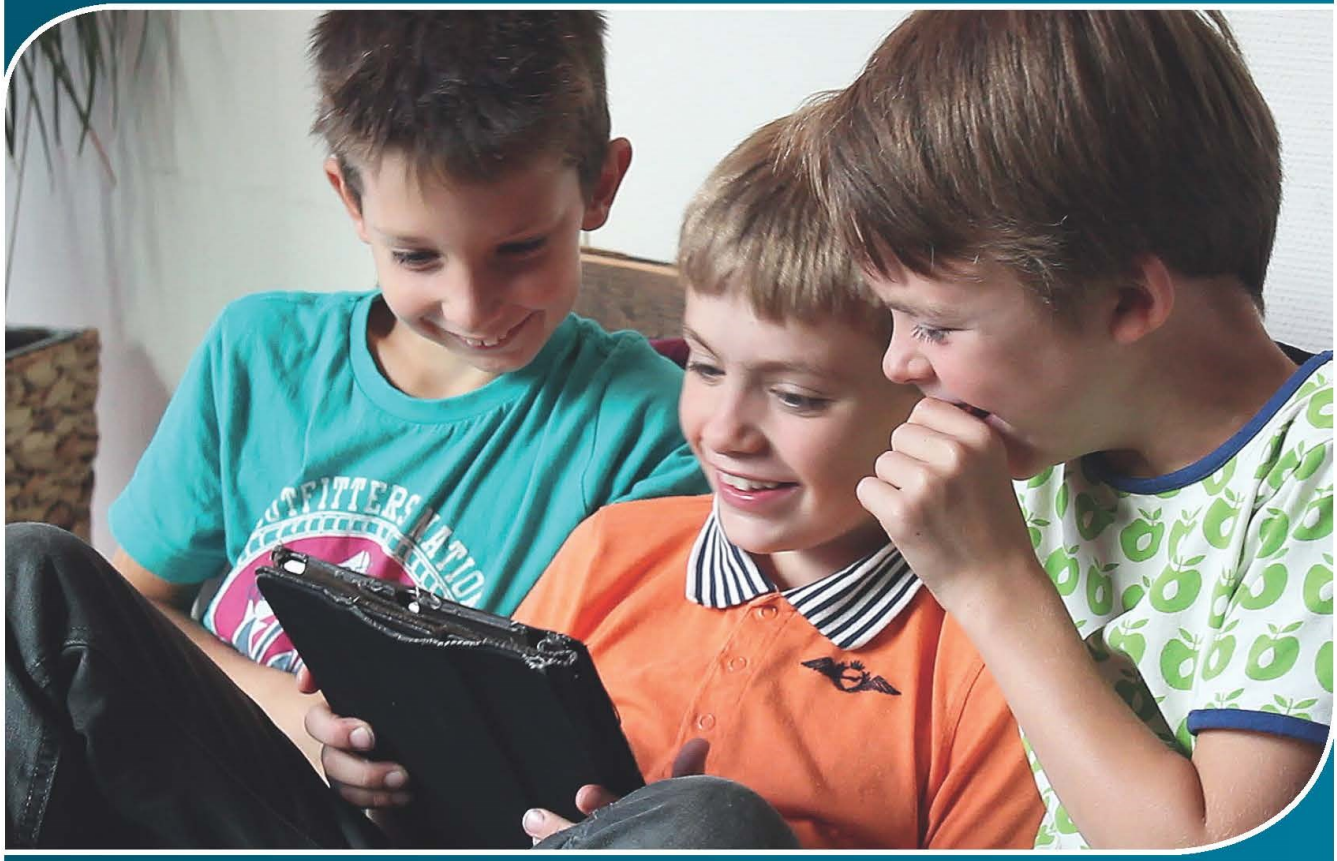


Beleidskader Informatieveiligheid 2017-2020

Van de samenwerkende gemeenten

Versie: definitief 05-09-17

Deventer, Olst-Wijhe en Raalte: samen staan we sterker

1.0 Voorwoord

Dit beleidskader en bijbehorend uitvoeringsplan informatieveiligheid is een uitwerking van de DOWR i-Visie 2018-2022.

De dienstverlening van de DOWR gemeenten wordt steeds meer afhankelijk van een betrouwbare informatievoorziening. De gemeente gaat meer gegevens over burgers vastleggen, mede door nieuwe taken voor de gemeenten. De burger moet erop kunnen vertrouwen dat gegevens goed beschermd zijn. De gemeente gaat ook steeds meer samenwerken met andere partijen. Hierbij is een betrouwbare gegevensuitwisseling van groot belang.

In het kader van de i-Visie DOWR 2017-2020 hebben de DOWR gemeenten richtinggevende uitspraken gedaan over het gemeenschappelijk ambitieniveau voor informatieveiligheid. Met dit beleidskader en bijbehorend uitvoeringsplan volgen we en voldoen we aan de de BIG, de Baseline Informatiebeveiliging Nederlandse Gemeenten.

Informatieveiligheid raakt alle facetten van ons werk. We hebben elkaar nodig om een succes te maken van informatieveiligheid binnen de DOWR.

Bedrijfsvoeringsraad DOWR,

Marcel Kossen, Dries Zielhuis en Karin Cornelissen

Inhoud

2.0 Inleiding

Als gemeente richten we ons primair op de uitvoering van de wetgeving met aandacht en respect voor toezichthouders en burgers. Deze uitvoering vergt de nodige aandacht bij het inrichten en uitvoeren van processen op een betrouwbare en controleerbare wijze. De volgende uitgangspunten zijn dan ook voor de DOWR gemeenten van groot belang.

