Informatiebeveiligingsbeleid 2018 - 2021

Versie: 1.0, Mei 2018

Instituut Fysieke Veiligheid
Bestuurs- en directieondersteuning
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Opdrachtgever:	Wim Papperse
Contactpersoon:	Leon Visser
Titel:	Startdocument informatiebeveiligingsbeleid
Datum:	Mei 2018
Status:	Versie 1.0
Versie:	1.0
Auteurs:	Projectgroep Privacy
Projectleider:	
Review:	
Eindverantwoordelijk:	

Versiebeheer

Versienr	Datum	Auteur(s)	Status	Opmerking
0.1	28 maart 2018	O. Huizenga	Concept	Concept richting projectgroep voor review
0.2	29 maart 2018	O. Huizenga	Concept	Eerste bespreking met projectgroep
0.3	4 april 2018	O. Huizenga	Concept	Bijlage 1 en hoofdstuk 3.1 toegevoegd.
0.4	12 april 2018	Projectgroep Privacy	Concept	Input van de projectgroep verwerkt en besproken.
1.0	24 april 2018	IFV	Versie 1.0	De versie zoals besproken in de stuurgroep project privacy

Inhoud

Managementsamenvatting en leeswijzer

Samenvatting

Voor u ligt het informatieveiligheidsbeleid van het Instituut Fysieke Veiligheid (IFV). Het beschrijft het te voeren informatiebeveiligingsbeleid. Dit beleid zal uitwerking vinden in meer gedetailleerde procedures, maatregelen en richtlijnen die voor het uitvoeren van het beleid van toepassing zijn. Deze worden separaat uitgewerkt. Dit document beschrijft de richting voor informatiebeveiliging zoals deze door de directie is bepaald. Het informatiebeveiligingsbeleid komt tot stand in overeenstemming met de bedrijfsmatige eisen voor effectieve en efficiënte bedrijfsprocessen, betrouwbare financiële verslaggeving en naleving van wetten en regelgeving.

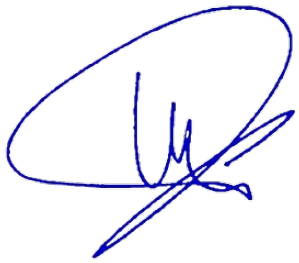
Voor het informatiebeveiligingsbeleid gelden de volgende vertrekpunten:

- De BIR2017 is het uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. De directie kan besluiten om op punten af te wijken van de voorgestelde maatregelen of aanvullende maatregelen treffen.[1]
- Het informatiebeveiligingsbeleid is van toepassing op het gehele IFV, inclusief IE Beheer BV.
- Alle onderdelen van het beleid worden uitgewerkt in concrete richtlijnen en maatregelen, toegesneden op de taken en verantwoordelijkheden van de betrokken eenheid en medewerkers.
- Periodiek, bij grote wijzigingen en bij de start van aanbestedingen wordt middels een risicoanalyse beoordeeld of voor specifieke gegevens of informatiesystemen aanvullende maatregelen noodzakelijk zijn. De frequentie van de beoordeling is gerelateerd aan de planning & control cyclus van het IFV. De naleving van genomen maatregelen wordt periodiek getoetst.[2]
- Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld[3].
- Uit het informatiebeveiligingsbeleid volgt het informatiebeveiligingsplan. Dit plan is een levend document waarin de concrete maatregelen worden uitgewerkt.
- Het IFV bevordert actief het beveiligings- en privacy-bewustzijn van haar medewerkers.

[1] Een overzicht van de BIR is opgenomen in bijlage 1.
[2] Conform VIR artikel 4
[3] Conform BIR 2017 norm 5.1.2.1

- Alle medewerkers zijn verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.

Namens de directie,



Ing. W. Pappers

Leeswijzer

In Hoofdstuk 1 wordt het **informatiebeveiligingsbeleid** van het IFV beschreven in doelstellingen en uitgangspunten.
Hoofdstuk *2* beschrijft de **verantwoordelijkheden en bevoegdheden** van de verschillende functies en rollen voor beveiliging.
In Hoofdstuk 3 is de **Beheersing** van beveiliging opgezet.

Bijlage 1 bevat een overzicht van de onderwerpen die in de **BIR** aan de orde komen.

1 Informatiebeveiligingsbeleid

1.1 Het informatiebeveiligingsbeleid

Informatie is essentieel voor het succes van het IFV. Met het informatiebeveiligingsbeleid wordt vanuit een strategisch oogpunt bepaalt, vastgelegd en gecommuniceerd hoe het IFV informatie ontvangt, gebruikt en deelt met andere partijen. Het IFV draagt zorg voor een effectieve beveiliging. Daarvoor is het noodzakelijk dat de gegevens, die aan de basis liggen van informatie, voldoen aan de gestelde eisen van vertrouwelijkheid, integriteit en beschikbaarheid. Effectieve beveiliging wordt bereikt door te werken met passende gedragsregels, in overeenstemming met de wetgeving, en het uitvoeren van het vastgestelde beleid en de gewenste richtlijnen uit de praktijk. Hiertoe conformeert het IFV zich aan de BIR:2017.

