Veiligheidsregio Haaglanden

Strategisch informatiebeveiligingsbeleid

Veiligheidsregio Haaglanden

2021 t/m 2025

VERSIEBEHEER

Versie	Datum	Auteur
1.0	25-05-2021	CvK
1.1	30-06-2021	CvK
2.0	30-01-2024	CvK

Inhoud

1 Inleiding

De wereld digitaliseert snel. Als organisatie halen we hier ons voordeel uit. Zo kunnen we vanaf verschillende locaties bij data en informatie die voor ons werk van belang is. Ook kunnen we op een efficiënte wijze communiceren met collega's, inwoners en ketenpartners. De verwachting die de samenleving heeft, is hierdoor ook veranderd. Er wordt verwacht dat we onze dienstverlening, zowel digitaal als niet-digitaal, op orde hebben. En hier hoort bij dat de processen die hiervoor van belang zijn te allen tijde beschikbaar en betrouwbaar zijn, en dat er daarnaast veilig omgegaan wordt met de (persoons)gegevens die hierbij betrokken zijn. Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's, welke direct en indirect maatschappelijke, economische- en imagoschade tot gevolg kunnen hebben. Denk hierbij aan de kosten voor het herstellen van systemen, schade aan de dienstverlening door onjuiste, onbetrouwbare of het niet beschikbaar zijn van informatie als gevolg van een hack, maar ook aan het negatief in beeld komen bij media.

Binnen de VRH wordt het efficiënt en effectief verwerken en het kunnen werken met bedrijfsinformatie nagestreefd. Daarnaast wil het een betrouwbare partner zijn. Het is daarom belangrijk dat de VRH de informatiebeveiliging op orde heeft, en daarmee de dreigingen op dit gebied afweert. Enerzijds heeft dit te maken met het verkleinen van de kans op een incident, anderzijds betreft dit het weerbaar en veerkrachtig kunnen optreden wanneer er een incident plaatsvindt. Er wordt hierbij onderscheid gemaakt tussen dreigingen van interne en externe aard. Een dreiging van interne aard houdt in dat het eigen personeel schade kan aanrichten, bijvoorbeeld door het bedoeld of onbedoeld delen van informatie met externen. Bij een externe dreiging probeert een buitenstaander de systemen binnen te dringen, om zo informatie te stelen of een organisatie plat te leggen.

Dit document beschrijft het strategische informatiebeveiligingsbeleid van de VRH, voor de jaren 2021 tot en met 2025 en vervangt het eerdere informatiebeveiligingsbeleid uit 2017. Het beleid geeft algemene beleidsuitgangspunten over informatiebeveiliging die ertoe moeten bijdragen dat binnen VRH verantwoord wordt omgegaan met informatie en met de uitwisseling hiervan. Dit om bekende en onbekende dreigingen af te weren.

De Baseline Informatiebeveiliging Overheid (BIO[1]) is een normenkader voor informatieveiligheid en beschrijft de minimale eisen waaraan een overheidsorganisatie moet voldoen. Het hebben van een vastgesteld beveiligingsbeleid is een van de verplichte beheersmaatregelen van het BIO-normenkader. Er is echter geen standaard antwoord op beveiligingsvraagstukken vanuit de BIO. Variatie en maatwerk is de standaard: voor ieder individueel vraagstuk wordt bekeken wat de wijze van beveiliging

[1] Er wordt VRH-breed ingezet op het voldoen aan de wettelijke eis te werken conform de Baseline Informatiebeveiliging Overheid. Voor processen binnen de geneeskundige tak geldt dat de NEN-normen voor de zorg, waaronder de NEN-7510, leidend zijn. Dit geldt voor processen waarbij zorggegevens worden verwerkt, zoals het uitwisselen van informatie tussen verschillende personen of partijen.

is die passend is bij het risico. Dit zorgt voor een beveiliging van gegevens die past bij de werkzaamheden van de Meldkamer(s), GHOR en Brandweer en de ondersteunende processen (bijv. de werkplaatsen, vakbekwaamheid enz.).

2 Informatiebeveiliging binnen de VRH

Informatiebeveiliging is de verzamelnaam van het geheel aan processen dat ingericht wordt om de betrouwbaarheid van de informatievoorziening van VRH, de gebruikte informatiesystemen en de daarin opgeslagen gegevens, te waarborgen.

Het is het proces van vaststellen van de vereiste en passende beveiliging in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van een samenhangend pakket van maatregelen.

- **Vertrouwelijkheid**

  Het beschermen van informatie tegen ongeautoriseerde toegang of mutatie (manipulatie).

- **Integriteit** (juistheid en volledigheid)

  Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en de informatieverwerking.

- **Beschikbaarheid** (continuïteit)

  Het zorgdragen voor de beschikbaarheid van informatie en de informatiesystemen en –middelen op de juiste tijd en plaats voor de gebruikers.

Scope

De scope van dit beleid omvat alle processen, informatiesystemen, informatie en gegevens van de veiligheidsregio, en de uitwisseling van gegevens intern en met externe partijen, in de breedste zin van het woord. Het omvat zowel digitale als analoge informatie. Informatieveiligheid wordt daarmee gedurende de hele levenscyclus van informatiesystemen toegepast, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet enkel tot ICT-vraagstukken, maar heeft betrekking op het bestuur en alle medewerkers, burgers, gasten, bezoekers en relaties. Het beslaat niet enkel informatie die digitaal wordt verwerkt, maar heeft ook betrekking op papieren en niet geschreven informatie(bronnen).

De scope is tijd-, locatie- en apparaat onafhankelijk.

Het beleid beschrijft informatieveiligheid op een strategisch niveau: het wordt gebruikt om doelen en uitgangspunten te borgen en daarmee richting te geven aan de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Specifieke maatregelen die worden genomen of keuzes die worden gemaakt op operationeel niveau worden in dit stuk niet behandeld.

