gemeente Opsterland

# GEMEENTEBLAD

Officiële uitgave van de gemeente Opsterland

Nr. 44505

2 februari 2026

## Informatiebeveiligingsbeleid OWO-gemeenten

*Veilige dienstverlening als basis voor vertrouwen in de gemeente*

### Hoofdstuk 1 – Aanleiding & inleiding

In de gemeentelijke organisatie hebben digitalisering en informatisering een grote rol bij het werken met (persoons)gegevens. De inwoner mag verwachten dat deze gegevens bij de gemeente in goede handen zijn en dat deze passend worden beveiligd. We beschikken als OWO-gemeenten over veel gevoelige gegevens en we worden als gemeenten met al onze ketenpartners steeds afhankelijker van goed werkende informatievoorzieningen en -systemen.

Om als gemeente te borgen dat we consistent veilig werken met (persoons)gegevens is het van belang een actueel informatiebeveiligingsbeleid te hebben. Dit OWO-informatiebeveiligingsbeleid is opgesteld om ondersteuning te bieden aan het college, gemeentesecretaris, directie, management en de algehele organisatie bij de sturing op en het beheer van informatieveiligheid. Met dit beleid zetten de gemeenten Ooststellingwerf, Opsterland en Weststellingwerf een volgende stap om de beveiliging van (persoons)gegevens binnen de gemeenten te versterken.

**Harmonisering van informatiebeveiligingsbeleid**
Waar de drie gemeenten voorheen afzonderlijk strategisch beleid hadden voor informatiebeveiliging, kiezen de gemeenten er nu voor om gezamenlijk beleid op te stellen. In een tijd van constante verandering op het gebied van digitale technologie en wet- en regelgeving, vereenvoudigt geharmoniseerd beleid de naleving en uitvoering ervan.

**Opzet van het OWO-informatiebeveiligingsbeleid**
Dit beleidsdocument is richtinggevend en kaderstellend en wordt door de gemeenten verder uitgewerkt en geconcretiseerd in protocollen, gedragsregels, procedures, rapportages en werkinstructies op tactisch en operationeel niveau. Ook worden de rollen en verantwoordelijkheden aangaande informatiebeveiliging beschreven.

Dit beleid hangt samen met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen zijn gesteld, met betrekking tot de Wet Basisregistratie Personen (Wet BRP), de Algemene Verordening Gegevensbescherming (AVG), Paspoort uitvoeringsregeling Nederland 2001 (PUN), Reglement Rijbewijzen (RR), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en de Wet open overheid (Woo). Voor bepaalde taken gelden op grond van deze en wet- en regelgeving specifieke beveiligingseisen. Deze worden in aanvullende documenten uitgewerkt.

**Wat is informatiebeveiliging?**
Onder informatiebeveiliging (IB) verstaan we het zorgen voor een bewuste en veilige omgang met informatie door het toepassen van een combinatie van organisatorische en technische maatregelen. Deze maatregelen zijn erop gericht op de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van gemeentelijke processen, de gebruikte informatiesystemen en om de daarin opgeslagen gegevens aantoonbaar te beschermen tegen (on)opzettelijk misbruik. De Baseline Informatiebeveiliging Overheid (BIO) is de gestandaardiseerde norm voor informatiebeveiliging binnen de overheid.

Het begrip ‘informatiebeveiliging’ heeft betrekking op de volgende kwaliteitsaspecten:
- beschikbaarheid: het zorgdragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
- vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- controleerbaarheid: het regelmatig controleren op de uitvoering van de beheersmaatregelen om (achteraf) vast te stellen of deze goed werken.

De maatregelen uit de BIO borgen de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid bij de medewerkers, en – in het geval van incidenten – de eventuele gevolgschade van de incidenten te beperken.

**Informatiebeveiliging is meer dan alleen digitale veiligheid – integraal werken**
Informatiebeveiliging is breder meer dan alleen digitale veiligheid. Beschikbare en betrouwbare informatie is essentieel voor het goed functioneren van de gemeente en het optimaal organiseren (kwaliteit) en faciliteren van de bedrijfsvoering. Daarnaast is besluitvorming van de gemeente op basis van beschikbare en betrouwbare informatie de hoeksteen voor het vertrouwen van inwoners en ondernemers richting de gemeente.

Dit vereist meer en meer een integrale aanpak omdat Informatiebeveiliging geen op zichzelf staand beleidsveld is. Het ondersteunt de gemeente bij het uitvoeren van diens taken en is onderdeel van alle organisatieonderdelen. Dit betekent tevens dat iedere teammanager/-leider verantwoordelijk is voor de veiligheid en beveiliging van zijn eigen team/organisatieonderdeel, de processen die daaronder vallen en de (persoons)gegevens die daarbinnen worden verwerkt.

### 1.2 Doelstellingen van dit beleid

#### 1.2.1 Het doel van dit informatiebeveiligingsbeleid
De doelstelling van het informatiebeveiligingsbeleid is het richting geven aan de invulling van informatiebeveiliging binnen de OWO-gemeenten. Er worden concrete eisen en doelen gesteld voor informatiebeveiliging (op basis van wet- en regelgeving). Daarnaast worden taken en verantwoordelijkheden beschreven en wordt aandacht gegeven aan het creëren van bewustwording. Op deze manier vormt dit beleid de informatiebeveiligingsorganisatie van de gemeenten en geeft hier invulling aan.

Het informatiebeveiligingsbeleid is tevens de basis voor het inrichten van een procesgerichte benadering van informatiebeveiliging, ook wel het Information Security Management System (ISMS). Dit proces hanteert een Plan Do Check Act cyclus (PDCA) en sluit aan bij de planning en control-cyclus (P&C) van de gemeente. Ook is vanuit het ISMS de mate van compliance af te lezen conform de BIO inclusief bijbehorende beheersmaatregelen en bewijslast.

Het informatiebeveiligingsbeleid biedt de uitgangspunten, normen en kaders voor de veiligheid van alle onderliggende gemeentelijke (informatie)processen.