In dit hoofdstuk wordt het informatiebeveiligingsbeleid beschreven. Dit geeft richting aan de meer gedetailleerde maatregelen en richtlijnen die van toepassing zijn binnen het IFV. Voor de leesbaarheid van dit document is ervoor gekozen om verdere invulling van dit beleid te verwerken in separate documenten.

1.1.1 Doelstellingen

De doelstellingen van dit beleid zijn:

- Het **beschermen van alle informatie**systemen binnen het IFV (met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, software en gegevens) en het beperken van de risico's van diefstal, verlies, misbruik, of beschadiging van deze systemen.
- Het waarborgen van de **privacy** van medewerkers en overige betrokkenen conform de privacywetgeving.
- Het zorgen voor een **veilige en betrouwbare werking** van de informatiesystemen voor het personeel en andere geautoriseerde gebruikers.
- De borging van het **beheer** (exploitatie) van informatiesystemen om onbedoelde wijzigingen, met mogelijke nieuwe risico's, te voorkomen.
- Het zorgen voor een systematiek van **incidentenregistratie**, analyse en selecteren van gepaste maatregelen om informatieveiligheid te vergroten.
- Een kader bieden voor een adequate **continuïteitstrategie** om het onderbreken van bedrijfsactiviteiten tegen te gaan, kritieke processen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en het bewerkstelligen van tijdig herstel.
- De **bewustwording** bij medewerkers creëren met betrekking tot de bekendheid en naleving van alle huidige en relevante interne procedures en richtlijnen, alsmede van wetgeving op het gebied van informatieveiligheid, zodat ze op de hoogte zijn van hun verantwoordelijkheid voor de bescherming van de vertrouwelijkheid en de integriteit van de gegevens die zij behandelen.

- Het beschermen van het IFV tegen **aansprakelijkheid** of schade door het misbruik van haar informatiesystemen en faciliteiten.

1.1.2 Reikwijdte

Het informatiebeveiligingsbeleid is van toepassing op het gehele IFV, inclusief IE Beheer BV. Het beleid heeft betrekking op alle door het IFV gebruikte gegevens en hieraan gerelateerde informatiesystemen, de fysieke aspecten met betrekking tot deze gegevens, privésystemen die zijn aangesloten op het netwerk van het IFV én op software in eigendom van het IFV of via licentie verkregen.

1.1.3 Uitgangspunten

- De inhoud van dit beleid dient bekend te zijn bij alle geautoriseerde gebruikers van het IFV. Op de naleving ervan wordt toegezien. Om dit te bereiken zal het onderwerp 'informatiebeveiliging' deel uitmaken van het inwerkprogramma van nieuwe IFV-medewerkers.
- Informatiebeveiliging is een continu proces. Een regelmatige herijking van beleid en audits is daarvoor nodig. Technologische en organisatorische ontwikkelingen binnen en buiten het IFV maken het noodzakelijk om periodiek te beoordelen of men nog wel op de juiste wijze bezig is de (informatie)beveiliging te waarborgen. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency (controleerbaarheid).
- Het IFV is als rechtspersoon al dan niet getrapt verantwoordelijk van de informatie die onder haar wordt verwerkt, tenzij dit op basis van wettelijke gronden anders is overeengekomen.
- Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Classificatie dient hierbij als hulpmiddel; paragraaf 1.3.
- Bij veranderingen, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met informatiebeveiliging.
- In het beleid is tevens bepaald welke systemen als kritiek worden beschouwd en welke eisen er worden gesteld aan de beschikbaarheid, exclusiviteit en integriteit.
- Door het IFV is een normenkader vastgesteld waartegen toetsing van de uitvoering van het beleid en genomen maatregelen mogelijk is. Dit normenkader is, op basis van een uitgevoerde risicoanalyse, afgeleid van de BIR2017.

1.2 Risicoanalyse en continuïteit

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van die waarde en van de risico's van mogelijke schade de grondslag is van dit beleid en daarmee sturend moet zijn in het nemen van maatregelen. Het is de taak van de directie en het lijnmanagement om ervoor te zorgen dat dit bewustzijn bij de medewerkers aanwezig is.
Om reproduceerbaar en eenduidig de waarde van informatie (-systemen) en gepaste beheersmaatregelen te kunnen bepalen wordt er gebruik gemaakt van een kwalitatieve risicoanalyse met een 'Business Impact Analyse' om onderbouwd de belangrijkste risico's te

identificeren. De risicoanalyse wordt elke drie jaar herhaald, of tussentijds in het geval van substantiële wijzigingen.
Alle informatie (-systemen) heeft een eigenaar[4]. De waarde van de informatie (-systemen) wordt vastgesteld door de eigenaar o.b.v. een uniforme methodiek voor classificatie van beveiligingsniveaus voor informatie (-systemen) zie tabel 1. De waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid.