Visie en ambitie

De samenleving verandert steeds meer in een informatiemaatschappij. Er spelen allerlei maatschappelijke en technologische ontwikkelingen die van invloed zijn op de informatiehuishouding.
Dit is van invloed op de manier waarop de VRH werkt. Wijziging van wet- en regelgeving, technologische ontwikkelingen en strengere maatschappelijke eisen wijzen de VRH op de noodzaak mee te bewegen.
Daarnaast heeft de VRH de eigen wens om een betrouwbare organisatie te zijn. Er is een sterke afhankelijkheid van informatie binnen de primaire processen. Inwoners, medewerkers en partners moeten erop kunnen vertrouwen dat de VRH werkt met betrouwbare informatie en dat er op een veilige manier wordt omgegaan met informatie. Tegelijkertijd moet er efficiënt worden gewerkt, waarbij informatie snel en gemakkelijk ingezien kan worden vanaf verschillende locaties en verschillende apparaten. Informatie moet niet enkel veilig worden bewaard, maar ook veilig kunnen stromen tussen verschillende systemen.

Al tezamen zorgt dit ervoor dat informatiebeveiliging steeds belangrijker wordt binnen de processen van de VRH. Dit vereist een integrale aanpak op gegevensbeveiliging. Hierbij dient gekeken te worden naar de verschillende facetten van informatieveiligheid, zoals netwerkbeveiliging, toegangsbeveiliging en leveranciersmanagement. Hierbij staat het in kaart brengen van risico's en dit managen centraal: risicomijdend werken is geen doel op zich, maar het minimaliseren van risico heeft wel de focus.

Doelstelling

Dit document beschrijft het strategische informatiebeveiligingsbeleid voor de jaren 2021 t/m 2025. Het beleid is als een leidraad verweven in alle processen van de VRH. Het heeft als doel te komen tot een gestructureerd en controleer- en stuurbaar geheel aan principes, uitgangspunten en randvoorwaarden met betrekking tot de beveiliging van informatie. Beveiliging van gegevens en informatie is een integraal aspect van de bedrijfsvoering. Informatieveiligheid is niet iets dat door individuen in een organisatie gedragen kan worden: een organisatie moet dit gezamenlijk doen. Vandaar dat ook het beleggen van eigenaarschap en verantwoordelijkheid als belangrijke voorwaarde voor het beleid wordt zien.
Het beleid beschrijft de strategische visie. De uitwerking van dit beleid wordt jaarlijks vertaald naar concrete maatregelen en activiteiten.

Actualiseren

Er vinden continu ontwikkelingen plaats die van invloed zijn op het informatiebeveiligingsbeleid en de actualisatie hiervan. Basis voor dit beleid wordt gevonden in:

- baselines voor informatieveiligheid, zoals de ISO normen 27001:2017 en 27002:2017, de NEN 7510 (voor de meldkamer [2]), en – voornamelijk – de Baseline Informatiebeveiliging Overheid (BIO v 1.04)
- het landelijk programma Informatievoorziening 2020-2025 in opdracht van het veiligheidsberaad, waarbij continuïteit van de organisaties in de vorm van digitale weerbaarheid benoemd staat als een van de vier strategische doelen
- het dreigingsbeeld informatiebeveiliging, Informatiebeveiligingsdienst (IBD)
- wetgeving die invloed heeft op de uitvoering van het beleid, zoals de AVG
- de resultaten uit risicoanalyses en impactanalyses
- de uitkomst van audits, zoals de collegiale toetsing onder veiligheidsregio's

Naast bovengenoemde invloeden analyseert de VRH ook de eerder ervaren incidenten. Deze analyses geven waardevolle informatie en dienen als directe input voor het informatiebeveiligingsbeleid en het daarbij horende beveiligingsplan.

Dit beleidsdocument beschrijft de globale kaders en richting voor de aankomende vijf jaar. Gezien de ontwikkelsnelheid van het informatiebeveiligingsdomein wordt dit beleidsstuk iedere drie jaar geëvalueerd om te zien of de uitgangspunten nog actueel zijn. Indien nodig, wordt dit document na de evaluatie gewijzigd en opnieuw vastgesteld. Drie jaar is tevens de evaluatietermijn die beschreven staat in het BIO-normenkader.

[2] **Geneeskundige meldkamer Haaglanden** De Geneeskundige meldkamer Haaglanden is, als onderdeel van de VRH, middels een SLA verbonden aan de Regionale Ambulancevoorziening Haaglanden. De Directie VRH heeft het IB-beleid van de RAV Haaglanden (op basis van NEN7510) van toepassing verklaart op de meldkamer ambulancezorg zolang dat niet conflicteert met het eigen IB-beleid van de VRH.

3 Principes van informatieveiligheid

De VRH streeft ernaar in control te zijn. In dit verband betekent 'in control' zijn dat de organisatie met een bepaalde zekerheid kan aangeven wat het niveau van informatieveiligheid is. De organisatie is bekend met de dreigingen, genomen maatregelen en openstaande risico's. Voor de openstaande risico's worden nog te nemen maatregelen opgesteld in de vorm van verbeterplannen, om zo continue verbetering van het niveau van informatieveiligheid te realiseren. Verder kan er op een professionele wijze verantwoording afgelegd worden.

In dit hoofdstuk wordt inzicht gegeven in welke doelen en uitgangspunten de VRH nastreeft op het gebied van informatieveiligheid. Daarnaast worden er randvoorwaarden benoemd die essentieel zijn voor het kunnen realiseren van de uitgangspunten.

Strategische doelstellingen

De VRH streeft de volgende doelen na:
- Informatiebeveiliging is binnen de organisatie belegd
- Bedrijfsmiddelen worden adequaat beschermd
- Risico's van en door menselijk gedrag worden geminimaliseerd
- Toegang tot informatie en informatiesystemen wordt beheerst. Ongeautoriseerde toegang wordt voorkomen
- De veiligheid van informatiesystemen wordt gewaarborgd
- De organisatie is digitaal weerbaar: er wordt adequaat gereageerd op incidenten.
- Incidenten worden geëvalueerd om als leermoment te fungeren.
- Kritieke bedrijfsprocessen worden beschermd
- Persoonsgegevens van inwoners, medewerkers en andere betrokkenen worden correct verwerkt en beschermd
- Het niveau van informatiebeveiliging wordt getoetst door middel van audits, analyses en evaluaties.

Uitgangspunten

Uitgangspunten reflecteren standaarden die de VRH nastreeft wat betreft informatieveiligheid. Ze zijn op strategisch niveau geformuleerd. De strategische richting wordt op tactisch en operationeel niveau ingericht door middel van procedures, richtlijnen en andere beleidsstukken. Dit wordt gedaan voor bijvoorbeeld het wachtwoordbeleid, dataclassificatie en toegangsbeveiliging. Voor ieder uitgangspunt geldt dat dit een streven is. Het betekent niet dat deze uitgangspunten al volledig ingericht en belegd zijn binnen de organisatie. Om (beter) te voldoen aan de uitgangspunten, is een ontwikkelplan gecreëerd. Dit plan geeft aan op welke uitgangspunten de komende jaren gerichte focus ligt. Dit plan is nader toegelicht in het hoofdstuk 'Ontwikkel pad'.

