Evalueert periodiek de beleidskaders en stelt deze waar nodig bij. • Belegt de verantwoordelijkheid voor informatieveiligheidscomponenten en systemen. • Verantwoordelijk voor het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid.
Afdelingsmanagers	• Verantwoordelijk voor de juiste implementatie van beveiliging in de bedrijfsprocessen en systemen. • Wijst voor ieder (informatie)systeem een proceseigenaar aan. • Verantwoordelijk voor 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. • Verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen. • Verantwoordelijk voor het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn). • Verantwoordelijk voor het rapporteren, via de controller, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de organisatie in de P&C rapportages.
CISO	• Is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. • Rapporteert rechtstreeks aan de eigen directie. • Stelt voor de organisatie de informatieveiligheidsanalyse op en zorgt voor de actualisatie hiervan. • Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan Informatieveiligheid. • Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid. • Ondersteunt het bestuur en de afdelingshoofden met kennis over in formatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen. • Is aanspreekpunt voor medewerkers van de organisatie 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. • Wordt door de medewerkers geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. • Rapporteert over de informatieveiligheid in de P&C managementrapportages. Hierbij bundelt de CISO de deelbijdragen van de afdelingsmanagers. • Neemt deel aan regionale en landelijke informatieveiligheidsoverleggen.

	• Richt een organisatie in, stelt procedures op en zorgt voor bewustwording bij het bestuur, management en medewerkers, zodanig dat aan de eisen van het Informatieveiligheidsbeleid wordt voldaan.
Controller informatieveiligheid	• Is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten. • Voert periodieke toetsing uit 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. • Controleert de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid. • Controleert de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse. • Toetst/bewaakt het niveau van informatieveiligheid • Toetst/bewaakt het evaluatieproces van beveiligingsincidenten. • Neemt deel aan intern afstemmingsoverleg informatiebeveiliging.

Beveiligingsbeheerders
➢ BRP
➢ Reisdocumenten en rijbewijzen
➢ DigiD SIM
➢ DigiD iBurgerzaken
➢ DigiD ZorgNed
➢ Facilitaire zaken
➢ DIV
➢ HRM
	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van eigen vakgebied.
	• 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.
	• Voorbereiden en coördinatie van audits en (zelf)evaluaties.
	• Preventie en detectie van beveiligingsincidenten en het geven van een adequate respons.
	• Coördineren van het toepassen van specifieke wet- en regelgeving.
	• Rapporteert aan de coördinator informatieveiligheid en de controller informatieveiligheid.
	• Een vertegenwoordiging van de beveiligingsbeheerders neemt deel aan intern afstemmingsoverleg informatiebeveiliging.
	• Extra voor BRP: Ten aanzien van de BRP worden loggingsrapportages minimaal maandelijks beoordeeld door de BRP beheerder.
	• Extra voor 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.
	  • Verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).
	• Extra voor HRM: Verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke adviesrol op het gebied van organisatie en informatieprocessen.
	• Extra reisdocumenten en rijbewijzen: Verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten en rijbewijzen.

De autorisatiebevoegde reisdocumenten / aanvraagstations	• Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumenten modules (RAAS en aanvraagstations).
De autorisatiebevoegde rijbewijzen	• Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
Gegevensbeheerder	• De gegevensbeheerder is voor een of meerdere informatiesystemen verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening. • Neemt deel aan intern afstemmingsoverleg informatiebeveiliging en gegevensbescherming.

Intern afstemmingsoverleg informatiebeveiliging en gegevensbescherming	• Onderwerpen van het afstemmingsoverleg: • Voortgang uitvoering maatregelen uit de analyses en/of uit het actieplannen informatieveiligheid en gegevensbescherming. • Beveiligingsincidenten. • Planning en voorbereiding van Audits, controles en zelfevaluaties.

Overige rollen

Rol	**Taken en verantwoordelijkheden informatiebeveiliging**
Privacy Officer	• Adviseert binnen de organisatie over gegevensbescherming en over activiteiten ter bescherming van persoonsgegevens. • Beheert het register van verwerkingen van persoonsgegevens tegen de achtergrond van de kaders van de privacywetgeving. • Adviseert proceseigenaren bij wijzigingen in procesuitvoering en bedrijfsvoering. • Coördineert en voert namens de organisatie een DPIA uit. • Neemt als adviserend lid deel aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens. • Geeft uitleg over de privacy voorschriften uit de privacywetgeving. • Coördineert de privacy werkzaamheden. • Verzorgen van meldingen van datalekken en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (Apen op basis van het advies van de Functionaris voor de gegevensbescherming (FG). • Coördineren van AVG verzoeken van betrokkenen zoals inzage, correctie, verwijdering en verzet ten aan zien van persoonsgegevens en adviseren over de afhandeling. • Inrichten van procedures voor het afhandelen van datalekken. • Onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen. • Advisering en ondersteuning bij het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van procedures. • Neemt deel aan intern afstemmingsoverleg informatiebeveiliging en gegevensbescherming.
Functionaris Gegevensbescherming	• Interne toezichthouder op de verwerking van persoonsgegevens. Houdt toezicht op de toepassing en naleving van de privacywetgeving. • Verantwoordelijk voor de uitvoer van de klachtenafhandelingsprocedure betreffende het nakomen van de AVG door de gemeenten en de gemeenschappelijke regeling. Dit betekent het initiëren, doorlopen, verzorgen van interne en externe communicatie en afsluiten van de klachtenafhandelingsprocedure. • Neemt deel aan intern afstemmingsoverleg informatiebeveiliging en gegevensbescherming. • Neemt deel aan regionaal afstemmingsoverleg gegevensbescherming. • Adviseert concern breed over meldingen van (mogelijke) datalekken door dit op te nemen in een register van (mogelijke) datalekken en adviseert de organisatie of melding aan de Autoriteit Persoonsgegevens en betrokkenen vereist is. • Adviseert de organisatie over DPIA's en houdt toezicht op de uitvoering daarvan. • Bewustmaken en opleiden van medewerkers op het gebied van gegevensbescherming. • Werkt op diens verzoek samen met de Autoriteit Persoonsgegevens. • Treedt op als contactpersoon op het gebied van gegevensbescherming voor burgers • Adviseert de gemeente en samenwerkingspartijen over hun verplichtingen op het gebied van gegevensbescherming. • Beheert het register van verwerkingen op basis van meldingen van proceseigenaren.

