2023

Rollen en verantwoordelijkheden informatiebeveiliging

Veiligheidsregio Flevoland
Veiligheidsregio Gooi en Vechtstreek

Versiebeheer

Versienr.	Datum	Auteur(s)	Status	Opmerking
0.1	03-03-2022	Jasper Zweers	Concept	Concept op basis van template
0.2	03-03-2022	Arold Sonke	Concept	Nadere invulling specifiek voor de VR's
0.3	07-03-2022	Yara van der Laan	Concept	Review en tekstuele aanpassingen
0.4	15-04-2022	Jasper Zweers	Concept	Aanpassingen n.a.v. afstemming RACI
0.5	03-05-2022	Yara van der Laan	Concept	Concept voor bredere afstemming binnen de veiligheidsregio's. Deze versie bevat: -aanpassingen na afstemmingen over de RACI matrix. -aanpassingen naar veiligheidsregio's.
0.6	17-05-2022	Yara van der Laan	Concept	Aanpassingen na feedback FG en bespreking in IB-projectgroepoverleg 17-05.
0.7	09-08-2022	Arold Sonke	Concept	Feedback O&HR verwerkt. Aanpassing organigram.
1.0	01-11-2022	Arold Sonke	Concept	Versie voorgelegd aan het GMT ter meningsvorming.
1.1	01-11-2022	Arold Sonke	Concept	Commentaar GMT ism het projectoverleg verwerkt.
1.2	28-11-2022	Jasper Zweers	Concept	Versie na aanbieding document als 'voorgenomen besluit' aan de Veiligheidsdirectie.
1.3	25-05-2023	Arold Sonke	Concept	Versie om aan te bieden aan het Algemeen Bestuur.

Autorisatie

Door	Datum	
GMT	25 oktober 2022	Meningsvormend
Veiligheidsdirectie	16 november 2022	Meningsvormend
OR		Advisering / Instemming
Algemeen Bestuur		Besluitvormend

Classificatie en herzieningsdatum

Dit document is alleen voor intern gebruik binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

Het document heeft een geldigheidsduur van 2 jaar vanaf het moment van definitief vaststellen.

Inhoudsopgave

1 Inleiding

De voorzitter van de Veiligheidsdirectie van de Veiligheidsregio Flevoland en de Veiligheidsregio Gooi en Vechtstreek, vindt het van groot belang dat de informatiebeveiliging op orde is waarbij wordt voldaan aan de Baseline Informatiebeveiliging Overheid (BIO). In het kader hiervan hebben de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland een Information Security Management System (ISMS) ingericht. Dit document met de beschrijving van rollen en verantwoordelijkheden t.a.v. informatiebeveiliging is hiervan een onderdeel.

1.1 Achtergrond

Dit document beschrijft de organisatie van de informatiebeveiliging van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Informatievoorziening is van essentieel belang voor de continuïteit van de primaire bedrijfsvoering van de VR's. Onze organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Om de organisatie van informatiebeveiliging goed in te regelen is het definiëren en vastleggen van de rollen en verantwoordelijkheden op dit gebied essentieel. Een en ander is vastgelegd in het onderhavige document.

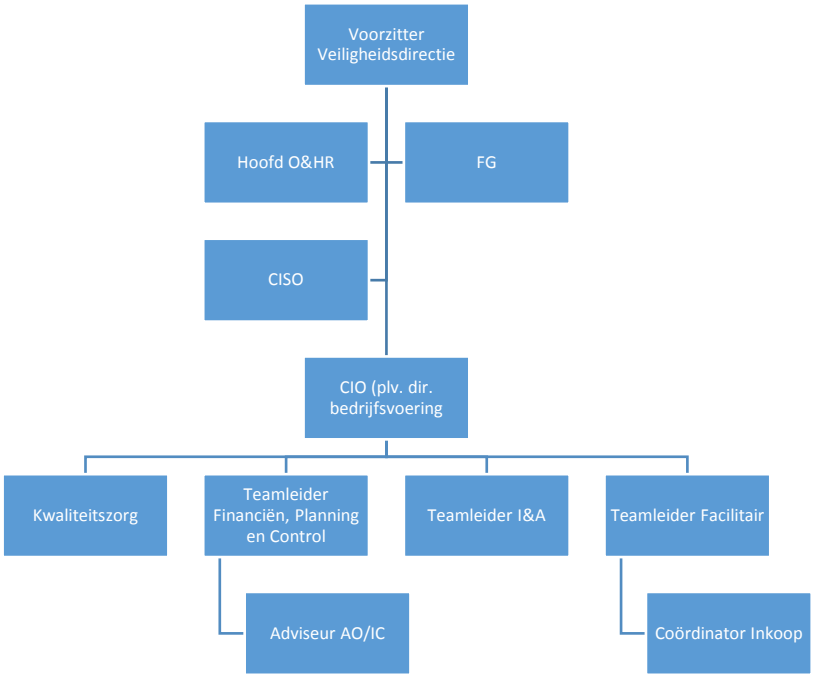
1.2 Samenhang tussen informatiebeveiliging en bescherming van persoonsgegevens