Risicomanagement staat centraal

De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Bij de inrichting van een nieuw proces of het herzien van een bestaand proces, worden risico's bekeken. Voor het inventariseren van de risico's biedt de organisatie onder andere een Basis Impact Analyse-tool aan, waarmee op basis van de BIO risico-afwegingen gemaakt kunnen worden. Dit wordt aangevuld met een analyse van bekende kwetsbaarheden en dreigingen. Het CIO-bureau helpt door het bieden van de juiste ondersteuning bij de uitvoering van de analyse en het leveren van kaders voor maatregelen. Afdelingsmanagers zijn er echter verantwoordelijk voor dat – bij een wijziging in het proces, of bij het bekend worden van een nieuwe dreiging – een analyse wordt uitgevoerd.

Risicomijdend te werk gaan is niet het doel: op basis van functionele behoefte van gebruikers moet gekeken worden hoe risico's verminderd al dan niet vermeden kunnen worden. Maatregelen passen bij de risico's die gelopen worden en hierin is het hebben van een geaccepteerd restrisico mogelijk. Het is een verantwoordelijkheid van het lijnmanagement om ook met het gebruik van nieuwe technologie in control te zijn op het gebied van inrichting en beveiliging van informatie. Bij iedere wijziging aan een proces of een systeem zal daarom gekeken worden naar de risico's die voortvloeien uit deze wijziging. Risicomanagement is daarmee een repetitief proces.

De gebruiker staat centraal bij de implementatie van maatregelen

Informatiebeveiligingsmaatregelen nemen gaat niet enkel om het opleggen van beperkingen. Het beperken van mogelijkheden zorgt er vaak voor dat medewerkers zelf manieren gaan zoeken om buiten de systemen om – en daarmee vaak onveilig – te werken. Informatieveiligheid wordt nagestreefd, terwijl er ook focus ligt op de facilitering van de gevraagde functionaliteit. Alhoewel er intern standaarden voor informatieveiligheid gelden die gevolgd worden, is maatwerk een essentieel onderdeel van het formuleren en inrichten van maatregelen.

Data wordt geclassificeerd

Informatieveiligheid gaat niet enkel over het beveiligen van toegang tot gegevens, het gaat ook om het beveiligen van de gegevens zelf. De beveiliging van gegevens wordt bepaald door een risicoafweging. Hierin vormen beschikbaarheid, integriteit en vertrouwelijkheid de leidende criteria. Naar deze criteria worden gegevens en bestanden geclassificeerd. De classificatie verduidelijkt vervolgens voor het personeel wat er met informatie gedaan kan worden: of informatie bijvoorbeeld gedeeld of bewerkt mag worden.

Informatieveiligheid is een continu leerproces

Door periodieke controle, organisatie-brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Informatiebeveiliging is

een continu verbeterproces. Er dient een vast proces gevolgd te worden: 'Plan, Do, Check en Act'. Dit vormt samen het managementsysteem van informatiebeveiliging.

Informatieveiligheid is een onderdeel van leveranciersmanagement
Het werk van de VRH heeft een sterke afhankelijkheid van leveranciers. Er wordt veel gebruik gemaakt van externe systemen, voor het verwerken, opslaan, beheren en inzichtelijk maken van gegevens en informatie. De VRH maakt met de leverancier afspraken over de borging van vertrouwelijkheid, integriteit en beschikbaarheid. Deze afspraken worden contractueel vastgelegd. Wanneer het verwerken van persoonsgegevens betreft, wordt hier ook een verwerkersovereenkomst voor getekend. Het nakomen van deze afspraken is iets dat periodiek geëvalueerd dient te worden.

Bovendien worden veel systemen aan elkaar gekoppeld. Beveiliging dient plaats te vinden in dit hele netwerk van systemen. Een zwakke schakel beïnvloedt de gehele ketting. Er worden hoge eisen gesteld aan identificatie en autorisatie van gebruikers: een koppeling tussen systemen voor gegevensoverdracht staat niet gelijk aan een koppeling qua autorisatie.

Informatieveiligheid is locatie- en apparaat onafhankelijk
Informatiebeveiliging gaat over het waarborgen van de betrouwbaarheid van informatie. Hierbij is de fysieke locatie van de persoon die toegang tot informatie verkrijgt in theorie onbelangrijk: vanaf iedere locatie moet de toegang tot informatie passend beveiligd zijn. Ook het apparaat waarmee toegang wordt verkregen dient niet te resulteren in een andere standaard van informatieveiligheid: informatieveiligheid wordt gegarandeerd op ieder apparaat.

In de praktijk kan dit wel resulteren in andere maatregelen: wat passende maatregelen zijn hangt af van de risico's die gelopen worden. Zo worden er betreffend logische toegangsbeveiliging voor thuiswerken strengere beveiligingseisen gesteld dan voor het werken op kantoor. Ook kan toegang met privé apparatuur worden beperkt, dit ten opzichte van toegang met zakelijk apparatuur.

Privacy wordt gewaarborgd
Sinds maart 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Deze wetgeving verplicht iedere organisatie om de privacy van betrokkenen, zoals medewerkers en inwoners, te beschermen. Informatieveiligheid en privacybescherming zijn nauw aan elkaar verbonden. Informatieveiligheid gaat over het beschermen van alle informatie binnen een organisatie, waar privacybescherming enkel gaat over het beschermen van persoonsgegevens. De term persoonsgegevens wordt daarbij gedefinieerd als gegevens die leiden of herleidbaar zijn tot een geïdentificeerde of identificeerbare natuurlijke persoon.

Privacybescherming richt zich op de noodzakelijkheid en juridische grondslag voor het verwerken van gegevens, waarbij informatieveiligheid kijkt naar de maatregelen om dit vervolgens zorgvuldig te doen. Binnen processen waarin persoonsgegevens worden verwerkt, wordt naar beide gekeken. De AVG benoemt specifiek dat voor processen 'passende' beveiligingsmaatregelen genomen moeten worden. Dit is wederom een afweging van risico's en maatregelen.