#### 1.2.2 Wat het realiseren van dit doel tot gevolg heeft
Informatie is een van de belangrijkste bedrijfsmiddelen van onze gemeente. Zonder actuele en betrouwbare informatie, op de juiste tijd en de juiste plaatst, kunnen wij onze taken niet naar behoren en afdoende veilig vervullen. We werken met informatie om diensten te leveren aan onze inwoners en bedrijven, en om richting te geven aan de ontwikkeling van onze gemeente. Daarnaast is onze gemeentelijke informatie van belang voor andere overheidsorganisaties.
We zijn open en transparant in wat we doen en waarom we het doen. We helpen onze inwoners en bedrijven ‘in een keer goed’ en voorkomen dat we dezelfde vraag twee keer stellen door goed gebruik van de informatie die we hebben. Om dit te kunnen doen zien wij informatie als ‘open, tenzij’, maar met een nadrukkelijke ‘tenzij’ omdat informatie de privacy of belangen van personen of organisaties kan schaden. Daarom dient alle informatie te worden geclassificeerd zodat we goed in staat zijn en blijven om de rechten te beschermen die gelden op het gebied van gegevensbescherming en iedereen erop kan vertrouwen – en de gemeente het kan aantonen – dat we zorgvuldig met (persoons)gegevens omgaan en ieders privacy gewaarborgd blijft. We zoeken daarbij naar een goede balans tussen te nemen maatregelen en het behouden van goede en efficiënte dienstverlening, een transparant proces en passende kosten.

De OWO-gemeenten zetten met dit beleid de komende jaren in op het optimaliseren van de informatiebeveiliging en het verder inrichten en professionaliseren van de informatiebeveiligingsfuncties.

### 1.3 De visie en ambities van de OWO-gemeenten

#### 1.3.1 De visie van de OWO-gemeenten
➔ “De OWO-gemeenten zijn digitaal weerbaar en zetten privacy en informatiebeveiliging actief in voor een veilige en transparante dienstverlening, waarin het vertrouwen van inwoners, samenwerkingspartners en eigen medewerkers in de gemeenten centraal staan”.

#### 1.3.2 De ambities van de OWO-gemeenten
Om onze visie na te streven, zijn onderstaande ambities geformuleerd. De ambities zijn de bouwstenen van onze visie en vervullen stuk voor stuk een essentiële rol in de (door)ontwikkeling naar onze toekomstbestendige privacy- en informatiebeveiligingsorganisatie.

1. ***Wendbare, weerbare en aantoonbare organisatie op het gebied van informatiebeveiliging en privacy***
   De ambitie van de OWO-gemeenten is dat zij wendbaar, weerbaar en aantoonbaar zijn op het gebied van informatiebeveiliging en privacy. Dit vraagt dat de gemeenten aan voldoende veranderkracht beschikken op het moment dat ontwikkelingen, bijvoorbeeld op het gebied van digitale technologie of wetgeving, veranderingen van ons verlangen. Tot slot zorgt aantoonbaarheid van een passend beveiligingsniveau voor vertrouwen van inwoners en (keten)partners en medewerkers.
2. ***Privacy en informatiebeveiliging staan ten dienste van de organisatie***
   Het is van groot belang dat bij de beoordeling van risico's en de implementatie van (nieuwe) maatregelen op het gebied van privacy en informatiebeveiliging de kernactiviteiten van de gemeenten in acht worden genomen. Daarnaast horen maatregelen passend te zijn en in verhouding te staan tot de risico's. Op deze manier staat de kernactiviteit van de gemeenten centraal én verwerken we informatie veilig.
3. ***Privacy en informatiebeveiliging zijn integraal onderdeel van bedrijfsprocessen***
   Privacy en informatiebeveiliging maken integraal deel uit van bedrijfsprocessen, en zijn niet slechts toevoegingen. Het integraal inbedden van privacy en informatiebeveiliging zorgt voor gepaste beveiligingsmaatregelen die beter aansluiten op bedrijfsprocessen. Dit maakt bedrijfsprocessen efficiënt, effectief, veilig en verbetert tot slot de continuïteit ervan.
4. ***Privacy en informatiebeveiliging is van ons allemaal***
   Het waarborgen van informatiebeveiliging en het grondrecht op privacy hoort gedragen te worden door iedereen in de organisatie. Iedereen hoort zich hiervoor verantwoordelijk te voelen, van directie tot medewerkers. Alleen samen kunnen we ervoor zorgen dat we misbruik van informatie voorkomen en een betrouwbare en veilige dienstverlening bieden aan inwoners en (keten)partners, nu én in de toekomst.

### 1.4 Leeswijzer

In dit document worden eerst de aanleiding en doelstelling van dit beleidsstuk en de visie van de OWO-gemeenten op privacy en informatiebeveiliging besproken. In hoofdstuk 2 worden de interne en externe ontwikkelingen op het gebied van informatiebeveiliging besproken. Hoofdstuk 3 beschrijft vervolgens de beleidsdoelstellingen van de OWO-gemeenten met betrekking tot informatiebeveiliging. In hoofdstuk 4 worden de belangrijkste risico's genoemd die nu, en in de toekomst een bedreiging kunnen vormen voor de dienstverlening van de OWO-gemeenten. Hoofdstuk 5 gaat in op de rollen, taken en verantwoordelijkheden van o.a. de gemeenteraad, het college van B&W, de directie, het management en medewerkers. In hoofdstuk 6 wordt aandacht besteed aan de borging van dit informatieveiligheidsbeleid in de OWO-gemeenten.

## Hoofdstuk 2 – Interne en externe ontwikkelingen

### 2.1 Interne ontwikkelingen

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging steeds belangrijker wordt. Enerzijds omdat inwoners en ondernemers snel(ler) digitaal geholpen willen worden, anderzijds omdat persoonsgegevens een steeds lucratiever doel vormen voor kwaadwillenden. Gemeenten hebben een hoop persoonsgegevens en lopen daardoor een groter risico, omdat zij daardoor een doelwit zijn.

#### 2.1.1 Naar de cloud

Een ontwikkeling is de steeds verdere verschuiving van in huis geïnstalleerde en beheerde applicaties naar extern gehoste SaaS-oplossingen en webapplicaties. Dataverwerking gebeurt steeds meer en meer in de 'cloud'. Ook de OWO-gemeenten hanteren het principe 'Cloud, tenzij'. Ons voorkeur cloud-servicemodel gaat uit van een SaaS-oplossing met als randvoorwaarde dat ze voldoen aan de gestelde eisen uit ons informatiebeveiligingsbeleid, waaronder de BIO. Het betekent ook een rolverschuiving naar regie op leveranciers. De gemeente is afnemer (klant) en dient actief te rapporteren over en sturen op meetbare criteria waaraan de leverancier hoort te voldoen.

#### 2.1.2 Plaats-, apparaat- en tijdonafhankelijk werken

Als gemeente willen we plaats-, apparaat- en tijdonafhankelijk werken. Dit heeft tot gebruik van meer mobiele apparaten (smartphones, tablets, laptops en IoT-apparatuur) tot gevolg, maar ook gevolgen voor de connectiviteit en netwerken. Er wordt steeds meer gegevens gedeeld in ketens. Denk hierbij aan het sociaal domein. Informatie moet snel, duidelijk en betrouwbaar voorhanden zijn. Dit stelt ook nadere eisen aan de bescherming van gegevens, met name de vertrouwelijke gegevens.