Systeem Classificatie	Kenmerken van informatie (-systemen)
Vitaal	Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het Informatiesysteem. Inzet van het Informatiesysteem is van levensbelang voor een goede uitvoering van het bedrijfsproces. Het Informatiesysteem is wezenlijk voor de beheersing of besturing van de bedrijfsactiviteiten. **(Onontbeerlijk voor het proces)** **Op deze classificatie is BBN3 (conform de BIR) van toepassing**
Aanzienlijk	Het Informatiesysteem levert een aanzienlijke bijdrage aan de activiteiten binnen het proces en/of de voortbrenging van producten/diensten. Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk indien het systeem niet beschikbaar is. Inzet van het Informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. **(Groot belang voor de ondersteuning – hoge beschikbaarheidseis).** **Op deze classificatie is BBN3 (conform de BIR) van toepassing**
Nuttig	Het Informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de voortbrenging van producten/diensten. Voortzetting van het proces is mogelijk door het volgen van alternatieve procedures/activiteiten. Inzet van het Informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. **(Belangrijke ondersteuning voor het proces)** **Op deze classificatie is BBN2 (conform de BIR) van toepassing**
Support / Ondersteunend	Het Informatiesysteem geeft support bij de activiteiten binnen het bedrijfsproces en is 'handig om te hebben'. **(Kan eventueel gemist worden)** **Op deze classificatie is BBN1 (conform de BIR) van toepassing**

Tabel 1 - Systeem classificatie

1.2.1 Uitkomsten uit de risicoanalyse

De onderstaande strategische risicogebieden zijn vanuit de risicoanalyse geïdentificeerd. De komende drie jaar is het beleid erop gericht om deze risicogebieden verder te beheersen.

- Verdere implementatie en inbedding van de AVG-wetgeving in het IFV

[4] Met eigenaar wordt bedoeld de persoon/functionaris, doorgaans de proceseigenaar, die verantwoordelijk is voor alle aspecten ten aanzien de exploitatie, aanpassingen en toekomstige vervangingen van het systeem.

- Uitvoering geven aan de BIR:2017 met als doel het IFV te certificeren op de ISO27001

1.2.2 Strategie voor Continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door de directie vastgesteld, acceptabel niveau. Ondanks goede beheersmaatregelen kan een incident zich voordoen. Voor kritieke ICT-diensten en informatiesystemen is een continuïteitsplan aanwezig. Hierin is opgenomen hoe, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem zo snel mogelijk operationeel gemaakt kan worden. Een continuïteitsplan kan variëren van een goede back-upvoorziening of het geografisch spreiden van de ICT-dienst tot een complete uitwijk. Continuïteitsplannen worden minimaal één keer per jaar op actualiteit geëvalueerd en in overeenstemming met het testplan gecontroleerd.

1.3 Informatieclassificatie

Alle informatie binnen het IFV wordt geclassificeerd naar één van de drie niveaus van vertrouwelijkheid, zoals hieronder vermeld.

Gegevensclassificatie	Kenmerken van informatie
Openbaar	Deze informatie kent geen eisen ten aanzien van de vertrouwelijkheid en integriteit en is daardoor voor **iedereen** binnen het IFV beschikbaar en toegankelijk. **Op deze classificatie is BBN1 (conform de BIR) van toepassing**
Intern	Dit betreft de informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van het IFV. De eisen ten aanzien van vertrouwelijkheid en integriteit zijn gering. **Op deze classificatie is BBN2 (conform de BIR) van toepassing**
Vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers. De informatie wordt beschikbaar gesteld op basis van het "need to know" principe[5]. Schending van deze classificatie kan direct of indirecte schade toebrengen aan het IFV, onderdelen van het IFV of personen binnen het IFV. **Op deze classificatie is BBN3 (conform de BIR) van toepassing**

1.4 Naleving van wet- en regelgeving

Het IFV dient zich te houden aan alle relevante wet- en regelgeving die van toepassing is op het uitvoeren van de dagelijkse werkzaamheden. De relevante wet- en regelgeving is vertaald naar richtlijnen en gedragscodes die van toepassing zijn op alle medewerkers van

[5] **Need to know principe**. Dit principe houdt in dat functionarissen slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

het IFV en voor het overige van toepassing zijn op extern personeel en stagiaires van het IFV of derden (zoals leveranciers) die gebruik maken van informatievoorzieningen van het IFV. In het bijzonder gelden in dit verband de volgende richtlijnen en codes:

- Gedragscode internet- en e-mail-gebruik van het IFV.
- Integriteitscode.
- Regeling melden misstanden?
- Procedure melden datalekken
-

Wettelijke voorschriften die opgevolgd dienen te worden:

- Voorschrift informatiebeveiliging rijksdienst 2007 (http://wetten.overheid.nl/BWBR0022141/2007-07-01)
- Wet computercriminaliteit III
- Algemene Verordening Gegevensbescherming
- Auteurswet.
- Archiefwet.
- Wet veiligheidsregio's
- Algemeen Rijksambtenarenregelement (ARAR)

Daarnaast gelden de afspraken die contractueel gelden met leveranciers waarmee het IFV afspraken heeft gemaakt.
Verdere informatie en samenvattingen van de wetgeving met betrekking tot het informatieveiligheidsbeleid van het IFV is te vinden in de ondersteunende richtlijnen en/of gerelateerde documenten.
Indien het IFV schade ondervindt door nalatigheid bij het gebruik of het opzettelijke misbruik van informatievoorzieningen (plichtsverzuim), wordt de geldende rechtspositionele wet- en regelgeving toegepast en op basis daarvan worden maatregelen genomen door of namens de directie.