De organisatie streeft naar digitale weerbaarheid
In de afgelopen jaren zien we een verschuiving in het gedachtegoed van informatiebeveiliging: het is niet alleen voldoende om de juiste maatregelen te nemen, je moet als organisatie ook scherp zijn op signalen die aangeven dat er mogelijk een incident plaatsvindt en voorbereid zijn om vervolgens snel en effectief te handelen. Een incident is tenslotte niet altijd te voorkomen. VRH heeft een incident responsplan (handboek) en traint via oefeningen voor het moment dat een cyberincident zich daadwerkelijk voordoet.

Randvoorwaarden

Randvoorwaarden beschrijven wat er minimaal ingericht moet zijn om informatieveiligheid op een duurzame wijze te borgen.

Eigenaarschap en verantwoording afleggen
Alle informatiesystemen en alle informatiebronnen binnen de VRH hebben een systeemeigenaar. De eigenaar bepaalt de waarde van vertrouwelijkheid die de informatie heeft. De eigenaar is in staat om hierover verantwoording af te leggen. De primaire verantwoordelijkheid van het beschermen van de informatie in de systemen en bronnen ligt dan ook bij de systeemeigenaar.

De verantwoordelijkheden op het gebied van informatieveiligheid zijn bij iedereen in de organisatie bekend. Dit geldt dus zowel voor het management als de beveiligingsfunctionarissen en iedere medewerkers en vrijwilliger.

Capaciteit
De organisatie stelt voldoende mensen en middelen beschikbaar om eigendommen en werkprocessen volgens dit beleid te kunnen beveiligen. Medewerkers moeten veilig met informatie kunnen en willen omgaan. De VRH ondersteunt door te voorzien in heldere regels, middelen en adviezen. Expertise en samenwerking op het gebied van informatiebeveiliging en aansluiting op de primaire processen van de brandweer en geneeskundige tak zijn hiervoor essentieel.
Er dient daarom voldoende capaciteit beschikbaar te zijn om de kennis en het bewustzijn van de medewerkers daar waar nodig te vergroten.

Aansluiting bij de PDCA-cyclus

Er wordt cyclisch en methodisch (via een *plan/do/check/act* proces) omgegaan met informatiebeveiliging.

Doelstellingen voor informatiebeveiliging worden – op basis van een risicobeoordeling – geformuleerd, en maatregelen worden getroffen, gemonitord en beoordeeld op basis van de uitkomsten. De uitkomsten leiden weer tot nieuwe doelstellingen. Hierbij is het essentieel dat keuzes die gemaakt worden, op het gebied van maatregelen, worden vastgelegd in documentatie. Dit ten behoeve van de interne communicatie over maatregelen en de interne kennis over eventuele restrisico's. Bovendien dient dit als onderbouwing bij verschillende audits.

Plan

Een risicoanalyse benoemt huidige dreigingen en de kans dat dit optreedt. Het uitvoeren van een risicoanalyse is tevens belangrijk voor het identificeren van nieuwe dreigingen, het benoemen van mogelijke maatregelen en het bepalen van het restrisico. Op basis van deze analyse stelt de VRH een beveiligingsplan op.

Do

Op basis van de risico's en het plan wordt besloten welke maatregelen er daadwerkelijk genomen gaan worden. Beheersmaatregelen worden geselecteerd en per systeem of proces wordt een implementatieplan voor het invoeren van maatregelen opgesteld. Dit kunnen maatregelen van zowel technische als organisatorische aard zijn. De selectie van maatregelen is afhankelijk van het gewenste niveau van informatieveiligheid.

Check

De naleving van het beleid en de effectiviteit van de maatregelen worden gecontroleerd en geëvalueerd. Voorbeelden hiervan zijn de landelijke collegiale audit en de controle vanuit de accountant. Over de bevindingen wordt een audit rapport opgesteld. Audit rapporten worden, met advies van het CIO-bureau, aangeboden aan het Directie Overleg.

Binnen het (standaard) wijzigingsmanagementproces van VRH is nadrukkelijk aandacht voor informatiebeveiliging. Dit mede door domein-overleggen waaraan informatieadviseurs periodiek deelnemen, zodat zij kunnen sturen op eventuele aansluiting op informatiebeveiliging.

Bij wijzigingen die mogelijk grote impact hebben op het niveau van informatieveiligheid, wordt de wijziging tevens besproken met de Change Advisory Board (CAB) van de VRH. Zij toetsen vervolgens de wijziging aan het informatiebeveiligingsbeleid. De CAB staat onder begeleiding van de ICT-Adviseur.

Act

Op basis van de uitkomsten van de audit wordt bekeken welke gebieden binnen de VRH meer aandacht behoeven. Hiervoor wordt een verbeterplan opgesteld.

4 Organisatie, taken en verantwoordelijkheden

Binnen de VRH worden verschillende verantwoordelijkheden en taken onderscheiden. Een juiste plaatsing van verantwoordelijkheid leidt tot het waarborgen van informatieveiligheid binnen de gehele organisatie en het uitstralen van een eenduidig beeld hierover.

In bijlage 1 is een overzicht gegeven van verschillende taken op het gebied van informatieveiligheid. Dit is onderverdeeld in verschillende onderwerpen en opgesplitst in verantwoordelijke, ondersteunende en adviserende rollen. Daarnaast staat benoemd wie er over een onderwerp wordt geïnformeerd. Deze lijst geeft een indicatie van het soort taken dat bij een functie hoort; de taken beperken zich niet tot deze lijst.

Organisatie van informatiebeveiliging (aansturing)

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het sturen op de strategische visie van het informatiebeveiligingsbeleid. Zij zijn in staat draagvlak te creëren voor informatieveiligheid en prioriteit te stellen voor bepaalde onderwerpen.

Directie

De Directie van VRH is eindverantwoordelijk voor alle informatiebeveiliging aangelegenheden. Iedere directeur van elk onderdeel houdt voor de eigen directie de verantwoordelijkheid voor de beveiliging en kwaliteit van de informatie en de informatiesystemen. De directie geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie.

De Directeur Bedrijfsvoering is voorzitter van het MT Bedrijfsvoering en tevens portefeuillehouder van de portefeuille informatieveiligheid. De portefeuillehouder bewaakt voortgang op het gebied van informatieveiligheid en stelt binnen het management de juiste kritische vragen. De Directeur Bedrijfsvoering wordt gevoed met informatie vanuit de CISO en ISO.