### 2.2 Externe ontwikkelingen

#### 2.2.1 Baseline informatiebeveiliging Overheid

De Baseline informatiebeveiliging overheid (BIO) is van toepassing op alle overheidsinstellingen en daarmee ook op de OWO-gemeenten. De BIO is de standaardnorm voor informatiebeveiliging, en de

norm op basis waarvan dit informatiebeveiligingsbeleid wordt vormgegeven. In 2026 wordt een nieuwe versie van BIO verwacht, de BIO2. De inwerkingtreding van de Cyberbeveiligingswet (Cbw) zorgt ervoor dat naleving van de BIO2 verplicht wordt, o.a. voor gemeenten.

### 2.2.2 NIS2
De Network en information security directive (NIS2) betekent een wettelijke verplichting voor gemeenten om passende maatregelen te nemen om cyberbeveiligingsrisico's te beheersen. Gezien het feit dat gemeenten nu al een zorgplicht (BIO), een meldplicht (IBD) en toezicht (Eenduidige Normatiek Single Information Audit, ENSIA) hebben zal de impact van NIS2 voor gemeenten afhankelijk zijn van de mate waarin voldaan wordt aan de BIO. De NIS2 is een Europese richtlijn en wordt geïmplementeerd in de vorm van de Cbw in Nederland. De verwachting is dat de Cbw in het tweede kwartaal van 2026 in werking treedt.

### 2.2.3 Dreigingsbeeld Nederlandse gemeenten
Het Dreigingsbeeld Nederlandse gemeenten geeft een actueel zicht op incidenten en facturen uit het verleden. Het dreigingsbeeld richt zich op de ambtelijke organisatie, het bestuur, de politiek, de inwoners en de ondernemers.

### 2.2.4 De basis op orde (GGI – Veilig en basismaatregelen van het NCSC)
Met de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) bouwen gemeenten aan een veilige, samenhangende digitale infrastructuur die samenwerken tussen gemeenten en andere overheden, beter, veiliger en gemakkelijker maakt.

### 2.2.5 Common Ground
Met de visie Common Ground leggen gemeenten een basis voor een toekomstgerichte informatievoorziening die gemeente in staat stelt op een flexibele en moderne manier maatschappelijke vraagstukken, dienstverlening en bedrijfsvoering op te pakken. Door gegevenshuishouding volgens de Common Ground principes in te richten is het mogelijk om snel en flexibel te vernieuwen, te voldoen aan privacywetgeving en efficiënt om te gaan met gegevens.

### 2.2.6 Applicaties en toepassingen zijn standaard en bewezen
Voor de ondersteuning van de bedrijfsprocessen gebruiken we standaard applicaties die meegroeien met ontwikkelingen. We zetten daarom in op het gebruik van bewezen oplossingen die door meerdere partijen gebruikt worden. Tevens borgen we hiermee de toekomstbestendigheid, omdat we meegroeien met ontwikkelingen.

### 2.2.7 Internet of Things
Voorheen 'domme' objecten worden slim gemaakt (IoT) en maken besturen gemakkelijker. Bijvoorbeeld camera's die drukte meten bij bruggen. Echter is beveiliging niet altijd in afdoende mate geborgd waardoor dit de informatiebeveiliging en de bescherming van persoonsgegevens onder druk zet. De IoT-apparatuur en –software die we hiervoor inzetten, zorgt voor meer risico's en kwetsbaarheden. Zeker als ook de scheiding tussen de gemeentelijke ICT en IoT niet goed wordt geregeld; een verouderd camerasysteem in het gemeentelijke netwerk kan dan de ongewilde entree zijn tot gegevens en systemen van de gemeente.

### 2.2.8 Kunstmatige intelligentie
Bij Kunstmatige intelligentie (ook wel Artificiële intelligentie (AI)) gaat het om de mogelijkheid van een systeem (zelfstandig) te leren en beslissingen te nemen. Hiervoor worden bepaalde algoritmen gevolgd. Algoritmen, die de basis vormen voor veel software, zijn niet per definitie neutraal. Nederlandse gemeenten zetten in toenemende mate AI in voor uiteenlopende taken van het opsporen van problematische schulden, het detecteren van fraude en het stellen van betere diagnoses in de zorg. AI heeft ook een andere kant. Met de inzet van AI kunnen grondrechten in het gedrang komen. Daarom staan mensenrechten en publieke waarden bij de toepassing en ontwikkeling van deze technologie centraal. AI moet belangrijke waarden – zoals transparantie, non-discriminatie, privacy en veiligheid – borgen en waar mogelijk versterken. Menselijke alertheid en controle is nodig om ongewenste effecten te voorkomen.

### 2.3 Bewustwording
Vanwege de toenemende verandering van (digitale) technologie, het dreigingslandschap en de verantwoordelijkheden van de gemeente in dit speelveld is het van belang dat iedereen in de organisatie zich bewust is van zijn of haar verantwoordelijkheden.

**Informatiebeveiliging is meer dan alleen techniek**
Informatiebeveiliging gaat over veel meer dan ICT. Uiteindelijk is menselijk gedrag en informatiebeveiligingsbewustzijn de belangrijkste factor voor het veilig houden van informatie en de dienstverlening.

Een groot deel van de informatiebeveiligingsincidenten uit de recente geschiedenis zijn terug te herleiden naar een menselijke fout. Het is noodzakelijk dat alle medewerkers de juiste instelling hebben ten aanzien van informatieveiligheid en privacy en dat het College, de gemeentesecretaris, de directie en het management dit actief uitdraagt en stimuleert. Op deze manier wordt het juiste gedrag bevorderd en ontstaat een cultuur waarin men elkaar aanspreekt op fout en goed gedrag.

**De gemeente faciliteert, stimuleert en handhaaft veilig gebruik van informatie**
Veilig gedrag ontstaat niet zomaar. De gemeente faciliteert en stimuleert de verbetering van bewustwording planmatig en structureel door middel van leerzame en interessante (bewustwordings)trainingen, lezingen, en speciale interventies zoals: het uitnodigen van een mystery guest of het organiseren van phishing campagnes. Het uitgangpunt hiervoor is het positief stimuleren van medewerkers om draagvlak en intrinsieke motivatie bij hen te creëren om veilig te werken.