De AVG (Algemene Verordening Gegevensbescherming) richt zich op de zorgvuldige omgang met persoonsgegevens. Dit zijn bijvoorbeeld gegevens van medewerkers of burgers. Informatiebeveiliging richt zich op de beveiliging van vertrouwelijke gegevens, waaronder persoonsgegevens. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren dus een bijdrage aan de bescherming van persoonsgegevens.

2 Organisatie van informatiebeveiliging

In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging zijn belegd.

De competenties voor rollen in informatiebeveiliging die voor de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland zijn opgesteld, zijn gebaseerd op de vaststelling hiervan door het Platform voor InformatieBeveiliging (PvIB). Zie voor de uitwerking van vereiste vaardigheden bijlage II.



Figuur 1: Organisatie informatiebeveiliging

In bovenstaand figuur zijn de afdelingen en functies binnen de veiligheidsregio's benoemd die binnen de inbedding van informatiebeveiliging specifieke rollen en verantwoordelijkheden hebben. Het is dus geen volledig organogram, maar richt zich op de afdelingen en functionarissen met een kernfunctie binnen informatiebeveiliging.

In de volgende paragrafen worden de verantwoordelijkheden van de verschillende genoemde functionarissen die rollen vervullen relevant voor informatiebeveiliging nader omschreven. De RACI-matrix met vastlegging over specifieke rollen en verantwoordelijkheden is in de bijlage terug te vinden.

2.1 Voorzitter van de Veiligheidsdirectie

De voorzitter van de Veiligheidsdirectie is eindverantwoordelijk voor de bekrachtiging van het informatiebeveiligingsbeleid en de daarin opgenomen richtlijnen. Het Veiligheidsberaad heeft vastgesteld dat veiligheidsregio’s zich moet conformeren aan de BIO en de GHOR aan NEN 7510.

De eindverantwoordelijkheid van de voorzitter van de Veiligheidsdirectie voor informatiebeveiliging omvat:

- Het goedkeuren van het informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen.
- Het goedkeuren van besluiten over eventuele uitzonderingen op het informatiebeveiligingsbeleid of standaarden.
- Het goedkeuren van de gedragscode voor het gebruik van de digitale werkomgeving van de veiligheidsregio’s.
- Vaststellen van de benodigde middelen voor implementatie van informatiebeveiligingsmaatregelen of accepteren restrisico’s.
- Het uitvoeren van de managementbeoordeling van het informatiebeveiligingsproces.

- Het afstemmen van beleid en afleggen van verantwoording over het gevoerde beleid aan de het veiligheidsberaad en IFV.

2.2 Plaatsvervangend Directeur Bedrijfsvoering/Chief Information Officer

Binnen de veiligheidsregio's zijn de Chief Information Officer (CIO) taken ondergebracht bij de Plaatsvervangend Directeur Bedrijfsvoering. De Plaatsvervangend Directeur Bedrijfsvoering/CIO is verantwoordelijk voor de coördinatie van alle activiteiten die betrekking hebben op informatievoorziening en digitale werkomgeving en daarmee valt informatiebeveiliging ook in de CIO-portefeuille.

