Hoogheemraadschap van
Delfland

INFORMATIEBEVEILIGINGSBELEID DELFLAND

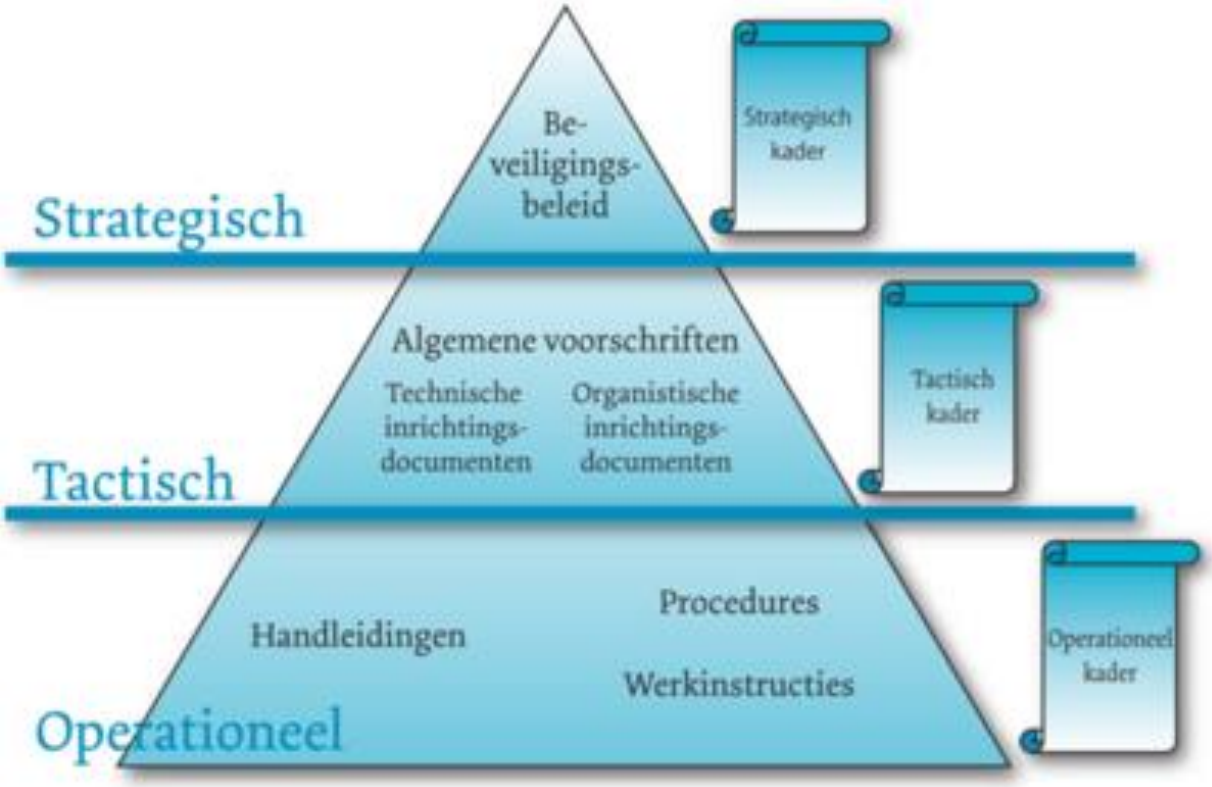
INHOUD

1. Inleiding

1.1 Context

Waterschappen behoren tot de kritische infrastructuur en hebben een verantwoordelijkheid de risico's te onderkennen en maatregelen te nemen op beveiligingsgebied. Het betreft fysieke beveiliging van gebouwen, beveiliging van het dataverkeer en de verantwoordelijkheid en het bewustzijn van de medewerker hoe om te gaan met deze middelen.

Dit document beschrijft de informatiebeveiligingsdoelstellingen. Er is voor gekozen deze beschijvingen kort te houden. Nadere uitwerkingen met passende maatregelen zijn opgenomen in de matrix informatiebeveilingsplan. Het beleid wordt op hoofdlijnen beschreven en sluit aan bij de Baseline informatiebeveiliging Waterschappen[1] (= BIWA). In deze Baseline is het strategische en tactisch normenkader beschreven en vastgesteld.



In de jaarlijkse team uitvoeringsplannen worden de maatregelen opgenomen die uit dit Informatiebeveiligingsplan voortvloeien. De uitvoeringsplannen worden op teamniveau samengesteld door en voor de medewerkers. Dit zorgt voor bewustzijn en betrokkenheid van het personeel bij de informatiebeveiliging.

