Strategisch Informatie Veiligheidsbeleid Veiligheidsregio Fryslân 2023-2026

Veiligheidsregio Fryslân (VRF) staat voor een gezond en veilig Fryslân.
Zij hecht er belang aan dat haar cliënten en partners vertrouwen kunnen hebben in de wijze waarop zij hierbij omgaat met het gebruik van informatie. VRF voelt zich verantwoordelijk dat informatie die zij nodig heeft, ook beschikbaar en betrouwbaar is en dat gegevens die van cliënten en derden worden ontvangen zorgvuldig en rechtmatig worden gebruikt. Om dit te bewerkstelligen wordt geïnvesteerd in processen en maatregelen ter verbetering van de beschikbaarheid en kwaliteit van haar informatie en eveneens in processen ten aanzien van het goed omgaan met vertrouwelijke gegevens. Verder wordt aandacht gegeven aan de weerbaarheid van de VRF tegen inbreuken op gebied van informatieveiligheid en tevens aan het vergroten van het herstelvermogen bij incidenten op dit vlak.

Vastgesteld door het Dagelijks Bestuur van Veiligheidsregio Fryslân

Op: ……. *Handtekening: …….*

Versie 0.5
Datum 8-9-2022

Documentbeheer

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	4-5-2022	Ruijs	Eerste versie ter bespreking in BIO projectteam
0.2	23-5-2022	Ruijs	Versie t.b.v. afstemronde met zg. 'BIO afgevaardigden'
0.3	21-6-2022	Ruijs	Reactie van zg. 'BIO afgevaardigden' verwerkt
0.4	29-6-2022	Ruijs	Reactie van IM-stuurgroep 28-6 verwerkt
0.5	8-9-2022	Ruijs	Reactie van MT-ronde verwerkt

Gerelateerde documenten

Documenttitel	Omschrijving
Algemene Verordening Gegevensbescherming (AVG)	Europese privacy-verordening
Baseline Informatiebeveiliging Overheid (BIO)	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013
NEN 7510 – Informatiebeveiliging in de Zorg	Nederlandse richtlijn voor de zorgsector, gebaseerd op de internationale standaard ISO/IEC 27001:2013

Inleiding
Met dit document voor risicomanagement wil VRF voldoen aan norm van de BIO en NEN 7510. In deze normen is vastgelegd dat de organisatie beleidsregels dient te hebben op het gebied van informatieveiligheid. Deze beleidsregels zijn in dit document verwoord.

Scope en doelgroep
Dit beleid is van toepassing op alle informatie en informatiesystemen van VRF. De doelgroep bestaat uit managers en staffunctionarissen van VRF.

Rollen en verantwoordelijkheden
De CISO van VRF is verantwoordelijk voor de inhoud van dit beleidsdocument. Managers en proceseigenaren bij GGD zijn verantwoordelijk voor het toepassen van dit beleid.

Doelstelling volgens BIO
Het formuleren van beleid dat bijdraagt aan het minimaliseren van de risico's die een bedreiging vormen voor de doelstelling en de continuïteit van onze organisatie, haar taken en dienstverlening.

Onderhoud van het document
De CISO onderhoudt dit document en communiceert wijzigingen naar de betrokken stakeholders.

Inhoud

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatieveiligheidsbeleid van Veiligheidsregio Fryslân (VRF). Het beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en eventueel werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatie Veiligheidsbeleid 2023-2026' zet VRF een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen VRF te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid zijn de Baseline Informatiebeveiliging Overheid (BIO) en tevens de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG. Voor het GGD onderdeel van de organisatie zijn de (aanvullende) NEN normen voor Informatiebeveiliging in de Zorg het uitgangspunt.

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de afdelingsmanagers, de CISO, het dreigingsbeeld van de IBD, de eigen incidenten en de uitkomsten van risico-analyses en/of audits. In het plan staan dan ook de acties en planning vermeld om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft hoe de taken en verantwoordelijkheden in de VRF belegd zijn. Hoofdstuk 4 vat de BIO samen. Hoofdstuk 5 beschrijft de kritieke processen van VRF.

1.2 Wat is informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn de beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van VRF en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatie en informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op het bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties van onze organisatie.

1.3 Ambitie en visie

De missie en dienstverlening van VRF is gericht op een veilig en gezond Fryslân.
Met informatieveiligheid streven we hierin de volgende ambitie na:

- Waarborging van de kwaliteit, vertrouwelijkheid en continuïteit van de bedrijfsvoering en de primaire processen van de organisatie en mede ook van de interacties die zij heeft met haar ketenpartners en cliënten.
- Minimalisatie van de schade en de eventuele andere gevolgen voor de organisaties als gevolg van beveiligingsincidenten.
- Voldoen aan wet en regelgeving

Informatiesystemen zijn langzamerhand het zenuwcentrum geworden van onze organisatie. De dreigingen en de kwetsbaarheid van deze informatiesystemen vormen een groot risico, waarvan de

organisatie haar klanten en partners zeer nadelige gevolgen kunnen ondervinden. Het is dus zaak door middel van zowel preventieve als repressieve maatregelen deze risico's zoveel mogelijk te beperken.

VRF hecht er belang aan dat haar cliënten en partners vertrouwen kunnen hebben in de wijze waarop zij omgaat met informatie die zij over hen of van hen registreert. VRF voelt zich verantwoordelijk dat informatie die zij nodig heeft, ook beschikbaar en betrouwbaar is en dat gegevens die van cliënten en derden worden ontvangen zorgvuldig en rechtmatig worden gebruikt. Om dit te bewerkstelligen wordt geïnvesteerd in processen en maatregelen ter verbetering van de beschikbaarheid en kwaliteit van haar informatie en eveneens in processen ten aanzien van het goed omgaan met vertrouwelijke gegevens. Verder wordt aandacht gegeven aan de weerbaarheid van de VRF tegen inbreuken op gebied van informatieveiligheid en tevens aan het vergroten van het herstelvermogen bij incidenten op dit vlak.

Maar het zijn niet 'slechts' deze redenen waarom de VRF haar informatievoorziening moet beveiligen. Ook de wetgever stelt eisen. Zo worden in de Algemene Verordening Gegevensbescherming (AVG) eisen gesteld welke zich tegen "verlies of enige vorm van onrechtmatige verwerking van gegevens" richten. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking, dus ook tot externe gegevensverwerkers (bewerkers/verwerkers) in opdracht van VRF.

De kwaliteit van onze dienstverlening is gefundeerd met de kwaliteit van de gegevens die wij ten behoeve van deze dienstverlening gebruiken en vastleggen. De bescherming van de kwaliteit van deze gegevens is zeker ook een aandachtgebied waar informatiebeveiliging op toeziet.

Voor kritische gegevensverwerkingen is de inrichting van informatieveiligheid op zich ook niet meer voldoende, je moet je als organisatie ten opzichte van belanghebbenden kunnen verantwoorden dat er daadwerkelijk conform de regels is gewerkt. En je moet meebewegen, continu verbeteren en zicht blijven houden op zich ontwikkelende nieuwe dreigingen en kwetsbaarheden.

1.4 Beschikbaarheid, vertrouwelijkheid en integriteit

In informatiebeveiliging worden 3 aspecten van informatie beheerst, te weten:

1. Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers ervan;
2. Exclusiviteit/vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor diegenen die hiertoe geautoriseerd zijn;
3. Integriteit/betrouwbaarheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

In bijlage 1 zijn deze aspecten uitgewerkt in betrouwbaarheidscriteria en normklassen waarmee concreetheid gegeven kan worden aan afspraken op gebied van informatieveiligheid.

2. Strategisch beleid

2.1 Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatie Veiligheids Beleid' voor de jaren 2023 tot en met 2026. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

2.2 Actualisering beleid

Het beleid wordt elke 4 jaar herzien en wordt zo in sync gebracht met het Meer Jaren Beleids Plan (MJBP). Het Strategisch Informatie Veiligheids Beleid wordt tevens ondergebracht in de Planning en Control (P&C) cyclus. De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

2.2.1 De BIO en de NEN

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. Voor zorgorganisaties is een andere norm van toepassing, nl. de NEderlandse Norm (NEN) voor Informatieveiligheid in de Zorg. De normen zijn niet statisch maar veranderen mee met de laatste inzichten op gebied van informatieveiligheid. VRF zal derhalve ook meebewegen met de ontwikkeling van deze normen.

2.2.2 De 10 principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader van de BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

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

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen VRF-processen dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van VRF. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel. De 10 principes voor informatiebeveiliging zijn uitgewerkt in bijlage 2.

2.2.3 Dreigingsbeelden

De dreigingsbeelden van verschillende organisaties zoals van de gemeentelijke Informatie Beveiligingsdienst (IBD), Nationaal Cyber Security Center (NCSC) en Zorg-Computer Emergency Response Team (Z-Cert) geven een actueel zicht op incidenten en risicofactoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dreigingsbeelden zijn daarmee goede documenten om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging. Ook andere dreigingsbeelden kunnen hiervoor worden gebruikt.

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

VRF kent ook eigen registratiesystemen waarin (beveiligings)incidenten en datalekken worden vastgelegd. Deze systemen geven ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook goede input bij het actualiseren van het beleid.