De controller houdt toezicht op de escalatie van eventuele beveiligingsincidenten die te maken hebben met persoonsgegevens. Dit in relatie tot de naleving van het informatiebeveiligingsbeleid en de wettelijke verplichtingen vanuit de AVG. Bij incidenten met grote impact deelt de controller informatie over het incident en de getroffen maatregelen binnen de Directie.

Systeemeigenaar

Enkele informatiesystemen die gebruikt worden binnen de VRH hebben een systeemeigenaar. Een systeemeigenaar bekijkt overkoepelend of de juiste maatregelen worden genomen om het systeem te beveiligen. Dit wordt gedaan vanaf de aankoop van een systeem. Tezamen met Inkoop, Contractmanagement, ICT-Beheer en het CIO-bureau wordt bekeken aan welke initiële eisen het systeem dient te voldoen. Basis hiervoor is een analyse van de risico's. In dit proces houdt de systeemeigenaar regie en is hij of zij verantwoordelijk voor het maken van keuzes. De verantwoordelijkheden van de systeemeigenaar zijn nauw verwant aan die van een proceseigenaar. Afhankelijk van het systeem, kan een systeem ondersteunend zijn aan verschillende processen. Andersom kan een proces ook over verschillende systemen lopen. Daarnaast kan een systeemeigenaar ook een proceseigenaar zijn. De analyse van het beveiligingsniveau van een lopend systeem wordt niet (altijd) door de systeemeigenaar gedaan. Wel is het de verantwoordelijkheid van de systeemeigenaar er scherp op te zijn dat dit plaatsvindt. Hierbij is ondersteuning van een proceseigenaar, functioneel beheerder en informatieadviseur benodigd. De systeemeigenaar signaleert vervolgens of de gekozen maatregelen worden genomen. Het afwegen en in gang brengen van extra of andere maatregelen valt ook onder de verantwoordelijkheid van de systeemeigenaar.

Proceseigenaar

In de BIO, het normenkader van informatiebeveiliging voor de overheid, wordt de rol van de proceseigenaar benadrukt. De verantwoordelijkheid wordt expliciet(er) bij de proceseigenaar neergelegd. De achterliggende gedachte hierbij is dat de proceseigenaar ook eigenaar is van de informatie binnen een proces, en hierbij de verantwoordelijkheid heeft deze informatie veilig te houden. De proceseigenaar signaleert vroegtijdig waar risico’s liggen: de proceseigenaar bepaalt welke kwetsbaarheden zich kunnen voordoen binnen het proces dat onder zijn/haar verantwoordelijkheid wordt uitgevoerd en hoe groot het risico is als een kwetsbaarheid zich manifesteert. Hierbij wordt de proceseigenaar gevoed door de functioneel beheerder, (C)ISO en informatieadviseur. Op basis van risicoanalyses wordt bepaald welke beveiligingsmaatregelen getroffen dienen te worden om uiteindelijk op een door de proceseigenaar geaccepteerd risico uit te komen.

Naast het bepalen van de maatregelen is het ook aan de proceseigenaar intern aan te kaarten welke processen qua beveiliging nog niet zoals gewenst verlopen. Zo kan er tijdig ingegaan worden op mogelijke risico’s en kunnen er extra maatregelen worden genomen. Bij het uitvoeren van een analyse is het belangrijk dat er een juiste samenwerking is tussen de aansturende (proceseigenaren, systeemeigenaren), uitvoerende (functioneel beheerders) en adviserende en ondersteunende rollen (ISO, informatieadviseurs). Daar waar nodig stuurt de proceseigenaar op verbeterplannen. Hierbij geldt een ondersteunings- en adviesrol voor het CIO-Bureau en team ICT-Beheer. Binnen de VRH is de afdelingsmanager of het teamhoofd over het algemeen de proceseigenaar van de processen die door de afdeling worden uitgevoerd. Het is de wens

dat voor afdelings-overschrijdende processen specifiek een proceseigenaar wordt benoemd. Waar dit nog niet het geval is, wordt een proceseigenaar toegewezen.

Rollen in de organisatie (uitvoering)

Informatiebeveiliging is niet iets dat bij enkele individuen binnen de organisatie is belegd: de gehele organisatie speelt een rol in het veilig omgaan met informatie.

CISO

In opdracht van de Directeur Bedrijfsvoering is de uitvoerende rol van Chief Information Security Officer (CISO) voor VRH belegd bij het teamhoofd CIO-bureau. De CISO is verantwoordelijk voor de coördinatie, de regie en de ketenafstemming t.a.v. de implementatie van het Informatiebeveiligingsbeleid binnen VRH. In het geval van landelijke- en organisatieontwikkelingen heeft de CISO de verantwoordelijkheid de Directie met informatie te voeden. De CISO neemt hier een actieve rol in, door periodiek informatie te delen over de stand van zaken rondom informatiebeveiliging. Hierin kunnen verschillende ontwikkelingen worden meegenomen: interne ontwikkelingen op het gebied van systemen, processen en maatregelen, en externe ontwikkelingen op het gebied van dreigingen. Ook worden waargenomen incidenten meegenomen.

(Information) Security Officer

De coördinatie op de implementatie en evaluatie van de beveiligingsactiviteiten van een afdeling wordt door het management gedelegeerd aan de (Information) Security Officer (ISO). De Security Officer treedt op als uitvoerder van het informatiebeveiligingsplan. De Security Officer heeft binnen de organisatie de ruimte om gevraagd en ongevraagd advies te geven. Bij vraagstukken kan de Security Officer direct advies geven aan proceseigenaren, systeemeigenaren en functioneel beheerders. Daarnaast heeft de Security Officer in veel beveiligingsprocessen, zoals het uitvoeren van risicoanalyses of het implementeren van maatregelen, een ondersteunende rol. Tenslotte heeft de Security Officer een signalerende rol wat betreft dreigingen en daaraan gekoppelde risico's. De Security Officer houdt daarbij nauw zicht op ontwikkelingen binnen en buiten de organisatie. Directe communicatie met de functioneel beheerders en proces- en systeemeigenaren is daarin essentieel.

