Strategisch beleid informatiebeveiliging BVO JeugdFV

2026 tot 2030

Opdrachtgever	Bestuur BVO JeugdFV
Opdrachtnemer	Directeur BVO JeugdFV
Versie	1.0
Datum:	13-11-2025

Versiebeheer:

Versie	Versiedatum	Status
0.7	7-11-2025	Concept ter review Strat. Adviseurs gem. Ede
0.8	11-11-2025	Concept ter review Kwartiermaker BVO JeugdFV
0.9	11-11-2025	Concept ter beoordeling directeur BVO JeugdFV
1.0	13-11-2025	Definitief ter vaststelling Bestuur BVO JeugdFV

Distributielijst:

Versie	Versiedatum	Verspreid aan
0.7	7-11-2025	Strat. Adviseurs en CISO gem. Ede
0.8	11-11-2025	Kwartiermaker BVO JeugdFV
0.9	11-11-2025	Directeur JeugdFV
1.0	13-11-2025	Definitief ter vaststelling Bestuur BVO JeugdFV

Inleiding....4
Leeswijzer....4
Hoofdstuk 1: Het strategisch informatiebeveiligingsbeleid....5
1.1 Wat is informatiebeveiliging?....5
1.2 Doelstelling strategisch beleid....5
1.3 Reikwijdte van het strategisch informatiebeveiligingsbeleid....5
1.4 Ordening van het beleid....5
1.5 Vaststelling, geldigheidsduur en evaluatie van het strategisch beleid....6
Hoofdstuk 2: Informatiebeveiligingskaders....7
2.1 Fundamentele beveiligingsprincipes....7
2.2 Informatiebeveiligingsstandaarden....7
2.3 Wettelijke basis en controle beveiligingsnormen....7
2.4 Omgevingsmonitoren en landelijke agenda's....8
Hoofdstuk 3: Visie en strategische doelen informatiebeveiliging....9
3.1 Opgave en visie op informatiebeveiliging BVO JeugdFV....9
3.2 Doelen informatiebeveiliging BVO JeugdFV....10
Hoofdstuk 4: Sturing op informatiebeveiliging....11
4.1 Informatiebeveiliging als onderdeel van organisatie brede governance....11
4.2 Managementsystematiek ISMS:....11
4.3 Dubbele PDCA-cyclus voor continue verbetering en handhaving weerbaarheid....11
Hoofdstuk 5: Organisatie, taken en verantwoordelijkheden....12
5.1 Verdeling van verantwoordelijkheden....13
5.1.1 De eerste lijn: verantwoordelijkheid en uitvoering....13
5.1.2 De tweede lijn: Advisering....14
5.1.3 De derde lijn....14
5.2 Communicatiestructuren....15
5.3 Bewustwording en training van personeel....15
5.4 Disciplinaire procedure....15
Hoofdstuk 6: Planning van activiteiten informatiebeveiliging....16
6.1 Informatiebeveiligingsplan BVO JeugdFV....16
6.2 Projectmanagement....16
Hoofdstuk 7: Risicomanagement....17
Hoofdstuk 8: Incidentrespons en Bedrijfscontinuïteitsmanagement....18
8.1 Incidentrespons....18
8.2 Bedrijfscontinuïteitmanagement....18
Hoofdstuk 9: Naleving op informatiebeveiliging....19
Bijlage 1 afkortingenlijst....20

Inleiding

Voor u ligt het Strategisch informatiebeveiligingsbeleid van de gemeenschappelijke regeling Bedrijfsvoeringsorganisatie Jeugdhulpregio JeugdFV (BVO JeugdFV). In dit document wordt beschreven welke doelen de organisatie nastreeft met informatiebeveiliging en hoe zij die doelen wil bereiken. Het document is gebaseerd op en voldoet aan het normenkader voor informatiebeveiliging voor de overheid: de BIO2[1].

De BVO JeugdFV is een informatie-intensieve organisatie met een primaire focus op publieke dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. Enerzijds moeten de medewerkers van de BVO JeugdFV en hun ketenpartners kunnen beschikken over betrouwbare informatie om inwoners en organisaties optimaal te kunnen helpen en adviseren. Anderzijds moeten inwoners en bedrijven erop kunnen vertrouwen dat hun gegevens bij de BVO JeugdFV in goede handen zijn en dat informatie beschikbaar is wanneer zij een beroep doen op onze publieke dienstverlening.

Informatiebeveiliging beperkt zich niet tot ICT en kan niet door slechts enkele medewerkers en systemen afdoende geregeld worden. Iedereen in onze organisatie heeft hierin een rol, zowel de bestuurders, de directeur als de medewerkers. Uitgangspunt is dat de verantwoordelijkheid voor dit onderwerp bij de directeur ligt en dat van iedere medewerker veilig gedrag verlangd wordt. Informatiebeveiliging vraagt daarnaast continue aandacht. De BIO2-norm schrijft voor dat hier een continu verbeterproces volgens de plan-do-check act systematiek wordt ingericht en dat dit proces verankerd moet zijn binnen de governance structuur. Uitgangspunt hierbij is dat informatiebeveiliging uiteindelijk een vorm van risicomanagement is. Deze aspecten worden in dit document verder uitgewerkt.