De verantwoordelijkheid van de CIO voor informatiebeveiliging omvat:

- Het vaststellen van de rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging.
- Het goedkeuren van de informatiebeveiligingsdoelstellingen van de veiligheidsregio's.
- Het vaststellen van het autorisatiebeleid.
- De CIO bewaakt, samen met de Chief Information Security Officer (CISO), de samenhang tussen het informatiebeveiligingsbeleid en de informatievoorziening van de veiligheidsregio's.
- De CIO adviseert samen met de CISO aan de voorzitter van de Veiligheidsdirectie over het informatiebeveiligingsbeleid, de strategie en de kaders voor de informatievoorziening van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.
- De CIO toetst met de CISO voorstellen voor de verbetering van informatiebeveiliging, zoals de security-architectuur. Deze voorstellen worden vervolgens ingebracht in de besluitvorming van de voorzitter van de Veiligheidsdirectie.
- Verantwoordelijk voor het afsluiten van verwerkersovereenkomsten met verwerkers van persoonsgegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.
- Legt verantwoording af aan de voorzitter van de Veiligheidsdirectie over informatiebeveiliging en de implementatie van de BIO.

2.3 Chief Information Security Officer

De Chief Information Security Officer (CISO) signaleert risico's, adviseert over en ziet toe op de te treffen en getroffen informatiebeveiligingsmaatregelen. De Chief Information Security Officer (CISO) is verantwoordelijk voor de ontwikkeling en implementatie van het informatiebeveiligingsbeleid en verleent ondersteuning bij het vaststellen van de benodigde maatregelen. De CISO houdt toezicht op naleving van de Baseline Informatiebeveiliging Overheid (ISO 27001 en 27002).

De verantwoordelijkheden van de CISO omvatten onder meer:

- Adviserend aan de CIO en de voorzitter van de Veiligheidsdirectie ten aanzien van informatiebeveiliging en de treffen beheersmaatregelen.
- Vervult de rol als contactpersoon en vraagbaak voor het management op het gebied van informatiebeveiligingsrisico's, risicoanalyses en implementatie van maatregelen.

- Vaststellen en actualiseren van beleid, procedures en richtlijnen voor informatiebeveiliging in samenspraak met lijnmanagers van de veiligheidsregio's (in ieder geval teamleiders I&A, O&HR, Facilitair, Financiën en P&C, AO/IC en Kwaliteitszorg).
- Het vaststellen van de informatiebeveiligingsdoelstellingen van de veiligheidsregio's en uitvoering van de monitoring daarop.
- Het verzamelen en registreren van informatie over de aanwezige beveiligingsmaatregelen.
- Het ontwikkelen van dashboards en het opstellen van managementrapportages over informatiebeveiliging.
- Bewaken van wet- en regelgeving op het gebied van informatiebeveiliging en relevante wijzigingen daarin.
- Adviseren bij het opstellen van verwerkersovereenkomsten met verwerkers van persoonsgegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.
- Het uitvoeren of initiëren van risicoanalyses en interne audits gericht op informatiebeveiliging.
- Het opzetten of initiëren van een registratie voor informatiebeveiligingsincidenten, evenals het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.
- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging ter bevordering van het bewustzijn van risico's gerelateerd aan informatiebeveiliging.
- Het toezien op de naleving van het informatiebeveiligingsbeleid door de organisatieonderdelen. Daarvoor stelt de CISO een auditplan op (voor de verplichte interne audit) en levert ondersteuning bij het uitvoeren van de daarin gedefinieerde taken.
- Rapporteert aan de voorzitter van de Veiligheidsdirectie over de integrale status van informatiebeveiliging op basis van monitoring, audits en evaluatie.
- Overleggen met de OR over medezeggenschap.

2.4 Functionaris gegevensbescherming

De Functionaris voor de gegevensbescherming (FG) informeert en adviseert de organisatie en de werknemers over de Algemene Verordening Gegevensbescherming (AVG) en ziet toe op de naleving van de AVG. De FG helpt en geeft advies bij Data Protection Impact Assessments en treedt op als aanspreekpunt voor de Autoriteit Persoonsgegevens o.a. voor melding van datalekken. Daarnaast adviseert de FG ook bij het opstellen van verwerkersovereenkomsten.

Om deze taken goed te kunnen uitvoeren is in de AVG vastgelegd dat de FG toegang moet krijgen tot alle informatie die hij/zij hiervoor nodig heeft. De Functionaris voor de gegevensbescherming (FG) is verantwoordelijk voor het toezicht op de naleving van de Algemene verordening gegevensbescherming (AVG) binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Deze functionaris doet hiertoe aanbevelingen voor bescherming van verwerkingen van persoonsgegevens. De FG houdt bij de uitvoering van zijn/haar taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de context en de verwerkingsdoeleinden.