Functioneel beheerder

De uitvoering en controle van de beveiligingsmaatregelen worden belegd bij de functioneel beheerders van de betreffende applicaties of omgevingen. Zij dragen zorg voor de instandhouding van de maatregelen. Hierbij worden zij aangestuurd door een proces- of systeemeigenaar en voeden zij hen actief met informatie.
De functioneel beheerder speelt een actieve rol in het identificeren van risico's en incidenten binnen een proces of systeem. Daarnaast wordt verwacht dat de functioneel beheerder een ondersteunende rol speelt bij het analyseren van en rapporteren over

incidenten. Daarnaast is de functioneel beheerder het eerste aanspreekpunt van de leverancier en vice versa.

Afdeling Inkoop

De afdeling inkoop speelt, naast de standaard verantwoordelijkheden die medewerkers hebben, een extra rol met betrekking tot beveiliging. Zij zijn betrokken bij alle aankopen van nieuwe ICT-systemen. Alhoewel zij geen beoordeling uitoefenen op de maatregelen die genomen worden, kunnen zij wel toetsen of er aandacht is voor informatiebeveiliging. Hierbij kan gewezen worden op het betrekken van de juiste personen op het gebied van informatiebeveiliging, zoals de informatieadviseur of Security Officer. Daarnaast wordt er bij aanbestedingstrajecten gewerkt met ICT-inkoopvoorwaarden. Eisen en wensen op het gebied van informatiebeveiliging worden hierin meegenomen. Bij een hernieuwing van de voorwaarden zijn functionarissen op het gebied van informatiebeveiliging en privacy betrokken.
De contractmanager ICT heeft een speciale rol binnen het inkoopproces, op het gebied van informatieveiligheid. De contractmanager ontwikkelt en beoordeelt de verwerkersovereenkomst en SLA (Service Level Agreement) en houdt zicht op het afsluiten van dit document. Binnen dit proces wordt aansluiting bij de Security Officer en FG gezocht.

Medewerkers

Medewerkers, oftewel gebruikers van informatie en informatiesystemen van VRH, hebben ieder een eigen verantwoordelijkheid. Er is de verplichting zich te houden aan de verstrekte richtlijnen aangaande de omgang met informatie, informatieverwerking en bedrijfsmiddelen. Richtlijnen voor de omgang met informatie en informatiemiddelen staan beschreven in de integriteitsverklaring. Daarnaast zijn medewerkers vaak initiatief nemend wanneer het gaat om nieuwe processen of systemen. Bij het aangaan van een nieuw proces of de aanschaf van een systeem is het aan de projectleider – vaak een medewerker van een team – om te letten op de standaarden rondom informatieveiligheid. Hierover kan advies worden ingewonnen bij de ISO.

Toezichthoudende rollen

Change Advisory Board (CAB)

Binnen het (standaard) changemanagementproces van VRH is nadrukkelijk aandacht voor informatiebeveiliging. Voorgestelde wijzigingen worden hiertoe altijd getoetst op de impact op informatiebeveiliging en getoetst aan het informatiebeveiligingsbeleid. In geval van een wijziging van het proces of systeem die leidt tot een wijziging van maatregelen of het niveau van informatieveiligheid, zal dit ook in opdracht van de wijzigingscommissie worden vastgelegd. De wijzigingscommissie bestaat uit een select aantal functioneel beheerders en de ICT-adviseur.

Functionaris Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) vereist dat een overheidsorganisatie een Functionaris Gegevensbescherming (FG) aanstelt[3]. Dit is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van privacywetgeving. De FG heeft vereiste expertise en vaardigheden, of wordt in staat gesteld dit te verkrijgen. Dit houdt onder andere in dat de FG kennis heeft van nationale en Europese wetgeving over privacy en begrip heeft van de organisatie en hoe zij gegevens verwerkt. Net als de Security Officer adviseert de FG, gevraagd en ongevraagd, over risico's en het nemen van maatregelen. De FG heeft daarnaast een toezichthoudende rol als het gaat om het uitvoeren van de maatregelen. Datalekken die leiden tot een grote inbreuk van privacy worden door de FG bij de Autoriteit Persoonsgegeven en eventueel bij betrokkenen gemeld.

Overlegvormen

Informatiebeveiliging heeft een plek op de agenda van verscheidene vergadertafels. Dit doordat informatieveiligheid nauw is verbonden aan allerlei andere onderwerpen, zoals functioneel beheer en communicatie.
Daarnaast zijn er specifiek vergadertafels opgericht voor het bespreken van vraagstukken rondom informatiebeveiliging. Er zijn zowel VRH-interne overleggen als nationale overleggen.

Privacy-overleg

Het privacy-overleg is ontstaan toen de AVG-wetgeving van kracht ging. In het overleg wordt de strategische richting van privacy en de ontwikkelingen hierbinnen op tactisch en operationeel vlak besproken. Daarnaast wordt aandacht besteed aan de voortgang op lopende casussen en projecten. Bij dit overleg sluiten de FG, de Security Officer en de contractmanager ICT aan. Daarnaast sluit ook de CISO wanneer nodig aan. Bij strategische beslissingen of richtingbepalende keuzes treft het privacy-overleg de voorbereiding om de keuze aan de Directie voor te leggen.
Dit overleg vindt op reguliere basis plaats; ongeveer een keer per maand.

Vakgroep informatieveiligheid

De beveiligingsfunctionarissen van alle VR regio's komen tezamen tijdens de Vakgroep Informatieveiligheid. Naast vertegenwoordigers van de veiligheidsregio's zijn er ook personen vanuit het IFV (Instituut Fysieke Veiligheid) aanwezig. Ieder lid van deze vakgroep kan onderwerpen aandragen voor de agenda van dit overleg. Onderwerpen die regelmatig op de agenda staan, zijn de ontwikkeling van wetgeving, risicoanalyses van nieuwe systemen, en landelijke ICT-projecten. Het is een laagdrempelige manier om informatie tussen veiligheidsregio's uit te wisselen. Er vindt iedere twee jaar een

[3] Art. 37 Algemene Verordening Gegevensbescherming

collegiale toetsing plaats. De uitkomsten van deze collegiale toetsing worden binnen de organisatie gedeeld en dienen als input voor organisatie-brede verbeterplannen.
Dit overleg vindt op reguliere basis plaats; ongeveer eens per drie maanden.