2.2.5 Informatie uit risicoanalyses en/of audits

De bedoeling van het uitvoeren risicoanalyses is het identificeren van risico's waarbij in analyse wordt vastgesteld op welke wijze de risico's beheerst kunnen worden, of teruggebracht kunnen worden tot een aanvaardbaar niveau. Het permanent uitvoeren van risicoanalyses wordt risicomanagement genoemd en is zowel binnen de BIO als in de NEN, maar ook bijvoorbeeld vanuit de Harmonisering Kwaliteit Zorginstellingen (HKZ) een belangrijke voeding voor het verbeteren van de informatieveiligheid. Hetzelfde geldt voor audits op gebied van informatieveiligheid. Deze audits gaan uit van de van toepassing zijnde normen en worden periodiek uitgevoerd om de opzet, bestaan en werking van de beheersmaatregelen te toetsen.

2.2.6 Informatie over de context van de organisatie

De (veranderende) context van de organisatie geeft ook voeding aan het beleid, de beleidsplannen en prioriteiten op gebied van informatieveiligheid. Wie zijn bijvoorbeeld de klanten, zijn er nieuwe opdrachtgevers of ketenpartners en welke (aanvullende) eisen stellen zij eventueel op vlak van informatieveiligheid. Wat is het toepassingsgebied van het beleid en het managementsysteem voor informatieveiligheid. Welke onderwerpen binnen of buiten de organisatie zijn van belang om de doelstellingen op gebied van informatieveiligheid te behalen? In bijlage 3 is een overzicht opgenomen die inzicht geeft in deze context van de organisatie.

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001. De maatregelen uit hoofde van informatieveiligheid worden op basis van de NEN-ISO/IEC 27002 genomen.

Voor de ondersteuning van overheidsorganisaties zoals VRF bij het formuleren en realiseren van haar informatiebeveiligingsbeleid is in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht. Deze BIO is afgeleid van beide NEN-normen. De BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

De BIO gaat uit van 3 Basis Beveiligings Nivo's (BBN's).
-BBN1: minimaal beveiligingsnivo welke altijd van toepassing is voor overheidsinformatiesystemen
-BBN2: uitgangspunt voor overheidsinformatiesystemen
-BBN3: uitgangspunt voor overheidsinformatiesystemen die beveiligd zijn tegen statelijke actoren
VRF gaat voor de beveiliging van haar informatie en informatiesystemen uit van minimaal het nivo BBN2.

Voor zorgorganisaties is een andere norm van toepassing, nl. de NEderlandse Norm (NEN) voor Informatieveiligheid in de Zorg. Deze norm is in onze organisatie voor m.n. de GGD van toepassing. Deze norm valt weer uiteen in onderstaande subsets:
-NEN 7510 Informatieveiligheid in de Zorg,
-NEN 7512 Vertrouwensbasis voor gegevensuitwisseling
-NEN 7513 logging op patiëntdossiers,
-NTA 7516 E-mailen in de zorg
De NEN is niet vrijblijvend: zorginstellingen in Nederland moeten o.a. aan de Inspectie Gezondheidszorg en Jeugd (IGJ) kunnen aantonen dat ze beschikken over de juiste informatiebeveiliging. Bij deze toetsing vormt de NEN 7510 de leidraad.

GGD gaat voor de beveiliging van persoonsgegevens in (zorg)informatiesystemen uit van minimaal het nivo BBN2 aangevuld met het BIV classificatienivo B2I2V2+. Dit betreft dan het beschermingsnivo behorende bij bijzondere categorieën van persoonsgegevens zoals genoemd in artikel 9 AVG, niet zijnde de medische/zorg gegevens en het betreft hier persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals genoemd in artikel 10 AVG.

GGD gaat voor de beveiliging van medische persoonsgegevens in zorginformatiesystemen uit van minimaal het nivo BBN2 aangevuld met het BIV classificatienivo B2I2V3. Dit betreft dan het beschermingsnivo behorende bij medische/zorg gegevens die onder een medisch beroepsgeheim vallen en ook gegevens waarop een wettelijk bepaalde geheimhoudingsplicht rust, zoals tijdens een strafrechtelijk onderzoek. Op deze gegevens zijn boven de standaard BIO-BBN2 controls en maatregelen, de hierop aanvullende NEN normen voor zorginformatie van toepassing.

2.4 ISMS

De moderne kijk op Informatieveiligheid vereist dat een organisatie een Information Security Management System (ISMS) heeft ingericht. Het doel van dit ISMS is het stelselmatig en ook procesmatig sturen, ontwikkelen, verbeteren en borgen van de informatieveiligheid bij VRF.
Een ISMS omvat een PDCA (Plan, Do, Check, Act) gerichte verbetercyclus voor informatieveiligheid. Een vast onderdeel van die verbetercyclus, en in feite de basis van het ISMS, is de uitvoering van ISO 27001 risicoanalyses. Daarmee worden specifieke interne en externe organisatierisico's rondom informatiebeveiliging in kaart gebracht en vervolgens verlaagd door passende beveiligingsmaatregelen. Het management maakt hierbij continu afwegingen en keuzes of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.5 Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om een aantal uitgangspunten te formuleren en om daarmee de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacybescherming op tactisch en operationeel niveau. Hierbij kan gedacht worden aan zaken als het formuleren van beleid rondom het begrip risicomanagement, het beleid voor toegangsbeveiliging, het beleid omtrent gebruik en beveiliging van mobiele apparatuur, het implementeren van een meldingsprocedure voor informatie-beveiligingsincidenten of het implementeren van een afhandelingsprocedure voor datalekken.

2.6 Scope informatiebeveiliging

De scope van dit beleid omvat alle VRF-processen, de onderliggende informatiesystemen, de informatie en gegevens van VRF (in eigen huis als in de cloud) en tevens haar gegevensdelingen met externe partijen (bijvoorbeeld met de meldkamer of een zorgpartij), het gebruik van VRF informatie en informatiesystemen door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategisch VRF Informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullend) beleid, zoals bijvoorbeeld voor de omgang met patiënt- en kinddossiers, het gebruik van zorg-uitwisselingssystemen of voor het gebruik van C2000. Deze aanvullingen zijn in (externe) (wets) documenten geformuleerd. Hier is geen limitatief overzicht van zulk beleid opgenomen.

2.7 Uitgangspunten

Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid sluit aan bij het algemene beleid van VRF en sluit aan bij de relevante landelijke en Europese wet- en regelgeving.

Het bestuur, de directie en het afdelingsmanagement spelen een cruciale rol bij het uitvoeren van het informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor VRF heeft, de risico's die VRF hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management (aanvullend) beleid voor informatiebeveiliging op en ondersteunt en bewaakt de uitvoering ervan.

Het management van VRF geeft duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door o.a. het uitdragen en handhaven van het informatiebeveiligingsbeleid van en voor de hele VRF.

2.7.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het beschermen van de bedrijfsprocessen en het waarborgen van een veilige informatievoorzieningen.
- Het beschermen en correct verwerken van persoonsgegevens van cliënten en medewerkers.
- Het adequaat beschermen van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het beheersen van de toegang tot informatiesystemen.
- Het voorkomen van ongeautoriseerde toegang tot informatiesystemen en (persoons)informatie.
- Het adequaat reageren op incidenten en datalekken.

2.7.2 Belangrijke uitgangspunten

Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan en privacyplan het fundament onder een veilige informatievoorziening. In het informatiebeveiligingsplan en privacyplan worden de veiligheid en vertrouwelijkheid van de informatievoorziening organisatiebreed benaderd. Deze plannen worden periodiek bijgesteld op basis van o.a. nieuwe ontwikkelingen, dreigingen, registraties in het incidentenregister en informatie uit risicoanalyses en audits.

De belangrijkste uitgangspunten van het beleid zijn:

- Alle informatie en informatiesystemen zijn van belang voor VRF, bepaalde informatie is van vitaal en kritiek belang.
- Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging en privacybescherming van VRF.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen de basis van het managementsysteem voor informatiebeveiliging welke onderdeel is van het integrale management- en risicomanagementsysteem van VRF.
- De directie verbindt zich te blijven voldoen aan de van toepassing zijnde eisen in verband met informatiebeveiliging. Zij richt hiervoor een managementsysteem voor informatiebeveiliging in dat voldoet aan de BIO/NEN norm.
- De directie draagt zorg voor de Governance op informatieveiligheid door toewijzing van taken, verantwoordelijkheden en bevoegdheden (TVB) in de processen van VRF en draagt tevens zorg voor rapportage omtrent de prestaties van het managementsysteem voor informatieveiligheid aan de directie.

- Verantwoordelijkheden voor informatieveiligheid zijn vastgelegd en in het DT vastgesteld.
- De directie stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- De directie stelt een informatiebeveiligingsmanagementforum in, om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van (gezondheids)informatie.
- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het management/afdelingshoofden.
- Alle informatiebronnen en -systemen die gebruikt worden door VRF hebben een interne (proces, systeem, data) eigenaar die via toets- en/of classificatie de vertrouwelijkheid, beschikbaarheid en integriteits-eis bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de classificatie en daarmee de bescherming van informatie op het vereiste nivo ligt bij de eigenaar van de informatie.
- Het management/afdelingshoofden zijn eveneens verantwoordelijkheden voor de veiligheid van ketens van informatiesystemen.
- Het management/afdelingshoofden dragen verder zorg voor de bevordering van het beveiligingsbewustzijn bij de medewerkers.
- Medewerkers, zowel vast als tijdelijk, intern of extern, zijn verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken of risico's hiervan melding te maken.

