1. Samenvatting voorstel

Vaststelling beleid informatiebeveiliging
Het Dagelijks Bestuur heeft in de vergadering van 8 november het beleid informatiebeveiliging van de Veiligheidsregio Hollands Midden (VRHM) vastgesteld. Dit beleid is richtinggevend en kaderstellend, het strategische document omschrijft o.a. wat VRHM onder informatiebeveiliging verstaat, welke doelstellingen het kent, welke uitgangspunten hierbij worden gehanteerd, hoe de risicomanagement aanpak wordt gehanteerd, hoe de taken en verantwoordelijkheden zijn belegd en hoe informatiebeveiliging structureel in een managementcyclus (Plan-Do-Check-Act) wordt geborgd.

Informeren projectmatige implementatie en ambitieniveau
VRHM informeert het Algemeen Bestuur hierbij tevens over de projectmatige aanpak van de implementatie waarin het beleid tactisch en operationeel wordt vormgegeven, en over het ambitieniveau. Hiervoor is een projectgroep en een stuurgroep ingericht.

2. Algemeen

Onderwerp:	Beleidsinformatiebeveiliging Veiligheidsregio Hollands Midden	**Opgesteld door:**	Marijn Riemens, afdelingshoofd Informatiemanagement / CISO VRHM
		Afgestemd met:	DT, stuurgroep informatiebeveiliging VRHM
Voorstel t.b.v. vergadering:	Algemeen Bestuur	**Datum:**	29 november 2018
Agendapunt:	B.6	**Bijlage(n):**	
Portefeuille:	H.J.J. Lenferink (DB) H. Zuidijk (VD)	**Status:**	Informatief
Vervolgtraject besluitvorming:	N.v.t.	**Datum:**	N.v.t.

3. Toelichting

Sinds 2017 is VRHM bezig om structureel meer aandacht aan informatiebeveiliging te besteden. In het Veiligheidsberaad is in 2016 besloten dat alle Veiligheidsregio's binnen een paar jaar flink moeten groeien in de volwassenheid van de mate waarin de betrouwbaarheid van hun informatievoorziening is geregeld. Hiertoe is een Auditkader Informatiebeveiliging Veiligheidsregio's vastgesteld waaraan de Veiligheidsregio's dienen te voldoen. Het informatiebeveiligingsbeleid is onderdeel van het geheel aan informatiebeleid van de VRHM en omvat de gehele informatievoorziening binnen de VRHM; de gegevensverzamelingen, de documenthuishouding, de applicaties en technische ICT-infrastructuur.

Werkingsgebied
Het werkingsgebied van dit beleid beperkt zich tot de VRHM als Gemeenschappelijke Regeling. De RDOG kent haar eigen informatiebeveiligingsbeleid, dat ook geldt voor de GHOR en voor andere partners zoals de Politie en haar organisatieonderdelen (zoals de GMK). Op basis van het VRHM

beleid worden wel afspraken gemaakt met de benoemde partners om tot veilige gegevensverwerking te komen.

Landelijk traject
Met dit beleid wordt een belangrijke stap gezet in het gestructureerd en risicogericht veiliger maken en houden van de informatievoorziening binnen VRHM. Het landelijke spoor dat vanuit het Programmaplan Informatievoorziening en het Veiligheidsberaad is aangegeven (hierin is Informatiebeveiliging één van de speerpunten) wordt hiermee door VRHM gevolgd.

Projectmatige implementatie
Door middel van een projectmatige implementatie aanpak wordt het beleid tactisch en operationeel vormgegeven. Het project binnen VRHM is gestart per oktober 2017 en heeft een doorlooptijd tot eind 2018. Eind 2018 zal bepaald worden op welke wijze het verbetertraject wordt voortgezet: of in een voortgezette projectaanpak, of (deels) in de lijnorganisatie belegd.

De resultaten van een uitgevoerde nulmeting en een audit hebben de status van de volwassenheid van informatiebeveiliging binnen VRHM bepaald. Op basis van nulmeting is een Plan van Aanpak vastgesteld. Hierin worden concrete activiteiten en producten benoemd, inclusief de verantwoordelijke uitvoerders en de planning. Ter borging van de management- en verbetercyclus is een projectleider benoemd en zijn een stuurgroep en rapportagecyclus ingericht. In Q1 2019 vindt een tweede audit plaats, in de vorm van een collegiale toetsing door een andere Veiligheidsregio, onder begeleiding van M&I partners, een externe consultancy partij.

Ambitieniveau
In de voornoemde audit is het niveau voor de 32 controls van het Auditkaderkader Informatie-beveiliging binnen VRHM in de meeste gevallen op volwassenheidsniveau 1 of 2 gesteld, in enkele gevallen op 3. VRHM heeft bij aanvang van het project vastgesteld dat het door het Veiligheidsberaad vastgestelde ambitieniveau van volwassenheidsniveau 4 voor de kritische systemen van VRHM, binnen een jaar tijd, niet realistisch is. Dit baseren wij op ervaring en best practices ten aanzien van overeenkomstige (veranderings-)trajecten.

Het is verder ingegeven door de reorganisatie binnen VRHM, en de significante weerslag die deze heeft op m.n. de nieuwe wijze van werken binnen de VRHM organisatie; primair is hier de aandacht en inspanning naar uit gegaan, dit zal de komende periode veelal zo blijven, is de verwachting.
Een “werkend en gedocumenteerd (en kwantitatief beheerd) proces” zoals wordt gevraagd bij een niveau 4, is voor veel controls in korte tijd niet haalbaar.

Een optimale score bij de audit in 2019 is niet het doel op zich. De te implementeren maatregelen zijn een middel om het doel te halen, namelijk om Informatiebeveiliging als proces in te richten en VRHM bewust en bekwaam te maken op dit thema. De continue aandacht en het permanent verbeteren in dit kader, i.c. de inrichting van een structurele managementcyclus in dezen is het doel. Het geaccepteerde eigenaarschap door proceseigenaren (integrale management-verantwoordelijkheid) conform de ingezette procesbenadering na de VRHM organisatiewijziging, zal hieraan bijdragen.
Een wezenlijke gedrags- en cultuurverandering bij management en medewerkers door een uitgebreid gefaciliteerd ”awareness” programma is vooral de doelstelling.

Realistische aanpak
Binnen het project is daarom de focus gelegd op een adequate verbetercyclus, waarin gestructureerd en gestaag wordt toegewerkt naar een “gedefinieerde situatie”, die hoort bij een volwassenheids-

niveau 3. In veel gevallen is het bereiken van een niveau 2 of 3 per 31 december 2018 een doel dat wél realistisch is.

Huidige status
In opzet zijn veel relevante documenten en procedures die het Auditkader voorschrijft reeds beschreven of in concept gereed. De planning is dat deze eind 2018 door de stuurgroep informatiebeveiliging en/of andere relevante VRHM Managementteams (MT's) of het Directieteam (DT) zijn vastgesteld.
Te denken valt aan ICT beheer processen (w.o. back-up, continuïteit), Verwerkersovereenkomsten met leveranciers, de procedure melding datalekken, clean-desk beleid, beleid mobiele apparatuur, procedures rondom fysieke beveiliging (toegangspassen). Ook worden risicoanalyses in de vorm van Business Impact Analyses en een uitgebreid "Awareness" programma uitgevoerd.

Belangrijke aandachtspunten zijn de controls m.b.t. de inrichting van een effectief beheerst proces autorisatiebeheer (toekennen en intrekken accounts voor VRHM applicaties), het ICT logging- en monitoring proces en de uitvoering van technische audits op systemen en netwerk /infrastructuur (zgn. pentesten en web vulnerability scans). Onder andere voor deze onderwerpen is de opzet en de werking nu nog onvoldoende.

Financieel
In de Programmabegroting VRHM 2019 is vastgesteld dat, vooruitlopend op initiële activiteiten als de eerste nulmeting, risicoanalyses en vervolg statusbepalingen t.a.v. de volwassenheid van informatiebeveiliging, een structurele investering van 50 K per jaar aan de orde is.

Deze wordt aangewend voor o.a. de implementatie van (technische) ICT maatregelen, w.o. technische security audits en de verbetering / aanschaf van beheertooling t.b.v. de VRHM infrastructuur en het netwerk. De inhuur van specifieke expertise en consultancy, ter ondersteuning van deze implementatie, is ook een kostenpost waar rekening mee wordt gehouden.
Bij de bepaling eind 2018 op welke wijze het verbetertraject wordt voortgezet, wordt, voor zover mogelijk, een inschatting in de financiële consequenties vastgesteld.

Uit de structurele risicomanagement aanpak binnen VRHM tenslotte, kunnen aanvullend voorgestelde maatregelen op (kritische) informatie systemen voortvloeien. Hierin zal op voordracht van de systeem/proceseigenaren een afweging gemaakt worden tot prioritering en mogelijk aanvullende financiering.

Capaciteit
De projectmatige aanpak van de implementatie is er in de vorm van een ingerichte projectorganisatie informatiebeveiliging en bestaat uit een projectleider en een viertal projectleden, als stakeholders uit de VRHM-bedrijfsvoering organisatie (P&O, ICT, Functioneel Beheer en Facilitaire Zaken (w.o. Inkoop en Contractmanagement). De projectorganisatie komt onder leiding van een externe projectleider tweewekelijks bijeen om af te stemmen over de voortgang van de implementatie.
De projectleider rapporteert aan de afdelingsmanager Informatiemanagement, dit is de (gedelegeerde) opdrachtgever namens de VRHM-organisatie, en aan de Stuurgroep Informatiebeveiliging. Deze bestaat uit de afdelingsmanager Informatiemanagement (senior supplier) en afgevaardigden (senior users) van de sectoren Risico- en Crisisbeheersing (directeur), Bedrijfsvoering (directeur) en Brandweerzorg (afdelingsmanager). Binnen de Stuurgroep worden voorstellen van de projectorganisatie goedgekeurd en vastgesteld.

