

Hoogheemraadschap van Rijnland
Hoogheemraadschap van Schieland en de Krimpenerwaard

Beleid Informatieveiligheid

Datum	10-2020
Versie	3.0
Opgesteld door	Fred Hoogland, Gerard de Groot, Peter van der Els, Henny Kalloe, Hans Smit Ronald Marseille, Albert van As
Vastgesteld door	Directie
Corsa	13.38344

Inhoudsopgave

Inhoudsopgave	2
1. Aanleiding	4
1.1. Doel van het Beleid Informatieveiligheid	4
1.2. Ambitie van informatieveiligheid	5
1.3. Kaders van het Beleid Informatieveiligheid	5
2. Reikwijdte van het Beleid Informatieveiligheid	7
2.1. Werkingsgebied	7
2.2. Doelgroep	7
2.3. Structuur	7
2.4. Hiërarchie beleid	8
2.5. Bijstelling van beleid	8
3. Strategische uitgangspunten en randvoorwaarden van informatieveiligheid	9
4. Managementsysteem voor informatieveiligheid (ISMS)	11
5. Organisatie van Informatieveiligheid	15
5.1. Informatieveiligheid is een lijnverantwoordelijkheid	15
5.2. Risico-eigenaar	17
5.3. Systeemeigenaren	17
5.4. Maatregeleigenaren	17
5.5. Overlegvormen voor informatieveiligheid	18
6. Risicobeheersing	19
6.1. Niveaus van risicobenadering	19
6.2. Bepalen van risico's	20
6.3. Beoordeling van risico	21

7. Uitwerking	22
7.1. Invoering van het Beleid Informatieveiligheid	22
7.2. Omgaan met uitzonderingen	22
Bijlage A. BIO-controls	23
Bijlage B. Impact kwalificaties	27
Bijlage C. Versiebeheer	28

1. Aanleiding

De hoogheemraadschappen van Rijnland (HHR) en Schieland en de Krimpenerwaard (HHSK) hebben als missie dat zij ten dienste van mens en milieu in zijn gebied, samenwerkend met anderen, zorgen voor een duurzame veiligheid tegen en met water en zorgen voor blijvend genoeg water van goede kwaliteit op de juiste plaats.

Informatie is een essentieel bedrijfsmiddel van HHR en HHSK. Zonder informatie stoppen alle processen, is het niet mogelijk activiteiten goed uit te voeren, geautomatiseerde systemen te besturen, contracten te beheren of financiën te beheersen.

Daarnaast is er wet- en regelgeving die HHR en HHSK verplicht maatregelen te treffen om te voorkomen dat er ongelukken gebeuren met informatie en informatieverwerking. Voorbeelden daarvan zijn de Algemene verordening gegevensbescherming (AVG) en de verplichte open standaarden van het Forum Standaardisatie.

HHR en HHSK hebben een aantal strategische beslissingen genomen om de bescherming van informatie voor HHR en HHSK richting te geven. Die beslissingen zijn vastgelegd in dit Beleid Informatieveiligheid.

1.1. Doel van het Beleid Informatieveiligheid

Informatiebeveiliging is erop gericht HHR en HHSK passend te beveiligen door 1) risico's van uitval, manipulatie en onbevoegde kennisname van gegevens te reduceren tot een acceptabel niveau en 2) passende preventieve, curatieve en correctieve maatregelen te nemen.

Het Beleid Informatieveiligheid heeft in het verlengde hiervan de volgende doelen:

- Het waarborgen van de bedrijfscontinuïteit en dienstverlening van HHR en HHSK
- Het voorkomen en zo goed mogelijk afhandelen van incidenten
- Het minimaliseren van de eventuele gevolgen van incidenten

Dit beleidsdocument is bedoeld als richtlijn en handvat voor directie, management en uitvoerend verantwoordelijken van HHR en HHSK om met informatieveiligheid om te gaan. Het geeft de keuzes aan die door HHR en HHSK zijn gemaakt. Het beschrijft principes en accenten, gaat in op de verdeling van verantwoordelijkheden, en verduidelijkt hoe er met betrekking tot informatieveiligheid wordt gerapporteerd.

Het document is bindend voor HHR en HHSK. Daarbij geldt dat de geest belangrijker is dan de letter. Het belang van de informatieverwerking staat voorop.

1.2. Ambitie van informatieveiligheid

“Bij HHR en HHSK vindt bescherming van informatie risicogebaseerd plaats en wordt het information security management system (ISMS) in een plan-do-check-act cyclus beheerst. Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief. De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld (indien nodig verbeterd) en gerapporteerd aan het management.”

Deze ambitie correspondeert met het ‘ambitieniveau 4’ zoals vastgesteld door de Commissie Bestuurszaken, Communicatie en Financiën (CBCF) van de Unie van Waterschappen in 2014.

1.3. Kaders van het Beleid Informatieveiligheid

De volgende gemeenschappelijke betrouwbaarheidseisen en normen zijn voor HHR en HHSK van toepassing (BIO 5.1.1.1d):

- **Wet- en regelgeving**

Bestaande wet- en regelgeving is voor HHR en HHSK onverminderd van kracht. Bij het beveiligen van informatie bij HHR en HHSK wordt rekening gehouden met de verwerking van persoonsgegevens. De BIO biedt in een bijlage een overzicht van vigerende wet- en regelgeving. In de BIO-controls zijn waar relevant verwijzingen opgenomen naar bestaande wet- en regelgeving.

- **Normen voor informatiebeveiliging**

Naast wet- en regelgeving geldt voor overheidsorganisaties in Nederland, en daarmee ook voor HHR en HHSK, de Baseline Informatieveiligheid Overheid (BIO), een norm voor informatieveiligheid welke in 2018 is vastgesteld in het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). De BIO-standaarden fungeren als kader voor de tactische en operationele invulling van het Beleid Informatieveiligheid. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt.