## Hoofdstuk 3 – Beleidsdoelstellingen

Om te voldoen aan de visie en ambities van de OWO-gemeenten wordt gewerkt met de beleidsdoelstellingen die door de Informatiebeveiligingsdienst (IBD) zijn geformuleerd. De OWO-gemeenten omarmen deze beleidsdoelstellingen. Deze beleidsdoelstellingen sluiten aan bij de eigen visie en ambities, het realiseren ervan waarborgt de beveiliging van informatie binnen de OWO-gemeenten.

### 3.1 De beleidsdoelstellingen van dit beleid

**De beleidsdoelstellingen, zoals geformuleerd door de IBD**:

- het managen van de informatiebeveiliging;
- adequate bescherming van bedrijfsmiddelen;
- het minimaliseren van risico's van menselijk gedrag;
- het voorkomen van ongeautoriseerde toegang;
- het beheersen van de toegang tot informatiesystemen;
- het garanderen van betrouwbare en veilige informatievoorzieningen;
- het waarborgen van veilige informatiesystemen;
- het adequaat reageren op incidenten;
- het beschermen van kritieke bedrijfsprocessen;
- het beschermen en correct verwerken van persoonsgegevens van inwoners, medewerkers en samenwerkende partijen;
- het waarborgen van de naleving van dit beleid.

**De 10 bestuurlijke principes voor informatiebeveiliging**
De 10 bestuurlijke principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader van de BIO en de beleidsdoelstellingen van de IBD. De principes gaan over de waarden die de bestuurder zichzelf oplegt en uitdraagt aan de gemeentelijke organisatie. De principes worden verwerkt binnen alle gemeentelijke processen.

Bestuurders hebben een rol in het op orde brengen van de informatiebeveiliging. Onjuiste en/of onvolledige informatiebeveiliging kan leiden tot misbruik van informatie en heeft (in)directe nadelige gevolgen voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

De 10 bestuurlijke principes voor informatiebeveiliging:

1. bestuurders bevorderen een veilige cultuur;
2. informatiebeveiliging is van iedereen;
3. informatiebeveiliging is risicomanagement;
4. risicomanagement is onderdeel van de besluitvorming;
5. informatiebeveiliging behoeft ook aandacht in (keten)samenwerking;
6. informatiebeveiliging is een proces;
7. informatiebeveiliging kost geld;
8. onzekerheid dient te worden ingecalculeerd;
9. verbetering komt voort uit leren en ervaring;
10. het bestuur controleert en evalueert.

### 3.2 Realiseren beleidsdoelstellingen

De uitwerking van de beleidsdoelstellingen vindt plaats in de jaarplannen voor informatiebeveiliging van de drie OWO-gemeenten. Ook werken de drie gemeenten samen, waaronder met team OWO-ICT, om uitvoering te geven aan dit beleid.

In de afgelopen jaren zijn er al stappen gezet. Gedurende de looptijd van dit beleid versterken de OWO-gemeente hun informatiebeveiliging verder – en waar dat nog niet het geval is – brengen zij deze in

lijn met dit beleid. In het bijzonder gaan de drie gemeenten in de eerste twee loopjaren van dit beleid een intensieve samenwerking aan om de BIO verder te implementeren.

## Hoofdstuk 4 – Belangrijkste risico's

Onze gemeente digitaliseert net als de samenleving om ons heen. Zodoende is informatiebeveiliging een onderwerp dat steeds belangrijker wordt. Inwoners en partijen waar wij mee samenwerken willen snel en digitaal geholpen worden maar daarmee nemen moderne en digitale dreigingen alsmaar toe. Het IBD brengt periodiek in kaart wat de actuele, meest belangrijke risico's zijn op het gebied van gemeentelijke informatiebeveiliging.

**4.1 De belangrijkste risico's zijn volgens de IBD als volgt**:

- **Uitval van dienstverlening en bedrijfsvoering**: als informatie niet beschikbaar is, leidt dat tot problemen in de dienstverlening en de bedrijfsvoering.
- **Vertrouwelijke informatie in verkeerde handen**: onterechte toegang tot gevoelige informatie kan uiterst nadelig uitvallen voor inwoners en ondernemers
- **Fouten in de dienstverlening**: informatiebeveiligingsincidenten kunnen leiden tot fouten in dienstverlening. Want als informatie niet integer is, kan dat leiden tot vertraagde of foute beslissingen, verkeerde handelingen en verspilling van tijd en menskracht.

Aanvullend op de genoemde risico's valt de IBD in het bijzonder drie soorten dreigingen op:

- **Meer ransomware, met destructievere gevolgen**: aan de lopende band proberen criminelen een ingang te vinden. De (potentiële) gevolgen van een aanval worden ook steeds ernstiger.
- **Steeds meer en ernstiger kwetsbaarheden in software**: kwetsbaarheden met een hoge kans op misbruik en ernstige gevolgen komen in de afgelopen jaren relatief steeds vaker voor.
- **Gevaren in ketens uit het zicht**: als gemeente neem je deel aan veel samenwerkingsverbanden. Dit heeft als gevolg dat er weinig zicht is op de feitelijke risico's als taken zijn uitbesteed.

Aanvullend op bovengenoemde bekende risico's voeren we als gemeente een eigen registratie waarin incidenten worden vastgelegd. Deze registratie geeft waardevolle informatie om van te leren en zodoende zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van beleid en procedures.

## Hoofdstuk 5 – Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen benoemd met de hieraan verbonden verantwoordelijkheden uiteengezet. Hiermee wordt duidelijk welke taken, verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging en privacy op welke plaats zijn belegd binnen de OWO-gemeenten.

**5.1. De organisatie van informatiebeveiliging**
Hieronder worden de taken en verantwoordelijkheden rondom informatiebeveiliging in het kort besproken. In bijlage 1 zijn de taken en verantwoordelijkheden nader uitgewerkt.

**De gemeenteraad**
De gemeenteraad heeft een controlerende en toetsende rol met betrekking tot informatiebeveiliging en ziet erop toe dat het informatiebeveiligingsbeleid en de doelstellingen die daaruit voortvloeien worden behaald.

**Het College van B&W**
Het College van B&W van de gemeenten Ooststellingwerf, Weststellingwerf en Opsterland zijn integraal verantwoordelijk voor de beveiliging (in de beslissende rol) van informatie binnen de werkprocessen van de gemeente.

Het College van B&W stelt kaders voor informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Dit doet het college van B&W o.a. door het vaststellen van het informatiebeveiligingsbeleid.

**De directie**
De directie (in de sturende rol) is verantwoordelijk voor het borgen van de uitvoering en naleving van het informatiebeveiligingsbeleid.