De DOWR gemeenten zijn een betrouwbare partner:

- De DOWR gemeenten dragen zorg voor een ongestoorde dienstverlening aan burgers, bedrijven, organisaties, ketenpartners en bezoekers;
- Burgers, bedrijven en organisaties weten dat hun gegevens veilig zijn bij de DOWR gemeenten;
- Management en medewerkers van de DOWR gemeenten zijn privacy- en beveiligingsbewust;
- De DOWR gemeenten dragen er zorg voor dat managers en medewerkers goed zijn opgeleid en over de noodzakelijke hulpmiddelen beschikken om hun verantwoordelijkheid voor informatieveiligheid te kunnen dragen;
- De DOWR gemeenten dragen er zorg voor dat de gegevens van managers en medewerkers betrouwbaar zijn en goed zijn afgeschermd;

De DOWR gemeenten willen up-to-date zijn met betrekking tot (cyber)security:

- De DOWR gemeenten zijn weerbaar tegen bedreigingen op het gebied van informatievoorziening, die het functioneren van de DOWR gemeenten als geheel in gevaar brengen (de DOWR gemeenten als “cyber resilient cities”);
- De DOWR gemeenten maken gebruik van de kennis en ervaring van anderen (o.a. burgers, bedrijven en partners als de IBD Informatiebeveiligingsdienst voor alle Nederlandse gemeenten) om de beveiliging van de digitale dienstverlening verder te verbeteren.

2.1 Wat is informatieveiligheid?

Informatieveiligheid is de verzamelnaam voor de processen en maatregelen, die ingericht worden om de betrouwbaarheid van bedrijfsprocessen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen dreigingen. Betrouwbaarheid van informatie en daarmee het beleidskader informatieveiligheid van de DOWR gemeenten berust op de volgende 3 pijlers:

- Beschikbaarheid (continuïteit): het zorgdragen voor het beschikbaar zijn voor de gebruikers van informatie en informatie verwerkende bedrijfsmiddelen op de juiste plaats en tijd;
- Vertrouwelijkheid (exclusiviteit): het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

2.2 Waarom is informatieveiligheid zo belangrijk?

Voor gemeenten is betrouwbaarheid een van de belangrijkste waarden. Dit geldt niet alleen ten aanzien van de producten en diensten, maar zeker ook ten aanzien van de betrouwbaarheid van informatie. De DOWR gemeenten zijn zeer kennis- en informatie intensieve organisaties. Het is daarom van groot belang dat informatie voortdurend en adequaat tegen een groot scala aan interne en externe bedreigingen wordt beschermd. Onvoldoende bescherming van informatie en informatieverwerking kan grote financiële, operationele en/of reputatie schade tot gevolg hebben.

De DOWR gemeenten vinden het daarom van groot belang dat een gestructureerde aanpak wordt gevolgd om de informatie afdoende tegen alle bedreigingen te beschermen en heeft behoefte aan periodiek inzicht in de status van de diverse maatregelen.

2.3 Wat zijn de aspecten van het beleidskader informatieveiligheid?

De beleidsaspecten van Informatieveiligheid zijn afgeleid van de Baseline Informatiebeveiliging Gemeenten (BIG). Deze zijn als volgt:

Informatieveiligheidskader	Het verschaffen van directie aansturing en verwerven van directiesteun voor informatieveiligheid in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.
Beveiligingsorganisatie	De organisatie van de informatiebeveiliging is zodanig, dat informatiebeveiliging permanente aandacht heeft, dat risico's bekend zijn en het voor alle medewerkers duidelijk is waar welke verantwoordelijkheden op dit gebied liggen.
Classificatie en beheer van bedrijfsmiddelen en informatie	Alle informatiesystemen en gegevens zijn toegewezen aan verantwoordelijken en worden periodiek geanalyseerd op hun impact op de bedrijfsvoering en beveiligd met daarbij passende maatregelen.
Beveiligingseisen ten aanzien van medewerkers	Medewerkers van de DOWR gemeenten, vrijwilligers en ingehuurd personeel dat ingezet wordt om diensten te verlenen aan de DOWR gemeenten, worden geïnformeerd en geïnstrueerd over de uitgangspunten van de informatiebeveiliging en de verwachte handelswijze.
Fysieke beveiliging en beveiliging van de omgeving	Fysieke beveiliging van de omgeving, gebouwen, ruimten en apparatuur voorkomt verstoringen van de informatievoorziening, diefstal of beschadiging van bedrijfsmiddelen en onveilige situaties voor bezoekers en medewerkers.
Beheer van informatie-, communicatie- en bedieningsprocessen	Voor het beheer van informatievoorzieningen moet het vastleggen van procedures en verantwoordelijkheden een correcte en veilige bediening van informatiemiddelen zoveel mogelijk waarborgen.
Toegangsbeveiliging	Toegang tot bedrijfsinformatie, zaakgegevens en persoonsgegevens (burgers en/of personeel) mag uitsluitend op grond van formeel verkregen autorisatie.
Aanschaf, ontwikkeling en onderhoud van systemen en apparatuur	Bij de aanschaf, ontwikkeling en het onderhoud van informatiesystemen moet informatiebeveiliging in acht worden genomen bij de functionele eisen van het informatiesysteem en bij de processen van ontwikkeling en onderhoud.
Beveiligingsincidenten	Alle medewerkers moeten bekend zijn met de procedure voor het rapporteren van beveiligingsincidenten en zijn verplicht alle beveiligingsincidenten die zij ontdekken of vermoeden te rapporteren.
Continuïteitsbeheer	Er zijn continuïteitsplannen en -voorzieningen om de continuïteit van de geautomatiseerde informatievoorziening en gegevensverwerking te waarborgen.
Naleving en beveiligingsbewustzijn	De naleving van het informatieveiligheidsbeleid, de daaruit voortkomende maatregelen en het stimuleren van en communiceren over beveiligingsbewustzijn van de medewerkers wordt actief bevorderd en gecontroleerd.