De CIO, de CISO en de FG stemmen regelmatig af om een goede taakverdeling met betrekking tot informatiebeveiliging en bescherming van verwerking van persoonsgegevens binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland te borgen.

De FG rapporteert aan de voorzitter van de Veiligheidsdirectie over ontvangen en verwerkte meldingen vanuit de veiligheidsregio's en stemt waar nodig af met de CISO en CIO.

2.5 Projectgroep Kwaliteitszorg

Er zijn relaties tussen de projectgroep Kwaliteitszorg en informatiebeveiliging. Beide onderwerpen richten zich namelijk op bepaalde aspecten van de bedrijfsvoering. Kwaliteitszorg richt zich op een continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren. Informatiebeveiliging richt zich op de beschikbaarheid, integriteit en de vertrouwelijkheid van de informatievoorziening. Hiermee kan informatiebeveiliging een bijdrage leveren aan de kwaliteit van de bedrijfsvoering.

De veiligheidsregio's bepalen na afloop van de projectgroep hoe de taken en verantwoordelijkheden m.b.t. Kwaliteitszorg in de bestaande organisatie geborgd zijn.

2.6 Teamleiders/hoofd afdeling

Het lijnmanagement is verantwoordelijk voor de uitvoering van informatiebeveiliging in de eigen lijn.

De Teamleiders/ leidinggevenden binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Hebben de volgende taken met betrekking tot informatiebeveiliging:

- Zorgen in het eigen organisatiedeel (afdeling, team) voor invoeren en naleven van het beleid voor informatiebeveiliging.
- De implementatie en het uitdragen van de maatregelen die voortvloeien uit de informatiebeveiligingseisen en verbeteracties.
- Informatiebeveiliging behandelen in werkoverleg, beoordelingen etc.
- Signaleert en meldt beveiligingsproblemen of –incidenten bij de CISO namens het eigen bedrijfsonderdeel.

Een aantal teamleiders heeft een specifieke rol ten aanzien van informatiebeveiliging, deze noemen we hieronder apart.

2.6.1 Teamleider I&A

De Teamleider I&A is verantwoordelijk voor het beschrijven en bewaken van de samenhang tussen applicaties en informatiestromen van het applicatielandschap. Dit heeft op vele onderdelen raakvlakken met informatiebeveiliging. Dit leidt tot de volgende verantwoordelijkheden in het kader van informatiebeveiliging:

- Vertaling van het informatiebeleid naar concrete beheersmaatregelen in de ICT beheerprocessen en de implementatie van die beheersmaatregelen.
- Het verantwoord doorvoeren van wijzigingen in de ICT omgeving.

2.6.2 Teamleider Facilitair

In het kader van informatiebeveiliging is de teamleider Facilitair verantwoordelijk voor de uitvoering van fysieke beveiligingsmaatregelen. Inkoop is ondergebracht bij de teamleider Facilitair, waarbij de coördinator inkoop van belang is voor informatiebeveiliging.

2.6.2.1 Coördinator Inkoop

In het kader van informatiebeveiliging is de teamleider Inkoop verantwoordelijk voor:

- De coördinator Inkoop is verantwoordelijk voor de uitvoering van leveranciersmanagement en draagt zorg voor de periodieke beoordeling van leveranciers.
- De Teamleider Inkoop is verantwoordelijk voor het adviseren, organiseren, uitvoeren van het tactisch beleid met betrekking tot de dienstverleningsafspraken tussen de (ICT-)organisatie en haar leveranciers. Daar waar relevant wordt in de dienstverleningsafspraken ook aandacht besteed aan informatiebeveiliging. De Teamleider I&A, Teamleider Facilitair, de CISO en Functionaris Gegevensbescherming stemmen hun activiteiten periodiek af.
- Inkoop houdt rekening bij aanbestedingen en selectie van leveranciers met relevante wet- en regelgeving en het voldoen van leveranciers aan het informatiebeveiligingsbeleid van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.
- Inkoop coördineert het afsluiten van verwerkersovereenkomsten met verwerkers van persoonsgegevens van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. En bewaakt de geldigheid van de overeenkomst en achterliggende beheersmaatregelen, waaronder certificering van de leveranciers.