2 Verantwoordelijkheden

Informatiebeveiliging dient als proces[6] te worden ingericht wat inhoudt dat dit onderwerp onderdeel uitmaakt van de jaarlijkse planning en controlecyclus. Op basis hiervan worden jaarplannen opgesteld, belegd in de organisatie en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen (Plan, Do, Check, Act).

2.1 Actoren

Verschillende actoren binnen het IFV verrichten gezamenlijk de activiteiten voor het beveiligingsproces. Elke actor heeft een bepaalde rol binnen het proces. Een goede verdeling van de taken, bevoegdheden en verantwoordelijkheden (TBV's) tussen de verschillende actoren is cruciaal voor een effectief en efficiënt procesverloop.
Voor beveiliging worden binnen het IFV de volgende actoren onderkend:

- De directie - strategische verantwoordelijkheid - besturing.
- De directeur bedrijfsvoering - strategische verantwoordelijkheid - beheersing.
- De security officer – beheersing, naleving en advies.
- De functionaris gegevensbescherming – Toezichthouder op naleving van de privacywetgeving AVG.
- Het lijnmanagement - tactische verantwoordelijkheid - aansturing.
- De medewerker (iedereen) - operationele verantwoordelijkheid - uitvoering.
- De externe auditor, onafhankelijk toetsen en beoordelen.

De **directie** is integraal verantwoordelijk voor het vaststellen van het beleid en de richtlijnen die ten grondslag liggen aan een adequaat systeem van informatiebeveiliging en voor het beoordelen van de efficiëntie en effectiviteit hiervan.
De gemandateerde verantwoordelijkheid berust bij de **directeur bedrijfsvoering** die het onderwerp informatiebeveiliging in portefeuille heeft en rapporteert aan de directie.
De gedelegeerde verantwoordelijkheid voor de effectieve en efficiënte toepassing van het beleid berust bij het lijnmanagement.
De **security officer** houdt namens de directie toezicht op de aanwezige controles ter identificatie, evaluatie en beheersing van risico's. Belangrijke taken vanuit de security officer zijn informeren, borging van de integrale kwaliteit en doelmatigheid van de diensten, adviseren, naleving van wet- en regelgeving en het eigen beleid en het uitvoeren van audits om van daaruit te komen tot verbetervoorstellen.
De dagelijkse verantwoordelijkheid berust bij het **lijnmanagement** die voortdurend toezien op naleving van de vastgestelde richtlijnen en de risico's beoordelen waarmee hun afdeling(en) worden geconfronteerd.
Elke **medewerker** (al dan niet in vaste dienst) van het IFV is verplicht om mee te werken aan de informatiebeveiliging. Dit geldt in het bijzonder voor de medewerkers die

[6] Voor de inrichting van het proces is de BIR2017 het uitgangspunt. De BIR verwijst hiervoor naar de VIR artikel 4

persoonsgegevens, financiële en/of managementgegevens of andere geclassificeerde gegevens behandelen. Zij zijn op individueel niveau verantwoordelijk voor een effectieve informatiebeveiliging van de aan hen toevertrouwde gegevens.
De **externe auditor** voert de onafhankelijke evaluatie & controle uit op de opzet, bestaan en werking van het proces van informatiebeveiliging van het IFV.

Voor sommige (werk)processen geldt dat deze (deels) worden uitgevoerd door externe partijen. Met de **externe dienstverleners** worden concrete en toetsbare afspraken gemaakt over de door hen te treffen beveiligingsmaatregelen. Deze afspraken worden vastgelegd in externe dienstverleningsovereenkomsten. In elke dienstverleningsovereenkomst wordt de door de dienstverlener te treffen beveiligingsmaatregelen beschreven. De security officer van het IFV controleert periodiek de correcte naleving van de gemaakte afspraken.

2.2 Evaluatie & Controle

Onder controle wordt verstaan zowel interne controle door de eigen organisatie als toetsing door een onafhankelijke auditor. De toetsing richt zich zowel op het beveiligingsbeleid als op de maatregelen die uit dit beleid voortvloeien. Dit betekent dat de volgende drie vormen van controle voorkomen:

1. Juiste naleving van het beleid en de interne werkafspraken.
2. Correcte werking van de beveiligingsorganisatie.
3. Toereikendheid van de vastgestelde beveiligingsmaatregelen gedurende een bepaalde periode.