Deze beleidsaspecten zijn verder uitgewerkt in de bijlage bij dit beleidskader.

2.4 Doel van beleidskader informatieveiligheid

Onderhavig beleid is gericht op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de bedrijfsvoering en het minimaliseren van de schade voor de DOWR gemeenten door te proberen beveiligingsincidenten te voorkomen en het minimaliseren van de gevolgen indien deze onverhoopt toch optreden.
Om deze doelstelling te bereiken is informatieveiligheid:

- Een normaal onderdeel van integraal management;
- Een organisatorisch vraagstuk met technische consequenties;
- Een afweging tussen risico's, kosten en werkbaarheid;
- Een samenstelsel van organisatie, mensen, informatie, fysieke omgeving en juridische vastlegging.

3.0 Uitgangspunten DOWR voor informatieveiligheid

De belangrijkste zaken die binnen de DOWR gemeenten moeten worden beschermd zijn de persoonsgegevens van burgers en de vertrouwelijke (zaak)gegevens van burgers, bedrijven en organisaties. De DOWR gemeenten kunnen zich bijvoorbeeld niet permitteren dat persoonsgegevens 'op straat komen te liggen'. Daarom zal in de komende beleidsperiode meer aandacht worden besteed aan privacy en gegevensbescherming. Voor leveranciers en ketenpartners op het gebied van ICT-dienstverlening betekent dit dat in contracten meer aandacht komt voor informatieveiligheid en privacybescherming.

Daarnaast is het van belang om voldoende aandacht te besteden aan toezicht van diensten ten aanzien van systemen waar de gemeenten eindverantwoordelijkheid voor dragen en die door externe partijen worden geleverd en beheerd. Denk hierbij aan systemen voor het toezicht en de sturing van het verkeer bij viaducten of bijvoorbeeld het gebruik van sluizen (zogenaamde SCADA-systemen). Gemeenten kunnen zich niet veroorloven dat deze diensten verstoord worden.

Als uitgangspunt voor de maatregelen en doelstellingen voor informatieveiligheid geldt dat de DOWR gemeenten volledig willen voldoen aan de Baseline Informatiebeveiliging Gemeenten (BIG), die gebaseerd is op de ISO27001/27002.

Afhankelijk van de informatie die door de DOWR gemeenten verwerkt wordt, worden eisen gesteld ten aanzien van de integriteit, vertrouwelijkheid en continuïteit. Daarbij zal een passend niveau van informatieveiligheid worden toegepast. Onderstaand schema geeft het ambitieniveau voor de DOWR gemeenten op het gebied van informatieveiligheid weer. De gekleurde vlakken in onderstaande schema geven aan dat we als basisniveau voor informatieveiligheid het niveau 'midden' hanteren. Dit komt overeen met de norm die in de BIG is opgenomen.

Afwijken van dit basisniveau zal worden toegestaan op basis van dataclassificatie en risicoanalyse op procesniveau.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-)fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Hoog	**Strikt vertrouwelijk** informatie is alleen toegankelijk voor een zeer beperkte groep van gebruikers. *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: gemeentelijke informatie op de website en strafrechtelijke informatie)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

De DOWR gemeenten willen groeien van het huidige volwassenheidniveau 'laag' op het gebied van informatieveiligheid naar een volwassenheidsniveau 'midden'. Hiermee wordt dan voldaan aan de norm zoals de BIG die voorschrijft. De DOWR gemeenten transformeren daarvoor op het gebied van informatiebeveiliging naar een proactieve organisatie op het gebied van informatieveiligheid.

Om informatieveiligheid op niveau 'midden' te laten functioneren zullen, voor alle 134 doelstellingen uit de BIG, maatregelen geïmplementeerd moeten zijn. De maatregelen moeten vervolgens minimaal functioneren op een volwassenheidsniveau dat ze 'herhaalbaar' zijn. Dit betekent dat ze procesmatig worden uitgevoerd en de werking gedurende langere tijd stabiel is.

Niveau	**Omschrijving**	**Kenmerk**
Geen	Initieel	Er zijn afspraken maar deze zijn (nog) niet vastgelegd of afspraken zijn vastgelegd maar de implementatie ervan is slechts beperkt uitgevoerd.
Laag	Herhaalbaar	Afspraken zijn vastgelegd en de implementatie ervan is grotendeels uitgevoerd.
Midden	Beheerst	Uitvoering en naleving van de vastgelegde afspraken zijn eenmalig geëvalueerd en waar nodig zijn de plannen bijgesteld.
Hoog	Geoptimaliseerd	Uitvoering en naleving van de vastgelegde afspraken zijn periodiek geëvalueerd, doeltreffend gebleken, geborgd en worden indien nog nodig bijgesteld.