Enkele taken en verantwoordlijkheden van de directie:

- De directie stelt periodiek onderliggend, flankerend beleid inclusief procedures, richtlijnen en beveiligingsmaatregelen vast;
- stuurt op concern risico's;

- controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen;
- controleert of deze maatregelen voldoende bescherming bieden en;
- evalueert periodiek beleidskaders en stelt deze waar nodig bij.

**Het lijnmanagement**
Het lijnmanagement is in de **vragende rol** verantwoordelijk voor de integrale beveiliging van hun organisatieonderdeel.

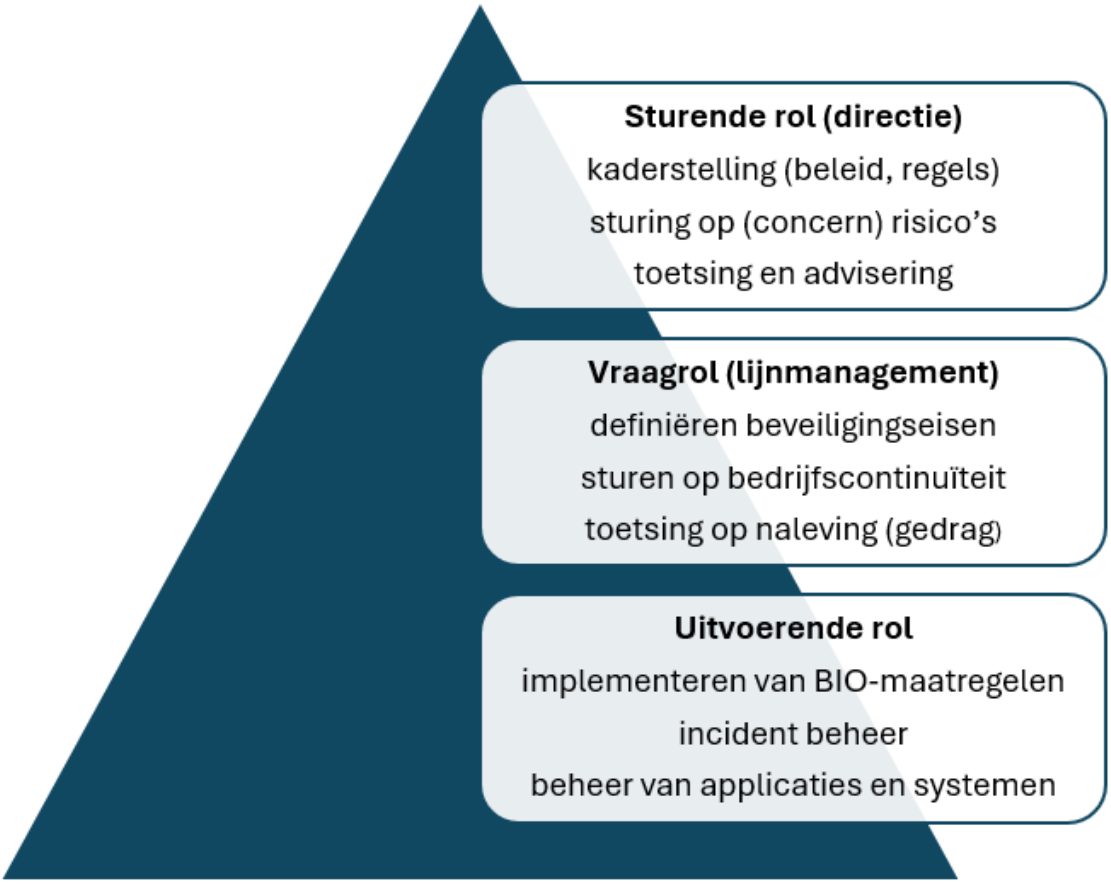
Enkele taken en verantwoordlijkheden van het lijnmanagement:
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- stelt op basis van een expliciete risicoafweging betrouwbaarheidseisen vast voor de informatiesystemen binnen zijn/haar team (classificatie);
- is verantwoordelijk voor de keuze en de implementatie van de beveiligingsmaatregelen die voortvloeien uit de betrouwbaarheidseisen;
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente aan de directie.

**Chief Information Security Officer (CISO)**
De CISO is verantwoordelijk voor het ontwikkelen, coördineren en bewaken van het gemeentelijke informatiebeveiligingsbeleid. De CISO vertaalt wet- en regelgeving (zoals de BIO) naar praktische maatregelen en adviseert bestuur en management over risico's. Daarnaast stelt de CISO jaarplannen op voor informatiebeveiliging en rapporteert hij of zij over informatiebeveiliging aan de directie.

**Medewerkers**
Medewerkers zijn verantwoordelijk voor het naleven van het informatiebeveiligingsbeleid binnen hun eigen dagelijkse werkzaamheden. Daarnaast hebben medewerkers ook een signalerende functie, denk hierbij aan: het melden van incidenten benaderen van hun lijnmanager of de CISO bij vragen over informatiebeveiliging (binnen processen).

Ook kunnen medewerkers aanvullende werkzaamheden worden toegewezen rondom informatiebeveiliging door hun lijnmanager, ze zijn dan actiehouder m.b.t. informatiebeveiliging (denk hierbij aan het implementeren van BIO-maatregelen). Deze actiehouders van de verschillende organisatieonderdelen (HRM, PSA, Beheer en Onderhoud, I&A, etc.) zijn dan in de **uitvoerende rol** verantwoordelijk voor de uitvoering van de beveiligingsmaatregelen.

**De sturende, vragende en uitvoerende rollen.**
In onderstaande piramide staan de sturende, vragende en uitvoerende rollen afgebeeld.




**Overzicht van de taken en verantwoordelijkheden**
In onderstaand overzicht staan de taken en verantwoordelijkheden voor de verschillende doelgroepen afgebeeld. In bijlage 1 worden de taken en verantwoordelijkheden uitgebreider beschreven.

| **Doelgroep** | **Relevantie voor het informatiebeveiligingsbeleid** |
|---|---|
| College van B&W | Integrale en bestuurlijke eindverantwoordelijkheid |
| Directie | Ambtelijk verantwoordelijk en sturing op informatieveiligheid |
| Lijnmanagement (proceseigenaren) | Implementatie en controle op naleving.<br>Classificatie: bepalen van beveiligingsniveau van informatie en implementatie van informatieveiligheid in het eigen bedrijfsproces |
| Beveiligingsfunctionaris (CISO) | Centrale coördinatie en toezicht op de uitvoering van het informatiebeveiligingsbeleid |
| Systeem en netwerkbeheerders<br>Functioneel beheerders<br>Wijzigingsbeheerders<br>Certificaatbeheerders | Operationele uitvoering |
| HRM en PSA | Arbeidsvoorwaardelijke zaken |
| Team Dienstverlening / Interne dienst (Facilitaire Zaken) | Fysieke toegangsbeveiliging |
| OWO ICT | Technische beveiliging |
| Medewerkers | Gedrag en naleving |
| Auditors | Onafhankelijke toetsing |
| Leveranciers en ketenpartners | Compliance aan het beleid en de BIO |

### 5.2 Belangrijkste uitgangspunten

Het bestuur, de directie en de managers spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Het management geeft een duidelijke richting aan informatiebeveiliging en laat zien dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente.