VR-ISAC
De VR-ISAC (VR- Information Sharing and Analysis Center) is in opdracht van het POI in juni 2020 opgericht, de VRH neemt vanaf februari 2021 deel. Het doel van de VR-ISAC is om de veiligheidsregio's te helpen met het voorbereiden van en acteren op digitale verstoringen. Er ligt een focus op cybercrime en cybersecurity.
Binnen dit overleg wordt in een vertrouwelijke setting informatie over en ervaring met kwetsbaarheden, dreigingen en incidenten gedeeld. Iedere veiligheidsregio kan hierbij twee vertegenwoordigers aanstellen die deelnemen aan dit overleg. Naast de veiligheidsregio's neemt ook het IFV deel aan dit overleg, en neemt zodoende de rol aan van 26e veiligheidsregio.
Dit overleg vindt op reguliere basis plaats; ongeveer eens per twee maanden.

Domeinoverleg functioneel beheerders
In 2020 is er een onderzoek gedaan naar functioneel beheer binnen de VRH. Uit dit onderzoek bleek dat er behoefte is aan een nauwere samenwerking tussen functioneel beheerders. Besloten is om systemen in te delen in Systeem Domeinen en hierbinnen een samenwerkingsverband te creëren. Het domein heeft een regulier domeinoverleg, waarbij er vaste onderwerpen op de agenda staan. Dit zijn onder andere belangrijke incidenten en wijzigingen. Dit kunnen ook beveiligingsincidenten zijn. Daarnaast wordt de invloed die een wijziging heeft op het niveau van informatieveiligheid en vice versa besproken. Ook kan hierbij een wens voor ondersteuning bij bijvoorbeeld het uitvoeren van risicoanalyses worden aangegeven. Daarnaast vinden er periodiek overleggen plaats waar alle functioneel beheerders uit de organisatie voor zijn uitgenodigd. De Security Officer neemt geregeld deel aan deze overleggen om thema's te bespreken, input te verzamelen of een boodschap over te brengen.

CIRT
In het geval van een cyberaanval is het essentieel dat er direct, snel en efficiënt wordt gereageerd. Hiervoor is een CIRT (Cyber Incident Response Team) samengesteld. Dit team bestaat uit medewerkers van verschillende afdelingen en externe partijen, die tezamen verantwoordelijk zijn voor het maken, uitvoeren, verantwoorden en communiceren van keuzes tijdens een grootschalig of impactvol cyberincident. Welke opschalingsstructuur er gehanteerd wordt, welke posities er betrokken zijn en wie er het mandaat heeft om keuzes te maken, staan beschreven in het responsplan (handboek). Dit plan sluit aan op onder andere de crisis-organisatie en het Plan operationele continuïteit. Cyberdreigingen met kleine impact worden afgehandeld via het standaard incidentenproces.

5 Ontwikkel pad

Dit beleidsdocument geeft de doelstellingen, uitgangspunten en randvoorwaarden van de organisatie weer. Een van de voorwaarden is dat personen binnen de organisatie in staat worden gesteld eigenaarschap te tonen en verantwoording af te leggen. Daarnaast dient er voldoende capaciteit te zijn belegd om taken in het kader van informatiebeveiliging te kunnen uitvoeren. De taken en verantwoordelijkheden binnen de organisatie zijn op hoofdlijnen beschreven in het hoofdstuk 'Organisatie, taken en verantwoordelijkheden'.

Hierbij wordt erkend dat informatiebeveiliging een thema is waar veel ontwikkeling op plaatsvindt. In de afgelopen jaren is er binnen de organisatie veel gedaan op het gebied van informatiebeveiliging. Hierbij wordt continu gezocht naar een niveau van beveiliging dat – gebaseerd op de risico's voor de organisatie – als passend wordt gezien. Echter, doorontwikkeling en het inzetten op het verder verhogen van het niveau van informatieveiligheid is, gezien wetgeving en groei van dreiging, benodigd.

Om ontwikkeling in de organisatie te beleggen, is er een jaarplan informatiebeveiliging opgesteld. Dit jaarplan benoemt verbeterpunten en daaraan gelinkte activiteiten.
Dit geschiedt op het gebied van technische toepassingen, maar ook op het gebied van heldere afspraken en kaders binnen de organisatie. Het jaarplan 2021-2023 beschreef een aantal thema's die tevens in de jaren 2024 en 2025 van belang zijn. Hier zal blijvend aandacht voor zijn. Een van die onderwerpen is het creëren van bewustwording van verantwoordelijkheden die behoren bij de functie die iemand bekleed. Dit ongeacht de functie: iedereen dient zich bewust te zijn van zijn of haar verantwoordelijkheden. Hier is in 2022 en 2023 veel aandacht aan besteed via bijvoorbeeld workshops en promotiemateriaal, dit zal in 2024 gecontinueerd worden.

Een ander hoofdonderwerp uit het jaarplan was de BIO (Baseline Informatiebeveiliging Overheid). In het jaar 2022 en 2023 is hard gewerkt aan een inventarisatie en zijn verscheidene verbeterslagen uitgevoerd. In de aankomende jaren zal er gekeken worden naar de vastlegging van de prestatie op de BIO en de hieraan gerelateerde risico's en verbeterpunten.
Een ander onderwerp wat extra aandacht zal krijgen in de aankomende jaren, betreft SOC en CERT. Hierbij gaat het om het tijdig ontdekken van inbreuken in de beveiliging en het adequaat reageren hierop. Dit verhoudt zich nauw met digitale weerbaarheid.

Bijlage 1 – Lijst van taken

In deze bijlage is een lijst van taken in het kader van informatiebeveiliging opgenomen. Deze lijst is slechts een selectie van taken; de taken die bij iedere functie behoren in relatie tot informatieveiligheid beperken zich niet tot onderstaande lijst.
De taken zijn verdeeld over onderwerpen. Per onderwerp kan een functie een verantwoordelijke, ondersteunende of adviserende rol aannemen. Daarnaast is het mogelijk dat een functie geïnformeerd dient te zijn over een proces of activiteit.