Uitdaging bij de realisatie van het niveau 'midden' voor informatieveiligheid is een aantal relevante ontwikkelingen. Met deze ontwikkelingen moet rekening gehouden worden:

- Terugtredende overheid en bezuinigingen op de overheid.
- Veranderende wet- en regelgeving:
    - Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), sinds 2013;
    - Overheid digitaal, per 2017;
    - De Digitale Agenda 2020 van VNG;
    - Europese Privacywetgeving, Algemene Verordening Gegevensbescherming (AVG), per 25 mei 2018.
- Technologische ontwikkelingen:
    - Steeds meer diensten in de 'cloud' (Software As A Service) in plaats van op eigen locatie;
    - Nieuwe manieren en communicatie in de dienstverlening;
    - Toename van cybercrime.
- Nieuwe manieren om informatieveiligheid te waarborgen.
    - Meer toezicht op de uitvoering en naleving van maatregelen;
    - Geautomatiseerde monitoring van technische maatregelen;
    - Strakkere sturing op incidenten, zgn. Incident Repons.
- Het nieuwe werken

- Plaats- en tijdsonafhankelijk werken voor medewerkers en derden;
- Onbeheerde middelen voor de toegang tot de informatievooriening van de DOWR gemeenten.
- Bring your own device (BYOD) of chose your own Device (CYOD).

4.0 Beveiligingsorganisatie en het informatieveiligheidsproces

4.1 Verantwoordelijkheden

Informatieveiligheid is een lijnverantwoordelijkheid en ligt primair bij de afdelingsmanagers van de DOWR gemeenten. De uitvoering en naleving van het beleid is een verantwoordelijkheid van iedere medewerker. Voor de algehele coördinatie van het lijnmanagement is de CISO verantwoordelijk.

Functie	**Verantwoordelijkheid**
College van B&W	Het College van B&W is integraal verantwoordelijk voor alle werkprocessen, dus ook voor informatieveiligheid. Zij stellen het Beleidskader informatieveiligheid formeel vast en dragen het beleid actief uit.
De Bedrijfsvoeringsraad	De Bedrijfsvoeringsraad (BVR) is verantwoordelijk voor ontwikkeling en implementatie van het beleidskader informatieveiligheid, de strategische aansturing en borging van continuïteit. De BVR adviseren de Colleges over vast te stellen beleid. De BVR controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden.
De directies en managers van de DOWR gemeenten	De directies van de DOWR gemeenten zijn integraal verantwoordelijk voor de informatieveiligheid van hun organisatieonderdelen. Zij zijn verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen. Tevens sturen zij op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn).
Medewerkers	Medewerkers zijn verantwoordelijk voor de eigen werkprocessen. Zij zijn verantwoordelijk voor het op de juiste wijze gebruiken van informatiesystemen, het naleven van de opgestelde maatregelen en richtlijnen. Het melden van afwijkingen en onregelmatigheden op het gebied van informatieveiligheid maakt hiervan onderdeel uit.
CISO	De CISO geeft namens de directies van de DOWR gemeenten op dagelijkse basis invulling aan de sturende rol van de hele beleidscyclus. De CISO analiseert en bereidt besluitvorming voor over beleidskader en te treffen maatregelen en ziet toe op de implementatie van het beleidskader en op de uitvoering van de te treffen maatregelen. De CISO toetst met regelmaat de naleving van de maatregelen in het kader van informatieveiligheid. De CISO bevordert en adviseert gevraagd en ongevraagd over informatieveiligheid.
ISO's	De coördinatie van dagelijkse werkzaamheden van informatieveiligheid is binnen de DOWR gemeenten belegd bij de Information Security Officers (ISO's) van de domeinen BRP,PUN, DigiD, BAG,BGT en Suwinet[1]. Zij rapporteren ieder kwartaal aan de CISO.

[1] Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

	De ISO's zullen jaarlijks de getroffen beheersmaatregelen om de risico's op aanvaardbaar niveau te houden (laten) toetsen.
ICT Security Officer (I-werkorganisatie)	De ICT security Officer is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van de ICT beveiligingsmaatregelen. Daarnaast is hij verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT security management, incident en probleem management. Hij levert verder technisch beveiligingsadvies.

*) In deze tabel is nog niet in de CIO rol voorzien, zoals die in het OO-plan wordt opgenomen.

4.2 Bevoegdheden CISO

(In lijn met de "Handreiking IB-functieprofiel Chief Information Security Officer (CISO)" van de IBD Informatie Beveiligings Dienst).

De CISO is de spin in het web voor inrichten en handhaven van het beleid inzake informatieveiligheid en in bovenstaande organisatie van taken en verantwoordelijkheden. Om aan de centrale rol invulling te kunnen geven, heeft de CISO de volgende bevoegdheden.

Voorwaarde om de functie CISO volledig te kunnen vormgeven, is de bevoegdheid om in voorkomende gevallen - na afstemming met Directeurenberaad en Bedrijfs Voerings Raad - gevraagd en ongevraagd te mogen rapporteren aan het college van B&W.

De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven binnen het vigerende Beleidskader informatieveiligheid.

Bij informatiebeveiliging is het noodzakelijk om centraal keuzes te maken, waarbij de CISO het keuzeproces organiseert en de voornaamste adviseur van de eindverantwoordelijken is.

De consultatie van de CISO is noodzakelijk bij het opstellen of wijzigen van andere aspecten van informatiebeleid en informatiearchitectuur.