Organisatie informatiebeveiliging
De ambtelijke eindverantwoordelijkheid is door het bestuur gemandateerd aan de directeur van VRHM. De directeur Bedrijfsvoering behartigt namens de directeur als portefeuillehouder het thema informatiebeveiliging binnen het DT. De Directeur Bedrijfsvoering is aanspreekpunt voor de Chief Information Security Officer (CISO) en Coördinator Informatiebeveiliging (CIB).

Aandachtspunten/risico's
Het DT van VRHM heeft bij aanvang van het project vastgesteld dat het door het Veiligheidsberaad vastgestelde ambitieniveau van volwassenheidsniveau 4 voor de kritische systemen van VRHM niet realistisch is. Dit baseren wij op ervaring en best practices ten aanzien van overeenkomstige (veranderings-)trajecten. Het is verder ingegeven door de reorganisatie binnen VRHM, en de significante weerslag die deze heeft op m.n. de nieuwe wijze van werken binnen de VRHM organisatie; primair is hier de aandacht en inspanning naar uit gegaan, dit zal de komende periode veelal zo blijven, is de verwachting. De planning t.a.v. de oplevering van (deel)producten door deze stakeholders wordt momenteel in sommige gevallen door een verminderde capaciteit en beschikbaarheid niet altijd gehaald. Binnen het project is daarom de focus gelegd op een adequate verbetercyclus, waarin gestructureerd en gestaag wordt toegewerkt naar een "gedefinieerde situatie", die hoort bij een volwassenheids-niveau 3. Voor veel controls is een niveau 2 of 3 per 31 december 2018 een doel wat wél realistisch is.

Het DT van VRHM heeft onderkend dat het nog niet volledig "compliant" zijn aan het Auditkader Informatiebeveiliging een risico voor de betrouwbaarheid (in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid) van zijn informatiehuishouding en –voorziening kan inhouden.
De kans is aanwezig dat bestuurlijke verantwoordelijkheid moet worden afgelegd, in geval van informatiebeveiligingsincidenten. Op het gebied van beschikbaarheid kan worden gedacht aan een applicatie die na uitval niet op tijd hersteld wordt, bij integriteit is het niet kunnen vertrouwen op de juiste informatie in een applicatie (t.b.v. besluitvorming) een voorbeeld, en bij vertrouwelijkheid kan worden gedacht aan het niet goed beheren en beheersen van autorisatiemanagement, met als gevolg een datalek van persoonsgegevens. Het imago van VRHM kan hierdoor worden geschaad.

4. Implementatie en communicatie
Het beleid is bedoeld als richtinggevend, kaderstellend stuk. De tactische en operationele uitwerking van het beleid hiervan, in plannen en maatregelen, wordt jaarlijks uitgevoerd door het management met ondersteuning vanuit Informatiemanagement. De voortgang hiervan wordt bepaald binnen de PDCA-cyclus. Maatregelen worden inclusief planning en – indien relevant - begroting opgesteld.
Ze komen mede tot stand op basis van de risicoanalyses en audits die worden uitgevoerd. Op deze wijze is er sprake van de structurele inrichting van een zgn. Information Security Management Systeem (ISMS).

De projectmatige implementatie en de vaststelling van het beleid zijn binnen VRHM uitgebreid naar het management, de medewerkers en de OR gecommuniceerd; er is vanaf voorjaar 2018 een uitgebreide "awareness" campagne gestart.

5. Bijlagen
Informatiebeveiligingsbeleid VRHM v1.0 dd. 29 mei 2018

Veiligheidsregio
HOLLANDS MIDDEN
Samen sterk voor meer veiligheid!

Informatiebeveiligingsbeleid VRHM

GEMEENTEN Hollands Midden
GHOR
BRANDWEER Hollands Midden

In de Veiligheidsregio Hollands Midden werken gemeenten, GHOR, brandweer, politie en andere partners samen aan de rampenbestrijding en crisisbeheersing in Hollands Midden.

Versiegeschiedenis	Versie	Datum	Gedeeld met
	0.1 Concept	15 februari	IMT
	0.2 Concept	2 maart	Arjan van de Watering; Hans Zuidijk; Management Middelen; Robert Zweegman; Projectteam
	0.3 Concept	20 maart	IMT Arjan van de Watering; Hans Zuidijk; Lilian Weber
	0.9 Definitief concept	12 april	DT (meningvormend)
	1.0 Definitief	29 mei	DT (vastgesteld)

Veiligheidsregio Hollands Midden
Afdeling Informatiemanagement
Postbus 1123, 2302 BC Leiden

Datum 22 mei 2018

Versie 1.0

Opsteller: Wout Knol, Beleidsmedewerker, Afdeling Informatiemanagement
Ton Schilder, Business Information Security Consultant, B-Able

Beheerder: Wout Knol, Beleidsmedewerker, Afdeling Informatiemanagement

Opdrachtgever: Marijn Riemens, Afdelingshoofd, Afdeling Informatiemanagement

Inhoud

1 Woord vooraf

Voor u ligt het Informatiebeveiligingsbeleid van de Veiligheidsregio Hollands Midden (VRHM). Dit document bevat de kaders en uitgangspunten die ertoe moeten bijdragen dat wij binnen VRHM verantwoord omgaan met onze informatie en met de uitwisseling hiervan. Om deze beheersbaar en betrouwbaar te houden is het noodzakelijk om een aantal gemeenschappelijke uitgangspunten te bepalen en uit te dragen vanuit vastgesteld beleid.

Informatiebeveiliging is voor VRHM van essentieel belang. Wij zijn de spin in het web om samen met onze ketenpartners crises te beheersen. Goede informatievoorziening is hierin, zoals ook blijkt uit de Wet op de Veiligheidsregio's, een van de belangrijkste factoren. Nog steeds neemt de behoefte aan informatie toe. De wijze waarop en de momenten wanneer deze informatie nodig is, worden ook steeds meer divers en zijn allang niet meer computer-, werkplek-, locatie- of zelfs organisatiegebonden. Bewust, maar ook onbewust, wordt veel informatie uitgewisseld en verspreid.

Uiteraard dient informatie beschikbaar en juist te zijn. Maar tegelijkertijd dient informatie te worden beveiligd tegen ongeoorloofd gebruik en dreigingen als phishing, diefstal, virusaanvallen, brand etc. Terwijl sommige informatie, gelet op bijvoorbeeld de Wet Openbaarheid van Bestuur, juist weer openbaar moet worden gemaakt, dienen gegevens ook niet zomaar in verkeerde handen terecht te komen of op straat komen te liggen. Ook ter bescherming van de privacy, voor de naleving van wet- en regelgeving en zelfs het imago van onze organisatie is aandacht voor het beschermen van informatie noodzakelijk. Medewerkers zijn zich lang niet altijd voldoende bewust van de risico's van het gebruik van ICT-middelen en het internet, als het gaat om de verspreiding van informatie en de afhankelijkheid van het beschikbaar zijn van die middelen.

Het is noodzakelijk om gericht en structureel maatregelen te treffen. Van 'wenselijk' is informatiebeveiliging daarom ook een 'onvermijdelijk' onderwerp geworden. Door vergaande digitalisering zijn er risico's ontstaan die we nog niet voldoende kennen, maar waarvan we ons bewust moeten zijn en waarop we ons gericht moeten voorbereiden. Het beschikbaar houden en het beschermen van (juiste) informatie begint met het definiëren van het kader: wat houdt informatiebeveiliging in en hoe wil de VRHM daar invulling aan geven. Ofwel: een eenduidige leidraad waarmee passende maatregelen rondom informatievoorziening getroffen kunnen worden, zodat informatie beschikbaar is en blijft voor de medewerker die daartoe bevoegd is.

Dit beleid vormt de kapstok voor beveiligingsmaatregelen en is gebaseerd op het Auditkader Informatieveiligheid Veiligheidsregio's en wordt regelmatig geactualiseerd. Actualisering is noodzakelijk, omdat zowel de organisatie als de omgeving van VRHM voortdurend in ontwikkeling zijn. Bovendien gaan de ontwikkelingen op het gebied van informatietechnologie razendsnel.

VRHM vindt het belangrijk dat iedere medewerker zich bewust is van de noodzaak om zorgvuldig met informatie om te gaan en hier ook naar handelt. Zodat we met zijn allen de risico's in de informatievoorziening binnen onze organisatie tot een aanvaardbaar niveau kunnen reduceren. Dit document is dan ook voor alle bij informatiebeveiliging betrokken functies van belang om te kennen en uit te dragen.

Hans Zuidijk, Algemeen Directeur Veiligheidsregio Hollands Midden

2 Samenvatting Informatiebeveiligingsbeleid

Informatiebeveiliging betreft het nemen en onderhouden van een samenhangend pakket aan maatregelen om de betrouwbaarheid van de informatievoorziening te garanderen. Het begrip informatiebeveiliging heeft betrekking op de volgende betrouwbaarheidsaspecten: *beschikbaarheid* (continuïteit); *integriteit* (correctheid, volledigheid, tijdigheid en controleerbaarheid) en *vertrouwelijkheid* (exclusiviteit). Informatiebeveiliging is gericht op het voldoen aan geldende normen, wet- en regelgeving. Daarmee streven we naar een optimaal niveau van beveiliging, op basis van passende maatregelen.

De doelstelling van het informatiebeveiligingsbeleid is het continu beschermen van bedrijfsinformatie tegen een variëteit aan bedreigingen, op een effectieve en efficiënte wijze, om bedrijfsdoelstellingen te borgen en bedrijfsrisico's te minimaliseren, investeringen te optimaliseren en kansen te maximaliseren. Dit beleid bevat de kaders voor het management om inhoud te geven aan informatiebeveiliging en de bijbehorende verantwoordelijkheden en is de kapstok om maatregelen aan op te hangen. Dit beleid omvat de gehele informatievoorziening binnen de VRHM en is leidend voor afspraken met partners over wederzijds gebruik van gegevens en diensten. Er is een aantal richtinggevende uitgangspunten voor het beleid en het inrichten van het proces van informatiebeveiliging. Het informatiebeveiligingsbeleid kent raakvlakken met andere processen en draagt specifiek bij aan het beleid en de inrichting van deze processen waar het gaat om de betrouwbaarheid van onze informatievoorziening.