Tevens geldt de IEC62443, de (internationale) norm die, aanvullend op de BIO, controls bevat specifiek voor de beveiliging van ICS/SCADA-systemen en -gebouwbeheersystemen. Het hanteren van de IEC62443 als norm voor de waterschappen is in 2019 vastgesteld door het

Uitvoerend Overleg van het Programma Informatieveiligheid bij Het Waterschapshuis.

In de bijlage 'BIO-controls' wordt een overzicht geboden van in dit Beleid Informatieveiligheid geadresseerde BIO-bepalingen.

- Bestaand beleid en regelingen van HHR en HHSK

Tot slot fungeren bestaand beleid en de geldige regelingen van HHR en HHSK als kader voor informatiebeveiliging. Denk hierbij aan het Privacybeleid, het Integriteitbeleid en het Beleid Risicomanagement¹.

- Relatie met Privacy

De Algemene Verordening Gegevensbescherming (AVG Art 5 en 32) verplicht de verwerker van persoonsgegevens 'passende' beveiliging toe te passen op persoonsinformatie, om nadelige gevolgen voor de betrokkenen te beheersen. Informatieveiligheid omvat ook de bescherming van persoonsinformatie. De Functionaris Gegevensbescherming ziet toe op zorgvuldige verwerking conform de AVG.

Onze informatiebeveiliging houdt rekening met de verwerking van persoonsgegevens, door eigenaarschap & classificatie van de verwerkingen, door evaluatie van security- en privacy-risico's en door de beveiligingsprocessen te integreren.

Alle organisatie-onderdelen (teams en/of afdelingen) voldoen controleerbaar aan bovenstaande kaders.

Bij twijfel over de toepasselijkheid van dit beleid, of twijfel over de interpretatie van hiervan, wordt van medewerkers verwacht dat zij de Security Officer (SO) of de Chief Information Security Officer (CISO) van HHR of HHSK raadplegen. Bij vergaande twijfel zal de directie besluiten op advies van de CISO.

¹ HHR en HHSK hebben geen gedeeld, samengevoegd Beleid Risicomanagement.

2. Reikwijdte van het Beleid Informatieveiligheid

2.1. Werkingsgebied

Dit Beleid Informatieveiligheid is van toepassing op de gehele organisaties- en op alle bedrijfsprocessen van HHR en HHSK:

- Alle informatieverwerking die plaatsvindt binnen- en namens HHR en HHSK
- Alle producten / diensten die worden geleverd en / of worden ingekocht
- Onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan- of namens HHR en HHSK.
- De middelen die hierbij worden ingezet, zoals (fysieke) toegangsbeveiliging en computers (zowel de kantoorautomatisering (KA) als de procesautomatisering (PA))

2.2. Doelgroep

Het Beleid Informatieveiligheid is in eerste instantie bestemd voor het management in de organisatie van HHR en HHSK. Het geeft hen richting in het nemen van verantwoordelijkheden op het gebied van informatieveiligheid.

In tweede instantie is dit document bestemd voor het bestuur en de rest van de organisatie, waaronder ook het tijdelijk personeel en personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie. Betrokkenheid van het bestuur is belangrijk om hen te informeren op het gebied van informatieveiligheid, zodat zij goed de afweging kunnen maken op nodige middelen. Betrokkenheid van de rest van organisatie is van belang om duidelijk te maken dat informatieveiligheid voor HHR en HHSK belangrijk is voor alle medewerkers.

Tenslotte is het Beleid Informatieveiligheid bedoeld voor de buitenwereld zodat die zich een beeld kan vormen dat HHR en HHSK serieus omgaan met informatieveiligheid.

2.3. Structuur

Dit Beleid Informatieveiligheid is het overkoepelende informatieveiligheidsbeleid voor de HHR- en HHSK, en is in tactische en operationele beleidsstukken verder uitgewerkt, bijvoorbeeld in een Beleid Fysieke Beveiliging, Beleid Backup en Restore en een Beleid Logische Toegangsbeveiliging.

De CISO zorgt voor publicatie online en voor communicatie van de wijzigingen naar de betrokken verantwoordelijken.

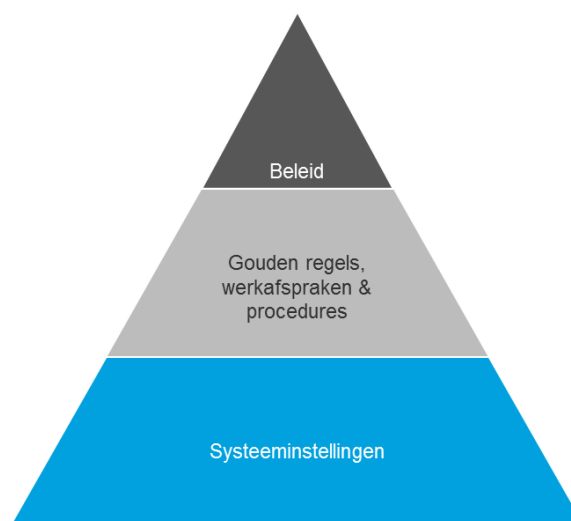
2.4. Hiërarchie beleid

Om informatieveiligheid te laten werken is het noodzakelijk dat er afspraken worden gemaakt binnen HHR en HHSK. Deze afspraken worden in 3 gebieden uitgesplitst.

Beleid: vastlegging van doelstellingen en aanpak van informatieveiligheid, benoemen van taken en verantwoordelijkheden, zowel strategisch (dit Beleid Informatieveiligheid) als verschillende stukken tactisch beleid.

Procedures: afspraken tussen medewerkers en management van HHR en HHSK hoe de processen moeten functioneren.

Systeeminstellingen: instellingen in systemen om effectief en efficiënt beveiliging toe te passen.



De piramide geeft de hiërarchie van de gemaakte afspraken weer. Hoe lager in de piramide de afspraken worden gemaakt, hoe gedetailleerder en praktischer van aard deze zijn.