Bij (grote) beveiligingsincidenten/-risico's heeft de CISO de bevoegdheid, zo nodig, direct in te grijpen (met verantwoording achteraf richting het management).

Bevoegdheid zonder budget werkt in de praktijk niet. Een eigen budget voor informatiebeveiliging is dus een andere belangrijke voorwaarde voor het goed functioneren.

4.3 Afstemming en verantwoording

Concern overleg

CISO, ISO's van alle DOWR afdelingen zijn vertegenwoordigd in het Concernoverleg Informatieveiligheid (CIV). Het overleg vergadert 1 keer in de 6 weken. De CISO is voorzitter. De CIV is een adviesorgaan van het DOWR Directieberaad.

Rapportage en escalatielijn voor informatieveiligheid

ISO → CISO → DOWR Directieberaad → BVR → Portefeuillehouder → College B&W

De CISO rapporteert ieder kwartaal over de stand van zaken aan de DOWR directies en de BVR en vermeldt hierin ook de planning voor het komende kwartaal.

De CISO verzorgt de jaarlijkse rapportage aan de verantwoordelijke portefeuillehouder (wethouder of burgemeester), BVR en DOWR directies.

De ISO’s rapporteren ieder kwartaal aan de afdelingsmanagers en aan de CISO over de voortgang en de status van informatieveiligheid.

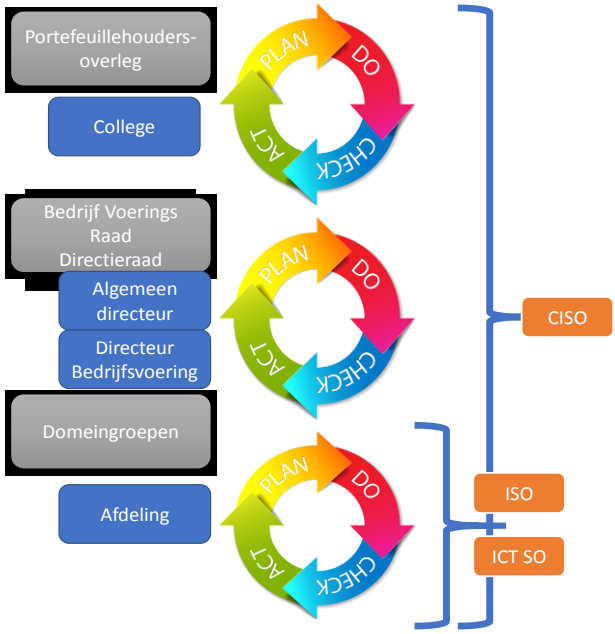
De directies van de DOWR gemeenten rapporteren over het voldoen aan wet- en regelgeving en algemeen beleid van de gemeenten in managementrapportages.

De ICT security officer rapporteert maandelijks aan de teammanager DOWR-i en aan de CISO. Informatiebeveiliging is ook onderdeel van de service management rapportage van de DOWR i-Werkorganisatie.

4.3 Procesmatige aanpak informatieveiligheid

Plan Do Check Act

Informatiebeveiliging is een continu verbeterproces, die kan worden bestuurd volgens de PDCA cyclus 'Plan, do, check en act'. De PDCA op drie niveau's vormt samen het management systeem van informatiebeveiliging op resp. bestuurlijk niveau, op topambtelijk niveau en op niveau van de domeinen en afdelingen[2]. De besturing vindt plaats op het niveau van de individuele gemeenten en in de DOWR brede samenwerking. Deze kwaliteitscyclus is in bijgaande figuur weergegeven.



Toelichting:

Plan: De cyclus start met beleid voor informatieveiligheid, gebaseerd op wet- en regelgeving, landelijke normen en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Het beleid wordt – mede met behulp van risicoanalyse - uitgewerkt in een uitvoeringsplan informatieveiligheid en op bestuurlijk niveau voorzien van de condities (incl. budget) voor uitvoering. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De specifieke activiteiten worden op niveau van de algemeen directeur in opdracht gegeven aan het midden management door middel van het gemeentelijk meerjarenplan informatieveiligheid van iedere gemeente afzonderlijk.

Do: Het gemeentelijk meerjarenplan informatieveiligheid is de basis voor het inrichten van organisatorische en technische maatregelen en de bevordering van het beveiligingsbewustzijn. Medewerkers ontvangen richtlijnen en instructies om op tactisch operationeel niveau de ingerichte maatregelen toe te passen. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces van iedere medewerker.

Check: Check vindt plaats op verschillende niveaus en in verschillende control cycli. Operationele control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT en compliance aan wet en regelgeving. Interne controle maatregelen worden ter uitvoering opgedragen aan de functionarissen informatieveiligheid van de betreffende afdelingen (ISO). Dat geldt ook voor de specifieke ICT processen door de ICT functionaris informatieveiligheid (ICT SO).
Externe controle: betreft de strategische controle buiten de primaire en tactische processen door een auditor[3]. Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd, waarbij de CISO feitelijk (gedelegeerd) opdrachtgever is. Bevindingen, analyses en aanbevolen verbeteracties worden gerapporteerd aan de BVR resp. college en portefeuillehoudersoverleg.

[2] NEN/ISO 27001
[3] van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en concern auditing (intern)

Act: De cyclus is rond met de uitvoering van vastgestelde verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning. De bevindingen worden in beginsel gerapporteerd aan de directies van de DOWR gemeenten. Voor ingrijpende verbeteracties wordt een gevraagd besluit voorgelegd.