VRHM hanteert het normenkader van de Veiligheidsregio's uit 2016 om maatregelen te treffen en te werken aan een bepaalde mate van volwassenheid met betrekking tot informatiebeveiliging. Het beleid en de te hanteren normen en maatregelen worden daarnaast gebaseerd op risico-inschattingen. De bevindingen uit risicoanalyses (interne audits) leiden tot inzicht op basis waarvan het management kan besluiten om beveiligingsmaatregelen te prioriteren. Er ontstaat zo een geactualiseerd plan op basis waarvan het informatiebeveiligingsbeleid en maatregelen nader kunnen worden ingevuld en vormgegeven. Daarnaast is er een voorname rol weggelegd binnen projectmanagement en wijzigingsbeheer. Aanpassingen in onze informatievoorziening worden voorafgegaan door een risico-afweging en analyse van de impact ten aanzien van de betrouwbaarheid ervan.

Er wordt onderscheid gemaakt naar verschillende verantwoordelijkheden binnen het thema informatiebeveiliging: op strategisch, tactisch en operationeel niveau wordt gezorgd voor de goede sturing en werking van het proces van informatiebeveiliging.

Een informatiebeveiligingssystematiek ondersteunt het informatiebeveiligingsproces van vaststellen van het beleid, het beoordelen van risico's en het treffen van maatregelen, het monitoren en beoordelen van de uitkomsten en het bijsturen en verbeteren van de maatregelen. In een geautomatiseerd systeem wordt de bewijsvoering voor het proces vastgelegd.

Classificatie is een van de middelen waarmee we in staat zijn om gericht maatregelen voor te stellen en te onderhouden. Door te classificeren leggen we de waarde van bedrijfsprocessen, de informatie en –systemen voor onze bedrijfsvoering vast en zijn we in staat om daar gericht maatregelen aan toe te wijzen om deze te beschermen en te beveiligen. Risicoanalyses worden gebruikt om conform de classificatie te prioriteren en passende maatregelen te treffen.

3 Introductie

3.1 Inleiding

In onze primaire processen en in onze bedrijfsvoering is betrouwbare informatie van toenemend belang. Zonder goede informatie zijn we beperkt in ons vermogen om te adviseren, te beheersen, te besluiten en te sturen. Onvoldoende informatieveiligheid, onjuiste of verouderde data bijvoorbeeld, kan leiden tot onacceptabele risico's in de uitvoering van risico- en crisisbeheersing. Beveiligingsincidenten en inbreuken (zoals datalekken) kunnen leiden tot (financiële) schade en imagoschade. Door de toenemende digitalisering doen zich steeds meer kwetsbaarheden voor en dienen zich nieuwe risico's aan. Het is van belang deze risico's daarom te kennen en hiertegen adequate maatregelen te treffen. Daartoe wordt het proces informatiebeveiliging ingericht.

3.2 Aanleiding

In het in 2014 vastgestelde programmaplan Informatiemanagement wordt informatiebeveiliging als belangrijk thema beschreven, vooral in relatie tot de beschikbaarheid van informatie en –systemen: betrouwbare informatievoorziening. Onderhavig beleid stelt hiervoor de richtlijnen.

Informatiebeveiliging krijgt binnen veiligheidsregio's de laatste jaren vanzelfsprekend steeds meer aandacht. Na een landelijke nulmeting is in 2016 het landelijke project Informatieveiligheid van start gegaan. Door het Veiligheidsberaad is toen besloten dat alle veiligheidsregio's een bepaalde mate van volwassenheid moeten nastreven op het gebied van informatiebeveiliging. Leidraad hierin is het van de BIG (Baseline Informatiebeveiliging Gemeenten) afgeleide Auditkader Informatiebeveiliging Veiligheidsregio's. Een van de stappen naar volwassenheid is het formuleren, vaststellen en communiceren van het informatiebeveiligingsbeleid, om daarmee voor het inrichten van een continu proces de basis te leggen. Een visie en vastgesteld beleid zijn noodzakelijk om ons naar een hoger niveau te brengen. Zij bieden het kader waarbinnen maatregelen worden opgesteld, uitgevoerd en getoetst.

Ook de Wet Veiligheidsregio's is een grond om onze informatievoorziening veilig te houden. In de Wvr wordt de veiligheidsregio immers verantwoordelijk gesteld voor het in stand houden van de informatievoorziening en voor bijvoorbeeld sluitende registraties. Aan zulke eisen kan alleen worden voldaan als ook informatiebeveiliging (en dan met name de beschikbaarheid en integriteit) goed is ingevuld.

3.3 Doel van dit document

De VRHM heeft de ambitie om met dit beleidsdocument te voldoen aan wet- en regelgeving en informatiebeveiliging structureel naar een hoger niveau te brengen en daar te houden, door de organisatie van de beveiligingsfunctie en het informatiebeveiligingsbeleid te beschrijven en vast te stellen. Dit beleid vormt het uitgangspunt voor het management om inhoud en richting te geven aan informatiebeveiliging en de bijbehorende verantwoordelijkheden en is de kapstok om maatregelen aan op te hangen, zowel structureel als projectmatig.

3.4 Scope van dit beleid (wet en organisatie)

Dit informatiebeveiligingsbeleid is onderdeel van het geheel aan informatiebeleid van de VRHM en omvat de gehele informatievoorziening binnen de VRHM; de gegevensverzamelingen, de documenthuishouding, de applicaties en technische ICT-infrastructuur. Het beleid staat ten dienste van de afnemer van de informatie en gebruiker van de informatiesystemen. Informatiebeveiliging gaat niet alleen over hardware en software, maar ook over het veilige gebruik ervan.

Voor privacy en het voldoen aan privacywetgeving (Algemene Verordening Gegevensbescherming) hanteren we afzonderlijk beleid (Privacybeleid VRHM), maatregelen en afspraken. Vanwege het specifieke karakter (bijvoorbeeld een specifiek normenkader) en verantwoordelijkheden (met name voor de Functionaris Gegevensbescherming) is bewust voor deze verdeling gekozen. Wel zijn er veel raakvlakken met informatiebeveiliging; de privacywetgeving beschrijft bijvoorbeeld dat er gepaste beveiliging van persoonsgegevens moet zijn, en het informatiebeveiligingsbeleid schetst daarvoor de kaders.

Het werkingsgebied van dit beleid beperkt zich tot de VRHM als Gemeenschappelijke Regeling. De RDOG kent haar eigen informatiebeveiligingsbeleid dat ook geldt voor de GHOR, en datzelfde geldt voor onze andere partners zoals de Politie en haar organisatieonderdelen (zoals de GMK). Op basis van ons beleid maken we wel afspraken met onze partners om tot veilige gegevensverwerking te komen.

3.5 Definitie informatiebeveiliging

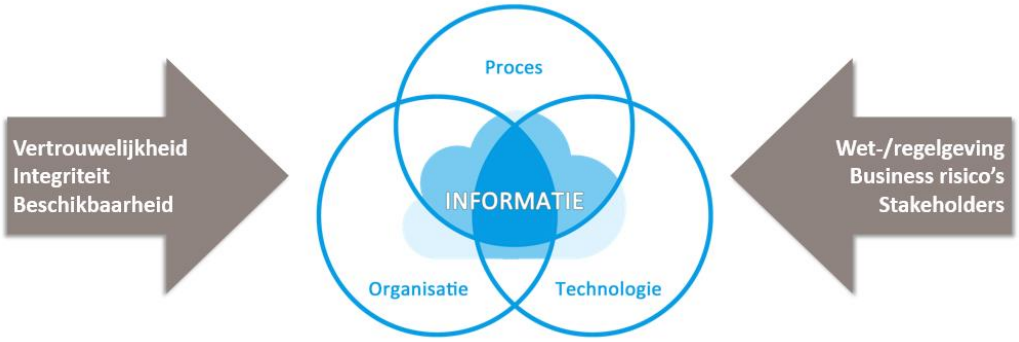
Informatiebeveiliging wordt gedefinieerd als: het treffen en onderhouden van een samenhangend pakket aan maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen. Het begrip informatiebeveiliging heeft dus betrekking op de volgende betrouwbaarheidsaspecten (ook bekend als BIV-aspecten):

- **Beschikbaarheid (continuïteit)**
  Het zorgdragen voor de beschikbaarheid van informatie, de informatiesystemen en informatiemiddelen op de juiste tijd en plaats voor de gebruikers.

- **Integriteit (juistheid en volledigheid)**
  Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en de informatieverwerking.

- **Vertrouwelijkheid**
  Het beschermen van informatie tegen ongeautoriseerde toegang alleen toegankelijk voor personen voor wie dit bestemd is.

Informatieveiligheid is het resultaat van informatiebeveiliging. Privacy wordt beschermd door maatregelen die voortkomen uit informatiebeveiliging. Deze begrippen zijn nauw verwant.



De aspecten van informatiebeveiliging

In andere woorden: informatiebeveiliging is de verzamelnaam van het geheel van processen die ingericht worden om de betrouwbaarheid van de informatievoorziening van VRHM, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen allerhande bedreigingen, zowel interne als externe, die zich al dan niet als gevolg van bewust handelen voordoen. Het is vooral in het belang van de proces- en systeemeigenaren dat hun informatie veilig en beschikbaar is. Informatiebeveiliging wordt daarmee impliciet onderdeel van onze processen.

Informatiebeveiliging is gericht op het voldoen van geldende normen, wet- en regelgeving. Daarmee streven we naar een optimaal niveau van beveiliging, op basis van passende maatregelen. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

De mens is de belangrijkste factor in het geheel. Als belanghebbende is hij gebaat bij een betrouwbare informatievoorziening, maar levert daar zelf ook de belangrijkste bijdrage aan. Stakeholders kunnen eigen medewerkers zijn, ICT-beheerders, externe partijen waar informatie mee wordt uitgewisseld: allemaal hebben ze hun eigen kwetsbaarheden in houding en gedrag. Het is daarom belangrijk de stakeholders te kennen en te betrekken om hun belang te behartigen.