Opstellen informatiebeveiligingsbeleid	
Verantwoordelijk	De **Directie** gaat akkoord met het strategische beleid en de algemene visie De **Directie** stelt strategische doelen De **Directie** en **directeur Bedrijfsvoering** houden zicht op de naleving van het strategisch beleid De **CISO** en **Security Officer** stellen het informatiebeveiligingsbeleid op De **Directie** stelt voldoende capaciteit beschikbaar voor de uitvoering van taken
Adviserend	De **CISO** geeft advies over de strategische richting
Geïnformeerd	De **Security Officer** informeert de **systeemeigenaren, proceseigenaren** en **functioneel beheerders** over aanpassingen aan het informatiebeveiligingsbeleid Het informatiebeveiligingsbeleid is beschikbaar voor alle **medewerkers**

Risicomanagement	
Verantwoordelijk	De **systeemeigenaar** houdt regie op veiligheid binnen alle processen waarbij het systeem een rol speelt De **systeemeigenaar** en **proceseigenaar** sturen op uitvoering van risicoanalyses De **systeemeigenaar** en **proceseigenaar** maken keuzes met betrekking tot risico's en maatregelen De **Functioneel beheerder** voert risicoanalyses uit bij wijzigingen aan bestaande processen of bij nieuwe relevante dreigingen De **Functioneel beheerder** formuleert, documenteert en implementeert (technische, organisatorische en fysieke) maatregelen
Ondersteunend	De **Security Officer** ondersteunt bij de uitvoering van een risicoanalyse en het formuleren en implementeren van maatregelen
Adviserend	De **Security Officer** en **FG** wijzen op de mogelijke wettelijke verplichting tot uitvoering van een risicoanalyse De **CISO** adviseert over keuzes met betrekking tot maatregelen en risico's
Geïnformeerd	De **Directie** heeft kennis van de bewust genomen risico's binnen de organisatie De **systeemeigenaar** en **proceseigenaar** worden door de **functioneel beheerder** gevoed over risico's en dreigingen

Incidentmanagement	
Verantwoordelijk	De **directeur Bedrijfsvoering** activeert wanneer nodig het crisisteam De **Controller** houdt zicht op de invloed die een mogelijke aanval heeft op de financiële ruimte De **CISO** escaleert, waar nodig, een incident naar een hoger niveau De **Security Officer** analyseert incidenten en rapporteert hierover De **proceseigenaar** of **systeemeigenaar** stuurt op mitigerende maatregelen De **Directeur Bedrijfsvoering, CISO, ISO, systeemeigenaren** en **functioneel beheerders** spelen een actieve rol in het geval van een cyberaanval Alle **medewerkers** hebben een plicht tot het intern melden van datalekken De **FG** meldt data lekken bij de Autoriteit Persoonsgegevens
Ondersteunend	De **functioneel beheerders** helpen bij het in kaart brengen van de ICT-architectuur De **functioneel beheerder** ondersteunt bij het analyseren van een incident De **functioneel beheerder** doet informatie-uitvraag bij de leverancier De **Security Officer** houdt zicht op de registratie van beveiligingsincidenten
Adviserend	De **Security Officer** adviseert over mitigerende maatregelen De **CISO** en **Security Officer** adviseren over het doen van een data lek melding bij de Autoriteit Persoonsgegevens of bij betrokkenen
Geïnformeerd	De **CISO** en **Security Officer** informeren de Directie over grote incidenten binnen de organisatie. De **FG** informeert de **Controller** bij incidenten met grote inbreuk op privacy

Wijzigingsbeheer en verbeterplannen	
Verantwoordelijk	De **Directeur Bedrijfsvoering** bewaakt voortgang op het gebied van informatiebeveiliging De **Security Officer** stelt organisatie-brede verbeterplannen op De **systeemeigenaar** en **proceseigenaar** stellen verbeterplannen op en houden zicht op de voortgang hierop De **functioneel beheerder** voert verbeterplannen uit en rapporteren hierover De **functioneel beheerder** monitort en analyseert de effectiviteit van genomen maatregelen
Ondersteunend	De **functioneel beheerder** signaleert wijzigingen die kunnen leiden tot een verandering in het niveau van beveiliging en rapporteert hierover naar de **systeemeigenaren** en **proceseigenaren**
Adviserend	De **Security Officer** kan advies leveren bij het opstellen van proces- of systeem specifieke verbeterplannen

	De **Change Advisory Board** toetst wijzigingen op de impact op informatiebeveiliging en de naleving van het informatiebeveiligingsbeleid
Geïnformeerd	De **CISO, proceseigenaren** en **systeemeigenaren** informeren de **Directeur Bedrijfsvoering** over organisatie-brede verbeterplannen De **Security Officer** rapporteert aan de **CISO** over de uitvoering van jaarplannen

Bewustwording	
Verantwoordelijk	De **Security Officer** zet acties en activiteiten op voor het verhogen van bewustzijn De **functioneel beheerder** controleert toegang tot en autorisaties binnen een systeem De **functioneel beheerder** stimuleert veiligheidsbewustzijn De **proceseigenaar** creëert richtlijnen en protocollen die helpen bij het veilig uitvoeren van een proces **Medewerkers** dienen zich te houden aan verstrekte richtlijnen en protocollen, waaronder het vertrouwelijk omgaan met bedrijfsinformatie en het veilig omgaan met bedrijfsmiddelen
Ondersteunend	De **CISO** levert input voor bewustwordingsacties **Medewerkers** signaleren behoeftes aan kennis en informatie
Adviserend	De **CISO** en **Security Officer** leveren gevraagd en ongevraagd advies

Delen van kennis	
Verantwoordelijk	Leden van **de Directie** nemen deel aan landelijke overleggen waar informatiebeveiliging op de agenda kan staan **De Directie** informeert de **CISO** over landelijke ontwikkelingen De **CISO** en **Security Officer** nemen deel aan de VR-ISAC De **CISO** houdt contact met autoriteiten
Geïnformeerd	**De Directie** en **CISO** wisselen kennis uit over landelijke ontwikkelingen

Leveranciersmanagement	
Verantwoordelijk	De **systeemeigenaar** stelt een lijst van eisen op waaraan een systeem moet voldoen De **proceseigenaar** of **systeemeigenaar** zorgt voor vastlegging van afspraken met leveranciers op het gebied van informatiebeveiliging
Ondersteunend	De **afdeling inkoop** wijst op de rol van informatiebeveiliging binnen het inkooptraject De **functioneel beheerder** heeft contact met de leverancier over nieuwe dreigingen en risico's De **contractmanager ICT** ontwikkelt en beoordeelt de verwerkersovereenkomst en SLA De **contractmanager ICT** houdt zicht op de afsluiting van de verwerkersovereenkomst en SLA

Adviserend	De **Security Officer** en **FG** hebben een adviserende rol bij vernieuwing van inkoopvoorwaarden De **Security Officer** en **FG** adviseren over de inhoud van de verwerkersovereenkomst De **Security Officer** adviseert over de inhoud van de SLA