Bijlage Verdieping beleidsmatige doelstellingen

De doelstellingen in dit beleidskader Informatieveiligheid zijn afgeleid van de Baseline Informatiebeveiliging Gemeenten (BIG). Hiermee wordt geborgd dat kan worden voldaan aan de norm ten aanzien van de volwassenheid die de BIG voorschrijft.

1 Informatiebeveiligingsbeleid

Het verschaffen van directieaansturing en verwerven van directiesteun voor informatieveiligheid in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

- Het beleidskader informatieveiligheid moet door de Bedrijfsvoeringsraad (BVR) onderhouden, goedgekeurd en kenbaar gemaakt worden aan alle medewerkers en relevante externe partijen.
- Het beleidskader informatieveiligheid is van toepassing op alle informatie(middelen) en alle (interne en externe) medewerkers.
- Zodra zich belangrijke wijzigingen in informatievoorzieningen of bedrijfsprocesen voordoen, of minimaal 3-jaarlijks moet het beleidskader informatieveiligheid beoordeeld en eventueel aangepast worden. Op deze wijze blijft het beleidskader informatieveiligheid dynamisch, toereikend en doeltreffend.

2 Beveiligingsorganisatie

De organisatie van de informatiebeveiliging is zodanig, dat informatiebeveiliging permanente aandacht heeft, dat risico's bekend zijn en het voor alle medewerkers duidelijk is waar welke verantwoordelijkheden op dit gebied liggen.

- De leiding van de DOWR gemeenten zorgt ervoor dat verantwoordelijkheden voor informatiebeveiliging worden toegewezen. Deze verantwoordelijkheden moeten duidelijk worden gedefinieerd en belegd, waarbij specifieke functies en/of taken worden beschreven en bekendgemaakt binnen de organisatie.
- De implementatie van maatregelen voor informatiebeveiliging moet worden gecoördineerd door aangewezen vertegenwoordigers.
- Het installeren en in gebruik nemen van nieuwe middelen voor de informatievoorziening moet via een proces worden goedgekeurd.
- Voor het onderhouden van contacten en de samenwerking met externe partijen bestaan procedures, om ervoor te zorgen dat incidenten snel en conform wettelijke bepalingen en/of onderlinge afspraken worden afgehandeld.
- De implementatie van informatiebeveiliging wordt periodiek en onafhankelijk beoordeeld om de effectiviteit van het beleid en de maatregelen vast te stellen.
- Tegen misbruik van en ongeautoriseerde toegang tot informatie van de DOWR gemeenten door externe partijen zijn speciale maatregelen getroffen.
- Om zeker te zijn van de naleving van de informatiebeveiligingseisen door externe partijen, worden in contracten clausules over informatiebeveiliging opgenomen.

3 Classificatie en beheer van bedrijfsmiddelen en informatie

Alle informatiesystemen en gegevens zijn toegewezen aan verantwoordelijken en worden periodiek geanalyseerd op hun impact op de bedrijfsvoering en beveiligd met daarbij passende maatregelen.

- De DOWR gemeenten moeten een volledig overzicht hebben van de middelen die bij de informatievoorziening een rol spelen, waarin het bedrijfsbelang voor de DOWR gemeenten en de verantwoordelijken zijn opgenomen.

- Gegevens van DOWR gemeenten zijn geclassificeerd en voorzien van een ‘label’, zodat duidelijk is hoe en waarvoor de gegevens gebruikt en behandeld mogen worden.

4 Beveiligingseisen ten aanzien van medewerkers

Medewerkers van de DOWR gemeenten, vrijwilligers en ingehuurd personeel dat ingezet wordt om diensten te verlenen aan de DOWR gemeenten, worden geïnformeerd en geïnstrueerd over de uitgangspunten van de informatiebeveiliging en de verwachte handelswijze.

- Relevante beveiligingseisen moeten worden opgenomen in functie- en/of taakbeschrijvingen.
- Tijdens de sollicitatieprocedure worden kandidaten passend ‘gescreend’.
- In het arbeidscontract is de verantwoordelijkheid op het gebied van informatiebeveiliging en, indien voor de functie van toepassing, zwijgplicht vastgelegd. Als onderdeel van het arbeidscontract wordt een geheimhoudingsverklaring ondertekend.
- Het management heeft de verantwoordelijkheid alle medewerkers te stimuleren om beveiligingsmaatregelen in acht te nemen, bijvoorbeeld via trainingen en bijeenkomsten.
- Voor medewerkers die de beveiliging bewust doorbreken bestaat er een disciplinair proces.
- Het vertrek van medewerkers wordt met een proces begeleid, zodat het risico van toegang tot informatie van de DOWR gemeenten niet meer bestaat.
- Medewerkers geven bij beëindiging van hun contract alle verstrekte eigendommen van de DOWR gemeenten terug en alle toegangsrechten worden ingetrokken.

5 Fysieke beveiliging en beveiliging van de omgeving

Fysieke beveiliging van de omgeving, gebouwen, ruimten en apparatuur voorkomt verstoringen van de informatievoorziening, diefstal of beschadiging van bedrijfsmiddelen en onveilige situaties voor bezoekers en medewerkers.