4 Doelstelling informatiebeveiliging

De doelstelling van informatiebeveiliging binnen VRHM is:

Het continue beschermen van bedrijfsinformatie tegen een variëteit aan bedreigingen, op een effectieve en efficiënte wijze, om bedrijfsdoelstellingen te borgen en bedrijfsrisico's te minimaliseren, investeringen te optimaliseren en kansen te maximaliseren.

Het informatiebeveiligingsbeleid is het kader voor passende technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatiesystemen en de informatie te beschermen en te waarborgen. Het beleid is gericht op het voldoen aan de relevante wet- en regelgeving, in lijn met de Wvr, (art 10.i, 14.c) en de afspraken die gemaakt zijn in het kader van het landelijke project Informatieveiligheid. De Baseline Informatiebeveiliging Gemeenten (BIG) is leidraad voor (initieel) een dertigtal maatregelen waaraan we ons als veiligheidsregio conformeren en waarmee we tot een zekere 'volwassenheid' willen komen. Deze maatregelen zijn beschreven in het Auditkader Informatiebeveiliging Veiligheidsregio's en bieden een basisset aan maatregelen. Bovenop die dertig zijn er veel meer maatregelen nodig en mogelijk om informatieveiligheid te

waarborgen. Die voeren we door als blijkt dat er risico's zijn die daartoe aanleiding geven en daarvoor gebruiken we naast de BIG bestaande normenkaders als referentie (zoals ISO27001/27002). Uiteindelijk levert dat een niveau van informatiebeveiliging op dat past bij onze taken en dienstverlening en daartoe ingerichte bedrijfsvoering.

4.1 Doel en middelen

Met de implementatie van het informatiebeveiligingsbeleid komt VRHM 'in control' en kan daarover op professionele wijze verantwoording afleggen. In control betekent in dit verband dat VRHM weet welke informatiebeveiligingsmaatregelen genomen zijn en daadwerkelijk werken en dat er een duidelijke planning is ten aanzien van het (continu) verbeteren van de informatiebeveiliging. Hiertoe richten we een systematiek (ISMS) in die verderop (Hoofdstuk 8) wordt beschreven. Periodiek worden informatiebeveiligingsplannen opgesteld waarin voor een bepaalde periode wordt beschreven welke maatregelen dienen te worden getroffen en welke middelen daarvoor nodig zijn. Door organisatiebreed risicomanagement zullen we tot een afweging en verdeling van middelen komen.

4.2 Ambitie

Het streven is om minimaal te voldoen aan de dertigtal maatregelen zoals deze in het Auditkader zijn opgesteld en hierin het voorgestelde volwassenheidsniveau (2-4 volgens CMMI) na te streven. Daarmee wordt in de periode tot 2019 een basisniveau van informatieveiligheid bereikt, waarop we extern getoetst worden en we ons na 2019 ook zelf voortdurend intern toetsen. De risicogerichte aanpak zorgt ervoor dat we gaandeweg steeds meer maatregelen gaan treffen om veiliger te worden en verder te groeien. Daarbij hanteren we de BIG, zonder dat we het streven hebben om daar volledig aan te gaan voldoen; dat is geen doel. Het is ook niet onze ambitie om ons op een andere manier (zoals ISO 27001) te certificeren of te laten toetsen dat we informatiebeveiliging op orde hebben.

5 Uitgangspunten informatiebeveiliging

5.1 Beleidsuitgangspunten

Informatiebeveiliging gaat over het blijvend op niveau houden van de veiligheid van onze informatie en informatievoorziening. We zien het als een continu proces van beschrijven, vaststellen, onderhouden, meten en verbeteren (in de beschrijving van de Plan-Do-Check-Act-cyclus in hoofdstuk 8 komt dit verder naar voren). Risicoanalyses en audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit.
We hanteren bij dit proces een aantal speerpunten:

- We voldoen aan relevante wet-, regelgeving;
- We werken risicogericht aan een optimaal en haalbaar niveau;
- Informatiebeveiliging is een verantwoordelijkheid van elke medewerker; bewustwording ligt daarom aan de basis en begint bij indiensttreding;
- Informatiebeveiliging is onderdeel van het thema 'integraal management' binnen onze organisatie; de leidinggevende heeft een taak in het onder de aandacht brengen van dit aspect van informatievoorziening en 'veilig werken';

- Informatiebeveiliging raakt de hele organisatie en is daarom terug te vinden op de verschillende niveaus van besluitvorming en in veel aspecten van bedrijfsvoering.

Om de bedrijfsrisico's te minimaliseren zijn de volgende specifieke uitgangspunten ten aanzien van de uitvoering van informatiebeveiliging onderkend:

- Informatiebeveiliging maakt deel uit van de algehele risicomanagementaanpak binnen VRHM, en richt zich specifiek op de risico's ten aanzien van de betrouwbare informatievoorziening (beschikbaarheid, integriteit en vertrouwelijkheid);
- Informatiebeveiliging is onderdeel van en borgt de kwaliteit en veiligheid van de informatiemanagementprocessen binnen VRHM;
- Gegevens worden te allen tijde veilig verwerkt conform geldende voorschriften en richtlijnen voortvloeiend uit wet-/ regelgeving of afspraken met de voor de data verantwoordelijke partij;
- De verwerking, opslag en het beheer van VRHM-gegevens door (en bij) externe leveranciers en (beheer)partijen vindt veilig plaats en wordt geborgd door een adequaat stelsel van afspraken;
- Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de potentiële schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Informatie is om die reden geclassificeerd;
- De VRHM is eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Voor alle informatie(voorzieningen) en ICT-middelen zijn eigenaren aangewezen die verantwoordelijk zijn voor de beveiliging ervan;
- Informatiebeveiliging is binnen de VRHM zo ingericht dat de rechten van betrokkenen die voortvloeien uit de Algemene Verordening Gegevensbescherming worden gerespecteerd;
- Wanneer (onderdelen van) de VRHM-samenwerkingsverbanden aangaan met externe partijen wordt aandacht besteed aan informatiebeveiliging; afspraken worden schriftelijk vastgelegd en op de naleving wordt toegezien;
- De VRHM faciliteert voor haar medewerkers continu bewustwording voor de omgang met de informatievoorziening;
- De VRHM stimuleert haar medewerkers om beveiligingsincidenten en beveiligingsrisico's te melden en faciliteert daartoe een ingericht proces;
- De integriteit van gegevens wordt ondersteund door gegevens uit de bron te halen. Bronnen zijn o.a. de overheidsbrede basisregistraties en de kernregistraties van de VRHM zelf; zoals de kernregistratie Personen. Audits op de kwaliteit van gegevens zijn noodzakelijk om de betrouwbaarheid van alle externe bronnen blijvend vast te stellen;
- Informatiebeveiliging is bij de VRHM een structureel onderdeel binnen projecten (door middel van risicoparagraaf) en de wijzigingsbeheerprocessen; informatiebeveiliging wordt bij voorbeeld vanaf de start in de geformuleerde eisen bij verwervingen meegenomen en wordt waar relevant meegenomen en doorvertaald in de overeenkomsten.

5.2 Auditkader

Het informatiebeveiligingsbeleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de norm en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen. Als uitgangspunt en leidraad bij de inrichting van een adequaat proces informatiebeveiliging met een stelsel van maatregelen wordt het *Auditkader informatieveiligheid Veiligheidsregio's* als norm gehanteerd. Dit is in 2016 door het landelijke project Informatieveiligheid vastgesteld. Hierin zijn de volgende clusters benoemd waarin tweeëndertig maatregelen terugkomen:

1. Beleid en Organisatie
2. Personeel

3. Ruimten en apparatuur
4. Continuïteit
5. Toegangsbeveiliging en integriteit
6. Controle en logging

Zie verder hiervoor de bijlage 1.

Na de initiële collegiale toetsen waarin wordt gekeken naar de volwassenheid hanteren we dit auditkader om met interne audits de stand van zaken te bepalen en maatregelen te treffen om te kunnen optimaliseren op de verschillende onderdelen. De maatregelen binnen dit kader zijn geen doel op zich maar een basis van waaruit we de informatiebeveiliging op orde krijgen. De interne audits worden gecoördineerd door de coördinator informatiebeveiliging.

5.3 Lagenmodel

Het proces informatiebeveiliging gaat uit van een lagenmodel waarin verschillende niveaus complementair zijn. Er bestaan in dit kader drie hiërarchische niveaus: strategisch, tactisch en operationeel.

5.4 Werkingsgebied (proces)

Het werkingsgebied van dit beleid omvat de bedrijfsprocessen van VRHM, de ondersteunende informatiesystemen; informatie en gegevens van VRHM en de door externe (keten)partijen aangeleverde gegevens; het gebruik daarvan door de medewerkers (zowel eigen als extern ingehuurd personeel) en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Het is van toepassing op het gehele proces van de informatievoorziening, van zowel geautomatiseerde- als niet geautomatiseerde informatiesystemen, ongeacht de classificatie en opslagwijze. Onze ketenpartners hanteren hun beleid conform de wetten en normen die voor hen gelden (zoals de NEN7510 voor de zorgsector); in de samenwerking en

uitwisseling maken we gezamenlijk afspraken over de aansluiting op elkaars standaarden en hoe we rekening houden met het voldoen aan wet- en regelgeving, die voor sommige partners verder strekt.

5.5 Geldigheid document

Het informatiebeveiligingsbeleid wordt periodiek, bij belangrijke wijzigingen of bij omvangrijke informatiebeveiligingsincidenten, beoordeeld en zo nodig bijgesteld door de coördinator informatiebeveiliging en door deze na consultatie van de belanghebbenden ter vaststelling aan het DT aangeboden.