2.7.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

- Het Dagelijks Bestuur stelt als eindverantwoordelijke dit informatiebeveiligingsbeleid vast.
- De directie evalueert 4-jaarlijks het vigerende informatiebeveiligingsbeleid.
- De directie stelt jaarlijks het informatiebeveiligingsplan en het privacyplan vast.
- De directie is verantwoordelijk voor het laten uitwerken en uitvoeren van generieke en onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directie is verantwoordelijk voor het vragen om informatie bij de afdelingsmanagers en ziet erop toe dat de afdelingsmanagers adequate maatregelen genomen hebben voor de bescherming van de informatie en informatiesystemen die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de veiligheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de directie.
- De Functionaris Gegevensbescherming (FG) ziet vanuit een onafhankelijke positie toe op de bescherming van de vertrouwelijkheid van informatie en rapporteert hierover rechtstreeks aan directie.
- In de P&C cyclus dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de proceseigenaren, FG en CISO. De onderwerpen, die als risicovol of onvolwassen worden gezien, moeten worden opgenomen in de auditplannen.
- De afdelingsmanagers zijn verantwoordelijk voor de uitvoering van het risicomanagement en de informatieveiligheid voor de processen waarvoor zij verantwoordelijk zijn.
- De beveiligingsmaatregelen worden mede bepaald op basis van risicomanagement. Managers voeren (diepgaande) risicoanalyses op informatiebeveiliging uit op basis van de BIO of NEN om risico-afwegingen te kunnen maken.
- Managers dienen erop toe te zien dat de controle op het rechtmatig verwerken van persoonsgegevens regelmatig wordt uitgevoerd.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- Medewerkers van VRF zijn getraind in het gebruiken en naleven van beveiligingsprocedures.

2.7.4 Randvoorwaarden

Belangrijke randvoorwaarden voor informatieveiligheid zijn verder:

- De informatiebeveiliging maakt deel uit van afspraken met leveranciers en ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging wordt actief bevorderd en geborgd.
- De organisatie zorgt voor aanwijzing van de CISO in een formele, onafhankelijk gepositioneerde functie en zorgt voor aanwijzing van ondersteunende rollen bij de proceseigenaren op gebied van privacy en information security
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CIO en CISO, gebaseerd op:
    - de uitkomsten van de risico-analyses en periodieke audits
    - de belangrijkste aandachtsvelden uit het privacyplan
    - de dreigingsbeelden van o.a. de IBD, NCSC, Z-Cert e.a;
    - de trends in het register met beveiligingsincidenten
- Jaarlijks wordt een privacyplan opgesteld onder leiding van de CIO en FG.

2.8 Verantwoording

De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de bestuurlijk portefeuillehouder en/of het bestuur. De directie rapporteert hierbij tevens over de mate waarin zij invulling heeft gegeven aan het uitwerken van tactische beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

2.8.1 Audit

De verantwoording over informatiebeveiliging geschiedt tevens middels audits.
Dat betekent dat er periodiek een audit wordt uitgevoerd en dat de informatie die nodig is voor het beantwoorden van vragen binnen de audit wordt opgehaald bij de verantwoordelijke afdelingsmanagers. De afdelingsmanagers leveren tijdig alle informatie die nodig is voor het invullen van de auditvragenlijsten. De centrale aansturing van deze audits is door directie expliciet belegd bij een afdelingsmanager en/of bij de concerncontroller.

3. Organisatie, taken & verantwoordelijkheden

3.1 Algemeen

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatieveiligheid op welke plaats belegd dienen te zijn binnen onze organisatie.

In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie hoofdrollen: de Secretaris/algemeen directeur, de proceseigenaar en de dienstenleverancier. Deze rollen zijn beschreven vanuit het perspectief van informatiebeveiliging. Het gaat hierbij om de verantwoordelijke voor de uitvoering van de BIO-controls.

Hoofdrollen in de BIO

Algemeen directeur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.
Proceseigenaar	Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
Diensten leverancier	Bedoeld wordt de dienstenleverancier (bv Shared Servicecenter) binnen de overheid of organisaties in de markt waaraan de algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt of uitbesteedt.

In de BIO staat aangegeven welke controls voor welke rol toepasselijk zijn. De BIO verplicht om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding.

Belangrijke ondersteunende rollen hierbij zijn weggelegd voor de CISO, de ISO, en de FG welke met name adviseren, coördineren en tevens toezien dat het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Het geheel wordt daarbij periodiek door een (interne/externe) Controller of auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.2 Bestuur

Dit Strategisch Beleid is een verantwoordelijkheid van het bestuur van VRF. Het beleid wordt vastgesteld in het Dagelijks Bestuur. Het bestuur van VRF stelt een portefeuillehouder informatievoorziening aan die tevens toeziet op de invoering en instandhouding van informatieveiligheid bij VRF en verantwoordelijkheid over de aansturing toewijst aan de directeur. De Auditcommissie adviseert het bestuur van de VRF over informatieveiligheid.

3.3 Directeur

De directeur(en) van VRF zal volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie. De directeur zorgt dat ketens van verwerkingen en alle daarbij horende processen en systemen en middelen altijd onder de verantwoordelijkheid vallen van een afdelingsmanager. De directie zorgt dat de afdelingsmanagers zich verantwoorden over de veiligheid en privacy van de informatie(voorziening) die onder hen berust. De directie zorgt dat de portefeuillehouder in het bestuur gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de organisatie

De directie stelt het door afdelingsmanagers aanbevolen beschermingsnivo (de BBN-toets, voor NEN en/of de BIV-classificatie) vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen. Informatiebeveiliging wordt door directie gezien als onderdeel van het integraal risicomanagement (directiebeoordeling) van VRF

De directie informeert de ondernemingsraad omtrent het informatiebeveiligingsbeleid en de hieruit voortvloeiende maatregelen en richtlijnen die een relatie hebben met medezeggenschap.

De directie stelt jaarlijks budget beschikbaar voor het ISMS, voor risicomanagement en risicomitigatie en voor de periodieke audits op gebied van informatieveiligheid.

3.4 Proceseigenaren

Informatiebeveiliging valt onder de expliciete verantwoordelijkheid van afdelingsmanagers. Afdelingsmanagers zijn door directie in de rol van proceseigenaar aangewezen en daarmee verantwoordelijk gesteld voor de invoering en instandhouding van de BIO/NEN normen in hun processen. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden eventueel wel. Zij dragen derhalve zorg voor voldoende kennis, mensen en middelen in het eigen organisatiedeel om deze verantwoordelijkheid waar te maken.

Alle processen, systemen, data, applicaties hebben altijd één (proces)eigenaar; er moet dus altijd iemand verantwoordelijk zijn. Proceseigenaren rapporteren als onderdeel van de P&C cyclus aan de directie over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen cq medewerkers over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het (afdelings/team/werk)overleg.

Belangrijke taken van de proceseigenaren in het kader van informatiebeveiliging zijn:

- Het beschermen van (ketens van) informatie, informatiesystemen en informatievoorziening die binnen hun eigenaarschap valt.
- Het vroegtijdig signaleren van de voornaamste risico's waaraan de informatie en informatievoorziening is blootgesteld en het nemen van maatregelen.
- Het bij medewerkers (laten) uitdragen van het beveiligingsbeleid en de daaraan gerelateerde instructies en procedures.
- Behandelen van beveiligingsincidenten en nemen van geëigende maatregelen.
- Het afsluiten van (verwerkers) contracten met leveranciers van IT-voorzieningen en het maken van afspraken met interne dienstenleveranciers, met passende aandacht voor informatieveiligheid en het uitvoeren van leveranciersmanagement hier op.
- Het leveren van input op beleid en maatregelen in het kader van informatieveiligheid.

3.5 Dienstenleveranciers

Het gaat hier om de dienstenleverancier binnen de VRF of organisaties in de markt waaraan de directeur of proceseigenaar (een deel van) de beveiligingstaak heeft inbesteed, respectievelijk uitbesteed. Een voorbeeld van een (interne) dienstenleverancier is de IT-afdeling of de HR-afdeling. Een voorbeeld van een externe dienstenleverancier is bijvoorbeeld Topicus of Afas.

Er wordt in beginsel geen onderscheid gemaakt in interne of externe dienstenleveranciers.
Bij de wijze waarop verantwoording wordt afgelegd over hun diensten worden interne en externe dienstenleveranciers gelijk behandeld. Dit betekent voor alle dienstenleveranciers het volgende:

- Periodiek leggen alle dienstenleveranciers verantwoording af via een Statement of Compliancy aan de opdrachtgever bij de VRF
- Naast de verantwoording over hun diensten zijn de dienstenleveranciers ook zelf als organisatie gebonden aan informatiebeveiligingsregels. Hierbij is wel een onderscheid aanwezig tussen interne en externe dienstenleveranciers:
- Interne dienstenleveranciers zijn, als onderdeel van de VRF, zelf ook rechtstreeks gebonden aan de BIO/NEN. De interne dienstenleverancier is ook gebonden aan het jaarlijks opleveren van een In Control Verklaring (ICV). Hierin verklaart de dienstenleverancier dat hij voor zijn eigen bedrijfsvoering aan de BIO/NEN voldoet
- Externe dienstenleveranciers zijn geen onderdeel van VRF en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO of het opleveren van een ICV. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd.