- Voor de toegang tot de omgeving en ruimten worden zones aangewezen die via barrières worden gescheiden. Voor beveiligde zones worden aanvullende maatregelen getroffen en richtlijnen uitgevaardigd.
- Apparatuur en kabels moeten veilig worden geplaatst, beveiligd worden tegen stroomstoringen en op correcte wijze worden onderhouden om misbruik en beschadiging te voorkomen, ook indien de apparatuur buiten de bedrijfslocatie wordt gebruikt.
- Voordat opslagmedia worden hergebruikt of afgevoerd, worden ze zodanig bewerkt dat de gegevens niet meer kunnen worden hersteld.
- Waar mogelijk wordt ongeautoriseerde toegang tot bedrijfsinformatie en informatiemiddelen voorkomen door het voeren van een ‘clear desk’ en een ‘clear screen’ beleid.
- Er moeten regels zijn voor het meenemen van bedrijfsmiddelen buiten de bedrijfslocaties.

6 Beheer van informatie-, communicatie- en bedieningsprocessen

Voor het beheer van informatievoorzieningen moet het vastleggen van procedures en verantwoordelijkheden een correcte en veilige bediening van informatiemiddelen zoveel mogelijk waarborgen.

- Bedieningsprocedures moeten worden gedocumenteerd, onderhouden en behoeven autorisatie van de leiding.
- Wijzigingen aan informatiemiddelen, zoals apparatuur, programmatuur en procedures, moeten beheerst en gecontroleerd worden doorgevoerd. Hiertoe zijn verantwoordelijkheden en procedures voor wijzigingsbeheer vastgelegd.

- Er zijn functiescheidingen aangebracht die het risico van nalatigheid en opzettelijk misbruik van systemen vermindert.
- De ontwikkel-, test-, opleidings- en productieomgeving zijn van elkaar gescheiden.
- In het contract met externe partners moeten passende beveiligingsmaatregelen worden opgenomen, die de DOWR gemeenten in staat stellen de dienstverlening regelmatig op beveiligingsaspecten te beoordelen (bijv. via een zgn. TPM (Third Party Memorandum) verklaring op basis van ISO27001).
- Eisen ten aanzien van informatiebeveiliging worden opnieuw betrokken bij wijzigingen in de dienstverlening.
- Het capaciteitsbeslag wordt bewaakt en met toekomstige capaciteitseisen wordt rekening gehouden, om storingen als gevolg van gebrek aan capaciteit te voorkomen.
- Wijzigingen aan informatiesystemen worden tegen vooraf vastgestelde acceptatiecriteria getoetst alvorens tot acceptatie kan worden overgegaan.
- Maatregelen moeten worden getroffen om de introductie van kwaadaardige programmatuur te voorkomen en te ontdekken.
- Van essentiële gegevens en programmatuur worden regelmatig volgens een periodiek te toetsen procedure reservekopieën gemaakt, waarvan bij de bewaartermijn rekening is gehouden met wettelijke eisen.
- Er moeten maatregelen getroffen worden voor de bescherming tegen ongeautoriseerde toegang van gegevens in netwerken en netwerkdiensten,
- Voor het beheer, afvoer en de behandeling van verwijderbare media moeten beveiligingsmaatregelen worden getroffen tegen schade, diefstal en ongeautoriseerde toegang, om de opgeslagen gegevens te beschermen tegen ongeoorloofde openbaarmaking of misbruik.
- Maatregelen moeten worden getroffen om systeemdocumentatie te beveiligen tegen ongeautoriseerde toegang, beschadiging en verlies.
- Voor de elektronisch uitwisseling van informatie moet er beleid en een overeenkomst worden opgesteld en maatregelen worden getroffen om gegevens te beveiligen tegen beschadiging, verlies, ongeautoriseerde toegang, misbruik en manipulatie.
- Voor de beveiliging van gegevens op verwijderbare media tijdens transport moeten maatregelen worden getroffen.
- Er moet beleid en richtlijnen worden opgesteld en geïmplementeerd om de zakelijke- en beveiligingsrisico's van informatiesystemen te beheersen.
- Publiek toegankelijke informatie moet beveiligd worden tegen ongeoorloofde wijziging.

7 Toegangsbeveiliging

Toegang tot bedrijfsinformatie, zaakgegevens en persoonsgegevens (burgers en/of personeel) mag uitsluitend op grond van formeel verkregen autorisatie.

- Op basis van regels en rechten voor toegang voor gebruikers, moet toegangsbeveiliging worden geconcretiseerd in beheersmaatregelen en procedures.
- Gebruikers worden opgenomen in een geformaliseerde gebruikersregistratie en krijgen de beschikking over een unieke gebruikersidentificatie (gebruikers-ID) voor persoonlijk gebruik.
- Voor de authenticatie van een gebruiker moet minimaal een wachtwoordsysteem worden gebruikt, waarbij procedures en regels zijn vastgesteld voor het instellen, wijzigen, intrekken en het zorgvuldig gebruik van wachtwoorden.
- Tijdelijk onbeheerde apparatuur moet door de gebruiker voldoende worden beveiligd en worden voorzien van een 'time-out' na een bepaalde periode van inactiviteit, om toegang door onbevoegden te voorkomen.