1.2 Doelstelling van informatiebeveiliging

Een betrouwbare informatievoorziening is essentieel voor het goed functioneren van de processen bij Delfland. Informatiebeveiliging is het proces waarmee de betrouwbaarheid van de informatievoorziening wordt geborgd en beheerd.

[1] De Unie van waterschappen heeft een normenkader vastgesteld rondom informatiebeveiliging. Delfland volgt dit normenkader.

vervolg 1.2

De klanten en partners van Delfland kunnen met deze borging er van uitgaan dat de bescherming tegen hoog water, de kwaliteit van het oppervlaktewater en zuivering van het afvalwater in goede handen is. Het informatiebeveiligingsbeleid borgt ook de vertrouwelijkheid van data waar de privacy van mens en bedrijf in het geding is.

De secretaris-directeur van het Hoogheemraadschap van Delfland is eindverantwoordelijk voor het informatiebeveiligingsbeleid en het management draagt het beleid ten volle uit binnen de organisatie.

1.3 Componenten van informatiebeveiliging

Informatiebeveiliging is gebaseerd op drie beveiligingsprincipes:

- **Beschikbaarheid**
  Doel: zeker stellen dat informatie en essentiële diensten op de juiste momenten en plaatsen beschikbaar zijn.

- **Integriteit**
  Doel: het waarborgen van de correctheid en de volledigheid van informatie en computerprogrammatuur.

- **Vertrouwelijkheid**
  Doel: het beschermen van gevoelige informatie tegen ongeautoriseerde kennisname.

Informatiebeveiliging streeft niet naar absolute veiligheid. Het streven is de bedrijfsdoelen door middel van organisatorische procedures en technische voorzieningen te realiseren. De verantwoordelijke partijen maken telkens een bewuste afweging tussen het bedrijfsbelang en de noodzakelijke informatiebeveiligingsmaatregelen.

1.4 Wettelijke basis

De wettelijke basis voor informatiebeveiliging zijn Europese richtlijnen en landelijke wet- en regelgeving:

- Wet computercriminaliteit
- Wet bescherming persoonsgegeven (WBP)
- Archiefwet
- Databankenwet
- Wet elektronisch Bestuurlijk Verkeer
- Wet gemeentelijke basisadministratie (GBA)
- Wet openbaarheid bestuur (WOB).

Deze regelingen bevatten een resultaatsverplichting tot een passend niveau van informatiebeveiliging. Binnen Delfland is de borging van de compliance met deze wet- en regelgeving belegd bij het team JVI (juridisch).

1.5 Standaarden

Er wordt uitgegaan van de open standaarden van de "pas toe of leg uit" lijst van het forum standaardisatie[2], de ISO 27001:2005 en 27002:2007. Deze lijst is een aanwijzing aan alle overheidsorganisaties in Nederland om deze standaard te gebruiken. Overheden mogen alleen afwijken ingeval van redenen van bijzonder gewicht. Overheden zijn verplicht om afwijkingen gemotiveerd vast te leggen in de administratie (bijvoorbeeld in het jaarverslag).

1.6 Bereik

Het bereik omvat de bedrijfsfuncties , ondersteunende middelen (apparatuur, gebouwen etc.) en informatie van het waterschap en is ook van toepassing op informatiesystemen die buiten het waterschap draaien en / of als taken aan derden zijn uitbesteed.

1.7 Status van het beleid

Dit beleid treedt in werking na vaststelling door het College van Dijkgraaf en Hoogheemraden.

[2] Overheden en semi-overheden zijn verplicht om bij de aanschaf van ICT-producten en -diensten te kiezen voor de relevante standaarden van de 'pas toe of leg uit'-lijst. Overheden en semi-overheden mogen alleen afwijken (d.w.z. *'niet toepassen'*) ingeval van redenen van bijzonder gewicht.

2. Implementatie informatiebeveiliging

Voor de implementatie van informatiebeleid bij Delfland worden telkens de volgende stappen, in een vaste volgorde, doorlopen:

Benoemen van verantwoordelijkheden.
Delfland koppelt de rol aan een functionaris.
In onderstaand schema zijn de functies en verantwoordelijkheden vastgelegd. De BIWA en de functie toedeling (of benaming) bij Delfland verschillen op een aantal punten. Een functionaris beveiliging en functionaris gegevensbescherming is niet geformaliseerd. Deze taken zijn belegd bij medewerkers met een andere functieomschrijving.