2.5. Bijstelling van beleid

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. (BIO 5.1.1.1e)

3. Strategische uitgangspunten en randvoorwaarden van informatieveiligheid

In dit hoofdstuk staan de principes cq. strategische uitgangspunten (BIO 5.1.1.1a) op het gebied van informatieveiligheid. Daarnaast dienen deze uitspraken als leidraad waar bestuur, directie, management en medewerkers op terug kunnen vallen wanneer er zich vraagstukken voordoen die niet verder zijn uitgewerkt.

1. **Informatieveiligheid is een verantwoordelijkheid van de lijn.** De security-organisatie van HHR en HHSK ondersteunt- en controleert de lijn hierbij.
2. **De Baseline Informatiebeveiliging Overheid (BIO) en de IEC62443 worden gehanteerd als kaders voor informatieveiligheid.** De BIO geldt voor de gehele HHR- en HHSK-organisatie. Waar relevant geldt hierop aanvullend voor de beveiliging van PA-systemen de IEC62443.
3. **Informatieveiligheid steunt op drie pijlers: mensen, processen en techniek.** Beveiliging van informatie vraagt om een driedelige aanpak waarbij voldoende aandacht is voor het samenspel van mens, techniek en organisatie.
4. **HHR en HHSK passen ‘security by design’ toe.** Om passende beschermingsmaatregelen van informatieveiligheid te kunnen treffen, houden HHR en HHSK rekening met informatiebeveiliging bij het ontwerp van objecten, processen of systemen.
5. **De aanpak van Informatieveiligheid is risicogebaseerd.** Risicomanagement ligt aan de basis van de informatieveiligheid bij HHR en HHSK. Maatregelen worden genomen op basis van analyses van risico's op het niveau van organisatie, van (werk)processen en/of van informatiesystemen. Maatregelen dienen in balans te zijn met de te beschermen waarde. Deze maatregelen kunnen aanvullend zijn op de BIO en de IEC62443.
6. **De eigenaar van een bedrijfsproces- gegeven-, applicatie- of object is verantwoordelijk voor de risicobeheersing daarvan** en het bepalen en opvolgen van maatregelen die uit de risico-analyse volgen.

7. **Informatiebeveiliging, privacy en bedrijfscontinuïteit zijn onlosmakelijk met elkaar verbonden.** Informatiebeveiliging maakt een continue bedrijfsvoering mogelijk. Beschermingsmaatregelen dienen in verhouding te staan tot en bij te dragen aan het belang van iemands privacy en/of – van de continuïteit van de bedrijfsvoering.
8. **Iedere medewerker is zelf verantwoordelijk voor het naleven van beveiligingsmaatregelen.** Hierdoor is sprake van individuele aansprakelijkheid. Directie en management stellen medewerkers in staat de verantwoordelijkheid te nemen.
9. **Iedere medewerker van Rijnland en Schieland en de Krimpenerwaard werkt uitsluitend onder zijn eigen gebruikersnaam en wachtwoord op geautomatiseerde systemen van HHR of HHSK.** Het wachtwoord is persoonlijk en wordt niet aan anderen verstrekt, ook niet aan assistenten.
10. **Beheersing van informatieveiligheid**

HHR en HHSK hebben het beleid- en processen van informatieveiligheid zodanig ingericht in een information security management systeem (ISMS), dat de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.
11. **Pas toe of leg uit**

Daar waar wordt afgeweken van vastgesteld beleid of (de niet verplichte BIO-) kaders², legt de verantwoordelijk manager voor toepassing van betreffend beleid dit specifiek vast in een formeel te accorderen verklaring. De verklaring bevat een risico-inschatting van de afwijking en de mogelijke consequenties.

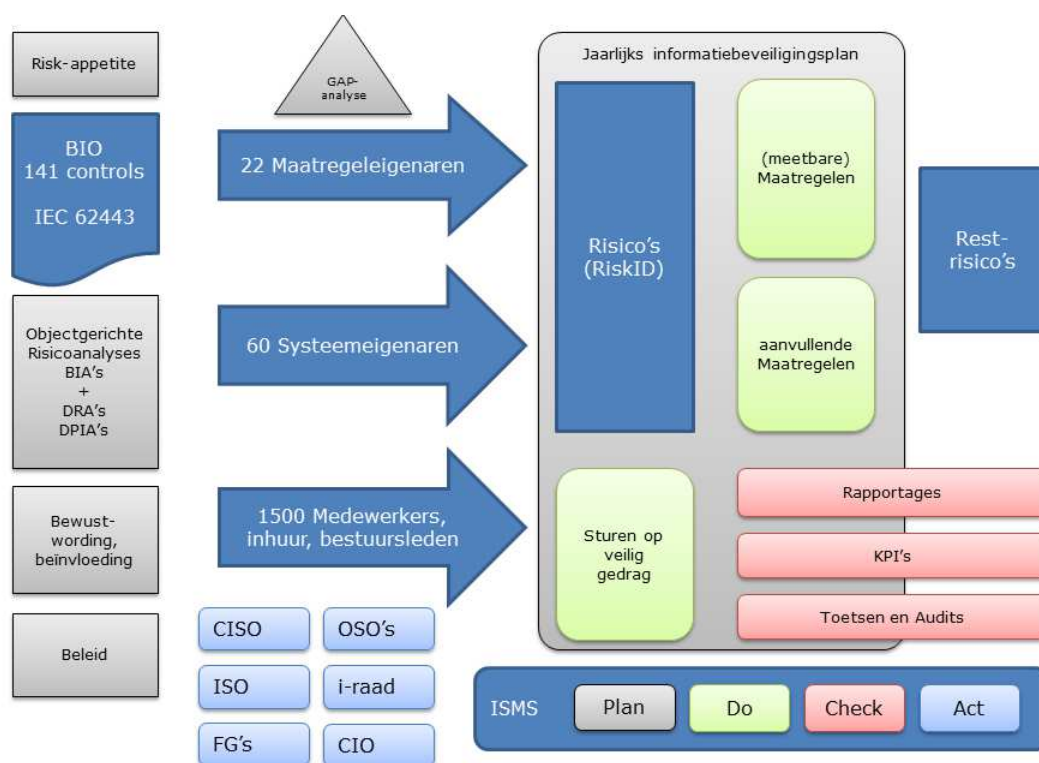
² De BIO schrijft voor veel controls verplichte overheidsmaatregelen voor waar niet van afgeweken mag worden.