2.6.3 Teamleider Financiën en Teamleider Planning en Control

De afdeling Financiën en Planning en control is in een geraadpleegde of geïnformeerde rol betrokken bij informatiebeveiliging. Raakvlakken zijn voornamelijk van toepassing bij kritieke datastromen en informatiesystemen en beheersing van risico's die raakvlakken hebben met informatiebeveiliging. Bovendien heeft de adviseur die onder de Financiën en Planning en Control valt, ook werkzaamheden die raakvlak heeft met informatiebeveiliging.

2.6.3.1 Adviseur Administratieve Organisatie/Interne Controle (AO/IC)

De adviseur AO/IC houdt zich bezig met verantwoording en controle op bedrijfsprocessen. Informatiebeveiliging kan van toepassing zijn op meerdere bedrijfsprocessen en daarom is deze functionaris in een geraadpleegde of geïnformeerde rol betrokken.

2.6.4 Hoofd O&HR

Het hoofd O&HR is verantwoordelijk voor het beheer van het personeelsbeleid van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Er is een relatie tussen personeelsbeleid en informatiebeveiliging, onder andere daar waar het beheer van personeelsgegevens betreft. Dit dient op een zorgvuldige manier te geschieden met de waarborging van een goede informatiebeveiliging. Hiertoe bewaakt het hoofd O&HR, samen met de CISO, de samenhang tussen personeelsbeleid en informatiebeveiliging.

In het kader van informatiebeveiliging is het hoofd O&HR verantwoordelijk voor:

- Het aanstellingsbeleid nieuwe medewerkers en uitvoering daarvan.
- Het in, door en uitstroomproces.
- Verantwoordelijk voor de gedragscodes voor het gebruik van de digitale werkomgeving, sociale media en analoge informatie.
- Verantwoordelijk voor het sanctiebeleid en het toezien op de consistente naleving.
- Het verzamelen, bewerken, documenteren en archiveren van personeelsinformatie met inachtneming van wettelijke vereisten en beheersmaatregelen voor informatiebeveiliging.

3 Informatiebeveiligingsoverleg

3.1 Regiegroep informatiebeveiliging

De regiegroep komt op periodieke basis bij elkaar te komen om informatiebeveiliging te monitoren, te adviseren en te rapporteren over de stand van zaken met betrekking tot informatiebeveiliging. Vaste deelnemers in de regiegroep zijn de Plaatsvervangend Directeur Bedrijfsvoering/CIO, de CISO, de Teamleider I&A en de FG. Daarnaast kunnen verantwoordelijke leidinggevenden (Teamleiders Financiën, Planning & Control, Facilitair, Communicatie, O&HR en Hoofd Veiligheidsbureau, crisis- en risicobeheersing en directeur Brandweerzorg) worden uitgenodigd (of zijn/haar plaatsvervanger).

Op het moment dat er onderwerpen zijn die impact hebben op het uitvoeren van de taken t.b.v. de repressie kan ook een liason vanuit de repressie (OL) betrokken worden.

Tijdens het overleg worden besproken:

- Lopende en te organiseren Informatiebeveiliging activiteiten.
- Issues in informatiebeveiligingsactiviteiten.
- Informatiebeveiliging verbetermaatregelen.
- Projectvoorstellen/major changes met een impact op informatiebeveiliging.
- Lessons learned uit IB-incidenten en datalekken.
- Nalevering en evaluatie van beleid.
- Risicobeheer.
- Rapportage uit de monitor, controles, audits.
- Nalevering en evaluatie van het IB beleid.

De tijdens het overleg behandelde presentatie is na verwerking van hetgeen besproken is de ‘IB en Privacy rapportage’ voor de voorzitter van de Veiligheidsdirectie. Van het overleg wordt tevens een actie- en besluitenlijst bijgehouden.

3.2 Operationeel overleg informatiebeveiliging

Dit overleg wordt eens per vier weken georganiseerd. Vaste deelnemers zijn de CISO, I&A Servicedesk vertegenwoordiging, Teamleider I&A, Interregionaal Crisis Centrum/meldkamer-vertegenwoordiging, Teamleider Communicatie en de Plaatsvervangend Directeur Bedrijfsvoering/CIO. Vertegenwoordiging vanuit de IT-leverancier(s) is niet standaard aanwezig, maar

wordt uitgenodigd als er agenda-items zijn die ook van toepassing zijn op de leverancier. Vastlegging van het overleg vindt plaats in de vorm van een actie-, issue- en besluitenlijst. Terugkoppeling van dit overleg vindt via de Plaatsvervangend Directeur Bedrijfsvoering/CIO plaats naar de voorzitter van de Veiligheidsdirectie.