5.6 Raakvlakken met andere processen

- **Informatiebeleid**

Informatiebeveiligingsbeleid is een voornaam onderdeel van het totale informatiebeleid binnen de VRHM. In dit beleid is beschreven hoe we richting geven aan de informatievoorziening binnen de VRHM. Binnen het informatiebeleid worden ook de processen beschreven waarmee de informatievoorziening in stand wordt gehouden. Deze beheerprocessen, en met name incidentbeheer en wijzigingsbeheer bieden de mogelijkheid om het aspect informatiebeveiliging te waarborgen. In procesontwerpen worden eisen opgenomen die vanuit informatiebeveiliging gevraagd worden.

- **Risicomanagement**

Informatiebeveiliging is sterk gerelateerd aan risicomanagement. Dit richt zich op het analyseren en beheersen van de organisatiebrede risico's waaraan de VRHM wordt blootgesteld. Dit kunnen financiële risico's zijn, of risico's met betrekking tot de paraatheid. Risicomanagement wordt voorgeschreven door wet- en regelgeving, zoals door de Commissie BBV (Besluit Begroting en Verantwoording). Artikel 11 van het BBV verplicht ons om een inventarisatie te geven van de risico's en van de weerstandscapaciteit, en een inventarisatie van het beleid daaromtrent. Informatiebeveiliging heeft specifiek betrekking op die risico's die verbonden zijn aan de beschikbaarheid van de informatievoorziening, de integriteit van gegevens en de omgang met vertrouwelijke informatie.

- **Continuïteitsmanagement**

Informatiebeveiligingsbeleid relateert ook aan het continuïteitsbeleid van de VRHM. Met dit beleid streeft de VRHM ernaar om de continuïteit van de bedrijfsvoering en de kritische bedrijfsprocessen zeker te houden en ook binnen een bepaalde tijdsduur weer beschikbaar te stellen in geval van een incident of calamiteit. In het continuïteitsbeleid worden ook de eisen aan informatievoorziening opgenomen die nodig zijn voor de continuïteit voor de bedrijfsvoering. Classificatie van gegevens is hiervoor een belangrijk hulpmiddel.

- **Kwaliteitsmanagement**

Informatiebeveiliging relateert ook aan de kwaliteitszorg binnen de VRHM. Beide processen dragen bij aan de kwaliteit van de dienstverlening en de benodigde kwaliteit bij ondersteunende processen. Het uitvoeren van de beleidscyclus, het uitvoeren van risicoanalyses en audits binnen onze versterken elkaar daarin. Bovendien is het bij de VRHM gebruikte kwaliteitszorgsysteem ook van toepassing op de informatievoorziening. Aspecten van informatiebeveiliging komen ook terug in onze kwaliteitszorg (afspraak is afspraak).

- **Leveranciersmanagement**

Informatiebeveiligingsbeleid relateert ook aan het leveranciersmanagement binnen de VRHM. Voor het aangaan van contracten, het uitbesteden van diensten en in algemene zin het maken van afspraken met leveranciers zijn de uitgangspunten van informatiebeveiliging van belang. Hiermee

worden de verantwoordelijkheden en de dienstverlening (bijvoorbeeld in het geval van verwerken) goed beschreven en belegd.

- **Facilitair management**

Facilitair management is naast het verlenen van diensten verantwoordelijk voor het ter beschikking stellen, beheren en onderhouden van (werkplek)faciliteiten, gebouwen en onderhoudsruimten en de toegang daartoe. Hiervoor zijn de uitgangspunten van informatiebeveiligingsbeleid van belang, omdat deze de toegankelijk en beschikbaarheid mede bepalen. Voor de toegang tot gebouwen en ruimten en onderhoud aan de installaties binnen onze gebouwen, zoals noodstroominstallaties.

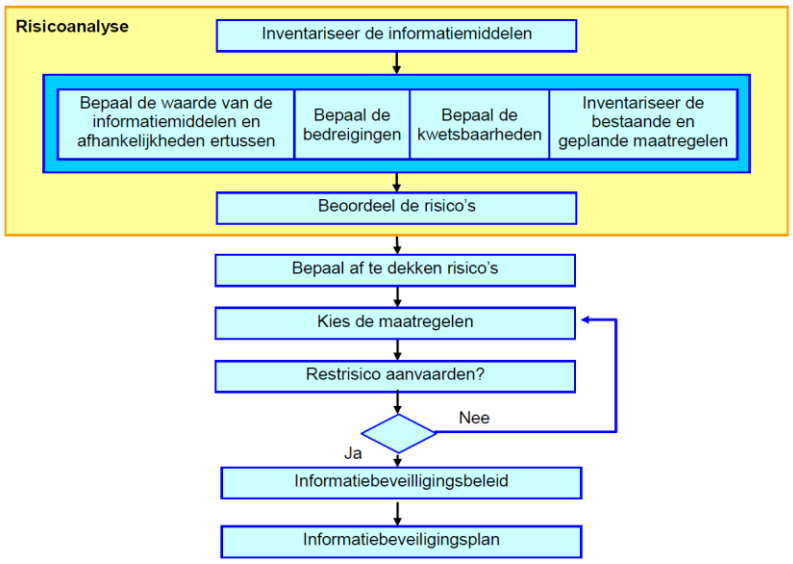
- **Personeelsmanagement**

Personeelsmanagement is verantwoordelijk voor het beleid en instrumentarium ten aanzien van functioneren en informeren van onze medewerkers, onder andere met betrekking tot hun rechten en plichten. Voor de personeelsprocessen zijn de uitgangspunten voor informatiebeveiligingsbeleid zeker relevant. Belangrijke onderdelen binnen de personeelsprocessen betreffen bijvoorbeeld het wervings- en selectieproces (beoordelen achtergrond op basis van een VOG); het vastleggen van (en toegang tot eigen) personeelsgegevens; het muteren bij wijzigingen (doorstroom en uitstroom); het bepalen van de betrouwbaarheid van medewerkers; vertrouwelijke omgang met persoonsinformatie en het opstellen en bewaken van gedragscodes behorend bij het ambtenaarschap.

6 Risicomanagement

6.1 Risicogerichte aanpak

De VRHM kiest voor een risicogerichte benadering van informatiebeveiliging, als onderdeel van de VRHM-brede aanpak met betrekking tot risicomanagement. Kern van deze risicogerichte benadering is dat de organisatie conform wet- en regelgeving haar risico's inventariseert aan de hand van de door haar belangrijk geachte onderdelen. Vervolgens worden de risico's geanalyseerd (oorzaak, omvang, impact) en wordt bepaald welke passende beheersmaatregelen nodig zijn voor de relevant geachte risico's. In onderstaand schema is de gebruikte aanpak weergegeven.



Om te bepalen aan welke risico's de informatie(voorziening) van VRHM bloot staat, is het nodig de bedreigingen en kwetsbaarheden te benoemen. Daarnaast is het van belang de gevolgen van een incident voor de organisatie te bepalen. Uit een inschatting van de waarschijnlijkheid dat een bedreiging tot een incident leidt, wordt daarmee het risico bepaald. Of dit risico aanvaardbaar is, wordt bepaald aan de hand van (classificatie)criteria die VRHM vaststelt.

Om de geïdentificeerde risico's te reduceren tot onder het aanvaardbare niveau zal VRHM daarvoor geschikte beheersmaatregelen inzetten en de effectiviteit hiervan regelmatig beoordelen.

De risicoanalyse kan leiden tot bijstelling van het informatiebeveiligingsbeleid en de daaruit voortkomende informatiebeveiligingsplannen; bij voorbeeld als blijkt dat door verandering in de omgeving of in de organisatie andere beleidsafwegingen of -uitgangspunten ten aanzien van (rest)risico's moeten worden gemaakt.

Het proces risicomanagement is ingebed in de PDCA-cyclus van het Information Security Management System (ISMS); zie hiervoor hoofdstuk 8.

6.2 Risicobeoordeling BIA en bedreigingen- en kwetsbaarhedenanalyse

De risicobeoordeling bestaat uit de systematische aanpak van het schatten van de omvang van de risico's (risicoanalyse) en het vergelijkingsproces van de ingeschatte risico's met risicocriteria om zo het belang van de risico's te bepalen. Voorbeelden hiervan zijn business impactanalyses (BIA). Deze worden in ieder geval voor de bedrijfskritische systemen uitgevoerd, met medewerking van de belanghebbenden, zoals eigenaren, gebruikers, beheerders en leveranciers. Waar nodig worden aanvullende bedreigingen- en kwetsbaarhedenanalyses uitgevoerd om risico's in beeld te krijgen.

6.3 Informatiebeveiliging binnen projectmanagement en wijzigingsbeheer

Binnen het (standaard) wijzigingsbeheerproces van VRHM is nadrukkelijk aandacht voor informatiebeveiliging. Voorgestelde wijzigingen worden hiertoe binnen het beheerdersoverleg of het verantwoordelijke CAB altijd getoetst op de impact op informatiebeveiliging en getoetst aan het informatiebeveiligingsbeleid. Daarnaast zijn informatiebeveiliging en de eisen op dit gebied altijd onderdeel van het ontwerp-, ontwikkel- of verwervingsproces van een oplossingsrichting. De functionaris gegevensbescherming wordt betrokken wanneer het privacygerelateerde wijzigingen betreft.

Een goedgekeurde wijziging kan leiden tot de noodzakelijkheid de risicoanalyse opnieuw uit te voeren (voor specifieke onderdelen). In sommige gevallen zullen ook de eisen (voor nieuwe onderdelen) moeten worden vastgesteld. Bij een aanbesteding van een nieuw informatiesysteem gaat het om een grootschalige wijziging waarvoor dus eisen worden opgesteld die de aspecten van informatiebeveiliging waarborgen.

Binnen het kader van de informatiebeveiliging bestaan er de volgende triggers voor het opstarten van het wijzigingsproces:

- Auditrapport: in dit rapport worden bevindingen gerapporteerd die (snel) opgelost moeten worden (bijvoorbeeld installeren security patches of het moeten treffen van nieuwe maatregelen n.a.v. toename van een bepaald soort beveiligingsincidenten);
- Verzoek van gebruiker/ vanuit de organisatie: dit soort verzoeken wordt altijd getoetst aan de eisen op gebied van informatiebeveiliging;

- Incidentmanagement: de oplossing of oplossingsrichting van een informatiebeveiligingsincident kan direct of indirect input zijn voor het wijzigingsbeheerproces.