Functie HHD	Volgens BIWA	Verantwoordelijk voor:
Dagelijks Bestuur	Dagelijks Bestuur	- Vaststellen informatiebeveiligingsbeleid
Secretaris Directeur	Secretaris Directeur	- Uitvoeren van het informatiebeveiligingsbeleid
Sectorhoofd Bedrijfsvoering	Directeur bedrijfsvoering	- Financieel toezicht op het informatiebeveiligingsbeleid
Teamleider (I&A)	Afdelingshoofd I&A	- Strategisch gebruik van management informatiesystemen - Verantwoordelijk voor het beveiligingsprogramma
Concern Control	Concern Control	- Focus op het bedrijfsproces van de gehele organisatie - Onderkennen van bedrijfsbrede risico's - Risico's naar een acceptabel niveau laten brengen
Niet	functionaris informatiebeveiliging	- Onderhoud van het beveiligingsprogramma - Borgen van informatiebeveiligingsmaatregelen - Rapporteren over afwijkingen en bedreigingen
Niet	Functionaris gegevensbescherming	- Bescherming van privacy gevoelige gegevens
Systeembeheer beveiliging	Systeembeheer beveiliging	- Beveiliging van informatiesystemen - Implementatie beveiligingsbeleid
Lijnmanagement	Lijnmanagement	- Voor de integriteit van gegevens binnen systemen/ applicaties en op gedrag medewerkers.

- **Delfland voert een GAP analyse uit.**
  Deze analyse geeft een beeld van de afstand tussen de actuele stand van zaken en de situatie waar Delfland naar toe wil. Het resulteert in een inventarisatie van maatregelen die nog genomen moeten worden. Naast de interne analyse wordt ook extern getoetst (waarborg objectiviteit). Het informatiebeveiligingsbeleid en de uitvoering hiervan wordt 1 keer in de 3 jaar getoetst onder eindverantwoording (sommige onderdelen vaker) van de functionaris Informatiebeveiliging. In de driehoek op pagina 3 worden documenten, handleidingen, procedures en werkinstructies genoemd. Deze analyse omvat de inventarisatie van de benodigde documenten en maatregelen die nodig zijn bij het ontbreken daarvan.

- **Delfland formuleert snel te behalen resultaten**

  De resultaten van de GAP analyse worden gebruikt voor het nemen van maatregelen die een aantal resultaten opleveren. Deze kunnen aansluiten op actuele speerpunten en / of hebben op korte termijn toegevoegde waarde.

- **Delfland heeft een implementatieplan**
  Delfland neemt maatregelen als resultante van bevindingen uit de GAP analyse. De voortgang wordt gerapporteerd aan het DMT door de functionaris informatiebeveiliging (of degene die deze taken uitvoert) genoemd in bovenstaande tabel.

3. Risico beoordeling en risico afweging

Informatiebeveiliging gaat uit van 3 basisprincipes:

- **Beschikbaarheid**
  Delfland definieert een basis-set met eisen aan de beschikbaarheid van de infrastructuur en voor de informatieuitwisseling.

- **Integriteit**
  Delfland heeft normen opgesteld voor de integriteit van datacommunicatie en opslag en voor de integriteit van de informatie in de applicaties (gerelateerd aan het proces).

- **Vertrouwelijkheid**
  Delfland neemt maatregelen waarbij de bescherming van gegevens voldoet aan het basisvertrouwelijkheidsniveau (vastgesteld door de waterschappen) en de WBP richtlijnen, risicoklasse 2 (vastgesteld door het CBP).

Het basisniveau voor informatiebeveiliging bij Delfland wordt getoetst aan deze 3 basisprincipes middels een risicoanalyse. Als het veiligheidsniveau (door de daartoe aangewezen functionaris) onvoldoende is worden maatregelen genomen dit naar een voldoende niveau te brengen.

4. Beveiligingsbeleid

Doelstelling (algemeen)
Delfland levert betrouwbare dienstverlening die aantoonbaar voldoet aan wet en regelgeving. De kritieke bedrijfsprocessen worden bij een calamiteit en beveiligingsincident voortgezet.

4.1 Vastlegging en goedkeuring

Het informatiebeveiligingsbeleid is vastgelegd in dit document. Het DMT stemt in met het informatiebeveiligingsbeleid. Het wordt besproken in het PFO en vastgesteld in het College van Dijkgraaf en Hoogheemraden.