Onder evaluatie wordt verstaan het nagaan of de kaders van de beveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van het beheer.
De evaluatie van het beleid is een heroriëntatie op de strategische uitgangspunten. Bij de evaluatie van het beheer wordt nagegaan of het vastgestelde beleid nog toereikend is.
De jaarlijkse controle op beveiliging bestaat uit drie onderdelen:

1. Om ervoor te zorgen dat geïmplementeerde beveiligingsmaatregelen worden nageleefd zal dit jaarlijks moeten worden gecontroleerd. De interne auditors zullen op basis van een nader vast te stellen werkprogramma (inclusief uitgewerkte kwaliteitseisen) een audit uitvoeren.
2. Om ervoor te zorgen dat de beveiligingsorganisatie correct werkt, wordt dit opgenomen in de interne auditstructuur. Er moet hierbij rekening gehouden worden met noodzakelijke functiescheiding. De functionarissen die zelf deel uitmaken van de beveiligingsorganisatie mogen geen deel uitmaken van het auditteam. Dit om belangenverstrengeling te voorkomen.
3. Om de drie jaar wordt het vastgestelde beleid (inclusief maatregelen) op de toereikendheid beoordeeld. Concreet betekent dit dat beoordeeld wordt of het beleid en de maatregelen zorgen voor een afdoende beveiliging van de processen en de informatiestromen van het IFV.

2.3 Sancties bij inbreuken op het informatiebeveiligingsbeleid

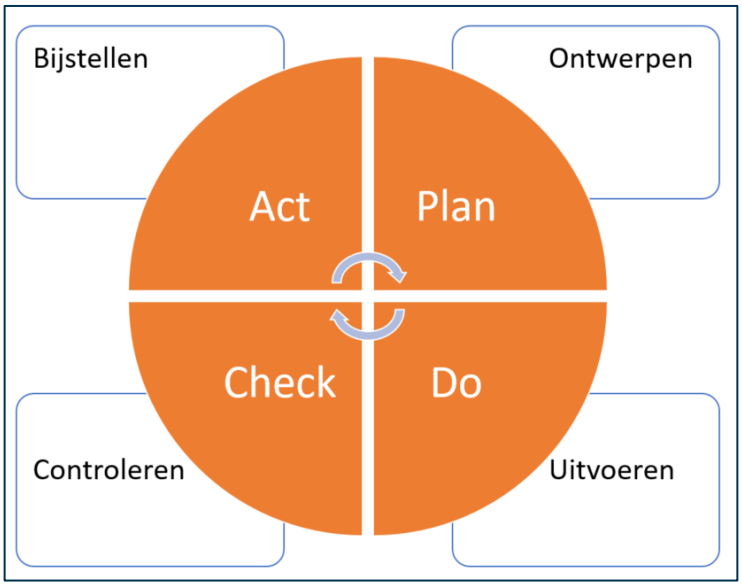
Het beleid is uitgewerkt in verschillende processen, procedures en richtlijnen die van toepassing zijn binnen het IFV.

Indien het IFV wordt aangesproken op de overtreding van eigendomsrechten, auteursrechten of overtreding van andere wettelijke bepalingen, zijn de wettelijke en binnen het IFV geldende regelingen van toepassing. In het geval dat door het onrechtmatig handelen schade ontstaat wordt de overtreder daarvoor aansprakelijk gesteld.

3 Beheersing van informatiebeveiliging

De informatiebeveiliging van het IFV is een cyclisch proces. Via de zogenaamde Plan-Do-Check-Act cyclus wordt gestreefd naar een adequaat niveau van informatiebeveiliging. De tussentijdse controles of constateringen kunnen aanleiding zijn om bij te sturen op de bestaande maatregelen. In de informatiebeveiligingsterminologie wordt dit het **ISMS** (Information Security Management System) genoemd.

De cyclus wordt jaarlijks tenminste éénmaal doorlopen. Het procesonderdeel toetsing wordt jaarlijks uitgevoerd wat betreft de toetsing van de opzet[7] en het bestaan, en **twee** jaarlijks wat betreft de toetsing van de werking (het bestaan gedurende een vastgestelde periode). Het proces en de cyclus zijn in onderstaand schema weergegeven.



Figuur 1 Weergave van het ISMS

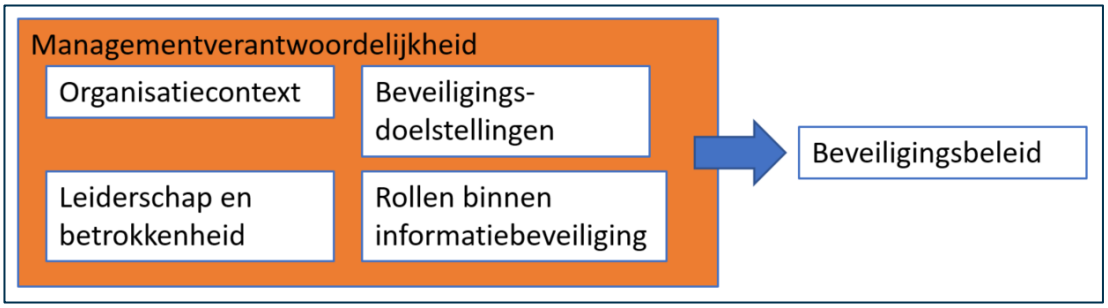
[7] Zie 3.1.3 voor een uitleg van deze terminologie.

3.1 Opbouw van het ISMS

De opbouw van het ISMS is weergegeven in de volgende schema's.