6.4 Risicostrategie en -behandeling

Deze aanduiding benadrukt het reduceren van risico's tot aanvaardbare niveaus, waarbij wordt erkend dat er nooit afdoende middelen beschikbaar zullen zijn om volledige risicovermijding te bereiken. Het gaat om de balans tussen (ingeschatte) bedreigingen en risico’s aan de ene kant en de risicomaatregelen, kosten en werkbaarheid aan de andere kant. Zie hiervoor ook paragraaf 5.6 voor de organisatiebrede benadering.

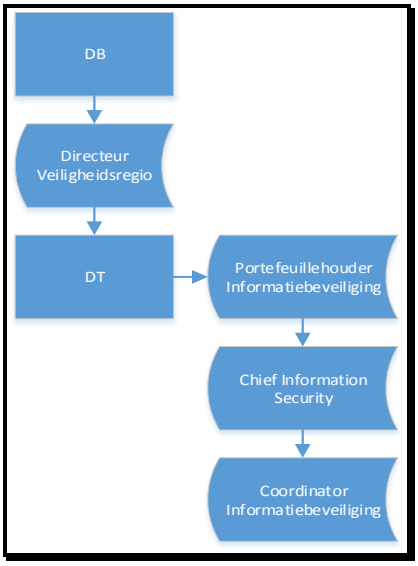
De risicostrategie is de verantwoordelijkheid van het management van VRHM. Deze bepaalt de wijze waarop VRHM met risico's omgaat en rechtvaardigt de kosten voor informatiebeveiliging.

VRHM kan besluiten bepaalde risico’s bewust te aanvaarden, mits wordt voldaan aan het beleid en de criteria voor risicoaanvaarding.

7 Organisatie van informatiebeveiliging

7.1 Organogram

In dit hoofdstuk wordt de organisatie van de informatiebeveiliging binnen VRHM beschreven. Het gaat hierbij vooral over wie verantwoordelijk is voor het bereiken van de doelstellingen van het informatiebeveiligingsbeleid. Daartoe wordt een aantal rollen en functies onderscheiden die hieronder verder worden toegelicht aan de hand van de verantwoordelijkheid binnen het proces.



7.2 Dagelijks Bestuur

Het Dagelijks Bestuur is bestuurlijk verantwoordelijk voor de informatiebeveiliging binnen de VRHM en stelt het informatiebeveiligingsbeleid vast. In het Dagelijks Bestuur is een portefeuillehouder informatievoorziening benoemd aan wie wordt gerapporteerd over aan informatiebeveiliging gerelateerde onderwerpen.

7.3 Directieteam VRHM

De ambtelijke eindverantwoordelijkheid voor informatiebeveiliging is door het bestuur gemandateerd aan de directeur van VRHM. Het DT ondersteunt informatiebeveiliging in de relevante facetten van de bedrijfsvoering. Het directieteam onderschrijft de beveiligingsmaatregelen die in het informatiebeveiligingsbeleid worden voorgeschreven en draagt deze actief uit.

De directeur van elke sector binnen VRHM is verantwoordelijk voor de beveiliging en voor de kwaliteit van de eigen informatie en informatiesystemen, zowel voor eigen gebruik als de aan anderen geleverde informatie en -diensten. Het DT mandateert het informatiebeveiligingsbeleid en faciliteert voldoende middelen voor passende maatregelen. Daarnaast ziet zij toe op de naleving en evaluatie van het informatiebeveiligingsbeleid.

De Directeur Bedrijfsvoering behartigt namens de directeur als portefeuillehouder het thema informatiebeveiliging (en privacy) binnen het DT. Hij brengt gevraagd en ongevraagd het onderwerp in het Dagelijks Bestuur in, en legt over relevante aangelegenheden verantwoording af. De Directeur Bedrijfsvoering is aanspreekpunt voor de Chief Information Security Officer (CISO) en Coördinator Informatiebeveiliging (CIB). De portefeuillehouder behartigt informatiebeveiliging binnen het DT en is binnen VRHM de ambassadeur voor informatiebeveiliging.

7.4 Chief Information Security (CISO)

De rol van Chief Information Security Officer (CISO) voor VRHM is belegd bij de afdelingsmanager Informatiemanagement, die direct onder het DT ressorteert. Namens de directeur Bedrijfsvoering is de CISO verantwoordelijk voor het opstellen van het beleid, de regie en de ketenafstemming voor de implementatie van het Informatiebeveiligingsbeleid binnen VRHM, hij helpt informatiebeveiliging naar het gewenste niveau zonder direct verantwoordelijk voor het resultaat te zijn.

.

7.5 Coördinator Informatiebeveiliging (CIB)

Deze rol is ondergebracht binnen de afdeling Informatiemanagement, bij de senior-adviseur Informatiemanagement, die onder de leiding van het afdelingshoofd (en CISO) valt. Uitvoerende taken (zoals het managen van incidenten en het adviseren op aspecten van informatiebeveiliging) liggen bij de CIB, evenals het toezien op het onderhouden van maatregelen en het adviseren bij de totstandkoming van maatregelen.

Afbakening t.a.v. Functionaris gegevensbescherming
De CIB heeft als werkterrein het implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging. Dit beschermt de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie door een risicobeheerproces. Concreet heeft de CIB dus een bredere scope dan de FG maar zonder een wettelijk verplicht kader. Daarnaast mag de CIB overwegingen (laten) maken vanuit een risicobenadering terwijl de FG veelal een duidelijk beperkt kader meekrijgt vanuit wet- en regelgeving op het vlak van privacy.
Voor afstemming tussen informatiebeveiligings- en privacygerelateerde zaken heeft de CIB regelmatig overleg met de Functionaris Gegevensbescherming (een rol die bij PPO is ondergebracht).
NB: De FG heeft als scope de verwerking van persoonsgegevens binnen de VRHM en de externe verwerkers van deze gegevens (zoals leveranciers van softwareoplossingen).

7.6 Eigenaar informatiesysteem

De eigenaar van een informatiesysteem heeft de eindverantwoordelijkheid voor de inrichting en uitvoering van de beveiliging van het aan hem toegewezen informatiesysteem. De eigenaar bepaalt de classificatie- en betrouwbaarheidseisen in termen van beschikbaarheid (inclusief levenscyclus), integriteit en vertrouwelijkheid (toegankelijkheid) van het informatiesysteem binnen de kaders van het informatiebeveiligingsbeleid. Dit geldt ook voor informatiesystemen die buiten de VRHM-infrastructuur zijn ondergebracht, zoals SaaS-oplossingen. Binnen een omgeving worden vaak meerdere processen ondersteund; de systeemeigenaar is aanspreekpunt in plaats van de afzonderlijke proceseigenaren.

7.7 Leidinggevenden

De afdelingsmanagers zorgen ervoor dat hun medewerkers op de hoogte zijn van de voor hen relevante aspecten van het informatiebeveiligingsbeleid en dat deze worden nageleefd. Hiertoe wordt het onderwerp regelmatig besproken in werkoverleggen. Het is een onderdeel van het bedrijfsvoeringselement Informatievoorziening (uit PIOFACH) dat deel uitmaakt van de integrale managementverantwoordelijkheid. Het (laten) opstellen van informatiebeveiligingsplannen en het implementeren van informatiebeveiligingsmaatregelen valt ook binnen het verantwoordelijkheidsgebied van een specifieke afdelingsmanager.

7.8 Functioneel beheer

Functioneel beheer is namens de systeemeigenaar verantwoordelijk voor een veilig beheer van de functionele inrichting (en autorisaties) binnen de applicaties. Dit beheer vindt plaats op basis van de door de systeemeigenaar gestelde betrouwbaarheidseisen. Functioneel beheer hanteert hierbij de maatregelen (zoals procedures) die voortkomen uit het informatiebeveiligingsbeleid.

7.9 Technisch beheer

Technisch beheer (ondergebracht bij ICT) is verantwoordelijk voor het veilig technisch beheer van de informatievoorziening, op basis van de door de systeemeigenaar gestelde betrouwbaarheidseisen. Zij zorgt voor het in stand houden van een operationeel systeem, bestaande uit apparatuur, programmatuur, gegevensverzamelingen, communicatiemiddelen en de beveiligingsvoorzieningen die daarbij gebruikt moeten worden. Technisch beheer hanteert hierbij de maatregelen (zoals procedures) die voortkomen uit het informatiebeveiligingsbeleid.

7.10 Gebruikers

Elke medewerker (in vaste dienst of ingehuurd) die gebruik maakt van de (informatie)voorzieningen binnen de VRHM is persoonlijk verantwoordelijk voor de naleving van het informatiebeveiligingsbeleid en de daaruit voortkomende regels en richtlijnen die de omgang met informatie, informatieverwerking en desbetreffende bedrijfsmiddelen betreffen. Ditzelfde geldt voor tijdelijke externe medewerkers en leveranciers, die onder verantwoordelijkheid van een opdrachtgever werken en door deze op de hoogte worden gesteld van de voor de werkzaamheden relevante richtlijnen. Eigen medewerkers worden geacht beveiligingsincidenten te melden. Hieronder verstaan we elke situatie die afwijkt van het vooraf besproken niveau van een betrouwbaarheidsaspect (BIV).

7.11 Ondernemingsraad

De ondernemingsraad wordt geïnformeerd over het informatiebeveiligingsbeleid en de hieruit voortvloeiende maatregelen en richtlijnen. Specifieke richtlijnen in relatie tot gedrag van medewerkers worden ter beoordeling voorgelegd aan de OR. Dit geldt ook voor privacygerelateerde onderwerpen. E.e.a. is in de WOR bepaald ten aanzien van advies- en instemmingsrecht.