Het is mogelijk dat een (externe) dienstenleverancier beschikt over een ISO27001-certificering, ISAE3402-certificering of een ander kwaliteitskeurmerk. Een dergelijk keurmerk geeft een waarborg over het proces dat bij de dienstenleverancier is ingericht, maar geeft niet aan op welk niveau de beveiliging is gerealiseerd. Hoewel dit dus wel meerwaarde heeft, overlap kent met de BIO/NEN-controls en gebruikt kan worden als onderdeel van de Statement of Compliancy, omvat en vervangt het niet volledig de verantwoording over de maatregelen uit de BIO/NEN. Er zullen dus altijd aanvullende afspraken gemaakt moeten worden en hierover moet ook worden verantwoord.

PIOFAH

In de informatiebeveiliging wordt de acroniem PIOFAH gebruikt om te duiden dat bepaalde beveiligingsmaatregelen thuis horen bij een VRF-brede actor die verantwoordelijk is voor een onderdeel van de bedrijfsvoering binnen de VRF. PIOFAH staat voor Personeel, Inkoop, Organisatie, Financiën, Automatisering, Huisvesting. De managers van deze processen hebben een afgeleide verantwoordelijkheid voor bepaalde beveiligingstaken. De proceseigenaren maken afspraken met deze interne dienstenleveranciers over de inrichting van informatieveiligheidsmaatregelen.

Personeel

De verantwoordelijke voor 'Personeel' draagt zorg voor maatregelen, betrekking hebbend op 'veilig personeel' zoals (beveiligings)procedures met betrekking tot in-, door-, en uitstroom, het beheer van (beveiligings) functieprofielen, de beoordelingssystematiek met aandacht voor beveiligings-verantwoordelijkheid, het bijhouden van bekwaamheidsontwikkelingen op gebied van informatieveiligheid etc.

Organisatie

De verantwoordelijke voor 'Organisatie' draagt zorg voor maatregelen, betrekking hebbend op de organisatie bv. de organisatie van informatieveiligheid, zoals functies, functiescheiding, competenties en de inrichting van processen die samenhangen met- of ondersteunend zijn aan informatieveiligheid, denk aan bv P&C cyclus, risicomanagement, procesmanagement, integraal management, projectmanagement, kwaliteitszorg, continuïteitszorg etc.

Inkoop

De verantwoordelijke voor 'Inkoop' draagt mede zorg voor maatregelen, betrekking hebbend informatieveiligheid bij verwervingen en het hier uit volgende leveranciersmanagement. Onderdelen hierin zijn het onderhandelen met leveranciers over inkoop- en verkoopvoorwaarden, beveiligingseisen in contracten, overeenkomsten, SLA's, rapportages en bijvoorbeeld het ondersteunen bij het leveranciersmanagement, mede via de zg. In Controle Verklaringen (ICV's).

Automatisering
De verantwoordelijke voor 'Automatisering' draagt zorg voor maatregelen betrekking hebbend op zg. technische informatieveiligheid. Bijna alle technische informatiebeveiligingsmaatregelen worden uitgevoerd door de afdeling ICT of zijn door de proceseigenaar uitbesteed aan een externe dienstenleverancier. De afdeling ICT draagt typisch zorg voor het beveiligen van de bij VRF zelf geplaatste informatie, informatiesystemen, netwerken en eindpunten en het regelen van de toegang tot informatiesystemen. Daarnaast draagt zij ook zorg voor voldoende herstel mogelijkheden bij incidenten en calamiteiten op gebied van informatievoorziening.

Huisvesting
De verantwoordelijke voor huisvesting neemt de maatregelen betreffende onder andere de fysieke beveiliging, de fysieke toegangsbeveiliging van bedrijfslocaties, de brandbeveiliging, de infrastructuur en nutsvoorzieningen, werkplekken, bedrijfsmiddelen en faciliteiten.

Financiën
De verantwoordelijke voor financiën neemt beveiligingsmaatregelen die specifiek samenhangen met de financiële functie/verantwoording denk hierbij bijvoorbeeld aan het zeker stellen van de rechtmatigheid van uitgaven door middel van functiescheiding en het toewijzen van autorisaties.

3.6 CISO

De beveiligingsfunctionaris oftewel CISO (Chief Information Security Officer) adviseert de directeur en het bestuur op gebied van informatieveiligheid. De CISO bewaakt de uniformiteit van het informatiebeveiligingsbeleid binnen de organisatie. Adviseert leidinggevenden en proceseigenaren bij de vertaling van beleid naar tactische plannen en maatregelen. De CISO heeft volgens de normen een eigenstandige functiebeschrijving en is door directie in die functie aangesteld en passend voor die functie in de organisatie gepositioneerd. De CISO:

- is verantwoordelijk voor het opstellen en beheren van het informatiebeveiligingsbeleid;
- ziet toe op de planning en realisatie van het beleid.
- draagt zorg voor een managementsysteem voor informatieveiligheid
- adviseert bij de afhandeling van beveiligingsincidenten.

3.7 ISO

De Information Security Officer (ISO of domein ISO) is een lokale rol in die in organisatie (domeinen) van de afdelingsmanagers (proceseigenaren) ondersteunend is bij de uitvoering van de taken van die afdelingsmanagers op gebied van risicobeheersing en informatieveiligheid.

3.8 CIO

De Chief Information Officer (CIO) is de door de directeur aangewezen functionaris die verantwoordelijk is voor de ontwikkeling van de informatievoorziening en informatie technologie bij (van) VRF. De CIO heeft een belangrijker rol bij het adviseren en formuleren van strategische doelen op dit vlak. Vanuit deze rol vervult de CIO namens de algemeen directeur tevens een ondersteunende en bevorderende rol op gebied van beleids- en besluitvoorbereiding van Informatieveiligheid binnen de VRF. Vanuit deze rol acteert de CIO als hoogst adviseringsorgaan op gebied van informatievoorziening voor directie. Geeft vanuit die rol ook inhoudelijke begeleiding en sturing aan de verschillende proceseigenaren (en leveranciers) bij VRF bij de implementatie van informatieveiligheid.

3.9 FG

De Functionaris Gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG) en de daarvan afgeleide 'Privacyreglementen Veiligheidsregio Fryslân'. De FG adviseert ter verbetering van de bescherming van persoonsgegevens.

3.10 Concerncontroller

De concerncontroller is o.a. verantwoordelijk voor de inrichting en executie van risicomanagement. Hiervoor ontwerpt en implementeert hij een proces om bedrijfsrisico's te inventariseren, te duiden en te beheersen. Het uitvoeren van interne audits maakt hiervan onderdeel uit.

De concerncontroller houdt toezicht op de werking van het managementsysteem van VRF.
Dit managementsysteem richt zich op de sturing en beheersing van de organisatie als geheel, om zo de strategische doelstellingen van VRF te bereiken. De P&C (planning en Control) cyclus en het risicomanagement vormen ankers van dit managementsysteem. Informatieveiligheid is onderdeel van dit managementsysteem.

De concerncontroller draagt zorg voor de periodieke beoordeling van het informatieveiligheidsbeleid. De beoordeling (audit) beperkt zich in beginsel tot de beoordeling van het beleid en de werking er van (is adequaat beleid aanwezig, is het geïmplementeerd, en werkt het?). Indien gewenst kan in opdracht van Bestuur of Directeur diepgaander onderzoek worden uitgevoerd.

3.11 Medewerkers

Medewerkers (aangesteld, ingehuurd) gaan actief om met informatieveiligheid. Medewerkers zijn ook zelf verantwoordelijk voor het kennisnemen en naleven van de richtlijnen op gebied van informatiebeveiliging. Medewerkers zijn verplicht om door hen geconstateerde beveiligingsincidenten en beveiligingsrisico's te melden.

4. Baseline Informatieveiligheid Overheid

4.1 Inleiding

De komst van de Baseline Informatiebeveiliging Overheid (BIO) betekent niet dat we helemaal opnieuw moeten beginnen. Het grootste deel van het vigerende beveiligingsbeleid blijft van kracht. De benadering van de BIO is wel anders. Deze gaat meer uit van het hanteren van risicomanagement. De proceseigenaar maakt, op basis van een analyse, de keuze welk beveiligingsniveau passend is voor de processen en de onderliggende informatiesystemen waar hij of zij verantwoordelijkheid voor draagt. Daarmee komt de sturing op informatiebeveiliging door de leidinggevende nadrukkelijker in beeld. Dit hoofdstuk beschrijft nader wat dit betekent en gaat in hoofdlijnen in op de tactische beheersmaatregelen die daarbij een rol spelen.

4.2 Basis beveiligingsniveaus

In de BIO wordt het begrip basis beveiligingsniveau (BBN) geïntroduceerd. Er worden 3 niveaus onderscheiden.

Voor BBN1 ligt de nadruk op “wat mag minimaal verwacht worden?”. Het gaat dan om een minimale set beveiligingsmaatregelen die past bij informatie die niet heel gevoelig of van groot belang voor de bedrijfsvoering is. De maatregelen kom voort uit wet- en regelgeving en algemeen geldende beveiligingsprincipes.

Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe “valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?” Dit niveau is passend voor vertrouwelijke informatie (privacy, commercieel vertrouwelijk) en/of informatie die belangrijk is voor de bedrijfsvoering. Het is tevens van toepassing als incidenten mogelijk leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en/of de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

BBN3 is van toepassing op gerubriceerde informatie, waarbij weerstand tegen statelijke actoren of vergelijkbare bedreigers nodig is. Dit betreft het hoogste niveau om gegevens die bijzonder gevoelig zijn en/of van cruciaal belang te beveiligen tegen ongeautoriseerde toegang, beschadiging en vernietiging.

Wanneer het BBN is bepaald door de proceseigenaar komen de beheersmaatregelen uit de BIO in beeld welke van toepassing zijn en moeten de operationele beveiligingsmaatregelen in werking worden gesteld die daarbij horen. Veelal zullen dit bekende maatregelen zijn omdat die ook al hoorden bij de eerder gehanteerde NEN beheersmaatregelen. Het BBN wordt bepaald met het doorlopen van de BBN-toets. Dit is een basis risico-afweging in de vorm van een vragenlijst.

4.3 Verplichte maatregelen

Een deel van de beheersmaatregelen is uitgewerkt in verplichte beveiligingsmaatregelen (in de BIO overheidsmaatregelen genoemd), omdat zij:

- voortvloeien uit wet- en regelgeving. Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;
- zo basaal zijn dat zij het fundament vormen van een betrouwbare c.q. professionele informatievoorziening;

- dienstbaar zijn aan de beveiliging in een procesketen of -netwerk; niet-naleving door een enkele organisatie is per saldo niet effectief voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit niet efficiënt. Voor een generieke dienst geldt een afweging die analoog is aan het ketenvraagstuk. In het geval dat een maatregel voor een specifiek geval niet van toepassing kan zijn vervalt de verplichting.

VRF dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit omvat uitleg volgens het 'pas toe of leg uit' principe. Daarbij worden de daaruit voortvloeiende risico's tevens aangegeven.

4.4 Verantwoording

Verantwoording over de juiste toepassing van de BIO is afhankelijk van basisbeveiligingsniveau. De BIO bepaalt dat het management vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.

- voor BBN1 is de proceseigenaar volledig verantwoordelijk voor het nemen van (verstandige) beslissingen. Slechts incidenteel en op verzoek informeert deze de CISO over de stand van zaken met betrekking tot zijn BBN1 informatiesystemen.
- voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp/ontwikkelfase) ter consultatie voorlegt aan de CISO.
- voor BBN3 geldt dat vooraf toestemming verleend moet worden door de Algemeen directeur voor het verwerken van bijzondere informatie.

Voor het verlenen van toestemming is mandatering mogelijk naar bijvoorbeeld de directeur Bedrijfsvoering, de CIO of de CISO.

4.5 Ketensamenwerking en dienstenleveranciers

De BIO zegt ook iets over ketensamenwerkingen en over dienstenleveranciers.

Ketensamenwerkingen

Binnen de overheid en met andere externe partijen wordt veel in ketens samengewerkt en daarom vormt de gemeenschappelijke veiligheid van informatieketens ook een basis voor de concretisering van overheidsmaatregelen.

Een keten is een samenwerkingsverband tussen organisaties die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) doelstellingen nastreven. Deze ketenpartners zijn zelfstandig, maar zijn ook afhankelijk van elkaar waar het gaat om het bereiken van de gezamenlijke (keten)doelstellingen. Een informatieketen betreft de uitwisseling van informatie binnen zo'n samenwerkingsverband.

In het geval dat informatie aan ketenpartners wordt toevertrouwd, blijft VRF er verantwoordelijk voor dat ketenpartners de toevertrouwde informatie zorgvuldig beschermen. VRF moet daarom (aansluit) voorwaarden eisen of stellen aan de leverende of afnemende partij. Tevens moet VRF leveringsgaranties bieden aan de afnemende partij. VRF moet hiervoor inzichtelijk hebben van welke informatiesystemen en infrastructuren zij afhankelijk is, welke informatiesystemen afhankelijk zijn van haar en hoe het beheer van beiden hierop is ingericht.

Dienstenleveranciers

In de BIO wordt bij het van toepassing verklaren van beheersmaatregelen en overheids-maatregelen geen onderscheid gemaakt in interne of externe dienstenleveranciers. Ook bij de wijze waarop verantwoording wordt afgelegd over hun diensten worden interne en externe dienstenleveranciers gelijk behandeld. Dit betekent voor alle dienstenleveranciers het volgende.

- Periodiek leggen alle dienstenleveranciers verantwoording af aan de opdrachtgever bij de VRF.
- De dienstenleveranciers volgen de beveiligingseisen die de VRF of ketenpartners stellen aan de diensten van de dienstenleverancier. Uit efficiëntieoverwegingen kan een dienstenleverancier een standaard beveiligingsniveau aanbieden, maar dit doet geen afbreuk aan de genoemde verantwoordelijkheid van de overheidsorganisaties.
- Voor diensten die aan één organisatieonderdeel worden aangeboden, legt de dienstenleverancier verantwoording af aan de opdrachtgever.
- Voor diensten die aan meerdere organisatieonderdelen worden aangeboden stelt de dienstenleverancier één verantwoording op ten behoeve van alle afnemers.

Naast de verantwoording over hun diensten zijn de dienstenleveranciers ook zelf als organisatie gebonden aan informatiebeveiligingsregels. Hierbij is wel een onderscheid aanwezig tussen interne en externe dienstenleveranciers:

- Interne dienstenleveranciers zijn, als onderdeel van VRF, zelf ook rechtstreeks gebonden aan de BIO. Ze zijn daarmee gehouden aan de reguliere verantwoording en toezichtprocedures van VRF. De interne dienstenleverancier is ook gebonden aan het jaarlijks opleveren van een In Control Verklaring (ICV). Hierin verklaart de dienstenleverancier dat hij voor zijn eigen bedrijfsvoering aan de BIO voldoet (inclusief de overheidsmaatregelen).

- Externe dienstenleveranciers zijn geen onderdeel van de overheid en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO of het opleveren van een ICV. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd.

4.6 Beheersmaatregelen

De beheersmaatregelen van de BIO zijn ingedeeld in de volgende hoofdstukken:
- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

4.6.1 Informatiebeveiligingsbeleid

Er is beleid nodig om informatiebeveiliging succesvol onderdeel te laten zijn van de bedrijfsvoering. Het biedt de directie een instrument om dit aan te sturen. Het beleid moet voldoende kwaliteit hebben en aansluiten bij de actualiteit. Evaluatie dient daarom regelmatig plaats te vinden.

4.6.2 Organiseren van informatiebeveiliging

Informatiebeveiliging ontstaat niet vanzelf en moet dus worden georganiseerd. Rollen en verantwoordelijkheden moeten helder zijn en er moet deskundige ondersteuning aanwezig zijn. Zie hiervoor o.a. ook het voorgaande hoofdstuk.

4.6.3 Veilig personeel

Om veilig te werken met de informatievoorziening moeten medewerkers aan (integriteits-)eisen voldoen en voldoende geëquipeerd zijn. Dat begint al voorafgaand aan de daadwerkelijke indiensttreding, waarbij wordt onderzocht of er mogelijk redenen zijn om de beoogde medewerker de toegang te ontzeggen. Arbeidsvoorwaarden, opleiding en training waarborgen dat bij de medewerkers voldoende bewustzijn is van de risico's die samenhangen met het werken met gegevens van de overheid. Daarbij dient VRF disciplinaire procedures te hebben ingericht als er, vanwege schendingen, moet worden opgetreden. Dit geldt zowel voor eigen medewerkers als voor ingehuurd personeel en externe gebruikers. Bij beëindiging of wijziging van het dienstverband gaat het om het bewerkstelligen dat betrokkenen de organisatie, vanuit het oogpunt van informatiebeveiliging, ordelijk verlaten dan wel dat wijziging van het dienstverband ordelijk verloopt.

4.6.4 Beheer van bedrijfsmiddelen

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen en dienen beschermd te worden. Van belang is dat alle relevante bedrijfsmiddelen bekend, geregistreerd en voorzien zijn van een eigenaar en duidelijk is wie verantwoordelijk is voor het handhaven van geschikte beveiligingsmaatregelen. Een categorie die daarbij speciale aandacht verdient wordt gevormd door de verwijderbare media zoals usb-sticks, geheugenkaartjes, externe harde schijven en back-upmedia. Ook de media die niet langer nodig zijn en dus moet worden afgevoerd verdient een zorgvuldige behandeling. Gegevensclassificatie naar de mate van beschikbaarheid, integriteit en vertrouwelijkheid is belangrijk om de juiste beveiligingsmaatregelen toe te passen. Het heeft weinig zin om gegevens die van minder belang zijn zwaar te beveiligen. Dat brengt onnodige moeite en kosten met zich mee. Aan de andere kant moeten gegevens die van groot belang en/of van gevoelige aard zijn uiteraard wel goed worden beschermd. De eigenaar van de gegevens bepaalt het niveau van classificatie en houdt daarbij eveneens rekening met wettelijke eisen.