4.2 Beoordeling van het informatiebeleid

Het informatiebeveiligingsbeleid en de uitvoering wordt minimaal één keer per drie jaar getoetst. Tevens vindt toetsing plaats bij belangrijke wijzigingen. Het beleid wordt zo nodig bijgesteld volgens de gebruikelijke werkwijze van Delfland.

5. Organisatie van informatiebeveiliging

5.1 Interne organisatie

Doelstelling

Het beheer van de informatiebeveiliging is belegd binnen Delfland. Duidelijk is wie waar voor verantwoordelijk is.

- Secretaris-directeur en het management team commiteert zich ten volle, geeft richting en kent verantwoordelijkheden toe. Deze zijn helder gedefinieerd.
- Activiteiten rond de informatiebeveiliging is belegd bij aangewezen medewerkers. Specifiek is de rol van Chief Information Security Officer[3] belegd of een daartoe aangewezen functionaris binnen Delfland.
- Het Delflandse besturingsmodel voor het I&A-domein kent een goedkeuringsproces voor wijzigingen en nieuwe aanvragen van ICT voorzieningen waarin structureel en specifiek aandacht is voor beveiliging.
- Delfland beschermt de informatie en gaat hier vertrouwelijk mee om. Medewerkers leggen bij indiensttreding een ambtseed of belofte af.
- Delfland heeft contacten met andere overheidsinstanties en partners voor actualisatie en verbetering van het informatiebeveiligingsbeleid.
- Delfland toetst het informatiebeveiligingsbeleid periodiek (minimaal 1x in de 3 jaar). Stelt waar nodig het beleid bij en neemt maatregelen bij risicoverhogende aspecten.

[3] De CISO adviseert gevraagd en ongevraagd over de beveiliging. Doet voorstellen tot aanpassing en verbetering.

5.2 Externe partijen

Doelstelling

Delfland beveiligt de informatie en ICT voorzieningen waartoe externe partijen toegang hebben en die bij deze partijen worden verwerkt en/of beheerd. Voor deze beveiliging hanteert Delfland de set van maatregelen zoals vastgesteld in de Baseline Informatiebeveiliging Waterschappen:

- Bij het contracteren van een externe partij is informatiebeveiliging een criterium voor de keuze.
- De toegang tot het netwerk en gegevens voor de externe partij zijn voorafgaand aan het afsluiten van het contract voor uitbesteding of externe inhuur vastgelegd (inclusief de informatie die onder de WBP valt). Bij verwerking van persoonsgegevens wordt een bewerkerovereenkomst afgesloten conform art 14 WBP.
- De toegangsrechten voor externen is vastgelegd (authenticatie en autorisatie).
- In het contract met de externe partij staan de vereisten van de beveiligingsmaatregelen. Naleving, controle en rapportage zijn standaard onderdeel.
- In contracten met externe partijen wordt uitgelegd hoe wordt omgegaan met geheimhouding en een geheimhoudingsverklaring

6. Beheer van bedrijfsmiddelen

6.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling

Delfland heeft een afdoende bescherming voor het beheer en bewaken van de bedrijfsmiddelen.

De volgende maatregelen worden toegepast:

- De bedrijfsmiddelen zijn geïdentificeerd en er is een actuele inventarisatie.
- Elk bedrijfsmiddel heeft een eigenaar. Bij Delfland is dit een leidinggevende.
- Delfland heeft regels voor het gebruik van de bedrijfsmiddelen. Deze zijn bekend bij de gebruikers.

6.2 Classificatie van Informatie

De informatie binnen Delfland is geclassificeerd met een eigen niveau van beveiliging. Helder is welke informatie gebruikt mag worden door wie en in welke omstandigheden.

7. Personele beveiliging

Doelstelling (algemeen)

Delfland zorgt er voor dat werknemers, ingehuurd personeel en externe gebruikers de verantwoordelijkheden begrijpen. In de rol die zij mogelijk vervullen wordt het risico van oneigenlijk gebruik geminimaliseerd.

7.1 Rollen en verantwoordelijkheden

Delfland legt de verantwoordelijkheden en rollen van een medewerker vast met een aantal maatregelen.