Leeswijzer

In hoofdstuk 1 wordt nader omschreven wat informatiebeveiliging nu precies is en wat de rol en het doel van dit document daarbij is. Ook wordt de reikwijdte en de relatie met onderliggende beleidsstukken, procedures en handreikingen beschreven.
Hoofdstuk 2 beschrijft de kaders waarbinnen het informatiebeleid moet worden vormgegeven: normenstelsels, wetgeving, richtlijnen en *best practices*.
Hoofdstuk 3 bevat een omschrijving van de doelstellingen en de visie van de BVO JeugdFV op informatieveiligheid beschreven.
Hoofdstuk 4 beschrijft hoe organisatie breed regie plaatsvindt op informatiebeveiliging d.m.v. governance-structuren die samen het Informatie Security Management Systeem (ISMS) vormen.
Hoofdstuk 5 beschrijft de wijze waarop informatiebeveiliging organisatorisch wordt vormgegeven.
Hoofdstuk 6 beschrijft de planvorming op informatiebeveiliging.
Hoofdstuk 7 beschrijft het proces van risicomanagement wordt uitgevoerd.
Hoofdstuk 8 beschrijft de kaders rondom incident afhandeling en vereisten voor bedrijfscontinuïteit.
Hoofdstuk 9 beschrijft de wijze van naleving en audit verplichtingen op informatiebeveiliging

[1] *De Baseline Informatiebeveiliging Overheid*

Hoofdstuk 1: Het strategisch informatiebeveiligingsbeleid

1.1 Wat is informatiebeveiliging?

Informatie is alles dat kennis toevoegt en zo onwetendheid, onzekerheid of onbepaaldheid vermindert. Met informatie vergaren we inzicht om waarde te creëren, te kunnen helpen en te adviseren. Informatie is een waardevol bedrijfsmiddel dat, net als andere waardevolle bedrijfsmiddelen, voortdurend op een passende manier beveiligd dient te zijn. Door de opkomst van de digitalisering en de daaruit voortvloeiende informatiemaatschappij en ICT is zowel het belang van informatie als de bedreigingen waaraan die informatie blootstaat enorm toegenomen.

Informatiebeveiliging zorgt voor het treffen en onderhouden van een samenhangend pakket aan maatregelen om de waarde van de informatievoorziening van de gehele organisatie te beschermen. Deze waarde wordt bepaald door de eisen aan de beschikbaarheid, de integriteit en de vertrouwelijkheid van deze informatie. Maatregelen zijn hierbij niet beperkt tot de techniek, ook organisatorische maatregelen zoals het helder definiëren van verantwoordelijkheden en procedures en medewerker gerichte maatregelen zoals het verbeteren van kennis en bewustzijn rondom bedreigingen en hoe hiermee om te gaan zijn essentieel. Informatiebeveiliging maakt daarmee onderdeel uit van bedrijfsprocessen en bedrijfsmiddelen op alle niveaus van de organisatie. De maatregelen dienen daarnaast aantoonbaar te zijn, dat betekent dat de gemeente kan bewijzen dat de beveiligingsmaatregelen zijn beschreven, uitgevoerd worden en over een langere periode hebben gewerkt.

1.2 Doelstelling strategisch beleid

Het strategisch informatiebeveiligingsbeleid geeft sturing en structuur aan de activiteiten op informatiebeveiliging. Op basis van de gewenste doelstellingen definieert het de kaders, verantwoordelijkheden, de belangrijkste processen en rollen met betrekking tot informatieveiligheid. Het informatiebeveiligingsbeleid geeft daarmee richting aan het inrichten van de informatiebeveiliging.

1.3 Reikwijdte van het strategisch informatiebeveiligingsbeleid

De reikwijdte van het strategisch informatiebeveiligingsbeleid beslaat de gehele organisatie en omvat alle processen, objecten, organisatieonderdelen, informatiesystemen, gegevens(verzamelingen) en betrokken medewerkers ongeacht locatie of tijdstip.

Daar waar BVO JeugdFV samenwerkingsverbanden aangaat met derden voor de uitbesteding van taken is dit beleid richtinggevend. Ketenpartners dienen waar relevant zelf zodanig maatregelen te treffen dat de doelstellingen van dit beleid gerealiseerd kunnen worden.

Dit strategische informatiebeveiligingsbeleid dekt ook aanvullende beveiligingseisen uit wetgeving af zoals voor de BRP of Jeugdwet. Voor bepaalde kerntaken gelden op grond van deze en andere wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen als verplichting voor BVO JeugdFV. Deze worden in onderliggende beleidsdocumenten geconcretiseerd.

1.4 Ordening van het beleid

Omdat informatiebeveiliging een brede reikwijdte heeft en op veel verschillende thema's betrekking heeft zijn er veel onderwerpen waarop beleid, richtlijnen of procedures moeten worden vastgesteld. In dit strategisch beveiligingsbeleid stellen we slechts een aantal kaders en hoofdlijnen vast, uitwerking geschiedt in onderliggend aanvullend beleid en in procedures of werkinstructies. Hiermee ontstaat de volgende indeling:

Strategisch niveau: Het *strategische beleid* richt zich organisatie breed op het "wat" en "waarom" van informatiebeveiliging voor de BVO JeugdFV en sluit daarbij aan op de organisatiedoelstellingen. Op enkele thema's wordt een concretiseringslag gemaakt om invulling te geven aan de wijze van sturing op concernniveau aan informatiebeveiliging. Vaststelling van dit beleid geschiedt door het Bestuur.

Tactisch niveau: Door *onderwerpspecifiek beleid* worden de diverse aparte thema's binnen het spectrum van informatiebeveiliging uitgewerkt met een inhoudelijke verdiepingsslag. Op dit niveau wordt het "hoe" ingevuld. Ook specifiek beleid dat voortvloeit uit normenkaders of wettelijke verplichtingen voor onderdelen (zoals AVG-verplichtingen) wordt op deze manier vormgegeven. Uitgangspunt is dat vaststelling geschiedt door de directeur.

Operationeel niveau: Op dit niveau wordt met *procedures of werkinstructies* het "hoe" verder gedetailleerd. Vaststelling geschiedt door de directeur.

Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

1.5 Vaststelling, geldigheidsduur en evaluatie van het strategisch beleid

Dit strategisch beleid wordt door het Bestuur vastgesteld met een looptijd van vier jaar. Het blijft van kracht totdat er een nieuw beleid is vastgesteld. In ieder geval zal het beleid geëvalueerd worden na drie jaar, zodat verbeteringen meegenomen kunnen worden voor nieuw vast te stellen beleid.
Bij grote veranderingen kan de directeur besluiten dit beleid tussentijds te evalueren en aan te passen.