**De belangrijkste uitgangspunten voor succesvolle naleving van het beleid**

- Alle informatie en informatiesystemen zijn vanuit het oogpunt van informatiebeveiliging van belang voor de gemeente, en mogelijk ook van vitaal en/of kritiek belang.
- Deugdelijke uitvoering en naleving van de governancestructuur zoals in H5.1 en bijlage 1 beschreven.
- Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Ooststellingwerf, Weststellingwerf en Opsterland hebben een interne eigenaar die het beveiligingsniveau bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, Do, Check en Act' vormen samen het managementsysteem van informatiebeveiliging (ISMS), zie hoofdstuk 6.
- (Operationele) regels en verantwoordelijkheden voor het informatiebeveiligingsbeleid dienen te worden vastgelegd en vastgesteld.

### 5.3 Informatiebeveiliging in de OWO-samenwerking

De OWO-gemeenten neemt deel aan verschillende samenwerkingsverbanden. Bij deze samenwerkingen is sprake van uitwisseling van informatie, waarvan de gemeente, eigenaar of beheerder is.

**OWO-samenwerking en I&A**

Bijzondere aandacht is er voor de bestuursovereenkomst OWO waarbij de ICT door de gemeente Weststellingwerf voor de drie gemeenten wordt uitgevoerd. Vanuit die hoedanigheid is OWO I&A de uitvoerende partij voor een groot gedeelte van de tactische en operationele informatiebeveiligingsrichtlijnen en -maatregelen. Binnen OWO I&A vervullen de Security Engineer (SE) en de Senior medewerker ICT een belangrijke rol bij de operationalisering van informatiebeveiliging op basis van dit beleid.

Concreet houdt dit onder andere in dat OWO I&A de technische beveiligingsmaatregelen voor onze infrastructuur neemt en ernaar streeft ons netwerk veilig te houden. Denk hierbij aan: back-up en restore, segmentatie van het netwerk en het bestrijden van informatiebeveiligingsincidenten. In de praktijk betekent dit ook veel afstemming tussen de CISO's, de SE en de Senior medewerker ICT.

**Samenwerking informatiebeveiliging in OWO-verband**

Om de samenhang in informatiebeveiliging tussen de OWO-gemeenten te waarborgen is er regulier overleg tussen de CISO's, de SE en de Senior medewerker ICT. In dit overleg worden de actualiteiten en ontwikkelingen (intern binnen OWO en extern) op het gebied van informatiebeveiliging besproken. Ook worden eventueel acties uitgezet om (strategisch) in te spelen op de actualiteiten en ontwikkelingen om informatiebeveiliging binnen de OWO-gemeenten te waarborgen. De drie gemeenten en de OWO-afdelingen zorgen ervoor dat zij elkaar voorzien van de benodigde informatie en tijdig afstemming met elkaar zoeken, waar nodig of wenselijk.

## Hoofdstuk 6 – Borging en verantwoording informatiebeveiligingsbeleid

### 6.1 PDCA-cyclus informatiebeveiliging

Om de borging van het informatiebeveiligingsbeleid en de daarvan afgeleide plannen te realiseren wordt onderstaande Plan, Do, Check, Act (PDCA)-cyclus doorlopen (afbeelding 1). De volgende uitgangspunten worden gehanteerd voor het doorlopen van de PDCA-cyclus (Information Security Management System (ISMS)).

**1. Plan (Plannen)**

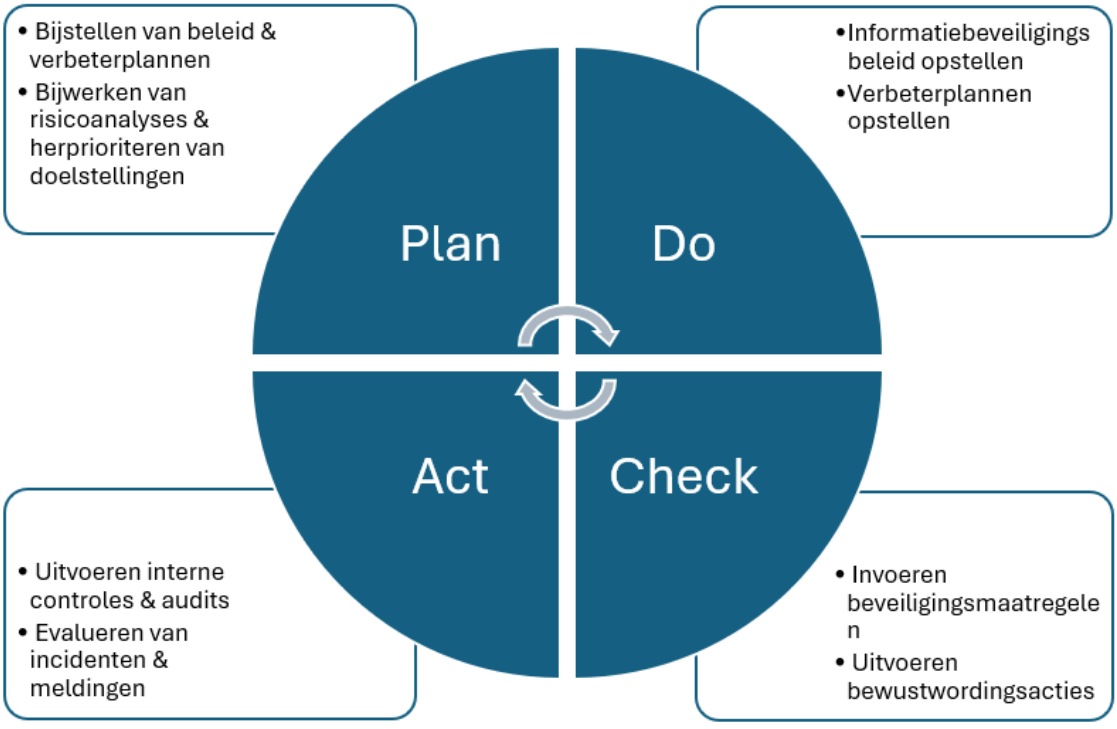
In deze fase wordt de basis gelegd voor het informatiebeveiligingsbeleid. De gemeente:

- Voert een risicoanalyse uit om kwetsbaarheden, dreigingen en risico's in kaart te brengen (bijv. via DPIA of risicobeoordelingen volgens BIO).
- Stelt beleid en doelstellingen op, afgestemd op wetgeving (zoals de BIO, AVG en Wpg) en gemeentelijke belangen.
- Bepaalt welke processen, systemen en informatiestromen beschermd moeten worden.
- Stelt een plan van aanpak op met maatregelen (zowel organisatorisch als technisch) en benoemt verantwoordelijkheden.