7.12 Incident-responsteam

Als zich incidenten voordoen met grote impact op de bedrijfsvoering dan kan conform het vastgestelde proces beheer informatiebeveiligingsincidenten op initiatief van de CISO of CIB een team bij elkaar worden geroepen om over te gaan tot oordeelsvorming en adequate maatregelen. Vaste leden van dit Incidentresponsteam zijn de CISO, de CIB, de coördinator ICT (of vertegenwoordiger), een functioneel beheerder van de betreffende applicatie, de Functionaris

Gegevensbescherming (als het privacy of verwerking van persoonsgegevens raakt) en de proceseigenaar (of een vertegenwoordiger) uit het proces waar het incident impact op heeft. Daarnaast kunnen een communicatieadviseur en een (vertegenwoordiger namens de) leverancier deel uitmaken van het overleg.

7.13 Samenvatting naar PIOFACH

Vertaald naar de I van PIOFACH-aspecten kunnen we de matrix als volgt uitbreiden:

	Medewerker **Verrichten** **Binnen het systeem werken**	**Leidinggevende** **Inrichten** **Aan het systeem werken**	**Directeur** **Mederichten** **Systeem bepalen**	**Reg. Commandant** **Eindverantwoordelijk voor richten** **Het systeem**
I	-Veilig gebruik informatie -Ziet toe op integriteit gegevens	-Faciliteert veilig gebruik -Hanteert richtlijnen en inrichtingseisen -Bespreekt veilig gebruik -Stelt maatregelen voor	-Stelt inrichtingseisen (BIV) systeem voor -Bepaalt business case voor maatregelen	-Stelt strategisch visie vast i.r.t. bedrijfsdoelstellingen -Toetst o.b.v. bestuurlijke prioriteiten

In de bijlage 2 worden de bovenstaande verantwoordelijkheden uitwerkt in taken voor CISO, CIB en FG.

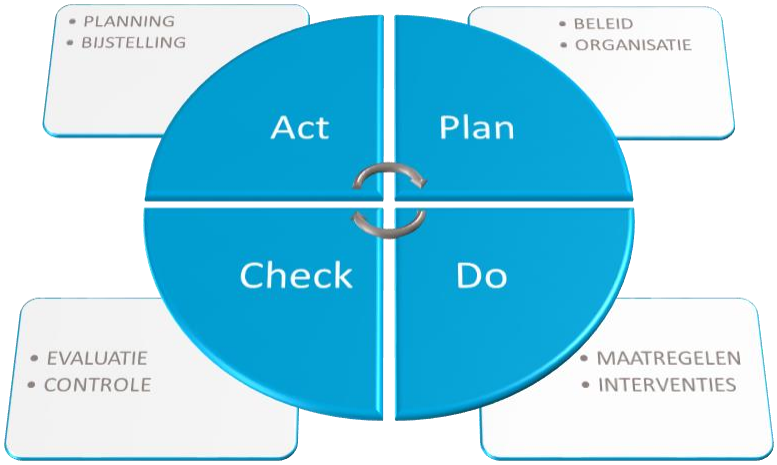
8 Managementsysteem voor informatiebeveiliging

8.1 Management systeem

Het 'Information Security Management System (ISMS)' ondersteunt VRHM bij de beheersing van informatiebeveiliging. De kern van het ISMS is het cyclische proces *(plan/do/check/act)* voor het bepalen van beveiligingsdoelstellingen op basis van een risicobeoordeling, het treffen van maatregelen en het monitoren en beoordelen van de uitkomsten. Voor deze systematiek wordt een geautomatiseerde oplossing gekozen, waarin het beleid, de plannen, de maatregelen en de stand van zaken wordt bijgehouden, inclusief de documenten waarin e.e.a. is vastgelegd.

De procesbenadering in deze vorm onderstreept voor VRHM het belang van:

a) Het inzicht in de eisen van de organisatie ten aanzien van informatiebeveiliging;
b) De noodzaak voor het vaststellen van beleid en doelstellingen voor informatiebeveiliging;
c) Het implementeren en uitvoeren van beheersmaatregelen om de risico's voor informatiebeveiliging voor de organisatie te beheren ten opzichte van de algemene bedrijfsrisico's van de organisatie;
d) Het controleren en beoordelen van de prestaties en de doeltreffendheid van het ISMS;
e) De continue verbetering, gebaseerd op objectieve meting.



Information Security Management System

- **Plan**
  Het vaststellen van het ISMS en de doelstellingen, processen en procedures die relevant zijn voor het risicomanagement en verbetering van de informatiebeveiliging;

- **Do**
  Het implementeren en uitvoeren van het ISMS; maatregelen, processen en procedures;

- **Check**
  Beoordelen en rapporteren van de werking van het ISMS;

- **Act**
  Corrigerende en preventieve maatregelen nemen om continue verbetering van het ISMS te bewerkstelligen.

8.2 Beleidsvorming

De beleidsvorming binnen VRHM bestaat uit het opstellen van het informatiebeveiligingsbeleid. Hier worden de doelstellingen en uitgangspunten voor informatiebeveiliging bepaald (onderhavig document). Deze worden (zo nodig) verder uitgewerkt in procedures en vereiste (technische) maatregelen.

Het beleid wordt periodiek beoordeeld en zo nodig aangepast (controle en evaluatie). Triggers voor het proces kunnen gewijzigde omstandigheden zijn zoals nieuwe technologische ontwikkelingen, organisatieontwikkelingen, sociale ontwikkelingen, wetgeving etc.

Onderdeel van de beleidsvorming is ook het vaststellen van de eisen die VRHM stelt aan de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Dit is elke keer nodig als er een wijziging (change) wordt geïmplementeerd die een verandering van de informatievoorziening tot gevolg heeft, of wanneer het informatiebeveiligingsbeleid wordt herzien.

8.3 Risicoanalyse

De risicoanalyse behelst het vaststellen van mogelijke bedreigingen en de kans van optreden. Dit is uitgebreid beschreven in het hoofdstuk over risicomanagement. Dit is van belang bij de identificatie van nieuwe bedreigingen of na implementatie van een beheersmaatregel. Voorbeelden hiervan zijn business impactanalyses (BIA) en privacy impact assessments (PIA). Op basis van deze methoden wordt steeds een objectieve risico-inschatting gemaakt van bedreigingen, rekening houdend met de eisen die VRHM stelt aan beschikbaarheid, vertrouwelijkheid en integriteit.

De risicoanalyse heeft tot doel:

- Inzicht te krijgen in de kwaliteit van de bestaande beveiligingsmaatregelen;
- Inzicht te krijgen in de risico’s die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen;
- Het gewenste niveau van informatiebeveiliging vaststellen in de vorm van een classificatie van bedrijfsprocessen, informatiestromen en gegevensverzamelingen.

Over de uitkomsten van de analyse van de bestaande situatie voor informatiebeveiliging wordt regelmatig gerapporteerd aan het Directieteam.

8.4 Opstellen informatiebeveiligingsplan

Op basis van de risicoanalyse worden beheersmaatregelen geselecteerd en een implementatieplan voor invoering van de maatregelen opgesteld. De selectie is afhankelijk van het gewenste niveau van informatiebeveiliging. De te implementeren maatregelen kunnen zowel technisch als organisatorisch van aard zijn.

Het implementatieplan of beveiligingsplan wordt als projectplan, inclusief planning en begroting opgesteld.

Het beveiligingsplan wordt (na afstemming in tactisch overleg) overlegd aan het DT die haar goedkeuring hieraan geeft. Dit zal veelal worden gedaan door goedkeuring voor het benodigde budget. Het directieteam treedt op als opdrachtgever voor de uitvoering van het informatiebeveiligingsplan.

8.5 Implementatie

De in het informatiebeveiligingsplan gedefinieerde maatregelen worden indien noodzakelijk projectmatig geïmplementeerd. Door het toepassen van een projectmanagement aanpak wordt geborgd dat de beoogde resultaten worden gerealiseerd en dat er sprake is van voortgangsbewaking. De bij VRHM toegepaste projectmanagementmethode is ook hier van toepassing. Over de voortgang wordt periodiek gerapporteerd aan het DT.

8.6 Controle en evaluatie

In deze fase wordt de naleving van het beleid en de effectiviteit van de maatregelen gecontroleerd en geëvalueerd. Over de bevindingen wordt een auditrapport opgesteld. Hierover wordt gerapporteerd naar het Directieteam. Een goede controle en evaluatie impliceert dat alle beveiligingsincidenten worden geregistreerd, opgelost en geëvalueerd.

De volgende methoden voor controle en evaluatie worden toegepast:

- Periodieke interne en externe security audits. Hierbij worden documenten gecontroleerd, geregistreerde incidenten geëvalueerd, etc.
- Periodieke health assessments en risk assessments, zowel self-assessments als door onafhankelijke externe partijen uitgevoerd. Tijdens deze tests worden bijvoorbeeld penetratietests op het netwerk en de infrastructuur uitgevoerd en wordt nagegaan of er in de configuratie nog niet-geïdentificeerde bedreigingen voorkomen.

9 Classificatie van informatie

9.1 BIV-classificatie

Voor het bepalen van de normen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatie en informatiesystemen, hanteren we een classificatieschema. Door te classificeren leggen we de waarde van bedrijfsprocessen, de informatie en –systemen voor onze bedrijfsvoering vast en zijn we in staat om daar gericht maatregelen aan toe te wijzen om deze te beschermen en te beveiligen. Classificatie stelt ons ook in staat daarin te prioriteren en de maatregelen (minimale en maximale regels) passend te laten zijn. We hanteren de BIA als classificatiemethodiek.

De bij de classificatie gebruikte kenmerken zijn:

- Beschikbaarheid betreft het gewenste niveau van dienstverlening dat is gericht op de beschikbaarheid van de dienst (of product) op de afgesproken momenten (zoals bedrijfsduur,

waarbij rekening wordt gehouden met uitvalstijden, servicewindows, verstoringen en incidenten). Kenmerken van beschikbaarheid zijn tijdigheid, continuïteit, robuustheid en herstelbaarheid.
- Integriteit betreft de mate waarin de informatie actueel en correct is. Kenmerken zijn juistheid en volledigheid en actualiteit (van informatie).
- Vertrouwelijkheid betreft de bescherming en toegankelijkheid, maar ook de exclusiviteit (van informatie).