Hoofdstuk 2: Informatiebeveiligingskaders

Dit hoofdstuk beschrijft de kaders waarbinnen het informatiebeleid is vormgegeven. Er zijn een aantal fundamentele principes te onderkennen waarop informatiebeveiliging gebaseerd is. Deze principes zijn in een standaarden en normenkaders uitgewerkt, waarbij de Baseline Informatiebeveiliging Overheid (BIO2) richtinggevend is voor onze organisatie. Hiernaast zijn er ook nog diverse wetten en regelingen die eisen en randvoorwaarden stellen aan informatiebeveiliging. Als laatste wordt er een kort overzicht gegeven van ontwikkelingen met betrekking tot de aandacht voor en verwachtingen bij de informatiebeveiliging van overheden.

2.1 Fundamentele beveiligingsprincipes

Informatiebeveiliging is een zaak die al sinds de ’70 er jaren speelt, maar rond het millennium met de opkomst van internet een grote vlucht heeft genomen. In de loop der jaren hebben zich een aantal principes uitgekristalliseerd:

- Informatiebeveiliging is een cyclisch, continu proces omdat de te beheersen risico’s en de bijbehorende bedreigingen steeds veranderen. Hiervoor wordt meestal aanpak uit kwaliteitsmanagement (de Plan-Do-Check-Act cyclus en het streven naar continue verbetering) gebruikt. Dit proces wordt verder uitgewerkt in hoofdstuk 4.
- Informatiebeveiliging heeft niet alleen te maken met techniek en middelen, maar ook met mensen en met organisatie. Lang niet alle bedreigingen zijn met technische hulpmiddelen te verminderen, weerbare medewerkers en een veilige manier van werken zijn essentieel. Dit wordt verder uitgewerkt in hoofdstuk 5
- Informatiebeveiliging is een lijnverantwoordelijkheid. Door de grote impact van medewerkers en processen op de mate van veiligheid is informatiebeveiliging niet bij een staffunctionaris neer te leggen. Ook sluit dit aan bij het beschouwen van informatieveiligheid als risicomanagement. Dit wordt verder uitgewerkt in hoofdstuk 5.
- Informatiebeveiliging kent drie kernwaarden: beschikbaarheid, integriteit en vertrouwelijkheid. Maatregelen richten zich altijd op het garanderen van een of meerdere van deze waarden. Dit wordt verder uitgewerkt in hoofdstuk 7.
- Informatiebeveiliging is een vorm van risicomanagement. Dit betekent dat informatiebeveiliging een genuanceerde en situationeel bepaalde aanpak heeft waarbij risico’s de prioriteit bepalen en geaccepteerd kunnen worden als de noodzakelijke maatregelen niet meer in verhouding staan tot het risico. Dit principe wordt uitgewerkt in hoofdstuk 7.

2.2 Informatiebeveiligingsstandaarden

Er zijn verschillende standaarden en normenkaders voor informatiebeveiliging waarin bovenstaande principes zijn uitgewerkt. De meest bekende en meest toegepaste is de internationale ISO 27001/27002 norm. De norm beschrijft de processen en uitgangspunten van informatieveiligheid en geeft een groot aantal, op best practices gebaseerde maatregelen die genomen kunnen worden. Iedere organisatie moet op basis van eigen risicoafwegingen bepalen welke maatregelen genomen moeten worden, deze norm schrijft geen maatregelen voor.

Voor onze organisatie is de Baseline Informatiebeveiliging Overheid (BIO2) het uitgangspunt. Het Forum Standaardisatie heeft de BIO2 opgenomen als één van de verplichte standaarden voor de publieke sector. De BIO2 is een uitwerking van ISO27001/27002 en schrijft een minimumset aan maatregelen voor die in ieder geval getroffen moeten worden. Hiermee definieert de BIO2 een basisbeveiligingsniveau voor de gehele overheid, op basis waarvan samenwerking en gegevensuitwisseling veilig en vertrouwd kan geschieden.

2.3 Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatiebeveiliging valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

Algemene verordening Persoonsgegevens (AVG)
Ambtenarenwet
Archiefwet/ Archiefregeling;
Auteurswet

Databankenwet
Telecommunicatiewet
Wet algemene bepalingen Burgerservicenummer
Wet Computercriminaliteit;
Wet digitale overheid
Wet elektronisch bestuurlijk verkeer
Wet elektronische handtekeningen
Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB)
Wet Open Overheid (Woo)
Wet op ruimte ordening (Wro)
Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)
Network and Information Security directive (NIS2)

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle. Deze komen soms in normenstelsels terug maar kunnen ook heel specifiek van aard zijn.

2.4 Omgevingsmonitoren en landelijke agenda's

Landelijke dreigingsbeeld

Voor het verkrijgen van overzicht op dreigingen en bijbehorende ontwikkelingen op weerbaarheid maakt de ICT-dienstverlener van BVO JeugdFV gebruik van landelijke informatiebronnen op het gebied van cyber en digitalisering. De belangrijkste zijn:
- Het jaarlijkse Cybersecuritybeeld Nederland van de Nationaal Coördinator terrorisme en Veiligheid (NCTV).
- het jaarlijkse dreigingsbeeld gemeenten van de VNG-informatiebeveiligingsdienst gemeenten (IBD).
- De maandelijkse maandmonitoren van de VNG-informatiebeveiligingsdienst gemeenten (IBD).

Landelijke koers

Onderstaande agenda's, resoluties en actieplannen zetten de toon op de Nederlandse koers.