**2. Do (Uitvoeren)**
De geplande maatregelen worden geïmplementeerd. Denk aan:
- Invoering van beveiligingsmaatregelen (zoals toegangsbeheer, encryptie, back-ups, logging).
- Opstellen en uitvoeren van procedures (incidentafhandeling, wijzigingsbeheer, classificatie van informatie).
- Bewustwordingsactiviteiten voor medewerkers (bijv. (onboardings)trainingen, phishingtests, workshops).
- Technische implementaties, zoals firewalls, monitoringtools of identity & access management.

**3. Check (Controleren)**
De gemeente controleert of de maatregelen effectief zijn en of het beleid wordt nageleefd:
- Uitvoeren van interne controles, audits en self-assessments (bijvoorbeeld BIO-audits of ENSIA).
- Evalueren van incidenten, meldingen en afwijkingen.
- Monitoren van prestaties en risico's via logging, rapportages en dashboards.
- Controleren of de informatiebeveiligingsdoelen worden behaald.

**4. Act (Bijstellen)**
Op basis van de uitkomsten uit de check-fase worden verbeteringen doorgevoerd:
- Bijstellen van beleid, procedures of maatregelen waar nodig.
- Behandelen van bevindingen uit audits of incidentanalyses.
- Bijwerken van risicoanalyses en herprioriteren van maatregelen.
- Stimuleren van continue verbetering via de managementcyclus en (eventueel) het ISMS.




*Afbeelding 1 PDCA-cyclus informatieveiligheid*

**6.2 De sturende, vragende en uitvoerende rol in de PDCA-cyclus uitgewerkt**
De invulling van de sturende, vragende en uitvoerende rol in een PDCA-cyclus zijn in onderstaand kader weergegeven.

| Wie | Plan: | Do: | Check: | Act: |
|---|---|---|---|---|

| | Kaderstelling | Uitvoering | Controle | Verbetering |
|---|---|---|---|---|
| **Sturen: Directie. (dagelijkse uitvoering: beveiligingsfunctionaris)** | Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning. | Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons. | Controle, audit. | Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ College van B&W |
| **Vragen: Lijnmanagement alle organisatie onderdelen** | Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen. | Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management. | Controle, sturen op naleving van regels door medewerkers (gedrag), compliancy. | Verbeteren bedrijfscontinuïteit. Rapportage aan beveiligingsfunctionaris. |
| **Uitvoeren: Sleutel functionarissen (HRM, PSA, Beheer en Onderhoud, I &A, BZ, SD)** | Beleidsvoorbereiding, (technische) onderzoeken (marktverkenningen). | Leveren van diensten en advies. Specifiek ICT: incidentbeheer, logging, monitoring en advies. | Evaluatie en rapportage. Specifiek ICT: pentesten /vulnerability scanning. | Uitvoeren verbeteracties. Adviseren directie over aanpassingen aan de informatievoorziening. |

**6.2 Audits (ENSIA) en controle**

Om te beoordelen of de organisatie zijn informatiebeveiligingsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke audits en controles uitgevoerd. Bij een audit toetst een onafhankelijke deskundige partij op de opzet, bestaan en voor een bepaald aantal normen op de werking van beheersmaatregelen. Hiervoor wordt doorgaans een externe partij, gecertificeerde auditor, ingeschakeld. De uitkomsten van de diverse interne en externe audits bieden input voor het actieplan zoals genoemd onder stap twee van de PDCA-cyclus. Als resultaat van de audit kunnen eventuele zwakheden in de beveiliging ontdekt worden en dit kan tot gevolg hebben dat er aanpassingen noodzakelijk zijn in het beveiligingsbeleid. De gemeente verantwoordt zich over informatiebeveiliging middels de jaarlijks verplichte ENSIA-systematiek (Eenduidige Normatiek Single Information Audit). De ENSIA toets door middel van zelfevaluaties en audits enerzijds de kwaliteit van de basisregistraties en anderzijds de informatiebeveiliging (afbeelding 3).

Naast de ENSIA en overige audits zijn er meer controles. De beheersing van de IT-omgeving maakt onderdeel uit van de accountantscontrole, onderverdeeld in de volgende onderwerpen: informatiebeveiligingsbeleid en AVG, leveranciersmanagement, wijzigingenbeheer, logische toegangsbeveiliging en continuïteitsbeheer. Informatiebeveiliging kan ook onderdeel uitmaken van een Rekenkameronderzoek. Om misbruik, oneigenlijk gebruik en fraude te voorkomen worden controles of onderzoeken uitgevoerd op onderwerpen als autorisatiebeheer en toegangscontrole. Ook controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel en input voor het actieplan. Ten slotte leren we van beveiligingsincidenten en indien daarbij persoonsgegevens zijn betrokken van datalekken door deze zorgvuldig te registreren en te evalueren.