4. Managementsysteem voor informatieveiligheid (ISMS)

Te beschermen informatie kan in allerlei gedaantes bestaan: digitaal, papier, gesproken woord, enzovoort. De mate waarin informatie blootstaat aan risico's van veiligheid, verandert daarbij voortdurend. Hierdoor beslaat bescherming van informatie een breed scala aan informatiebeveiligingsactiviteiten.

In control op risico's van informatieveiligheid

Middels het Information Security Management System (ISMS) hebben HHR en HHSK grip op het beveiligen van informatie. Hierin staat het risicobeheerproces centraal. Het ISMS is de motor van de informatiebeveiligingsactiviteiten en kent een plan-do-check-act cyclus. (BIO 1.1, 18.2.1.1).



Schema 1: ISMS HHR HHSK

Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het helpt HHR en HHSK onder andere om risico's te beheersen, passende beveiligingsmaatregelen te definiëren en - te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid van de informatievoorziening en bedrijfscontinuïteit te waarborgen.

Besturing en organisatie

Het informatielandschap is dermate groot, divers en complex dat goede besturing ('governance') essentieel is. Eindverantwoordelijk voor alles wat er met informatie gebeurt zijn de secretarissen (algemeen) directeur van HHR en HHSK. De directie legt verantwoordelijkheid af over informatieveiligheid aan het Dagelijks Bestuur en de Verenigde Vergadering. De directie stelt beleid en middelen van de informatiebeveiliging vast en belegt deze voor uitvoering bij de relevante rollen in de organisatie. Vanwege de samenhang tussen informatievoorziening, informatie-architectuur, documentbeheer, informatieveiligheid en privacy worden deze onderwerpen in samenhang besproken in de gezamenlijke i-raad, die een sleutelrol speelt in de governance. Meer hierover in Hoofdstuk 5 Organisatie van Informatieveiligheid.

Veiligheidscultuur

Veiligheid is mensenwerk, processen en systemen zijn uitsluitend een weerslag van keuzes van mensen. Dat betekent dat het ISMS alleen slaagt als alle betrokkenen hun rol naar behoren vervullen. Het gewenste gedrag van mensen vergt doorlopende aandacht. HHR en HHSK stimuleren voortdurend het informatiebeveiligingsbewustzijn. (BIO 5.1.1.1f).

Register van verwerkingen

Een van de belangrijkste voorwaarden voor een solide en aantoonbare beveiliging van informatie is een betrouwbaar overzicht van processen en systemen waarbinnen informatie verwerkt wordt. Hierin wordt vastgelegd welke informatie wordt verzameld, bewerkt en verspreid, de beveiligingsclassificatie, de (verwijzing naar de) risico-analyse en getroffen beschermingsmaatregelen en bovenal wie voor dat alles verantwoordelijk is.

Ordering van BIO-controls

HHR en HHSK realiseren een beheersbare beveiliging via logische opdeling van BIO-controls over de over de proces- en systeemeigenaren. De optimale toewijzing van de BIO-controls aan betreffende eigenaren binnen HHR en HHSK vindt plaats in afstemming met de directie.

Documenten

Naast gestructureerde verwerkingen kennen HHR en HHSK ook vele 'losse' documenten, in digitale- of papieren vorm. Deze zijn deels uitvoer van gestructureerde informatieverwerkingen, en deels het product van beleidsvoorbereiding en procesuitvoering door medewerkers. Documenten worden gegenereerd en opgeslagen, verzonden, bewaard en gearchiveerd in

informatiesystemen maar kennen hun eigen eigenaar en classificatie. Medewerkers dienen bij het verwerken van het document hiermee rekening te houden.

Ketens van informatie

In toenemende mate maken HHR en HHSK deel uit van ketens van informatieverwerkingen met andere organisaties cq partners. De verantwoordelijkheid voor de rol van HHR en HHSK in informatieketens berust bij benoemde eigenaren op dezelfde manier als voor verwerkingen die zich beperken tot binnen het eigen waterschap.

Security by design

Aandacht voor informatieveiligheid is bij HHR en HHSK organisatiebreed geïntegreerd in de primaire- en ondersteunende processen. De principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van processen, fysieke objecten en informatiesystemen en de beheersing van veranderingen hierin. (BIO 14.2.1.1)

Incidenten – detectie, melding & afhandeling

Incidenten van informatiebeveiliging worden bij HHR en HHSK consistent en doeltreffend geregistreerd en aangepakt, met inbegrip van communicatie over de beveiligingsgebeurtenissen en – over zwakke plekken in de beveiliging (BIO 16.1, 16.1.2.). Daar waar incidentprocessen binnen HHR en HHSK verschillen, zorgen de CISO's voor afstemming tussen de verschillende processen. De beheersing van informatiebeveiligingsincidenten is aangesloten op het organisatiebrede calamiteitenproces.

Informatiebeveiligingsplannen jaarlijks geactualiseerd

In het informatiebeveiligingsplan worden de verbeteractiviteiten voor de realisatie van het gewenste beveiligingsniveau vastgelegd. Jaarlijks wordt dit informatiebeveiligingsplan opgesteld, waaraan de specifiek benoemde maatregel-eigenaren zich aan committeren. Het bevorderen van het beveiligingsbewustzijn maakt een belangrijk onderdeel uit van het informatiebeveiligingsplan. Het informatiebeveiligingsplan wordt beoordeeld door de i-Raad en vastgesteld door de directies van HHR en HHSK.