- De functiebeschrijving voorziet in de afbakening van rol en verantwoordelijkheid en wordt expliciet aan de medewerker bekend gemaakt. Waar noodzakelijk worden aspecten van informatiebeveiliging opgenomen in de aanstelling en / of als instructie bij de werkzaamheden.
- De medewerker tekent de aanstelling. Bepalingen over informatiebeveiliging zijn opgenomen.
- De directie bevordert het gedrag van medewerkers door toepassen van het informatiebeveiligingsbeleid.
- Delfland verzorgt up to date kennis van het beveiligingsbeleid.
- Delfland hanteert de SAW voor disciplinaire maatregelen wanneer (bewust) inbreuk wordt gemaakt op de informatiebeveiliging.
- In de aanstelling is vastgelegd welke beveiligingsaspecten bij beëindiging van de aanstelling van kracht blijven voor de ex-werknemer.
- De exit procedure bij beëindiging van de aanstelling voorziet in het vastleggen van de beveiligingsaspecten die van kracht blijven voor de ex-werknemer. Bedrijfsmiddelen worden geretourneerd aan Delfland. Toegangsrechten en autorisaties worden geblokkeerd.

8. Fysieke beveiliging (en van de omgeving)

8.1 Beveiligde ruimten

Doelstelling

Delfland voorkomt onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

De volgende maatregelen zijn hiertoe van kracht:

- Delfland heeft de toegang beveiligd (receptie, toegangspasjes) om ruimten te beschermen waar zich informatie en IT voorzieningen bevinden.
- Hiertoe worden zoneringen, beveiligingsgrenzen en persoonsgebonden toegang toegepast.
- Toegang is alleen mogelijk na autorisatie.
- De toegangsmiddelen zijn geregistreerd (ook bij uitgifte) en worden beheerd.
- De toegang en beveiliging wordt periodiek getoetst en gerapporteerd.
- De ruimten van kantoren, ruimten en faciliteiten zijn fysiek beveiligd.
- Delfland heeft voorzieningen tegen bedreigingen van buitenaf (brand, overstroming etc.) en deze zijn vastgelegd in het calamiteitenplan.

8.2 Beveiliging van apparatuur

Doelstelling

Zekerstelling van de apparatuur waardoor continuïteit van de bedrijfsactiviteiten zijn gewaarborgd.

De apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. De apparatuur is beschermd tegen stroomuitval en andere storingen door onderbrekingen van nutsvoorzieningen. Onderhoud vindt periodiek plaats conform de voorschriften van de leverancier. Bij beëindiging van het gebruik van apparatuur of bij hergebruik buiten de organisatie wordt alle data verwijderd.

9. Beheer van communicatie en bedieningsprocessen

9.1 Bedieningsprocedures en –verantwoordelijkheden

Doelstelling

Het beheer is gericht op een correcte en veilige bediening van ICT-voorzieningen.

Het vastleggen van procedures en verantwoordelijkheden moet een correcte en veilige bediening van ICT-voorzieningen zo veel mogelijk waarborgen.

9.2 Systeemplanning en acceptatie

Doelstelling

Delfland beperkt het risico van systeemstoringen tot een minimum.

Dit wordt bereikt door capaciteitsbeheer. Gebruik van middelen wordt gecontroleerd en afgestemd in relatie tot de nodige capaciteitseisen in het nu en naar de toekomst. Er wordt een risicoanalyse gemaakt over de beschikbaarheid van een ICT voorziening en wat de impact bij uitval is.

9.3 Beheer van netwerkbeveiliging en media en hanteren van virussen

Doelstelling

Delfland beschermt de integriteit van programmatuur en informatie.

Het netwerk wordt beheerd en gemonitord ter voorkoming van verstoringen.
Een pakket van maatregelen zorgt ervoor dat de informatievoorziening veilig is en blijft.
Voor het overige zijn er procedures opgesteld voor:

- Beheer van media.
- Behandeling van informatie
- Beveiliging van systeemdocumentatie
- Toegang naar binnen (van buiten DMZ)
- Toegang naar buiten

9.4 uitwisseling van informatie

Doelstelling

Delfland beveiligt informatie bij uitwisseling.

Voor de kantoorapplicaties zijn richtlijnen voor de beveiliging van de informatievoorziening (toegang tot agenda's, documenten etc.)
Elektronisch berichtenverkeer is beschermd door een spamfilter (ongewenste email). Waar nodig is encryptie toegevoegd voor de beveiliging van het berichtenverkeer.

9.5 Controle

Doelstelling

Rechtmatig gebruik van informatieverwerkingsactiviteiten

Iedere medewerker handelt integer. Delfland zorgt voor een bewustwordingsproces voor alle medewerkers. Er vindt monitoring plaats van het gebruik van de voorzieningen. Oneigenlijk gebruik wordt geregistreerd en besproken met de medewerker. Eventueel volgt er een sanctie.