4.6.5 Toegangsbeveiliging

Logische toegangsbeveiliging is het geheel aan maatregelen met als doel de toegang tot gegevens en informatiesystemen van VRF te beheersen, zodat gegevens, informatiesystemen en middelen worden beschermd tegen ongeautoriseerde handelingen. Belangrijke aandachtsgebieden zijn:

- het definiëren van toegangsbeleid waarin is aangegeven aan welke bedrijfseisen de toegangsbeveiliging moet voldoen en waarbij rekening gehouden wordt met afzonderlijke bedrijfstoepassingen. Tevens wordt rekening gehouden met toegang via externe werkplekken (w.o. de thuiswerkplek) en via mobiele apparatuur;
- het beheer van de toegangsrechten van gebruikers binnen de VRF en het voorkomen van onbevoegde toegang tot informatiesystemen;
- de verantwoordelijkheid van gebruikers om zorgvuldig om te gaan met hun wachtwoorden en om onbeheerde gebruikersapparatuur passend te beschermen;
- de gebruikerstoegang tot netwerken en netwerkdiensten (denk aan internet) waarbij de veiligheid van het VRF-netwerk en bijbehorende netwerkdiensten niet in gevaar komt;
- het treffen van beveiligingsvoorzieningen bij het inloggen om onbevoegde toegang tot informatiesystemen te voorkomen;

- het afschermen van bijzondere rechten en de toegang tot (hulp)programmatuur die anderzijds toegang geeft tot informatie, tegen onbevoegd gebruik;
- het waarborgen van de informatiebeveiliging bij het gebruik van thuiswerken, telewerken en/of mobiele apparatuur.

4.6.6 Cryptografie

Cryptografie ofwel het versleutelen van gegevens wordt toegepast om te bewerkstelligen dat die alleen door bevoegde functionarissen kunnen worden gelezen. Zo worden bijvoorbeeld de gegevens die via het internet lopen standaard versleuteld zodat ze onderweg niet kunnen worden afgeluisterd of gewijzigd. Het doel is de bescherming van de vertrouwelijkheid, authenticiteit en/of integriteit te beschermen. Er moet voor VRF bepaald worden in welke gevallen cryptografische beveiligingsmaatregelen worden ingezet en voor welk type encryptie er gekozen wordt. Voor de encryptie en het (langdurig) weer leesbaar maken van de gegevens dient men te beschikken over een sleutel. Gezien het belang van de versleuteling, maar ook de ontsleuteling is zorgvuldig beheer van deze sleutels noodzakelijk.

4.6.7 Fysieke beveiliging en beveiliging van de omgeving

Fysieke beveiliging is gericht op het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein, de informatie van de organisatie, bedrijfsmiddelen én het voorkomen van de onderbreking van de bedrijfsactiviteiten van VRF. Aandachtsgebieden zijn de fysieke toegang tot gebouwen, publieke ruimten en werkruimten, maar ook het fysiek afschermen van ICT-voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen (bekabeling, computerruimte, etc.). Een ander aandachtsgebied is het naleven van een clear desk en clear screen beleid, ofwel ervoor zorgdragen dat elke werkplek na werktijd is opgeruimd (gevoelige en bedrijfskritische informatie op papier en verwijderbare opslagmedia), dat computerapparatuur is uitgeschakeld en dat sprake is van schermbeveiliging bij het tijdelijk verlaten van de werkplek.

4.6.8 Beveiliging bedrijfsvoering

Beveiliging van de bedrijfsvoering omvat alle ICT-gerelateerde maatregelen om de informatievoorziening te beschermen tegen verstorende invloeden. Belangrijke maatregelen zijn o.a. de bescherming tegen kwaadaardige software en digitale inbraak en het maken van reservekopieën (back-up). Daarnaast het toepassen van procedures om op een gecontroleerde wijze problemen op te lossen en wijzigingen door te voeren op de ICT-voorziening.

Ondanks beschermende maatregelen is het nog steeds mogelijk dat er verstorende invloeden plaatsvinden, al dan niet door kwaadwillende personen geïnitieerd. Daarvoor is het nodig om de ICT-voorziening te testen en te bewaken. Met penetratietesten wordt de 24 weerbaarheid in kaart gebracht en eventuele kwetsbaarheden opgespoord. Een continu monitoringsysteem dient om ongewenste gedragingen te detecteren.

Preventieve en detectie-maatregelen tezamen kunnen geen 100% veiligheid bieden. Er moeten ook zaken hersteld kunnen worden na een incident en er moeten dus recente (en periodiek geteste) reservekopieën (back-ups) voorhanden zijn van de gehele informatievoorziening.

Hackers en kwaadaardige software maken vaak gebruik van programmatuurfouten in software. Deze fouten worden door de softwareontwikkelaar opgelost en via updates aangeboden. Met een strak updateregime wordt de kwaadwillende een belangrijk wapen uit handen geslagen.

4.6.9 Communicatiebeveiliging

Transport van gegevens over netwerken, zowel intern als over internet moet worden beveiligd om ongewenste modificatie en ongeautoriseerde inzage tegen te gaan. Het is daarbij ook nodig om het interne netwerk in logische eenheden te scheiden. Bij elke eenheid kan dan voor een passend beveiligingsniveau gezorgd worden.

Bij transport over internet is vooral de inzet van sterke cryptografie noodzakelijk. Aangezien er dan veelal wordt gecommuniceerd met externe partijen is het nodig om afspraken over de wijze waarop dit gebeurt, de omgang met de gegevens en geheimhouding in overeenkomsten vast te leggen.

4.6.10 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Dit onderdeel gaat met name in op de beveiliging van informatiesystemen en het onderhoud op deze informatiesystemen. Informatiesystemen omvatten besturingssystemen, infrastructuur, bedrijfstoepassingen en toepassingen die ten dienste staan van de gebruikers. Belangrijke aandachtsgebieden van dit onderdeel zijn:

- het opnemen van het thema informatiebeveiliging in de inkoopprocedure ingeval van aanschaf van nieuwe informatiesystemen of onderdelen ervan;
- principes om bij de systeemontwikkeling beveiliging onderdeel te laten zijn van het ontwerp;
- het afschermen van alle operationele programmatuur en systeembestanden voor onbevoegde wijzigingen;
- het zorgvuldig kiezen, beschermen en beheersen van testgegevens. Het anonimiseren van persoonsgegevens en het aanpassen of onherkenbaar maken van gevoelige informatie wordt hierbij in acht genomen;
- het implementeren van wijzigingen via een formele procedure wijzigingsbeheer om het risico van storingen of/of fouten zoveel mogelijk te voorkomen;

Veel beheersmaatregelen in dit hoofdstuk gaan over softwareontwikkeling. VRF schaft standaardproducten aan en ontwikkelt dus zelf geen software en laat deze in beginsel ook niet ontwikkelen. Bij de selectie van standaardsoftware is het echter wel van belang om ingebouwde beveiligingsmaatregelen zwaar mee te laten wegen.

4.6.11 Leveranciersrelaties

In dit hoofdstuk gaat het erom bedrijfsmiddelen van de VRF, die toegankelijk zijn voor externe leveranciers te beveiligen. Dit speelt met name bij gebruik van softwaretoepassingen die via het internet worden aangeboden. Als gevolg daarvan komen gegevens van VRF op externe servers te staan en is er geen directe invloed op de beveiliging meer mogelijk. Om de gegevensbeveiliging dan toch onder controle te houden is het nodig om in overeenkomsten afspraken te maken over gestelde eisen. Nadat de overeenkomst tot stand is gekomen dient er gecontroleerd te worden of de afspraken door de leveranciers worden nageleefd. Wijzigingen in de dienstverlening worden beoordeeld op consequenties voor de gegevensbeveiliging. Zo nodig worden overeenkomsten aangepast om de beveiliging op een voldoende hoog niveau te houden.

4.6.12 Beheer van informatiebeveiligingsincidenten

Een beveiligingsincident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden en kan leiden tot financiële, imago en/of politieke schade voor VRF. Het doel is om het aantal beveiligingsincidenten zoveel mogelijk te voorkomen en indien een incident zich voordoet de schade zo beperkt mogelijk te houden. Belangrijk is dat een incident wordt gemeld bij de juiste personen (leidinggevende, proceseigenaar, CISO, FG). Hiervoor is een formele procedure nodig

waarin is aangegeven hoe de VRF omgaat met het beheer van beveiligingsincidenten. Dan gaat het over het signaleren, registreren, analyseren van incidenten en het voorkomen van escalatie (crisisbeheersing), het afhandelen van incidenten en het periodiek rapporteren over de stand van zaken. Tijdens het optreden van het incident dient er aandacht te zijn voor het verzamelen en bewaren van informatie die als bewijs kan dienen van kwaadwillende activiteiten. Alle medewerkers en externe gebruikers zijn op de hoogte van deze procedure. Uit de registratie van incidenten kan lering worden getrokken om maatregelen te treffen die de kans op herhaling beperken. Hierbij is ook aandacht nodig voor interne en externe communicatie ingeval sprake is van een hoge escalatie (ook VRF overstijgend).

4.6.13 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Continuïteitsbeheer zelf is geen onderdeel van het onderwerp informatieveiligheid. Bedrijfscontinuïteit gaat immers veel verder dan alleen informatiebeveiliging maar de beschikbaarheid van de informatievoorziening is wel cruciaal voor het kunnen voortzetten of herstellen van bedrijfsprocessen van VRF. Continuïteitsplannen waaronder uitwijkmogelijkheden en het periodiek testen en evalueren van deze plannen spelen hierbij een belangrijke rol.