Bij het classificeren hanteren we de volgende uitgangspunten:
- De eigenaar (van de gegevens en het systeem) bepaalt het vereiste beveiligingsniveau;
- Informatie wordt geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Het classificeren van een bedrijfsproces, informatiesysteem of informatie wordt gedaan door het uitvoeren van een risicoanalyse;
- Als het om een wettelijke eis of norm gaat wordt deze expliciet vermeld (m.b.t. verantwoording);
- De eigenaar bepaalt wie toegang krijgt tot welke gegevens in de eigen applicatie;
- De vastgestelde classificaties hebben betrekking op alle onderdelen van onze informatievoorziening; gegevensverzamelingen, gegevensdragers, informatiesystemen, servers, netwerkcomponenten;
- Voor die onderdelen die buiten onze eigen infrastructuur zijn ondergebracht worden afspraken gemaakt met leveranciers conform het van toepassing zijnde classificatieniveau;
- Voor de toegang tot onze gegevens hanteren we het open, tenzij principe. Dit met het oog op de toegankelijkheid (transparantie), anders onnodig hoge kosten en lasten. Het ‘tenzij…’ wordt gespecificeerd op werkprocesniveau;
- Wanneer we informatie classificeren bepaalt deze classificatie ook het niveau voor de informatiesystemen waarin deze is ondergebracht of de service waarbinnen deze wordt geleverd. Een hogere classificatie geldt dan voor het hele systeem of dienst, tenzij er maatregelen zijn getroffen binnen dat systeem of die dienst;
- De classificaties zijn vastgelegd in het ISMS en worden regelmatig geëvalueerd door de CIB;
- Rechten worden bij voorkeur toegekend op basis van een rol (en niet op individuele basis);
- Richtlijnen voor classificatie zijn in overeenstemming met het toegangsbeleid.

9.2 Het classificatieproces

Het classificeren van bedrijfsprocessen, informatiesystemen en informatie omvat de volgende activiteiten:
- Het kiezen van het object van analyse en classificatie; dit kan variëren van een bedrijfsproces, een informatiesysteem tot informatie (database, document, gegevensverzameling);
- Het bepalen van de juiste klasse van beschikbaarheid, integriteit en vertrouwelijkheid voor het object van analyse door het uitvoeren van een risicoanalyse (Business Impact Analyse);
- Het vastleggen en bekend maken van de classificatie van het object van analyse aan alle betrokkenen, o.a. door het beschrijven van het object van analyse en vaststelling hiervan door de eigenaar;
- Het toepassen van de regels voor de beveiliging bij de uitvoering van het bedrijfsproces, c.q. het gebruik van het informatiesysteem of de informatie.

De juiste klasse van beschikbaarheid, integriteit en vertrouwelijkheid voor het object van analyse wordt bepaald door het uitvoeren van een risicoanalyse, zoals een BIA. Deze activiteit wordt verricht door of namens de eigenaar van het bedrijfsproces, het informatiesysteem of de informatie.

In bijlage 3 staat een drietal classificatieschema's als uitwerking van bovenstaande.

BIJLAGE 1 AUDITKADER INFORMATIEBEVEILIGING VEILIGHEIDSREGIO'S

Cluster	Control
1. Beleid en Organisatie	1.1 Beleidsregels voor informatiebeveiliging
	1.2 Beoordeling van het informatiebeveiligingsbeleid
	1.3 Verantwoordelijkheden gedefinieerd en toegewezen
	1.4 Classificatie van informatie
	1.5 Analyse en specificatie van informatiebeveiligingseisen
	1.6 Opnemen beveiligingsaspecten in leveranciersovereenkomsten
	1.7 Verantwoordelijkheden en procedures incidentmanagement
2. Personeel	2.1 Arbeidsvoorwaarden
	2.2 Bewustzijn, opleiding en training informatiebeveiliging
	2.3 Toegangsrechten intrekken of aanpassen
	2.4 'Clean desk'- en 'clear screen'-beleid
	2.5 Vertrouwelijkheids- of geheimhoudingsovereenkomst
3. Ruimten en apparatuur	3.1 Beleid voor mobiele apparatuur
	3.2 Fysieke toegangsbeveiliging
	3.3 Onderhoud van apparatuur
4. Continuïteit	4.1 Wijzigingsbeheer
	4.2 Beheersmaatregelen tegen malware
	4.3 Back-up van informatie maken en testen
	4.4 Beheer van technische kwetsbaarheden
	4.5 Beperkingen voor het installeren van software
	4.6 Respons op informatiebeveiligingsincidenten
	4.8 Informatiebeveiligingscontinuïteit implementeren
5. Toegangsbeveiliging	5.1 Beleid voor toegangsbeveiliging
	5.2 Registratie en afmelden van gebruikers
	5.3 Beperking toegang tot informatie
	5.4 Beveiligde inlogprocedures

6. Controle en logging	6.1 Beoordeling van toegangsrechten van gebruikers
	6.2 Logbestanden van beheerders en operators
	6.3 Naleving van beveiligingsbeleid en –normen
	6.4 Beoordeling van technische naleving
	6.5 Beheer van incidenten: leren van informatiebeveiligingsincidenten

BIJLAGE 2 TAKEN EN TAAKVERDELING BINNEN DE ORGANISATIE VAN INFORMATIEBEVEILIGING

Chief Information Security Officer

- Verantwoordelijk voor het laten opstellen, bijstellen, vernieuwen en herzien van het Informatiebeveiligingsbeleid;
- Formeel aanspreekpunt voor informatiebeveiligingszaken;
- Adviseren van bestuur en DT op strategisch niveau over informatiebeveiliging;
- De VRHM vertegenwoordigen in externe overleggen met andere CISO's;
- Toezien op de bewaking van de PDCA-cyclus m.b.t informatiebeveiliging.

Coördinator Informatiebeveiliging

- Op de hoogte blijven van ontwikkelingen op het gebied van informatiebeveiliging en zo
- nodig met voorstellen komen voor aanvullingen of verbeteringen van producten, methodieken of werkwijzen met betrekking tot de informatiebeveiliging;
- Beheren van het Informatiebeveiligingsbeleid en de uniformiteit hiervan; fungeren als aanspreekpunt op dit beleid;
- Bewaken en ondersteunen PDCA-cyclus met betrekking tot informatiebeveiliging;
    - Laten controleren van de werking en naleving van het informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen
    - Laten uitvoeren van periodieke beveiligingsaudits, risico-, afhankelijkheids- en kwetsbaarheidsanalyses
    - Adviseren van het (lijn)management bij de uitwerking van het informatiebeveiligingsbeleid in informatiebeveiligingsplannen voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen
    - Adviseren over de implementatie van het gewenste niveau van informatiebeveiligingsbeleid, door middel van concrete richtlijnen en praktische voorbeelden
    - Zorgdragen voor de actuele stand van zaken met betrekking tot informatiebeveiliging in het ISMS
- Optreden als informatiebeveiligingsadviseur bij nieuwe IV- en ICT-voorzieningen (binnen projecten) en bij ingrijpende veranderingen in de infrastructuur;
- Rapportages (van externe leveranciers) op het gebied van de beveiliging (laten) beoordelen
- Laten initiëren van (periodieke) informatiebeveiligingsbewustzijnprogramma"s en adviseren over voorlichting en training van gebruikers in het correct omgaan met informatie(systemen);
- Coördineren, monitoren en adviseren bij beveiligingsincidenten en zo nodig optreden bij calamiteiten; advisering bij de afhandeling ervan door beheerders en specialisten;
- Periodiek rapporteren van beveiligingsincidenten en de afhandeling daarvan aan de CISO en Portefeuillehouder
- Aanspreekpunt voor leveranciers bij incidenten of aan informatiebeveiliging gerelateerde ontwikkelingen

Functionaris gegevensbescherming (deels wettelijk vastgelegd)

- Voorbereiden van aanpassingen van het privacybeleid;
- Het bestuur, directie(s) en de werknemers die persoonsgegevens gebruiken, informeren en adviseren over hun verplichtingen ten aanzien de wettelijke vereiste bescherming van persoonsgegevens.
- Toezien op naleving van de: a. AVG, b. andere Europese of nationale gegevensbeschermingsbepalingen, en c. van het beleid van het bestuur met betrekking tot de bescherming van persoonsgegevens (inclusief van verantwoordelijkheden, bewustmaking en opleiding van de medewerkers, en de betreffende audits
- Bewustmaking en opleiding van het administratief personeel dat bij de verwerking van persoonsgegevens is betrokken;
- Coördineren en bewaken van het proces en de procedure Meldplicht Datalekken;

- Adviseren over een interne gedragscode die bijdraagt aan een juiste toepassing van de wettelijke verplichtingen;
- Het houden van toezicht op verwerkingen van persoonsgegevens
- Toezien op een adequate beveiliging van gegevens en adviseren over betrouwbare ICT (privacy by design);
- Bij het in gebruik willen nemen van nieuwe informatievoorzieningsonderdelen adviseren over het uitvoeren van een voorafgaand onderzoek om de gevolgen voor de privacy in kaart te brengen - zogenoemde gegevensbeschermingseffectbeoordeling (ook wel bekend als Privacy Impact Analyse, PIA);
- Informatievoorziening naar betrokkenen over hun rechten en plichten;
- Organiseren van een frequente zelfevaluatie en een jaarlijkse privacy-audit;
- Met de Autoriteit Persoonsgegevens (AP) samenwerken en voor de AP optreden als contactpunt inzake met verwerking van persoonsgegevens verband houdende aangelegenheden, en – waar passend - overleg plegen over enige andere aangelegenheid aangaande privacy.
- Organiseren, inrichten en/of onderhouden van het verwerkingsregister (dataregister) met alle verwerkingen persoonsgegevens binnen VRHM
- Het (laten) afhandelen van klachten inzake privacy.