3.1.1 (Plan) Managementverantwoordelijkheid

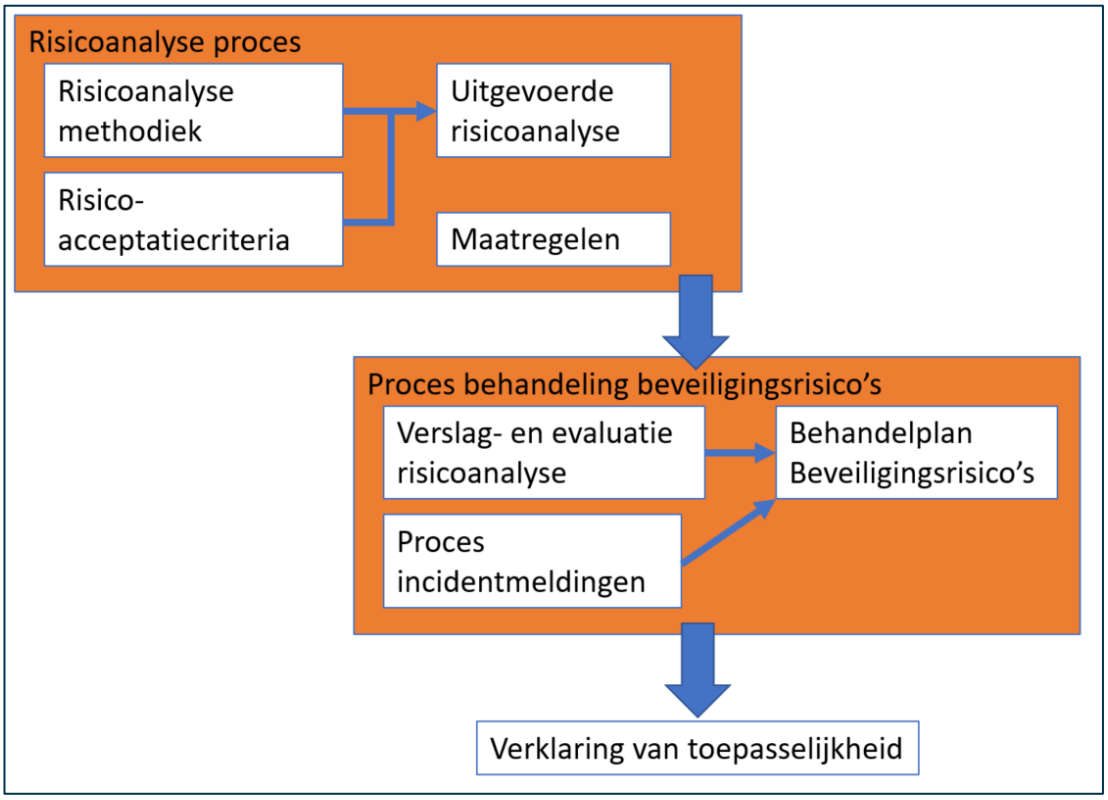
De eerste stap in het ISMS betreft het verkrijgen van het vereiste draagvlak van het management. Dit beveiligingsbeleid is hier een uiting van.



3.1.2 (Plan, Do) Risicoanalyse

De risicoanalyse is de basis voor het voeren van het informatiebeveiligingsproces. De twee belangrijkste resultaten hieruit zijn:

- **Het behandelplan** - Deze bevat SMART gespecificeerde maatregelen met als doel het verlagen van het risico. Dit behandelplan kan worden gezien als een levend werkdocument waarin alle openstaande acties worden bijgehouden.
- **Verklaring van toepasselijkheid** – Dit betreft het overzicht van alle normen van de BIR en of deze van toepassing zijn op de organisatie. Wanneer er bijvoorbeeld geen software wordt ontwikkeld, kunnen de normen die daarbij horen als 'niet van toepassing' worden verklaard.