- De DOWR gemeenten moet procedures en regels vaststellen voor het toekennen en intrekken van bevoegdheden, op basis van autorisatieregels die geformuleerd zijn door de verantwoordelijken voor de desbetreffende gegevens en informatiemiddelen.
- Toegang is alleen mogelijk in overeenstemming met geldige bevoegdheden en wordt door de verantwoordelijke op gezette tijden via een procedure gecontroleerd.
- De toewijzing en het gebruik van bijzondere bevoegdheden voor noodprocedures, systeembeheer en onderhoud moeten worden beperkt en regelmatig worden gecontroleerd.
- Er moet beleid worden geformuleerd voor het gebruik van netwerken en netwerkdiensten, dat onder andere voorziet in extra beveiliging van gevoelige of kritische informatiesystemen, denk bijvoorbeeld aan netwerkscheiding.
- Voor het gebruik van mobiele computers en telewerkvoorzieningen moet beleid worden vastgesteld, dat regels bevat om deze informatiemiddelen adequaat te beschermen.

8 Aanschaf, ontwikkeling en onderhoud van systemen en apparatuur

Bij de aanschaf, ontwikkeling en het onderhoud van informatiesystemen moet informatie-beveiliging in acht worden genomen bij de functionele eisen van het informatiesysteem en bij de processen van ontwikkeling en onderhoud.

- In het pakket van eisen voor een aanschaf of het ontwerp voor een wijziging in de informatievoorziening moeten beveiligingseisen worden betrokken.
- De invoer, interne verwerking en de uitvoer van gegevens moeten worden gevalideerd om de integriteit van de gegevens te waarborgen.
- Als bescherming van de inhoud van berichten van essentieel belang is, dan moet authenticatie van berichten overwogen worden.
- De DOWR gemeenten moeten beleid ontwikkelen voor het gebruik van cryptografische beveiligingsmaatregelen, om het gebruik te optimaliseren en onjuist gebruik te voorkomen.
- De implementatie van programmatuur en wijzigingen daarop moeten worden beheerst en rekening houden met de beveiliging.
- Testgegevens moeten worden beveiligd en beheerst en het gebruik van persoonsgegevens moet worden vermeden.
- Om de kans op verminking van informatiesystemen te beperken, is procedurele beheersing vereist bij de implementatie van wijzigingen van de informatiesystemen en besturingssystemen.
- Voor zover mogelijk en uitvoerbaar moeten softwarepakketten ongewijzigd worden gebruikt.
- Detectie van mogelijke verborgen communicatiekanalen (bijvoorbeeld veroorzaakt door zwakke plekken in programmatuur) en actieve bestrijding ervan is noodzakelijk.
- Bij uitbestede ontwikkeling van programmatuur moeten afspraken worden gemaakt over de beheersing van het ontwikkelproces en de kwaliteit van de programmatuur.

9 Beveiligingsincidenten

Alle medewerkers moeten bekend zijn met de procedure voor het rapporteren van beveiligingsincidenten en zijn verplicht alle beveiligingsincidenten die zij ontdekken of vermoeden te rapporteren.

- Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging en procedures om het systeemgebruik te bewaken moeten worden vastgelegd.
- Werkzaamheden van systeembeheerders en storingen die door gebruikers worden gerapporteerd moeten in een logboek worden bijgehouden.

- Om maatregelen te kunnen nemen tegen personen of organisaties is het nodig om over voldoende bewijsmateriaal te beschikken en is een procedure nodig voor het verzamelen van bewijsmateriaal.
- Er moet een procedure worden vastgesteld voor de melding van incidenten en zwakke plekken in de beveiliging.
- Er moet een procedure worden vastgesteld voor de afhandeling van incidenten en er moeten mechanismen zijn om de impact van incidenten te kwantificeren, kwalificeren en te bewaken.

10 Continuïteitsbeheer

Er zijn continuïteitsplannen en -voorzieningen om de continuïteit van de geautomatiseerde informatievoorziening en gegevensverwerking te waarborgen.

- Er moet een proces van continuïteitsbeheer worden geïmplementeerd om de verstoring als gevolg van calamiteiten en beveiligingsincidenten tot een aanvaardbaar niveau te beperken.
- Op basis van een risicoanalyse moet in een continuïteitsstrategie voor alle informatiesystemen en –processen het aanvaardbaar niveau van verstoring worden bepaald.
- Een continuïteitsplan moet worden gemaakt en voorzieningen worden getroffen om bij een onderbreking of verstoring van bedrijfsactiviteiten, kritische bedrijfsprocessen in stand te houden of tijdig te herstelen.
- Een continuïteitsplan moet regelmatig worden onderhouden, via evaluaties en actualisering, om de doeltreffendheid te waarborgen.

11 Naleving en beveiligingsbewustzijn

De naleving van het informatiebeveiligingsbeleid, de daaruit voortkomende maatregelen en het stimuleren van en communiceren over beveiligingsbewustzijn van de medewerkers wordt actief bevorderd en gecontroleerd.

- Van toepassing zijnde wettelijke, reglementaire en contractuele eisen moeten worden gespecificeerd en gedocumenteerd.
- Naleving van de privacywetgeving verlangt een sluitend overzicht van verwerkingen van persoonsgegevens.
- Voor het gebruik van informatiemiddelen van de DOWR gemeenten voor andere dan de beoogde doeleinden moet toestemming worden verkregen van de leiding.
- De naleving van beveiligingsprocedures door de procesverantwoordelijken moet met controle worden geborgd.
- Informatiesystemen moeten regelmatig worden geaudit, om na te gaan of wordt voldaan aan de beveiligingsnormen.
- Systeemaudits en andere controles moeten zorgvuldig worden gepland en goedgekeurd om het risico van verstoringen van bedrijfsprocessen te minimaliseren.
- De DOWR gemeenten stimuleren en ondersteunen actief het beveiligingsbewustzijn van medewerkers.