Beoordeling werking ISMS

HHR en HHSK volgen voor de beoordeling van de werking van ISMS en – van de beschermingsmaatregelen – het concept van de 3 verdedigingslinies:

- De 1e Linie is het lijnmanagement die zelf toeziet op haar diverse rollen en de beschermingsmaatregelen.
- De 2e Linie is de CISO, die de werking van het ISMS beoordeelt en evalueert voor verbetering.
- De 3e Linie wordt gevormd door de periodieke audit die opzet, bestaan én werking van het ISMS beoordeelt.

Rapportage

De CISO rapporteert over de activiteiten- en resultaten van het ISMS. Denk hierbij aan de voortgang van zijn eigen activiteiten, de stand van de implementatie van de BIO baseline, registratie en classificatie van objecten, de verwerking en realisatie van extra maatregelen, de veiligheidscultuur, incidenten en KPI's van informatieveiligheid.

De CISO rapporteert over de mate waarin de genomen beschermingsmaatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd (BIO 4.1).

Maatregелеigenaren rapporteren over de implementatie en werking van alle maatregelen vanuit zowel de baseline als de risicoanalyses, over incidenten en over geplande verbeteracties.

Systeemeigenaren rapporteren over de implementatie en werking van de systeemspecifieke maatregelen aan de directie via de CISO.

In de P&C-cyclus wordt gerapporteerd over naleving van beleid- en normen van informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring over de informatiebeveiliging (IB-ICV). Indien voldoende herkenbaar kan de IB-ICV voor informatiebeveiliging onderdeel zijn van de bestuursrapportage (BIO 18.2.2.1).

Ook informatiesystemen worden jaarlijks onderworpen aan een test op naleving van de beveiligingsnormen en op eventuele kwetsbaarheden. (BIO 18.2.3.1).

De directie neemt in een directievergadering kennis van de rapportage van het ISMS, verleent décharge aan de CISO en legt haar besluit vast.

5. Organisatie van Informatieveiligheid

5.1. Informatieveiligheid is een lijnverantwoordelijkheid

De secretaris-directeuren zijn integraal verantwoordelijk voor de beveiliging van de informatie die binnen- of uit hoofde van HHR en HHSK verwerkt wordt (BIO 1.2b, 1.2e). Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast (BIO 1.2f). De verantwoordelijkheid voor uitvoering van risico-analyses en het treffen van informatiebeschermingsmaatregelen is belegd bij de teamleiders en resultaatmanagers (HHR) en afdelingshoofden (HHSK) (BIO 1.2d). Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit (BIO 1.2g). De gehanteerde niveaus van risicobeheersing worden verder beschreven in hoofdstuk 6. Risicobeheersing.

Risico's van informatieveiligheid en hierbij passende beschermingsmaatregelen worden in een plan-do-check-act-cyclus beheerst (BIO 1.2c). Het management stelt jaarlijks beveiligingsplannen op, stuurt op uitvoering van risicoanalyses en stuurt op het nemen- en beheren van mitigerende maatregelen. Ook wordt periodiek getoetst-, gerapporteerd- en geëvalueerd over de effectiviteit van het beschermingsmaatregelen, en ten slotte over het doorvoeren van verbeterpunten.

De i-raad, waar beide waterschappen op managementniveau vertegenwoordigers in hebben afgevaardigd, bepaalt op hoofdlijnen de invoering van informatieveiligheid en neemt beslissingen over beleid, financiën, procedures en richtlijnen, personeel en projectinhoud. De i-raad adviseert de directies van HHR en HHSK.

Vanuit de HHR-HHSK-gezamenlijke Security Office worden de HHR- en HHSK-organisaties ondersteund bij het toezicht op- en de uitvoering van werkzaamheden van informatieveiligheid. De CISO van HHR en HHSK bepalen in onderling overleg wie voorzitter is van de Security Office en wie vervangend voorzitter.

In onderstaande tabel is in algemene zin een overzicht gegeven taken en verantwoordelijkheden op het gebied van het Informatieveiligheidsbeleid (BIO 5.1.1.1b, 6.1.1).

Rol / Functie / Afdeling HHR - HHSK	Taken en verantwoordelijkheden m.b.t. informatieveiligheid
Dagelijks Bestuur	Integrale verantwoordelijkheid
Secretaris (Algemeen) Directeur	Is eindverantwoordelijk voor informatieveiligheid en restrisico's, stelt het beleid vast en stuurt op toepassing van beleid
CISO	Monitort en toetst de werking van het ISMS. Zorgt voor bewustwording in de organisatie.
Security Officer	Ondersteunt de CISO en het lijnmanagement in toepassing van het beleid en is aanspreekpunt voor vragen en issues
CIO	Strategisch adviseur voor o.a. informatiebeveiliging en tevens voorzitter van de i-raad
i-raad	Stelt tactisch beleid vast
Adviseurs informatieveiligheid (Algemeen / PA)	Beheer beleid informatieveiligheid en adviserend aan de CISO
Functionaris gegevens- bescherming	Toeziens op de naleving van de Algemene verordening gegevensbescherming (AVG) binnen HHR en HHSK
HHR: Teamleider / stafhoofd HHSK: Afdelingshoofd	Invoeren, volgen en handhaven van het beleid, uitvoeren van risico-analyses en daaruit voorkomende maatregelen ter beveiliging van informatie. Stuurt op veilig gedrag van medewerkers.
Systeem- en objecteigenaar	Verantwoordelijk voor de veiligheid van het systeem of object
Beveiligingsarchitect	Borgt informatieveiligheidsaspecten bij het ontwerpen van informatiesystemen of -gebouwen
Beveiligingsspecialist	Implementeert en beheert ICT- of fysieke beveiligingsmaatregelen
Medewerkers	Leven het beleid na en signaleren- en melden problemen of incidenten
Concern Control (of een andere door de directie aangewezen onafhankelijke functionaris)	Opstellen jaarlijks auditplan en uitvoeren audits op opzet, bestaan en werking van het ISMS

Tabel 1. Taken en verantwoordelijkheden m.b.t. informatieveiligheid.