Tijdens het overleg worden besproken:

- Lopende en te organiseren IB-activiteiten.
- IB-incidenten en de opvolging hiervan.
- Changes met een IB-impact.
- Projectvoorstellen met een IB-impact.
- Voortgang en bevindingen uit de monitor, controles, audits.
- Voortgang van verbetermaatregelen.

Vastlegging van het overleg vindt plaats in de vorm van een actie-, issue- en besluitenlijst.

Bijlage I: RACI-matrix

Organisatie / Verantwoordelijkheden	Voorzitter Veiligheids directie	Plv. Directeur Bedrijfs-voering (CIO)	Team-leider I&A	FG	CISO	Hoofd O&HR	Team-leider Facilitair	Teamleider Financiën, P&C	Coördinator Inkoop	Functionaris AO/IC
Informatiebeveiligingsbeleid (IB Beleid)	A	C	C	C	R	C	C	C	C	I
Gedragscodes voor het gebruik van de digitale werkomgeving, sociale media en beveiliging van analoge informatie.	A	C	C	C	C	R	I	I	I	
Rollen en verantwoordelijkheden t.a.v. Informatiebeveiliging	A	R	C	C	C	C	C	I	I	
Contextanalyse	A	C	C	C	R	C	C	C	C	
Inventarisatie en naleven wet- en regelgeving en contractuele afspraken	A	R		C	C				C	
IB doelstellingen en monitoring	A	C	I		R	I	I	I	I	
ISMS beschrijving	A	C	I	C	R	I	I	I	I	C
Interne audit	A	C	I	C	R	I	I	I	I	
Ingericht risicomanagement	A	C		C	R					C
Directiebeoordeling	A	R		C	C					
Verbeterplan	A	C	C	C	R	C	C	C	C	
IT beheerprocessen	A	I	R	I	C					
Autorisatiebeleid	A	R	C	I	C					
Leveranciersmanagement	A	C		I	I				R	
ICT beheersmaatregelen	A	I	R	I	C					
Projectbeheer	A	R	C	I	I	I	I	I	I	
Bewustwordingsprogramma	A	C	C	C	R	C	I	I	I	
Fysieke beveiliging	A	C		C	C		R			

Organisatie / Verantwoordelijkheden	Voorzitter Veiligheids directie	Plv. Directeur Bedrijfs-voering (CIO)	Team-leider I&A	FG	CISO	Hoofd O&HR	Team-leider Facilitair	Teamleider Financiën, P&C	Coördinator Inkoop	Functionaris AO/IC
Overleg met OR over medezeggenschap	A	I	I	C	R	C				

- **R (*Responsible, NL: Verantwoordelijk*)**
  Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de functionaris die *accountable* is.
- **A (*Accountable, NL: Eindverantwoordelijk*)**
  Degene die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Als het erom gaat, moet hij/zij het eindoordeel kunnen vellen, vetorecht hebben. Er is slechts één functionaris Accountable.
- **C (*Consulted, NL: Geraadpleegd*)**
  Deze functionaris geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd. Dit is tweerichtingscommunicatie.
- **I (*Informed, NL: Geïnformeerd*)**
  Iemand die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten enz. Dit is eenrichtingscommunicatie.

Bijlage II: Competenties voor rollen in de informatiebeveiliging

In deze bijlage zijn de competenties uitgewerkt voor de rollen in de informatiebeveiliging, als nadere uitwerking van het ISMS van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

De Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland volgen de competenties in termen van opleidingsniveau, vereiste kennisgebieden en vaardigheden voor de belangrijkste/specifieke functies in de informatiebeveiliging, die zijn uitgewerkt in:

> 'Beroepsprofielen voor Informatiebeveiliging 2.0a, jan 2017, een basis voor uniforme kwalificatie van informatiebeveiligers' van de PvIB met name voor de CISO en de ISO
>
> (Beroepsprofielen Informatiebeveiliging 2.0 – PvIB)

De competenties van de FG worden gevolgd zoals beschreven in het visiedocument van de Autoriteit Persoonsgegevens met de titel "Positionering van de FG" van juni 2021.