Waar het bij dit beveiligingsaspect om gaat is dat in het continuïteitsplan en de uitvoerings-maatregelen daarvan, er ook aandacht is voor het behouden en/of herstellen van de informatieveiligheid zoals deze in de andere paragrafen van dit hoofdstuk zijn beschreven en die in feite onderdeel vormen van de te herstellen VRF processen en informatievoorziening.

4.6.14 Naleving

In dit onderdeel ligt de nadruk erop om schending van enige wetgeving, wettelijke en regelgevende (zoals de BIO/NEN) of contractuele verplichtingen bij VRF te voorkomen. Er zijn vele wetten en regelgeving van toepassing op VRF, een bijzondere is de naleving van de Algemene Verordening Gegevensbescherming. Een ander belangrijk punt is dat VRF voldoet aan de gestelde licentie-eisen op programmatuur om eventuele toekomstige boetes/claims van leveranciers te voorkomen. Om de naleving te toetsen dient er te worden gecontroleerd. Dit kan worden gedaan door een interne of externe auditor. Naleving van het vastgestelde technische beveiligingsniveau vindt plaats door gespecialiseerde testen.

5. Kritieke processen VRF

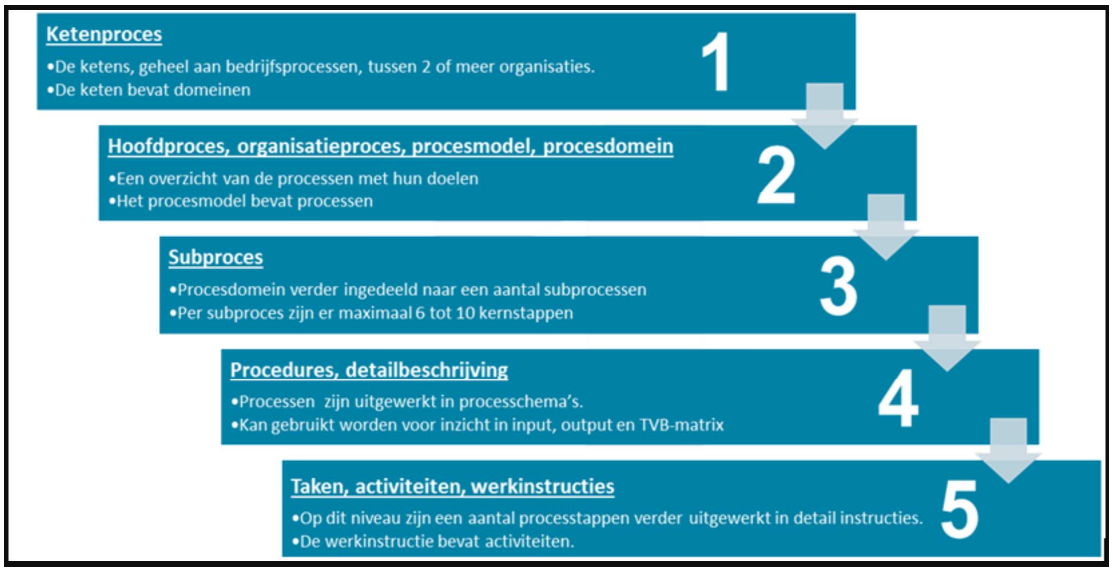
In dit document wordt veelvuldig het woord proces gebruikt; er wordt dan vooral gesproken over de bedrijfsprocessen van VRF. Het bedrijfsproces kan worden gedefinieerd als:

- Een ordening van activiteiten om een product of dienst te leveren die toegevoegde waarde biedt aan de klant.
- Een keten van activiteiten, gekoppeld en gestuurd door beslissingen.

Doorgaans wordt er onderscheid gemaakt in:

- primaire processen (of productieprocessen, operationele processen); Alle activiteiten waarvan de output direct bijdraagt aan het resultaat voor de klant. De primaire bedrijfsprocessen vormen het bestaansrecht van een organisatie.
- sturende processen (of managementprocessen); Alle activiteiten die benodigd zijn om de organisatie en de processen te kunnen besturen.
- ondersteunende processen; Alle activiteiten die benodigd zijn om het primaire proces te faciliteren.

Verder wordt ook vaak onderstaande proces ordening gehanteerd.



Bij VRF worden de proceseigenaren aangewezen op het nivo van de hoofd (c.q. bedrijfs)processen, De proceseigenaren beschermen de informatievoorziening van deze hoofdprocessen en ook de onderliggende nivo's ervan en beschermen tevens de (ketens van) informatie, informatiesystemen en informatievoorziening behorend bij dat hoofdproces.

Met het beveiligingsbeleid worden aanvullend ook de meest kritieke processen van VRF vastgesteld. De focus in de uitvoering komt hiermee op deze processen te liggen.
Dat betekent onder meer dat de gebruikte gegevens hierin geclassificeerd worden, er extra beheersing van en controle op de ondersteunende informatiesystemen wordt ingevoerd en het toezicht op eventuele leveranciers van software-oplossingen buiten de VRF wordt verstevigd.
Verder geldt dat deze processen en ook hun informatievoorziening, -dit zijn de zg kroonjuwelen op gebied van informatievoorziening-, voorrang krijgen bij situaties waarin prioritering aan de orde is.

Op basis van de volgende criteria worden de kritieke processen vastgesteld:

- Er is een wettelijke termijn waarbinnen het proces beschikbaar moet zijn.

- Verstoring of uitval heeft direct impact op de bedrijfsvoering en dienstverlening van VRF.
- Verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid levert schade op bij andere partijen.
- Verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid leidt tot imago schade voor VRF.
- Verstoring of uitval, onjuiste gegevens, schending van vertrouwelijkheid leidt tot een aanzienlijke kostenpost voor VRF.

Onder de BIO voert de eigenaar van een proces een BBN-toets uit waarmee bepaald wordt welk beveiligingsnivo voor een proces of applicatie noodzakelijk is. Deze toets wordt uiteindelijk uitgevoerd voor alle (hoofd)bedrijfsprocessen.

In eerste instantie zal deze toets (en eventueel aanvullende analyse) voor de kritieke processen worden uitgevoerd; daarna worden de overige (hoofd)bedrijfsprocessen nader onder de loep genomen.

Bijlage 1. Betrouwbaarheidscriteria en -normklassen

Inleiding
Betrouwbaarheid geeft de mate aan waarin VRF zich kan verlaten op een informatiesysteem voor zijn informatievoorziening. Bij de verwerving, inrichting en gegevensuitwisselingen binnen VRF of tussen VRF en andere instanties, worden afspraken gemaakt over de betrouwbaarheid van de informatiesystemen en van de informatie daarin en de wijze waarop zekerheid wordt verkregen over de realisatie daarvan. Vanzelfsprekend dienen betrouwbaarheidsafspraken schriftelijk gemaakt te worden in contracten, sla/dvo, convenaten etc. Deze betrouwbaarheidsafspraken kunnen op drie niveaus worden gemaakt:

- op het niveau van gevoeligheid, waarbij de afspraken betrekking hebben op de consequenties voor bedrijfsprocessen die van de informatie c.q. het informatiesysteem gebruik maken en voor de belangen van personen en instanties waarover gegevens worden uitgewisseld als er verstoring optreedt van de betrouwbaarheid van de informatie en de informatiesystemen;

- op het niveau van eisen, waarbij de afspraken betrekking hebben op de mate van betrouwbaarheid van de informatie en de informatiesystemen;

- op het niveau van maatregelen, waarbij de afspraken betrekking hebben op de realisatie van de betrouwbaarheid van de informatie en de informatiesystemen.

Duidelijk zal zijn dat afspraken op het niveau van gevoeligheid voor de partijen in uitwisseling weinig houvast biedt bij het invullen van de beveiliging (zekerstellen van de betrouwbaarheid) van de informatie en de informatiesystemen, terwijl afspraken op het niveau van maatregelen veel omvattend en complex zullen zijn en de geldigheidsduur van de afspraken ook beperkt zal zijn als gevolg van technologische en organisatorische ontwikkelingen. Afspraken over betrouwbaarheid van informatie en informatiesystemen moeten daarom gemaakt worden op het niveau van eisen. Bovendien is het zaak de eisen kwantitatief te formuleren, ten einde de afspraken meetbaar te maken.

In deze bijlage worden de criteria en -normklassen omschreven die door VRF dient te worden gehanteerd bij het formuleren van eisen inzake de betrouwbaarheid van informatie, informatiesystemen en informatieuitwisselingen.

Betrouwbaarheidscriteria
Beschikbaarheid wordt omschreven als: de mate waarin een informatiesysteem in bedrijf is op het moment dat VRF het nodig heeft. Voor het formuleren van beschikbaarheidseisen zijn er de volgende criteria.

- Beschikbaarheidsperiode: de tijd dat de informatie en het informatiesysteem nodig is. De beschikbaarheidsperiode wordt uitgedrukt in tijdseenheden, bijvoorbeeld kantoortijd, 7x24 uur, etc.

- Bedrijfszekerheid: de mate waarin de gegevensverwerking vrij blijft van storingen of, anders gezegd, de gemiddelde tijd tussen het optreden van beschikbaarheidsstoringen. De bedrijfszekerheid wordt uitgedrukt in uren, bijvoorbeeld: 1 beschikbaarheidsstoring per 200 uur is acceptabel.