- 2018 in samenhang met de Agenda Digitale Overheid komt er kamerbrief over de noodzaak van het verhogen van informatieveiligheid (BZK)
- 2019 Nederlandse Cybersecurity Agenda (NCSC)
- 2020 Vorming van het Nationaal Crisisplan Digitaal (NCTV)
- 2020 - 2024 ontstaan Agenda digitale veiligheid (VNG)
- 2021 Aangenomen resolutie 'digitale veiligheid: kerntaak voor gemeenten'(VNG)
- 2021 I-strategie rijk 2021-2025 Digitale weerbaarheid
- 2022 Voorstel hoofdlijnen beleid voor digitalisering
- 2022 -2028 Nederlandse Cybersecuritystrategie
- 2022-2023 actieplan Nederlandse cybersecuritystrategie
- 2023 -2028 Internationale Cyberstrategie
- 2024 Eu-wetgeving Digital Decade
- 2025 Nederlandse digitaliseringsstrategie
- 2026 NIS2/Cyberbeveiligingswet

Omgevingsanalyse BVO JeugdFV

Gecombineerd geven de dreigingsbeelden samen met de interne incidentregistratie zicht op de informatiebeveiligingen gerelateerde dreiging. Samen met wijzigingen in landelijke agenda's valt zo een handelingsperspectief voor BVO JeugdFV te vormen. Dit beeld wordt gedocumenteerd in het jaarlijkse document, omgevingsanalyse BVO JeugdFV, met als doel om de risico's te kunnen herijken en bijstellingen te kunnen doen op het beveiligingsplan.

Hoofdstuk 3: Visie en strategische doelen informatiebeveiliging

3.1 Opgave en visie op informatiebeveiliging BVO JeugdFV

Informatiebeveiliging ondersteunt de organisatiedoelen van de BVO JeugdFV, zoals vastgelegd in onder meer de oprichtingstekst. Het zorgt dat de informatievoorziening nodig voor de uitvoering van onze publieke taken en dienstverlening adequaat beschikbaar, betrouwbaar en vertrouwelijk waar nodig blijft.
Informatiebeveiliging is daarmee in essentie een vorm van risicomanagement en streeft naar de balans tussen voldoende bescherming van de informatievoorziening enerzijds en de uitvoerbaarheid van bedrijfsprocessen anderzijds om daarmee de organisatiedoelen te bereiken. Nu en in de toekomst.

Informatiebeveiliging vraagt continue aandacht en aanpassingsvermogen door ontwikkelingen om ons heen. Enerzijds neemt de digitalisering toe en komen nieuwe technologieën beschikbaar. Ook groeit informatie-uitwisseling en deling door bijvoorbeeld meer data gestuurd gaan werken en zijn er in toenemende mate nieuwe mogelijkheden in connectiviteit. Anderzijds moeten we ons weerbaar maken tegen nieuwe dreigingen die op ons pad komen. Informatiebeveiliging is dan ook een continu proces door deze dynamiek.

BVO JeugdFV laat zich hierbij leiden door bestaande standaarden en best practices, waarbij de BIO2 het uitgangspunt is en waar wij ons als BVO aan committeren. We brengen de BIO2 op orde in onze organisatie en volgen de ontwikkelingen uit landelijke agenda's. Aandacht voor informatiebeveiliging is een breed gedragen verantwoordelijkheid in alle lagen van onze organisatie, mensen, processen, middelen en techniek. Ook voor iedereen die met BVO JeugdFV samenwerkt.

De BVO JeugdFV is zich hierbij bewust van de grote verantwoordelijkheid met betrekking tot het bewaren en verwerken van vaak gevoelige (persoons)gegevens en van de voorbeeldfunctie naar inwoners en het bedrijfsleven.

Bestuurlijke commitment op informatiebeveiliging

De BVO JeugdFV beschouwt informatiebeveiliging als een breed gedragen verantwoordelijkheid richting onze samenleving. Zowel het Bestuur als de directeur demonstreren met "the tone at the top" dat zij informatiebeveiliging ondersteunen en zich hierbij betrokken voelen. Zij hebben een cruciale rol bij het vormgeven en uitdragen van deze verantwoordelijkheid richting de gemeentelijke organisatie. Als aanvulling op de BIO2 zijn 10 bestuurlijke principes uitgewerkt door de Vereniging van Nederlandse gemeenten (VNG) die haar leden bekrachtigen:

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

De 10 principes geven invulling aan de rol van het Bestuur bij het vormgeven van informatiebeveiliging in de GR. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de bij de BVO belegde processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeenten. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk chefsache.

3.2 Doelen informatiebeveiliging BVO JeugdFV

BVO JeugdFV wil met informatiebeveiliging de volgende doelen bereiken.
De doelen zijn een afgeleide van de BIO2-indeling:

- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op beveiligingsincidenten.
- Het managen van de informatiebeveiliging.
- Het waarborgen van de naleving van dit beleid.

Hoofdstuk 4: Sturing op informatiebeveiliging

4.1 Informatiebeveiliging als onderdeel van organisatie brede governance

De sturing op informatiebeveiliging staat niet op zichzelf, maar is op basis van de BIO2 onderdeel van de organisatie brede governance. Hierdoor kan informatiebeveiliging beter aansluiten bij de organisatiedoelstellingen, beveiligingsrisico's in samenhang met andere risico's worden gezien en kan de directeur zijn verantwoordelijkheid voor informatiebeveiliging beter nemen. Om dit te realiseren moet een Informatie Security Management System (ISMS) worden ingericht als onderdeel van de organisatie brede governance. Dit houdt minimaal in dat naast de opvolging van maatregelen uit het informatiebeveiligingsplan, ook continue monitoring van mogelijke risico's plaatsvindt.

Dit ISMS heeft de volgende doelstellingen:

1. Strategische afstemming van informatiebeveiliging met de bedrijfsstrategie. Informatiebeveiliging moet het bereiken van de organisatiedoelen ondersteunen.
2. Effectief risicomanagement door het regisseren en prioriteren van te treffen maatregelen om risico's te kunnen managen en mitigeren naar een beheersbaar niveau.
3. Zorgen voor een effectieve en efficiënte inzet van informatiebeveiligingsexpertise, infrastructuur en overige middelen.
4. Regie en toezicht door het meten, monitoren en rapporteren op uitvoering en effecten van informatiebeveiligingsmaatregelen.