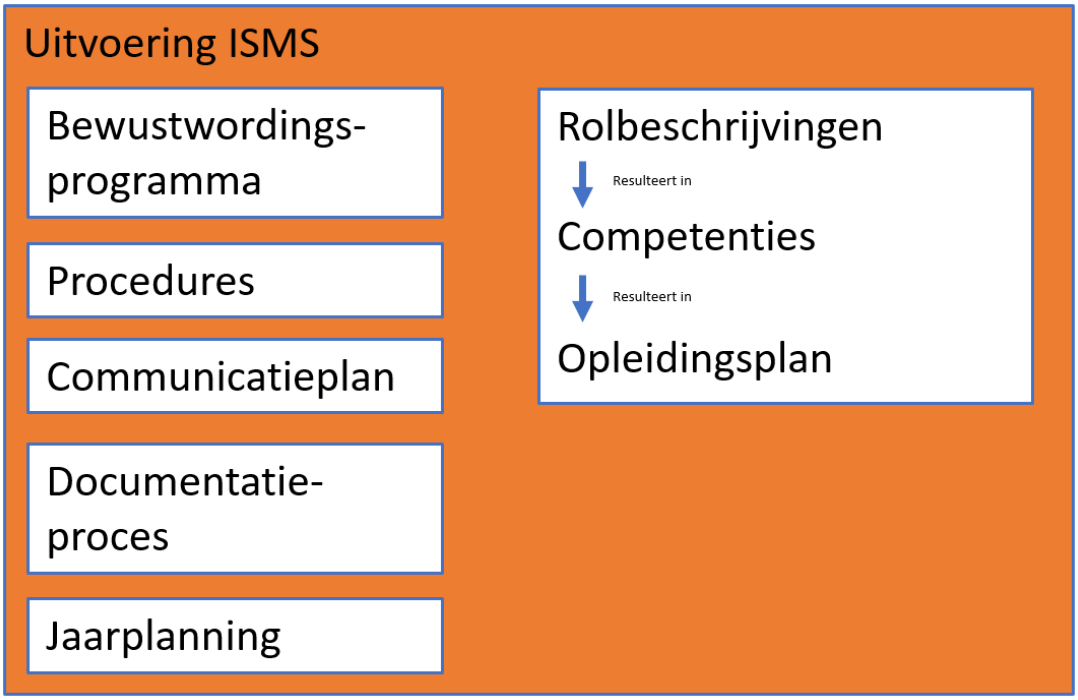


3.1.3 (Do) Uitvoering ISMS

De uitvoering van het ISMS omvat de meeste inspanning. De kern hier ligt, vooral de eerste keer dat het ISMS wordt doorlopen, bij de procedures. Voor alle normen moet worden beschreven hoe het IFV invulling aan de norm geeft. In audit-terminologie hebben we het hier over ‘de opzet’. Wanneer een auditor bij het IFV een audit uitvoert, wordt er gekeken naar ‘opzet’, ‘bestaan’ en ‘werking’.

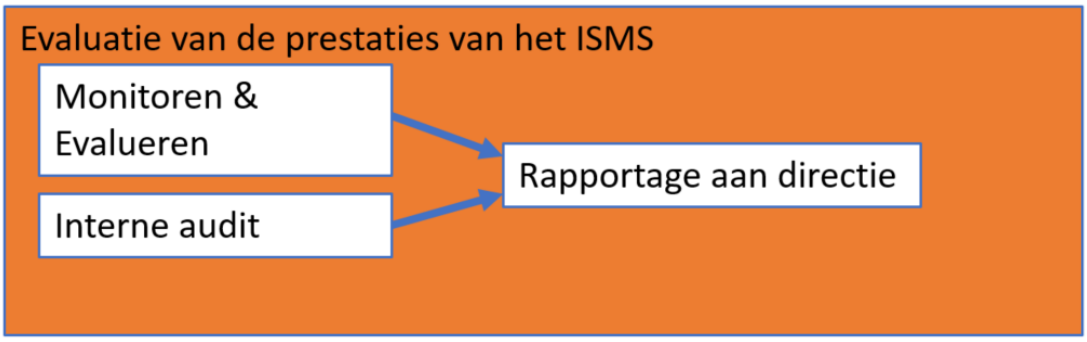
- Opzet = zeggen wat je doet.
- Bestaan = doen wat je gezegd hebt.
- Werking = dit aantonen over een langere periode.

De beschreven procedures behelzen dikwijls documenten met een beleidsmatig karakter maar ook werkprocedures, richtlijnen, etc.



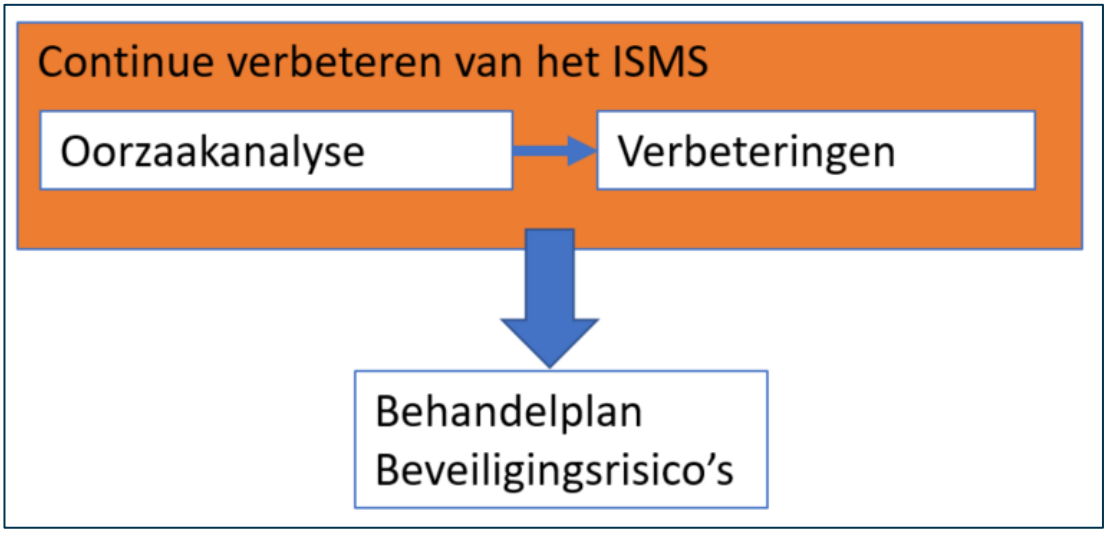
3.1.4 (Check) Evaluatie van het ISMS

Middels een monitoring, evaluatie en een interne audit wordt bepaald of en hoe het ISMS werkt. Dit wordt in een rapportage teruggekoppeld aan de directie.