- Herstelbaarheid: de snelheid waarmee de gegevensverwerking hersteld kan worden na een storing. Daarbij kan onderscheid gemaakt worden in:
    - de gemiddelde duur van een beschikbaarheidsstoring en
    - de maximaal toegestane duur van een beschikbaarheidsstoring, beide uitgedrukt in uren.

Beschikbaarheid wordt hier gespecificeerd in tijdafhankelijke criteria (het moment dat VRF het informatiesysteem nodig heeft), niet in locatieafhankelijke criteria (de plaats waar het informatiesysteem nodig is). Indien ook locatieafhankelijke beschikbaarheidseisen moeten worden gesteld, dan kunnen de hierboven genoemde criteria nader worden gespecificeerd per werkplek, afdeling of gebouw of organisatie.

Integriteit wordt omschreven als: de mate waarin een informatiesysteem zonder fouten is. 'Zonder fouten' wil zeggen dat de informatieverwerking plaatsvindt volgens vooraf vastgestelde specificaties. De randvoorwaarde voor het maken van afspraken over de integriteit van informatiesystemen en de informatie daarin is dus de aanwezigheid van specificaties van de verwerking, zowel de geautomatiseerde als de handmatige. Voor het formuleren van integriteitseisen zijn er de volgende criteria.

- Juistheid: het percentage van de gegevensverzameling dat door het informatiesysteem juist, conform specificaties, wordt verwerkt. Bijvoorbeeld: 95% van de gegevens wordt juist verwerkt.

- Volledigheid: het percentage van de gegevensverzameling dat door het informatiesysteem volledig (zonder manco's) en enkelvoudig (zonder doublures) wordt verwerkt.

- Tijdigheid: het percentage van de gegevensverzameling dat door het informatiesysteem binnen de gespecificeerde termijn wordt verwerkt.

- Hersteltijd: het aantal uren na constatering van niet-integer verwerkte gegevens waarbinnen herstel dient plaatsgevonden te hebben.

In die gevallen waarin de vereiste juistheid, volledigheid en/of tijdigheid nagenoeg 100% moet zijn, is het soms praktischer de eisen te formuleren in faalkansen, bijvoorbeeld: 1 onjuist verwerkte transactie per 1000 transacties is acceptabel.

Exclusiviteit wordt omschreven als: de mate waarin de toegang tot en kennisname van een informatiesysteem en de informatie daarin beperkt is tot een gedefinieerde groep van gerechtigden. Voor het formuleren van eisen inzake exclusiviteit kunnen de volgende criteria van dienst zijn.

- Autorisatie: de aanduiding van de groep van personen die voor toegang tot en kennisname van een informatiesysteem en de informatie daarin gerechtigd is. Hoewel autorisatie feitelijk een specificatie is van exclusiviteit en niet van zekerstelling van exclusiviteit, wordt ervan uitgegaan dat naarmate de groep van geautoriseerde personen nauwkeuriger omschreven wordt de noodzakelijke zekerstelling van de exclusiviteit hoger wordt.

- Geoorloofdheid: de mate van zekerheid dat toegang tot en kennisname van een informatiesysteem en van de informatie daarin uitsluitend voor personen die daartoe gerechtigd zijn mogelijk is. Geoorloofdheid wordt uitgedrukt in het percentage van de feitelijke gebruik van het informatiesysteem. Bijvoorbeeld: 99% van het feitelijk gebruik van het systeem is geoorloofd gebruik. In die gevallen waarin de vereiste geoorloofdheid nagenoeg 100% moet zijn is het vaak praktischer de eis te formuleren in faalkansen, bijvoorbeeld: 1 ongeoorloofde toegang per 1000 toegangen is acceptabel.

- Braakbestendigheid: de tijd dat het kost om ongeoorloofd toegang tot een informatiesysteem te verkrijgen, uitgedrukt in uren.

Normklassen
Als voor elk informatiesysteem specifieke betrouwbaarheidsnormen worden geformuleerd, dan ontstaat een complex normenstelsel. Wat te doen als het ene systeem een bedrijfszekerheidsnorm stelt van 1 storing per 200 uur, het volgende systeem een norm stelt van 1 storing per 240 uur en het derde weer een norm stelt van 1 storing per 300 uur? Voor het maken van afspraken zal het op den duur handiger blijken om normklassen te hanteren. In deze regeling worden vier normklassen onderscheiden: 'laag', 'gemiddeld', 'hoog' en 'zeer hoog'. Hieronder volgt een voorstel van een mogelijke invulling van normklassen voor de onderscheiden betrouwbaarheidscriteria.

Normklasse à Criterium	**Laag**	**Gemiddeld**	**Hoog**	**Zeer hoog**
Beschikbaarheid				
Beschikbaarheids-periode	Kantoortijd	Kantoortijd	7x24 uur	7x24 uur
Bedrijfszekerheid	200 uur	400 uur	1500 uur	6000 uur
Herstelbaarheid	8 uur	4 uur	2 uur	1 uur
Integriteit				
Juistheid	< 90%	90-95%	95-99,9%	>99,9%
Volledigheid	< 90%	90-95%	95-99,9%	>99,9%
Tijdigheid	< 90%	90-95%	95-99,9%	>99,9%
Hersteltijd	> 24 uur	24-8 uur	8-1 uur	< 1 uur
Exclusiviteit				
Autorisatie	Iedereen in VRF	specifieke afdelingen	specifieke functies	specifieke personen
Geoorloofdheid	90%	99%	99,99%	99,99%
Braakbestendigheid	< 8 uur	8-168 uur	168-672 uur	> 672 uur

Tot slot
De in deze bijlage beschreven verzameling van betrouwbaarheidscriteria is niet volledig en vaststaand. Zoals elke taal is ook de 'informatiebeveiligingstaal' in ontwikkeling. Op basis van ervaringen met het toepassen van de betrouwbaarheidscriteria en van de normklassen zullen aanpassingen en uitbreidingen van de verzameling van criteria en invullingen van de normklassen kunnen worden verwacht.

Bijlage 2: De 10 principes voor informatiebeveiliging

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1 Bestuurders bevorderen een veilige cultuur
Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting: Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen
Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het DT/MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar het bestuur en zorg ervoor dat deze ook zijn rol kan pakken op dit onderwerp.

Toelichting: Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement
Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting: Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een

plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming
Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting: U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking
Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van VRF en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld- en dat de juiste maatregelen getroffen worden.

Toelichting: Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. VRF dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces
Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting: Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld
Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting: Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 Onzekerheid dient te worden ingecalculeerd
De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen.

Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden. Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting: Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring
Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting: Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert
Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting: Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

Bijlage 3: De context van de organisatie

Behoeften en verwachtingen belanghebbenden
Het managementsysteem voor informatiebeveiliging kent onderstaande belanghebbenden.

Belanghebbenden	Eisen
Bestuur	Kwaliteit en continuïteit van dienstverlening. Compliancy wet en regelgeving
Medewerkers	Taken en verantwoordelijkheden goed kunnen vervullen
Klanten	Kwalitatief goede zorg en veiligheid. Bescherming persoonlijke levenssfeer
Ketenpartners	Heldere afspraken over eisen en kwaliteit onderlinge dienstverlening
Leveranciers	Heldere afspraken over eisen en kwaliteit dienstverlening

Toepassingsgebied van het managementsysteem voor informatiebeveiliging
Het managementsysteem voor informatiebeveiliging heeft het onderstaande toepassingsgebied.

Toepassingsgebieden	Raakvlakken en afhankelijkheden
Veiligheidsregio conform WVR	OOV, crisisbeheersing, sectoraal VR's
GGD conform WPG	Publieke gezondheid, Jeugdgezondheid, sectoraal GGD's
Meldkamer NN en LMS (beheer politie)	VR Meldpunt, Alarmeringsproces, opschalingsproces,
RCC	Crisislokatie en voorzieningen GRIP2 en hoger
GGDGHOR Nederland	Centrale applicaties/data w.o. CoronIT en GKVI etc
NIPV	VR Centrale applicaties w.o. LCMS, SIS, ELO, LK/VP etc
Ministerie J&V (via RCVD, NIPV en VB)	GMS, LCMS, 112, C2000, P2000, GMS, NL-alert, WAS
Ministerie VWS (via DPG raad, GGDGHOR)	CoronIT, GGDcontact
Informatiesystemen bij leveranciers	Subverwerkingen
RIVM	Aanleveren gezondheidsgegevens
CBS	Aanlevering statistieken

Inzicht in de organisatie en haar context
De onderstaande interne en externe onderwerpen zijn relevant zijn om de doelstelling van het managementsysteem voor informatiebeveiliging te behalen.

Interne onderwerpen	Externe onderwerpen
P&C cyclus VR	Opzet Paricipatie sectorale CERT's en ISACs
Proces risicomanagement VR	(Collectieve) Detectienetwerken, SOC/SIEM
CISO rol beschreven, benoemd, gepositioneerd	Convenanten MK/LMS, NIPV, GGDGHOR
Procesgericht, proceseigenaarschap, integraal mg	Industriestandaarden
Ondersteuning proceseigenaren (ISO)	Dreigingsbeelden
Budgetten en formatie informatieveiligheid	
Proces Leveranciersmanagement	
Proces Continuïteitsmanagement	