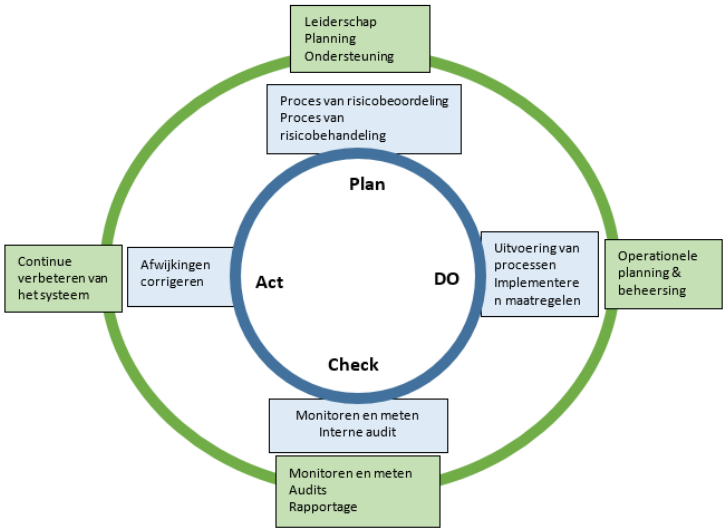
4.2 Managementsystematiek ISMS:

Een Information Security Management System (ISMS) is een procesgerichte benadering voor informatiebeveiliging. Het is een managementsystematiek waarin het risicobeheerproces centraal staat en door de bundeling van activiteiten een hogere mate van organisatievolwassenheid ontstaat op informatiebeveiliging. Het ISMS is de motor van de informatiebeveiligingsactiviteiten en bestaat uit de volgende onderdelen volgende onderdelen:

- Plan-do-check-act cyclus voor continue aandacht voor en verbetering van risicobeheersing
- Organisatie van verantwoordelijkheden en taken, zie hoofdstuk 5.
- Een methodiek voor risicomanagement, zie hoofdstuk 6.
- Gedefinieerde planvorming rondom informatiebeveiliging hoofdstuk 7.
- Rapportage lijnen voor controle op uitvoering en naleving. Hoofdstuk 9.

4.3 Dubbele PDCA-cyclus voor continue verbetering en handhaving weerbaarheid

De PDCA-cyclus wordt dubbelzijdig doorlopen waarbij de uitvoering (blauwe cirkel) zich bevindt in de dagelijkse operationele werkzaamheden binnen de werkprocessen en de governance (groene cirkel) zorgt voor de strategische (bij)sturing. De omloopsnelheid van de 2 cirkels kan onderling verschillen, maar de beide cirkels vormen samen één geheel en hebben onderling afstemming nodig.

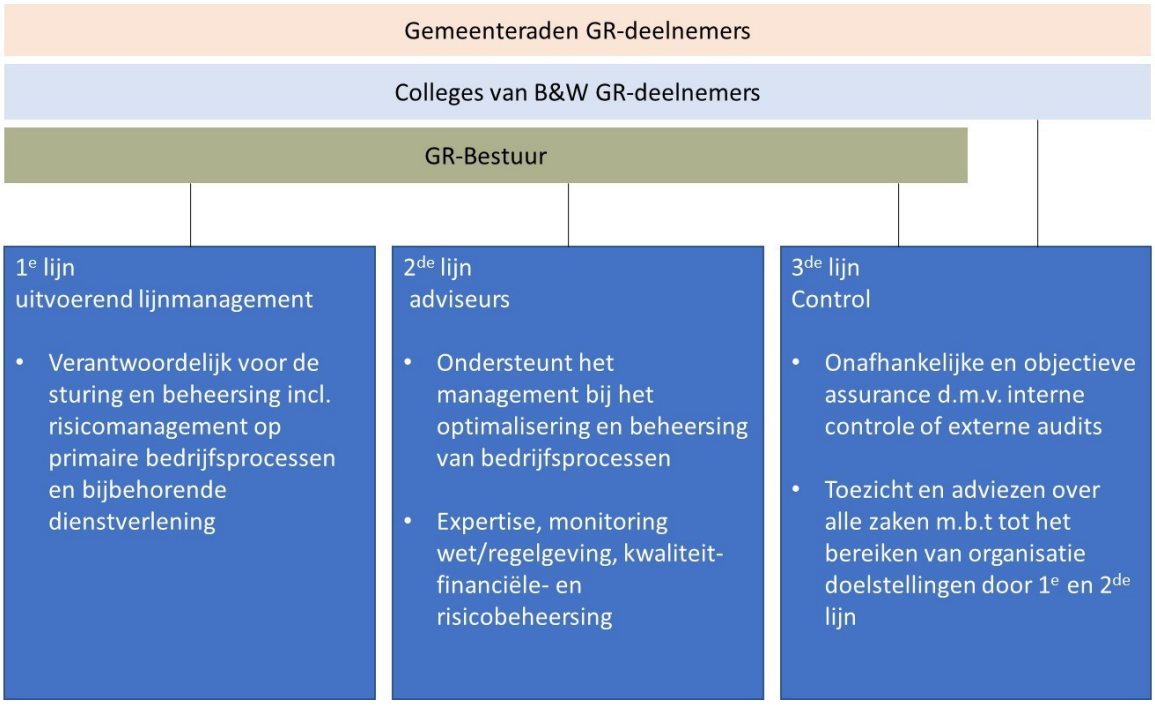


Hoofdstuk 5: Organisatie, taken en verantwoordelijkheden

Het Three Lines model

Het Three lines model is een generiek model voor organisaties wat helpt bij de governance op verantwoordelijkheden en rollen. Vanwege de herkomst risicomanagement is het ook geschikt voor de benodigde organisatie op informatiebeveiliging. Het brengt een bewust een scheiding van verantwoordelijkheden en taken om duidelijkheid te creëren en de kans op conflicterende taken en daarmee onbevoegd/onbedoeld wijziging van bedrijfsmiddelen te voorkomen.