5.2. Risico-eigenaar

De secretaris (algemeen) directeur van HHR en HHSK is als eindverantwoordelijke voor informatieveiligheid enig eigenaar van de informatierisico's (BIO 1.2e). Door op organisatieniveau in een bestuurlijke risicoanalyse (BRA) het risicobeeld ('risk appetite') te ontwikkelen en te communiceren naar de verwerkings- en maatregелеigenaren geeft de directie richting en gewicht aan de beveiligingsinspanningen binnen HHR en HHSK. Risicobeelden worden ook op het niveau van processen en informatiesystemen ontwikkeld en op het niveau van BIO-controls. Meer hierover in Hoofdstuk 6 Risicobeheersing.

5.3. Systeemeigenaren

Informatie die binnen een proces of systeem binnen HHR en HHSK verwerkt wordt, heeft een eigenaar, verder 'systeemeigenaar' genoemd. De verantwoordelijkheid voor de beveiliging van informatie omvat de hele levenscyclus ('van creatie tot archivering en verwijdering') van de informatieverwerking en omvat het organiseren en controleren van passende beveiliging. Bij HHR zijn de teamleiders de systeemeigenaren, bij HHSK de afdelingshoofden.

Deze systeemeigenaar stelt het beveiligingsniveau van de verwerking vast en past het algemene risicobeeld, aangereikt door de BIO, toe op 'zijn' verwerking, voegt het verwerkings-specifieke risicobeeld zoals naar voren gekomen tijdens de Business Impact Analyse (BIA) en de Diepgaande Risico Analyse (DRA) (en eventuele bijzondere eisen en kaders) toe (BIO 1.2f) en deelt dat met 'zijn' maatregelverantwoordelijke(n) (BIO 1.2g). Van het vereiste beschermingsniveau en de uitgevoerde risico-analyse verzamelt de systeemeigenaar bewijzen. De CISO rapporteert over de voortgang en monitort de kwaliteit van de risico-analyses. Meer over de BIA en de DRA in Hoofdstuk 6 Risicobeheersing.

5.4. Maatregелеigenaren

Om informatie te beveiligen dienen beschermingsmaatregelen getroffen te worden, minimaal op het niveau van de Baseline Informatiebeveiliging Overheid (BIO). Elke BIO-control – en daarmee elke beschermingsmaatregel - heeft een eigenaar, verder 'maatregелеigenaar' genoemd.

Bij HHR zijn de teamleiders de maatregелеigenaren, bij HHSK de afdelingshoofden. Onder deze maatregелеigenaren is ook de verantwoordelijkheid voor ketens van informatiesystemen belegd (BIO 5.1.1.1c). Ook externen (denk hierbij aan verwerkers, cloud) kunnen maatregelverantwoordelijkheid hebben.

De maatregeleigenaren ontwerpen en documenteren (BBN2-)baseline- en extra-maatregelen, vanuit de risicoanalyses en eventueel aanvullende eisen vanuit de proces- of systeemeigenaren, conform implementatierichtlijnen (BIO 1.2d).

Van ontwerp en werking van de maatregel verzamelt de eigenaar bewijzen. De CISO rapporteert over de voortgang en monitort de kwaliteit van ontwerp- en implementatie van de maatregelen.

5.5. Overlegvormen voor informatieveiligheid

Voor overleg, coördinatie en afstemming op het gebied van informatieveiligheid worden de volgende overlegvormen onderscheiden:

- Overleg tussen de directie, de CISO en de FG
- Overleg binnen de i-raad, waar de Chief Information Security Officers (CISO) deel van uitmaken
- Informatiebeveiligingsoverleg (ISO)

De directie, de CISO en de Functionaris Gegevensbescherming (FG) overleggen periodiek over informatieveiligheid en privacy in het HHR-HHSK-gezamenlijk directieoverleg. Ter sprake komen bijvoorbeeld zaken van beleid en strategie, tests/oefeningen en audits, de rapportage over KPI's, incidenten, afwijkingen, het risico-register, en de 'in control verklaring'.

De i-raad (waar de CISO's deel van uitmaken) overlegt periodiek over informatieveiligheid in samenhang met ICT-Servicemanagement, Projectportfoliomanagement, Architectuur en Informatiebeheer. In dit overleg wordt aandacht besteed aan (voortgangs)-rapportages, voorstellen voor het Dagelijks Bestuur, voorstellen voor wijzigingen van het informatiebeleid, investeringsvoorstellen voor beveiligingsmaatregelen. De CIO als voorzitter van de i-raad rapporteert periodiek aan het HHR-HHSK-gezamenlijk directieoverleg.

De werkgroep informatieveiligheid (ISO) komt periodiek bij elkaar onder leiding van de CISO om te bespreken de uitvoering van beleid en richtlijnen, de voortgang op de beveiligingsplannen, bewustwording, risico's en incidenten en rapportages.

6. Risicobeheersing

De basis voor informatiebeveiliging is risicomanagement. Risico is het effect van onzekerheid op het behalen van de (bedrijfs)doelstellingen (ISO31000).

Het optimale niveau van informatiebeveiliging wordt bereikt door een risicoanalyse en hieropvolgend een zorgvuldige afweging van kosten en baten van te nemen beschermingsmaatregelen.

Het tactisch deel van de BIO fungeert als norm en als toetsingskader voor de inrichting van de beheersing van risico's van informatieveiligheid.