10. Toegangsbeveiliging voor informatiediensten

10.1 Gebruikers en toegangsrechten

Doelstelling
De medewerkers hebben toegang tot de informatie die relevant voor ze is.

Gebruikers worden geregistreerd (aanmelding en afmelding). Per gebruiker worden toegangsrechten verleend voor de informatiesystemen en diensten binnen Delfland. Hiertoe vindt identificering en autorisatie plaats (toekennen wachtwoorden).

10.1 Verantwoordelijkheden van gebruikers

Doelstelling
Bevoegde toegang tot de informatievoorziening door gebruikers die geautoriseerd zijn en het veilig stellen van informatie en ICT-voorzieningen (incluis mobiele apparatuur).

De toegang wordt mogelijk door het toewijzen van een medewerker als gebruiker met een wachtwoord. Het wachtwoord voldoet aan een aantal vereisten en omgangsvormen. De gebruiker ontvangt een instructie hiervan.
Onbeheerde apparatuur is passend beschermd bij afwezigheid.
Vertrouwelijke informatie ligt niet onbeheerd op bureau of bij de printer. De schermbeveiliging gaat automatisch aan na 15 minuten inactiviteit.

10.2 Toegangsbeheersing voor netwerken en besturingssystemen.

Doelstelling
Toegang voor bevoegde personen tot netwerken en besturingssystemen.

Gebuikers wordt toegang verleend tot die dienst waartoe ze bevoegd zijn middels een beveiligde procedure (plaats en tijd onafhankelijk).

11. Verwerving, ontwikkeling en onderhoud van informatiesystemen

Doelstelling
Beveiliging maakt integraal deel uit van de informatiesystemen.

Bij de aanschaf, ontwikkeling en het onderhoud van informatiesystemen wordt informatiebeveiliging in twee opzichten in acht genomen. Functionele eisen voor informatiebeveiliging worden meegenomen in het ontwerp en de ontwikkeling van informatiesystemen. Bij buitengebruikstelling van informatiesystemen worden maatregelen getroffen. De gegevens die ingevoerd worden zijn juist en volledig. Gevoelige gegevens worden beveiligd door encryptie.

Risicoanalyse en risicomanagement worden geïntegreerd tijdens de ontwikkeling en het onderhoud van informatiesystemen om tijdig, regelmatig en adequaat de beveiligingsbehoefte te analyseren en de maatregelen te bepalen om hieraan te voldoen. Wijzigingen worden getoetst op beveiliging en geregistreerd.

12. Beheer van informatiebeveiligingsincidenten

Doelstelling
Beheersbaarheid van informatiebeveiligingsincidenten die verband houden met informatiesystemen.

Er is een procedure voor het melden, beheren en afhandelen van beveiligingsincidenten. Werknemers en derden melden beveiligingsincidenten zo spoedig mogelijk aan de functionaris informatiebeveiliging. Procedure, rollen en verantwoordelijkheden zijn bekend bij de medewerkers.

13. Bedrijfscontinuïteitsbeheer

Doelstelling
Onderbreken van bedrijfsactiviteiten tegengaan, en kritische bedrijfsprocessen beschermen tegen de gevolgen van rampen zoals omvangrijke storingen in informatiesystemen.

Delfland heeft een proces voor bedrijfscontinuïteit waarbinnen de eisen voor informatiebeveiliging worden meegenomen die nodig zijn voor de continuïteit van de bedrijfsvoering (zie handboek crisisbeheersing).

14. Naleving

Doelstelling
Voorkomen van schending van wetgeving, wettelijke en regelgevende of contractuele verplichtingen.

Alle van toepassing zijnde wettelijke, reglementaire en contractuele vereisten zijn expliciet gespecificeerd en gedocumenteerd voor relevante informatiesystemen. De intellectuele eigendomsrechten zijn bekend en wordt conform naar gehandeld. Bedrijfsdocumenten zijn beveiligd

tegen elke vorm van schade. Bescherming van gegevens is geborgd en gebruikers gaan integer om met de ICT voorzieningen.
De leidinggevenden zien er op toe dat de uitvoering van het beleid wordt nageleefd. Voor de controle op naleving worden periodiek audits gehouden (voorstel is 1 keer per 3 jaar). Tijdens deze audits wordt verstoring van de processen tot het minimum beperkt.