Het management is verantwoordelijk voor informatiebeveiliging binnen de eigen processen en het nemen van beheersmaatregelen conform BIO2. De tweede lijn van adviseurs ondersteunt, adviseert, coördineert en bewaakt of de directeur zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een auditor en/of Functionaris Gegevensbescherming van een objectief en onafhankelijk oordeel voorzien met mogelijkheden tot verbetering in de 1e en 2de lijn. In de context van de BVO JeugdFV kan dit worden uitgevoerd door of namens de CISO's van de deelnemende gemeenten. In dit hoofdstuk worden ook de belangrijkste communicatiestructuren tussen de verschillende actoren beschreven.



5.1 Verdeling van verantwoordelijkheden

De verdeling van verantwoordelijkheden en de daaruit voortvloeiende taken wordt per 'Line' beschreven.

5.1.1 De eerste lijn: verantwoordelijkheid en uitvoering

De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het management. Zij zijn veelal ook de systeem- en proceseigenaren en daarmee verantwoordelijk voor informatiebeveiliging in de praktijk. De directeur stuurt dit aan. Het Bestuur is eindverantwoordelijk voor informatiebeveiliging en legt hierover verantwoording af aan de gemeenteraden.

Het Bestuur

Het Bestuur is eindverantwoordelijk voor informatiebeveiliging. Om dit inhoud te geven heeft het Bestuur de volgende taken:

- Het vaststellen van het strategisch Informatiebeveiligingsbeleid
- Bestuurlijk commitment tonen op informatiebeveiliging conform de tien bestuurlijke principes van de VNG
- Afleggen van verantwoording af over informatiebeveiliging aan toezichthouders en de Raad

Het Bestuur geeft verder geen invulling en uitwerking van het informatiebeveiligingsbeleid en het treffen van passende technische en organisatorische beheersmaatregelen. Dit wordt gedelegeerd aan de directeur.

Directeur

De directeur stuurt de activiteiten inzake informatiebeveiliging aan. Deze heeft in ieder geval de volgende taken en verantwoordelijkheden:

- Het jaarlijks vaststellen van het Informatieplan.
- Het (laten) uitwerken en uitvoeren van verdiepend tactisch beleid dat aanvullend is op dit strategisch beleid
- Ervoor zorgen dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd een eigenaar hebben en verantwoordelijkheden goed zijn belegd en beschreven, óók bij ketenprocessen
- Erop toezien dat er adequate maatregelen getroffen zijn voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen
- Ervoor zorgen dat het personeel zich verantwoordt over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berusten
- Ervoor zorgen dat het Bestuur gevraagd en ongevraagd geïnformeerd wordt over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering
- Het leveren van input voor wijzigingen op maatregelen en procedures
- Het voldoen aan wet- en regelgeving die op de processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht zijn
- Het binnen de eigen organisatie uitdragen van het informatiebeveiliging-beleid, de daaraan gerelateerde procedures
- Het vroegtijdig (laten) signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld
- Het vroegtijdig betrekken van specialisten op het gebied van informatiebeveiliging en privacy bij nieuwe of gewijzigde processen
- Het (laten) uitvoeren van beveiligings- en risicoanalyses voor de processen en verwerkingen waar zij verantwoordelijk voor zijn. Op basis van deze analyses kunnen de juiste beveiligingsmaatregelen worden bepaald;
- Het bespreken van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.
- Het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.

- Het bewaken en stimuleren van het veiligheidsbewustzijn en digitale vaardigheden van eigen medewerkers.

Medewerkers

Alle medewerkers hebben een verantwoordelijkheid bij de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Van de medewerkers wordt het volgende verwacht:

- Kennis van de beveiligingsprocedures en voorschriften en daarnaar handelen
- Verantwoord omgaan met persoonsgegevens en andere informatie.
- Het melden van risicovolle en verdachte situaties en incidenten bij het Serviceplein en eigen leidinggevende.

Een bewustwordings- en trainingsprogramma draagt eraan bij dat medewerkers hier ook toe in staat zijn.

5.1.2 De tweede lijn: Advisering

De tweede lijn ondersteunt de organisatie bij het bewaken en verhogen van de beveiliging van de informatievoorziening. Zij doet dit door ondersteuning, advies en coördinatie. Ook bewaakt de tweede lijn of de directeur zijn verantwoordelijkheden op de juiste manier neemt. De tweede lijn kan op verschillende manieren ingevuld worden: door Information Security Officers (ISO's), experts die de directeur ondersteunen of andere medewerkers voor wie beveiliging een aandachtsgebied is. De BIO2 vereist in ieder geval de aanwijzing van een strategische security officer: de CISO. Deze rollen kunnen extern worden belegd.

CISO

De Concern Information Security Officer ondersteunt de organisatie vanuit een strategische en onafhankelijke positie.

- Definieert het strategisch informatiebeveiligingsbeleid voor de organisatie
- Zorgt voor organisatie brede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging.
- Monitort de relevante risico's en beheersmaatregelen voor de organisatie (bijvoorbeeld met een ISMS).
- Monitort en draagt bij aan de borging van de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen
- Informeert Bestuur en directeur over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen
- Zorgt voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, het veiligheidsdomein, huisvesting en bedrijfscontinuïteitsmanagement.
- Initieert en coördineert organisatie brede informatiebeveiligingsactiviteiten en -projecten
- Monitort en draagt bij aan de borging van informatiebeveiligingsbewustzijn binnen de organisatie

5.1.3 De derde lijn

De derde lijn controleert of het samenspel tussen eerste en tweede lijn soepel verloopt en uiteindelijk leidt tot inzicht in en beheersing van alle risico's op het gebied van informatiebeveiliging. De functies in de derde lijn dienen onafhankelijk gepositioneerd te worden t.a.v. eerste en tweedelijns functies in informatiebeveiliging. Gelet op de formele eindverantwoordelijkheid die bij de deelnemende gemeenten belegd blijft, is deze rol in eerste instantie toebedeeld aan de CISO's van deze gemeenten.