6.1. Niveaus van risicobenadering

Binnen HHR en HHSK worden 3 niveaus onderscheiden, waarop risico's van informatieveiligheid worden beheerst en op basis waarvan het risicobeeld tot stand komt:

- Niveau van organisatie: De secretaris (algemeen) directeurs van HHR en HHSK vormen hun risicobeeld (haar 'risk appetite') in een bestuurlijke risico analyse (BRA) op strategisch niveau en communiceren dit risicobeeld op organisatieniveau naar de verwerkings- en maatregeleigenaren.
- Niveau van objecten: proces- en systeemeigenaren vormen zich middels een 'business impact analyse' (BIA) een beeld van het 'belang' van de informatieverwerkende objecten en bovenliggende processen voor de organisatie en de voorziene impact bij verstoring. Afhankelijk van de aard van de impact kan een diepgaande risicoanalyse (DRA) worden uitgevoerd, waarmee een dieper inzicht wordt verkregen van risico's en noodzakelijke, op de BIO aanvullende, beschermingsmaatregelen.
- Niveau van controls: het minimale beschermingsniveau waarop HHR en HHSK informatie beveiligen is gedefinieerd in de controls zoals opgenomen in de BIO. Specifiek benoemde teamleiders of afdelingshoofden hebben in hun rol als maatregeleigenaar de verantwoordelijkheid uitvoering te geven aan de BIO-controls en worden betrokken bij het bepalen van de juiste toepassing van een BIO-control, het bepalen van het verschil tussen de huidige- en gewenste situatie en tot slot het bepalen van te realiseren beschermingsmaatregelen.

6.2. Bepalen van risico's

Bij de bepaling van het risico wordt gebruik gemaakt van de volgende formule:

Risico = Kans x Impact

Kans

In de context van informatieveiligheid, is kans een combinatie van bedreiging en kwetsbaarheid. HHR en HHSK onderscheidt drie niveaus van kans:

Hoge kans	<i>Er is een zeer reële waarschijnlijkheid dat de gebeurtenis zich voordoet.</i>	Vermoedelijk optreden van één of meerdere malen per jaar
Middel kans	<i>Er is een reële waarschijnlijkheid dat de gebeurtenis zich voordoet.</i>	Een vermoedelijk optreden tussen de eens per jaar en eens per vijf jaar
Lage kans	<i>Er is geen reële waarschijnlijkheid dat de gebeurtenis zich voor doet.</i>	Een vermoedelijk optreden minder dan eens per vijf jaar

Impact

Consequenties van (potentiële) incidenten worden in drie categorieën verdeeld: Hoog, Midden en Laag. De directie heeft de kwalificaties gebaseerd op overwegingen rond het huidige mandateringsbesluit en de volgende grondbeginselen:

Hoge impact	incidenten die leiden tot betrokkenheid van het dagelijks/algemeen bestuur
Middel impact	incidenten die leiden tot betrokkenheid van de directie
Lage impact	zijn incidenten die binnen de lijn kunnen worden opgelost

In Bijlage B is een tabel opgenomen met een volledig overzicht van de impact-kwalificaties in diverse categorieën.

6.3. Beoordeling van risico

Uit de vermenigvuldiging van kans en impact volgt de onderstaande matrix:

Kans	Hoog	Middel risico	Hoog risico	Hoog risico
	Midden	Laag risico	Middel risico	Hoog risico
	Laag	Laag risico	Laag risico	Middel risico
		Laag	Midden	Hoog
		Impact		

Geïdentificeerde en geanalyseerde risico's worden binnen HHR en HHSK als volgt behandeld:

Kwalificatie risico	Wenselijke behandeling van het risico
Hoog risico	Deze risico's zijn niet acceptabel. HHR en HHSK stellen alles in het werk om deze risico's te verminderen. <i>Wanneer een adequate behandeling niet mogelijk is of te kostbaar blijkt, mag alleen de directie een HOOG risico accepteren.</i>
Middel risico	Deze risico's zijn niet acceptabel. HHR en HHSK vereisen een volledige afdekking door de maatregelen in de BIO. <i>Wanneer een adequate behandeling niet mogelijk is of te kostbaar blijkt, mag alleen de directie een MIDDEL risico accepteren.</i>
Laag risico	Lage risico's zijn acceptabel. Voor lage risico's wordt alleen geïnvesteerd in maatregelen waarvan de waarde aantoonbaar is gemaakt.

7. Uitwerking

7.1. Invoering van het Beleid Informatieveiligheid

Dit Beleid Informatieveiligheid is van kracht vanaf het moment van goedkeuring door de Directie. De CISO's stellen het lijnmanagement op de hoogte van dit beleid en begeleiden de invoering.

7.2. Omgaan met uitzonderingen

In de praktijk zullen uitzonderingen op dit Beleid voorkomen. Daartoe is het nodig dat:

- Uitzonderingen op het gebied van Informatieveiligheid zijn goedgekeurd door de i-raad. De goedkeuring wordt schriftelijk vastgelegd; de details van de uitzondering ook.
- Om de uitzonderingen te monitoren rapporteert de CISO deze één keer per half jaar aan de Directie.
- Uitzondering zijn tijdelijk – er geldt een uiterste houdbaarheidsdatum.
- Na afloop van de actie/uitzondering worden de resultaten gemeld.

Bijlage A. BIO-controls

In dit Beleid Informatieveiligheid zijn de volgende BIO-controls geadresseerd:

1. Informatiebeveiliging bij de overheid

1.2. Informatiebeveiligingskader en uitgangspunten overheid

- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen).
- Informatiebeveiliging is een cyclisch proces volgens de Plan-Do-Check-Act cyclus).
- Deze Plan-Do-Check-Act cyclus maakt het lijnmanagement verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement.
- De secretaris/algemeen directeur van een organisatie is eindverantwoordelijk voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie.
- Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast
- Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit.

3. Basisbeveiligingsniveaus

3.2 BBN2

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. (..) De controls van het BBN2 omvatten de controls van BBN1. Dit geldt ook voor de maatregelen waarbij enkele maatregelen van BBN1 in de BBN2-variant verzwakt zijn.