3.1.5 (Act) Continu verbeteren

Het doel van de oorzaakanalyse is het vinden van de bronoorzaak van een bevinding. Dit leidt tot voorgestelde verbeteringen die worden opgenomen in het eerdergenoemde behandelplan.



4 Bijlage 1 – Overzicht BIR

Deze bijlage geeft een overzicht van de gehele BIR:2017. Per hoofdstuk is aangegeven wat de doelstelling is. De organisatie zal middels een risicoanalyse moeten bepalen op welke wijze invulling wordt gegeven aan het desbetreffende hoofdstuk.
De kolom ‘verantwoordelijke’ bevat de functionaris die doorgaans invulling geeft aan dit hoofdstuk.

BIG-hoofdstuk en onderwerp	Doelstelling	Verantwoordelijke
5.1 Aansturing door de directie van de informatiebeveiliging	Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.	Directie
6.1 Interne organisatie	Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.	Directie
6.2 Mobiele apparatuur en telewerken	Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.	Hoofd ICT
7.1 Voorafgaand aan het dienstverband	Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.	Hoofd HR
7.2 Tijdens het dienstverband	Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.	Lijnmanagement
7.3 Beëindiging en wijziging van dienstverband	Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.	Hoofd HR
8.1 Verantwoordelijkheid voor bedrijfsmiddelen	Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.	Hoofd ICT
8.2 Informatieclassificatie	Bewerkstelligen dat informatie een passend beschermingsniveau krijgt	Lijnmanagement

	dat in overeenstemming is met het belang ervan voor de organisatie.	
8.3 Behandelen van media	Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.	Hoofd ICT
9.1 Bedrijfseisen voor toegangsbeveiliging	Toegang tot informatie en informatieverwerkende faciliteiten beperken.	Hoofd ICT / lijnmanagement
9.2 Beheer van toegangsrechten van gebruikers	Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.	Hoofd ICT
9.3 Verantwoordelijkheden van gebruikers	Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.	Hoofd ICT
9.4 Toegangsbeveiliging van systeem en toepassing	Onbevoegde toegang tot systemen en toepassingen voorkomen.	Hoofd ICT
10.1 Cryptografische beheersmaatregelen	Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.	Hoofd ICT
11.1 Beveiligde gebieden	Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie-verwerkende faciliteiten van de organisatie voorkomen.	Hoofd ICT/hoofd facilitaire zaken
11.2 Apparatuur	Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.	Hoofd ICT
12.1 Bedieningsprocedures en verantwoordelijkheden	Correcte en veilige bediening van informatie- verwerkende faciliteiten waarborgen.	Hoofd ICT
12.2 Bescherming tegen malware	Waarborgen dat informatie en informatie-verwerkende faciliteiten beschermd zijn tegen malware.	Hoofd ICT
12.3 Back-up	Beschermen tegen het verlies van gegevens.	Hoofd ICT
12.4 Verslaglegging en monitoren	Gebeurtenissen vastleggen en bewijs verzamelen.	Hoofd ICT

12.5 Beheersing van operationele software	De integriteit van operationele systemen waarborgen.	Hoofd ICT
12.6 Beheer van technische kwetsbaarheden	Benutting van technische kwetsbaarheden voorkomen.	Hoofd ICT
12.7 Overwegingen betreffende audits van informatiesystemen	De impact van auditactiviteiten op uitvoerings- systemen zo gering mogelijk maken.	Hoofd ICT
13.1 Beheer van netwerkbeveiliging	De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.	Hoofd ICT
13.2 Informatietransport	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.	Hoofd ICT
14.1 Beveiligingseisen voor informatiesystemen	Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.	Hoofd ICT / Hoofd verwerving
14.2 Beveiliging in ontwikkelings- en ondersteunende processen	Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevens- cyclus van informatiesystemen.	Hoofd ICT
14.3 Testgegevens	Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.	Hoofd ICT
15.1 Informatiebeveiliging in leveranciersrelaties	De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.	Hoofd ICT / lijnmanagement
15.2 Beheer van dienstverlening van leveranciers	Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciers- overeenkomsten handhaven.	Hoofd ICT / lijnmanagement
16.1 Beheer van informatiebeveiligings-incidenten en -verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	Hoofd ICT / Security officer

17.1 Informatiebeveiligingscontinuïteit	Het inbedden van Informatiebeveiligingscontinuïteit in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.	Security officer
17.2 Redundante componenten	Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.	Hoofd ICT
18.1 Naleving van wettelijke en contractuele eisen	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.	lijnmanagement / Hoofd verwerving
18.2 Informatiebeveiligingsbeoordelingen	Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.	Security officer / externe auditor