Controller informatieveiligheid

De controller informatieveiligheid heeft de volgende taken:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatiebeveiliging
- De controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsplan
- De controle op de juistheid en volledigheid van de risicoanalyses

5.2 Communicatiestructuren

Communicatie van het strategisch beleid aan het personeel

Dit strategische beleid moet gedeeld worden aan al relevant personeel d.m.v. een publicatie op een centraal vindbare plaats, zoals het intranet.

Overlegstructuur

De BVO JeugdFV neemt diensten af bij derden, en kent daardoor verschillende rollen binnen verschillende organisaties die betrokken zijn bij informatiebeveiliging. In het kader van signaleren, zelfleren en verbeteren is het noodzakelijk dat de betreffende functionarissen elkaar periodiek bijpraten over ontwikkelingen op het gebied van informatiebeveiliging.

Bestuurlijke contactmomenten

Overleg met Bestuur

Met het Bestuur vindt periodiek een overleg plaats. Zo blijft het Bestuur betrokken bij informatiebeveiliging en kan deze de bestuurlijke bijdrage leveren in lopende zaken. Met het Bestuur wordt besproken wanneer en op welke wijze de gemeenteraden betrokken worden volgens tenminste een in dienstverleningsafspraken vast te leggen jaarcyclus.

Ambtelijke contactmomenten

CISO-overleg

Volgens nader overeen te komen dienstverleningsafspraken organiseert BVO JeugdFV een periodiek overleg met CISO's van deelnemende gemeenten.

Crisisoverleg

In tijden van crises en bij grote incidenten is het noodzakelijk dat er op adequate wijze wordt gereageerd. Daarvoor is een goed georganiseerd crisisteam noodzakelijk. De samenstelling van het crisisteam, de rol- en taakverdeling binnen het team en de belangrijkste acties gedurende een crisis, staan beschreven in de incidentresponsplannen van de ICT-dienstverlener(s).

5.3 Bewustwording en training van personeel

Alle medewerkers en contractanten die gebruik maken van informatiesystemen bij BVO JeugdFV hebben de verantwoordelijkheid bedrijfsinformatie en persoonsgegevens te beschermen. Hiervoor dient BVO JeugdFV een passende bewustzijnsopleiding en regelmatige bijscholing van beleidsregels en procedures te faciliteren. Nieuwe medewerkers en contractanten dienen, tenzij strenger normenkader van toepassing, binnen drie maanden van indiensttreding een passende bewustzijn opleiding te hebben gevolgd.

De directeur draagt bij door bijvoorbeeld in werkoverleggen aandacht te schenken aan informatiebeveiliging en attendeert personeel bij instroom, doorstroom en uitstroom op informatiebeveiliging.

5.4 Disciplinaire procedure.

BVO JeugdFV hanteert een gedragscode integriteit als formeel en gecommuniceerd kader. De Integriteitscommissie zal waar nodig onafhankelijk onderzoek laten uitvoeren en BVO JeugdFV adviseren inzake de uitkomsten van het onderzoek en eventuele juridische consequenties daar waar haar medewerkers een laakbare inbreuk hebben gepleegd op de informatiebeveiliging.

Hoofdstuk 6: Planning van activiteiten informatiebeveiliging

6.1 Informatiebeveiligingsplan BVO JeugdFV

Het strategisch beleid wordt gebruikt om de basis te leggen voor het jaarlijks te schrijven 'Informatiebeveiligingsplan BVO JeugdFV' waarmee richting wordt gegeven aan de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Het informatiebeveiligingsplan wordt op hoofdlijnen opgesteld onder leiding van de CISO. De inhoud van het informatiebeveiligingsplan is gebaseerd op:

- Aandachtspunten uit de 'Omgevingsanalyse informatiebeveiliging BVO JeugdFV' op basis van dreigingsbeelden NCTV en IBD en interne beveiligingsincidenten
- Aandachtspunten uit de 'Omgevingsanalyse Informatiebeveiliging BVO JeugdFV' op basis van nieuwe landelijke wet- en regelgeving en gemeentelijke agenda's (VNG).
- De uitkomsten van de FG-meting
- Implementatieplanning BIO2.
- Uitkomsten van (financiële) audits en interne controles die zijn gericht op Informatiebeveiliging.
- De door directeur en personeel zelf ingebrachte onderwerpen op de informatievoorziening.
- Training van personeel en beheer van rollen rechten/bevoegdheden tijdens instroom/doorstroom/uitstroom.
- Het adresseren van risico's afkomstig van risico-analyses binnen de werkprocessen van de organisatie
- Bijdrage aan implementeren van generieke BIO2-maatregelen die worden doorgevoerd door partijen waar diensten worden afgenomen

Het informatiebeveiligingsplan loopt één jaar vooruit en geeft zodoende één jaar de tijd voor planning ROPS en eventuele budgetaanvragen via de bestuurlijke cyclus (perspectiefnota's)

6.2 Projectmanagement

Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. Projectvoorstellen met een digitale component dienen vooral te worden gedeeld met de door de BVO geselecteerde dienstverlener op het vlak van automatisering voor het meenemen van de juiste waarborgen conform BIO2 en organisatie breed weerbaarheid tegen cyberaanvallen.

Hoofdstuk 7: Risicomanagement

De directeur dient te zorgen voor een ongestoorde bedrijfsvoering, zodat de doelstellingen van het bedrijfsproces op een effectieve en efficiënte wijze worden gerealiseerd. Om die doelstellingen te realiseren is informatiebeveiliging een randvoorwaarde. Informatiebeveiliging wordt bereikt door een geschikte verzameling maatregelen in te zetten om met risico's op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van gegevens om te gaan, in die zin is het niet anders dan het omgaan met andere risico's voor de bedrijfsvoering waarvoor de directeur verantwoordelijk is. Het is de rol van de directeur om afwegingen te maken in hoeverre risico's binnen zijn organisatieonderdeel acceptabel zijn.