VCIB	• Vertrouwde Contactpersoon Informatiebeveiliging voor de Informatie Beveiligingsdienst (IBD). Ontvangt incidentmeldingen of waarschuwingen waarvan de inhoud een vertrouwelijk karakter heeft. • Verantwoordelijk voor de afhandeling van de vertrouwelijke incidentmeldingen en waarschuwingen van de IBD.
ACIB	• Algemene Contactpersoon Informatiebeveiliging voor de IBD. De ACIB krijgt algemene waarschuwingen en informatie met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.
Beveiligingsbeheerder Parkstad-IT	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van de IT voorziening bij Parkstad-IT. • 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. • Voorbereiden en coördinatie van audits en (zelf)evaluaties.
Beveiligingsbeheerder Basisregistratie Adressen en Gebouwen (BAG)	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van de BAG • 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. • Voorbereiden en coördinatie van audits en (zelf)evaluaties. • Preventie en detectie van beveiligingsincidenten en het geven van een adequate respons. • Coördineren van het toepassen van specifieke wet- en regelgeving. • Rapporteert aan het afdelingshoofd
Beveiligingsbeheerder Basisregistratie Grootschalige Topografie (BGT)	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van de BGT. • 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. • Voorbereiden en coördinatie van audits en (zelf)evaluaties. • Preventie en detectie van beveiligingsincidenten en het geven van een adequate respons. • Coördineren van het toepassen van specifieke wet- en regelgeving. • Rapporteert aan het afdelingshoofd
Beveiligingsbeheerder Basis Registratie Ondergrond (BRO)	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van de BRO • 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. • Voorbereiden en coördinatie van audits en (zelf)evaluaties. • Preventie en detectie van beveiligingsincidenten en het geven van een adequate respons. • Coördineren van het toepassen van specifieke wet- en regelgeving. • Rapporteert aan het afdelingshoofd.
Manager Suwinet	• De manager is verantwoordelijk voor de aanvraag van mutaties in geval van in-, door- en uitstroom van medewerkers. Deze aanvraag wordt door de Security Officer SUWI gecontroleerd.
Beveiligingsbeheerder/Security Officer Suwinet	• Verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid bij de afdeling Sociaal, in het bijzonder voor Suwinet. • Verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informa-

	tieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden. • Voorbereiden en coördinatie van audits en (zelf)evaluaties. • Preventie en detectie van beveiligingsincidenten en het geven van een adequate respons. • Coördineren van het toepassen van specifieke wet- en regelgeving. • Beheert beveiligingsprocedures en maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. Dit laatste impliceert eveneens de kwaliteitszorg, de kwaliteitsborging en de controle op het toegang en gebruik van Suwinet. • Bevordert de beveiliging van Suwinet. • Ziet er op toe dat de beveiligingsmaatregelen worden nageleefd. • Adviseert en informeert medewerkers en management. • Doet voorstellen tot implementatie of aanpassing van plannen op het gebied van de beveiliging van Suwinet. • Evalueert de resultaten van verbetermaatregelen. • De Security Officer verzorgt periodiek een rapportage met betrekking tot de beveiligingsstatus en het gebruik van Suwinet aan het hoogste management en/of het college. • Controleert de aanvragen van mutaties door de manager. De Security Officer SUWI gaat hierbij na of de gevraagde autorisatie overeenkomt met de uit te voeren functie/rol. Indien de aanvraag akkoord is, worden de autorisaties en toegang inclusief wachtwoorden in orde gemaakt. • Vraagt meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet.

IT crisisbeheersing

➢ Voorzitter informatiebeveiligingsoverleg ➢ Coördinator IT ➢ Beveiligingsbeheerder IT ➢ Lid van het MT ➢ Lid van team communicatie ➢ Relevante experts	• Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. • Op basis van de mogelijke politieke gevolgen van het incident kiest de verantwoordelijk manager er voor om al dan niet de verantwoordelijke portefeuillehouder in te lichten.