De FG dient bovendien namens de verantwoordelijke organisatie ingeschreven te zijn in het FG-register bij de AP.
Het is verder aan te bevelen dat een FG lid is van beroepsverenigingen, zoals de NGFG (Nederland) en/of de IAPP (Internationaal).

Voor alle andere functies in het huis geldt dat het bewustwordingsprogramma een belangrijke bijdrage levert om de medewerkers voldoende competent te laten zijn en om te gaan met IB vraagstukken in hun praktijk. Voorbeelden hiervan zijn:

- Tijdens inwerktrajecten, waarbij o.a. de nadruk op omgaan met (vertrouwelijke) gegevens wordt gelegd.
- Van aanvraag, onderzoek, initiatie, uitvoer en evaluatie in projecten.
- Op intranet.
- Bij het inloggen op systemen, d.m.v. boodschappen of screensavers.
- Door middel van posters of kaarten door de gehele locaties van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

Bij het doorlopen van de jaarlijkse gesprekkencyclus in combinatie met het managen van de informatiebeveiligingsrisico's wordt vastgesteld in hoeverre medewerkers aanvullende kennis nodig hebben / medewerkers met aanvullende kennis (tijdelijk) nodig zijn in samenwerking met P&O, unit opleidingen.

Belangrijke generieke competenties in aanvulling op het bovenstaande om verantwoordelijkheid te dragen voor informatiebeveiliging binnen de organisatie zijn:

Kennis

- Een relevante vakgerichte (ten minste HBO-werk/denk niveau) eventueel aangevuld met een verdiepende opleiding op het gebied van informatiebeveiliging en privacy.
- Meerjarige relevante werkervaring is vereist aangaande informatiebeveiliging en risicoanalyse methoden.
- Kennis van actuele relevante wet- en regelgeving is vereist, zoals de Algemene Verordening Gegevensbescherming.
- Houdt ontwikkelingen in het vakgebied bij en past dit toe in het te ontwikkelen beleid.
- Kennis en ervaring in het projectmatig werken en projectmanagement.
- Kennis en ervaring op het gebied van advisering.
- Kennis en ervaring op het gebied van quality assurance.
- Kennis van relevante *best practices*.

Zelfstandigheid

- De werkzaamheden worden zelfstandig verricht binnen de opgestelde beleidskaders en werkafspraken.
- Draagt zorg voor zelfstandige prioritering en voortgangsbewaking, e.e.a. binnen de door wetgeving en organisatie bepaalde prioritering.
- Neemt initiatief bij het geven van adviezen en komt met oplossingen.
- Lost problemen in eerste instantie zelfstandig op, kan zo nodig terugvallen op leidinggevende
- Neemt initiatief bij optimaliseren van processen, bijvoorbeeld rondom testen, changemanagement.

Sociale vaardigheden

- Tact, stimuleren, overtuigingskracht en het overwinnen van weerstanden zijn nodig bij het implementeren van informatiebeveiligingsbeleid en bij de controle op naleving van richtlijnen, procedures en standaarden.
- Om kunnen gaan met verschillende disciplines en managementniveaus waarbij belangen tegengesteld kunnen zijn.
- Het kunnen hanteren van verschillende stijlen van advisering en het bepalen en bewaren van de eigen houding.
- Rolvastheid in combinatie met tact en inlevingsvermogen.

Uitdrukkingsvaardigheid

- Mondelinge en schriftelijke uitdrukkingsvaardigheid bij het adviseren op verschillende niveaus in de organisatie, het geven van voorlichting en het schrijven van beleid en rapportages.

Oplettendheid

- Signaleren van ontwikkelingen, leemtes en behoeften binnen het vakgebied.
- Het uitvoeren van audits, risico- en kwetsbaarheidsanalyses en andere controles (bijv. naleving procedures, quality assurance).
- Het toezien op naleving van richtlijnen, procedures en standaarden.

Overige functie-eisen

- Geduld en doorzettingsvermogen bij het ontwikkelen van beleid, leiden van projecten, het vergroten van het beveiligingsbewustzijn in de organisatie.
- Systematisch werken bij het in kaart brengen van informatieprocessen en bij het ontwikkelen van beleid.

- Integer handelen over vertrouwelijke informatie over informatieveiligheid van de organisatie.
- Representatief gedrag bij het onderhouden van de diverse in- en externe contacten.