Voor de directeur spelen specifiek twee aandachtsgebieden in relatie tot informatiebeveiliging een rol, namelijk:

- De personeelsverantwoordelijkheid. De directeur is verantwoordelijk voor het handhaven van de personele beveiliging, kennis en vaardigheden met eventuele ondersteuning door de afdeling Personeel & Organisatie
- De procesverantwoordelijkheid. De directeur is verantwoordelijk voor het uitvoeren van activiteiten in processen die door de directeur zijn toegewezen en het daarbij treffen van organisatorisch, procesmatige, technische en fysieke maatregelen met eventuele ondersteuning van stafafdelingen.

Baseline-toets:

Om de risico's voor informatiebeveiliging in kaart te brengen bestaat het instrument baseline-toets.
Dit instrument helpt om het benodigde beveiligingsniveau te bepalen en of er gebruik gemaakt kan worden van bestaande beheersmaatregelen of dat er aanvullende maatregelen nodig zijn.
Voor ieder gedefinieerd proces (of informatiesysteem) dient een baseline-toets aanwezig te zijn.
De baseline toetsen worden volgens de PDCA-cyclus bijgesteld bij wijzigingen.

Organisatie brede risico-inventarisatie

Ook wordt op strategisch niveau naar risico's gekeken die niet afdelingsspecifiek zijn d.m.v. van de organisatie brede risico-inventarisatie. Deze wordt 2-jaarlijks geactualiseerd.

Samen met de Baseline-toetsen is er een compleet beeld van risico's en benodigde beheersmaatregelen conform BIO2.

Risico-register

Geïdentificeerde risico's zonder aanwezige maatregel dienen schriftelijke te worden geaccepteerd en opgenomen in het risico-register door de directeur.

Hoofdstuk 8: Incidentrespons en Bedrijfscontinuïteitsmanagement

8.1 Incidentrespons

Definitie beveiligingsincident

Een beveiligingsincident Is een ongewenste of onverwachte gebeurtenis, of serie van gebeurtenissen, die de beschikbaarheid, juistheid of vertrouwelijkheid van de informatievoorziening rondom bedrijfsprocessen verstoort en schade kan veroorzaken.
Een beveiligingsincident waarbij persoonsgegevens geraakt worden heet een datalek.

Meldplicht beveiligingsincident:

Om eventuele schade van een beveiligingsincident te beperken en herstel van het bedrijfsproces te bespoedigen moeten deze zo spoedig mogelijk gemeld worden bij het aanspreekpunt van de ICT-dienstverlener (bijvoorbeeld Serviceplein gemeente Ede).
Dit geldt ook voor gebruikers van samenwerkende partijen die gebruik maken van de ICT van BVO JeugdFV.

Beveiligingsincidenten die grootschalige (kunnen) hebben effecten hebben op de bedrijfscontinuïteit van BVO JeugdFV of die van andere organisaties binnen Nederland dienen door de ICT-dienstverlener gemeld te worden aan de Informatie beveiligingsdienst gemeenten (IBD).

Incidentregistratie

BVO JeugdFV dient zorg te dragen voor een centraal registratiesysteem voor het beheer van beveiligingsincidenten en de rapportage over beveiligingsincidenten. De bewaartermijn van incidentregistraties dient minimaal 3 jaar te zijn.
Informatie uit incidenten wordt gebruikt ter lering en verbetering van de weerbaarheid op informatiebeveiliging.

Oefenen

Om adequaat te kunnen reageren op beveiligingsincidenten dient de crisisorganisatie voorbereid te zijn op een dergelijk voorval. Minimaal 2-jaarlijks wordt in overleg jmet de ICT-dienstverlener een crisisoefening met een cyberaanval scenario doorlopen.

8.2 Bedrijfscontinuïteitmanagement

De directeur brengt bedrijfskritische processen in kaart d.m.v. van een Business Impact Analyse (BIA of BBN-toets).
De continuïteitsplannen voor bedrijfskritische processen worden jaarlijks getest op geldigheid en bruikbaarheid.

Hoofdstuk 9: Naleving op informatiebeveiliging

FG-meting

Jaarlijks wordt door de Functionaris Gegevensbescherming een FG-meting uitgevoerd. In het jaarlijkse rapport van de FG-meting doet de Functionaris Gegevensbescherming bevindingen en aanbevelingen over de bescherming van persoonsgegevens wat ook betrekking heeft op informatiebeveiliging. De aanbevelingen worden aangeboden aan het Bestuur van de BVO JeugdFV.

Jaarverslag Informatiebeveiliging

Jaarlijks wordt aan het Bestuur een verdiepend jaarverslag informatiebeveiliging aangeboden om een samenvatting te geven van de gebeurtenissen van afgelopen jaar.

Bijlage 1 afkortingenlijst

ICT	Informatie Communicatie Technologie
BIO2	Baseline Informatiebeveiling Overheid
ISMS	Information Security Management Systeem
GR	Gemeentelijke Regeling
BRP	Basisregistratie personen
PNIK	Paspoorten en Nederlandse IdentiteitsKaarten
SUWI	*wet Structuur Uitvoeringsorganisatie Werk en Inkomen*
GeVS	Gemeenschappelijke elektronische Voorziening *Suwi*
IBD	InformatieBeveiligingsDienst gemeenten, onderdeel van VNG
VNG	Vereniging voor Nederlandse Gemeenten
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
BZK	Ministerie van Binnenlandse Zaken
ENSIA	Eenduidige normatiek Single Information Audit
CISO	Concern Information Security Officer
ISO	Information security Officer
FG	Functionaris Gegevensbescherming
PIOFACH	Personeel, Informatievoorziening, Organisatie, Financiën, Algemene zaken, Communicatie en Huisvesting
BIA	Business Impact Analyse
BBN	Basis BeveiligingsNiveau