4. Verantwoording over de BIO

4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau

Het lijnmanagement stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.

5. Informatiebeveiligingsbeleid

5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

Nummer BIO- control	BBN	Omschrijving
5.1.1	1	Beleidsregels voor informatiebeveiliging Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a. de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b. de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c. de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d. de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e. de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f. de bevordering van het beveiligingsbewustzijn.
		Handreikingen: BIO-001-Informatiebeveiligingsbeleid
5.1.2	1	Beoordeling van het informatiebeveiligingsbeleid Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
5.1.2.1	1	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.

6. Organiseren van informatiebeveiliging

6.1 Interne organisatie

6.1.1	1	Rollen en verantwoordelijkheden bij informatiebeveiliging Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6.1.1.1	1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.

6.1.1.2	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
6.1.1.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
6.1.1.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
		Handreiking: BIO-CISO-functieprofiel

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

14.2.1	1	Beleid voor beveiligd ontwikkelen Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.
14.2.1.1	1	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.

16. Beheer van informatiebeveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

16.1.2	1	Rapportage van informatiebeveiligingsgebeurtenissen Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd
--------	---	--

18. Naleving

18.2 Informatiebeveiligingsbeoordelingen

18.2.1	1	Onafhankelijke beoordeling van informatiebeveiliging De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor
--------	---	---

		informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.
18.2.1.1	2	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.
18.2.1.2	2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.
18.2.2	1	Naleving van beveiligingsbeleid en -normen De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
18.2.2.1	1	In de P&C-cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.
18.2.3	1	Bewoordeling van technische naleving Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
18.2.3.1	2	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.

Bijlage B. Impact kwalificaties

#	Toelichting	1: Lage impact	2: Middel impact	3: Hoge impact
1	Besturing/politiek Nadelige effecten op de besturing van de organisatie door politieke onrust.	Beperkt verlies van in control zijn (op te lossen in de lijn)	Significant verlies van in control zijn (directie-betrokkenheid vereist)	Totaal verlies van in control zijn (dagelijks/ algemeen bestuur betrokkenheid vereist, of erger)
2	Maatschappelijk Materiële schade en nadelige effecten op het welzijn en aan de ingelanden.	Materiële schade die is op te lossen in de lijn	Schade aan persoonlijk welzijn of materiële schade (directie-betrokkenheid vereist)	Dode(n), meerdere zieken of gewonden of materiële schade
3	Imago Imagoschade aan de organisatie / twijfel bij ingelanden aan bestaansrecht.	Beperkt verlies van vertrouwen (op te lossen in de lijn)	Significant verlies van vertrouwen (directie-betrokkenheid vereist)	Ernstig verlies van vertrouwen (dagelijks/ algemeen bestuur betrokken)
4	Financieel Verlies van inkomsten of eigendommen van de organisatie.	Vereist hooguit herbudgettering in de lijn	Vereist herbudgettering op organisatieniveau	Vereist begrotingswijziging.
5	Juridisch Nadelige juridische effecten door onrechtmatig handelen	De organisatie handelt rechtmatig (conform wet- en regelgeving). Er zijn geen juridische consequenties.	De organisatie handelt onrechtmatig* Directie-betrokkenheid vereist.	Dermate onrechtmatig handelen dat het dagelijks/ algemeen bestuur betrokken raakt
6	Productiviteit Verlies van productiviteit.	Productiviteitsverlies is op te lossen in de lijn	Productiviteitsverlies vereist betrokkenheid van de directie	Productiviteitsverlies vereist betrokkenheid van het dagelijks/ algemeen bestuur
7	Herstel Benodigde kosten of inspanningen voor herstel na een incident	Vereist hooguit herbudgettering in de lijn	Vereist herbudgettering op organisatieniveau	Vereist begrotingswijziging.

Bijlage C. Versiebeheer

Versie	Datum	Bijzonderheden	Auteur
0.1	6 maart 2013	Concept ter review	Jacques Cazemier / Albert van As
1.0	14 juni 2013	Definitief	Ronald Marseille / Albert van As
1.1	8 januari 2014	- Paragraaf 1.3: Aangevuld met Baseline Informatieveiligheid Waterschappen als kader - Paragraaf 1.3: Aangevuld met 'Het informatieveiligheidsbeleid wordt minimaal één keer in de drie jaar geëvalueerd en desgewenst bijgesteld'. - Paragraaf 4.1: toegevoegd verantwoordelijkheden Team Informatiemanagement - Hoofdstukken 4 en 5: Informatieveiligheidsoverleg (IBO) vervangen door Security Board. - Bijlage A. Kaders en standaarden/normen: verwijzing naar de NORA vervangen door de Baseline Informatieveiligheid Waterschappen	Ronald Marseille / Albert van As
2.0	november 2014	Toevoeging risicobeheersing in doel, hoofdstuk risicobeheersing en bijlage B: impact schaal. Beleid zowel van toepassing gemaakt voor HHR als HHSK	Ronald Marseille, Robert Dijkhoff, Albert van As
2.1	mei 2016	Verheldering reikwijdte tot en met procesautomatisering, update	Ronald Marseille, Jeroen Hendriks

		rolbeschrijvingen, aanpassen benamingen organisatie HHSK.	
2.2	september 2017	Vervanging Security Board door i-raad. Update taakbeschrijving CIO en security officer.	Ronald Marseille
2.3	Juni 2019	Organisatiewijzigingen Rijnland, wijzigingstermijn beleidsstukken, AVG vervangt WBP, introductie BIO	Albert van As, Ronald Marseille
3.0	Oktober 2020	Aanpassingen op basis van de BIO en op basis van organisatorische- en procesmatige wijzigingen bij HHR / HHSK	Albert van As, Ronald Marseille, Peter van der Els, Fred Hoogland