| ENSIA | Verantwoording over informatiebeveiliging aan gemeenteraad | Verantwoording aan toezichthouders |
|---|---|---|
| **Zelfevaluatie** | • Informatiebeveiliging binnen gemeente volgens Baseline Informatiebeveiliging Overheid (BIO).<br>• Domeinspecifieke vragenlijsten voor diverse stelsels.<br>• Zelfevaluatie afronden en vastleggen in ENSIA. | Vragenlijsten:<br>• RvIG: Informatiebeveiliging BRP & Reisdocumenten en Suwinet (BIO).<br>• BKWI: Informatiebeveiliging Suwinet (BIO).<br>• Logius: Informatiebeveiliging DigiD.<br>• DGBRW: Datakwaliteit en -integriteit BAG, BGT en BRO. |
| Opstellen | • Genereren en opstellen verantwoordingsrapportages.<br>• Audit door gecertificeerde RE-auditor over collegeverklaring Suwinet en DigiD.<br>• Opstellen rapportage ENSIA t.b.v. de gemeenteraad. | Producten:<br>• Collegeverklaring over Suwinet en DigiD.<br>• Rapportage BAG, BGT en BRO door college van B&W.<br>• Uittreksels BRP en Reisdocumenten.<br>• Rapportage ENSIA voor de gemeenteraad. |
| Verantwoorden | • Vaststellen en ondertekenen verantwoordingsrapportages door College van B&W.<br>• Uploaden en aanleveren verantwoordingsrapportages via ENSIA (Uittreksels BRP en Reisdocumenten verwerken in de rapportages uit de Kwaliteitsmonitor en daar uploaden). | Resultaten:<br>• De toezichthouders BKWI, Logius en DGBRW krijgen via ENSIA de verantwoordingsrapportages aangeleverd.<br>• RvIG krijgt de informatie uit de Uittreksels BRP en Reisdocumenten via de Kwaliteitsmonitor aangeleverd. |
| Versturen | • Opstellen paragraaf verantwoording informatiebeveiliging voor de paragraaf Bedrijfsvoering in het jaarverslag.<br>• Gemeenteraad neemt kennis van rapportage ENSIA.<br>• College van B&W stelt jaarverslag vast.<br>• Gemeenteraad keurt jaarverslag goed.<br>• Het college van B&W stuurt het gemeentelijk jaarverslag aan de provincie. | • De toezichthouders krijgen de antwoorden op de vragenlijsten digitaal aangeleverd.<br>• De vastgestelde jaarstukken zijn aan de provincie toegestuurd. |

*Afbeelding 2 Het verantwoordingsproces ENSIA*

gemeente Opsterland

## Bijlage 1 – Uitwerking rollen en verantwoordelijkheden informatiebeveiliging OWO-gemeenten

**De gemeenteraad**
Toetsing en controle: de gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente. Het College legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring/In Control Verklaring (ICV) – waarop door een auditor assurance wordt afgegeven – en daarnaast in het jaarverslag met een passage over informatiebeveiliging in de paragraaf bedrijfsvoering.

**College van B&W**
Het College van Burgemeester en Wethouders (B&W) keurt het strategisch beleid formeel goed en draagt zorg voor de naleving van het beleid in de gemeente. Ook is er een portefeuillehouder informatiebeveiliging vastgesteld.

Het college informeert de Raad over de informatiebeveiliging van de gemeente door een aparte paragraaf op te nemen in de jaarrekening van de gemeente of door het doorgeleiden van een jaarrapportage.

**Gemeentesecretaris**
De gemeentesecretaris zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een afdelingshoofd. De gemeentesecretaris zorgt dat de afdelingshoofden zich verantwoorden over de beveiliging van de informatie die onder hen berust. De gemeentesecretaris zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het College zich verantwoorden naar de raad. De gemeentesecretaris heeft o.a. de volgende taken en bevoegdheden:

- Het stellen van kaders en het geven van sturing voor de veiligheid van informatie (gewenste niveau van continuïteit en vertrouwelijkheid);
- Het sturen op concern risico's;
- Het periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het (waar mogelijk) inrichten van functiescheiding tussen beleidsbepalende, uitvoerende en controlerende taken met betrekking tot informatiebeveiliging;
- Vaststellen van procedures en toewijzen van maatregelen op het gebied van informatiebeveiliging.

**Teamleiders en teammanagers**
De belangrijkste taken en bevoegdheden van het teamleiders, in afstemming met CISO en FG in het kader van informatiebeveiliging zijn:

- Rapporteren aan de gemeentesecretaris over de onder hun verantwoordelijkheid tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten.
- Vaststellen van betrouwbaarheidseisen voor de informatiesystemen binnen zijn/haar team op basis van een expliciete risicoafweging (classificatie);
- Het kiezen en implementeren van de beveiligingsmaatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het vroegtijdig signaleren en melden van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het leveren van input voor nieuwe maatregelen en procedures en het uit laten voeren van maatregelen die voortvloeien uit o.a. adviezen.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid en de daaraan gerelateerde procedures waarbij er zorgt voor wordt gedragen dat de teams de CISO, FG en PO tijdig betrekken.
- Bespreking van beveiligingsincidenten en de mogelijke gevolgen hiervan op beleid en maatregelen.
- Het uitdragen van het beveiligings- en privacybewustzijn, bedrijfscontinuïteit en de naleving van regels en richtlijnen op deze vakgebieden.
- Het rapporteren over compliance aan wet- en regelgeving en algemeen beleid van de gemeente aan de directie.

**Applicatiebeheerder**
Binnen de teams zijn er bepaalde medewerkers, voornamelijk applicatiebeheerders die fungeren als eerste aanspreekpunt voor team informatiebeveiliging en privacy omdat zij proceseigenaar zijn van een brede set informatie, wat aanvullende taken met zich mee brengt qua beheer, de coördinatie en advies ten aanzien van informatiebeveiliging en privacybescherming van specifieke gegevensverzamelingen en specifieke wet- en regelgeving. De CISO adviseert de applicatiebeheerders bij de uitvoering van hun taken.

Tot de taken en bevoegdheden van elke applicatiebeheerder behoren:

- Controleren, signaleren, rapporteren en aanpassen van de processen en applicaties; Tevens eerste aanspreekpunt.
- Informatiebeveiliging en privacy meenemen in beslissingen over de lopende en nieuwe processen en voorschriften van de applicaties.
- Uitvoering, toezicht en rapportage op de voorbereiding en uitvoering van het beveiligingsbeleid en- plan (en wet- en regelgeving) en hiermee compliance aan het afdelingshoofd en CISO/FG m.b.t. de eigen processen en applicaties.
- Vastleggen en beheren van maatregelen ten behoeve van eigen processen en applicaties in het Information Security Management System (ISMS).
- Opstellen van gebruikersdocumentatie informatiebeveiliging (en configuratie applicatie) zoals handleidingen, procedures, werkwijzen.
- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen en het opstellen van betrouwbaarheidseisen van applicaties/systemen.
- Beoordelen, toekennen en monitoren van autorisaties aan gebruikers op basis van een vastgesteld proces en met behulp van een autorisatiematrix.
- Toezicht houden dat nieuwe medewerkers worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures. Inclusief medewerkers aanspreken op de verantwoordelijkheid in hun dagelijkse werkprocessen en hiermee het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen.

We onderscheiden o.a. de volgende applicatiebeheerders:

- Applicatiebeheerders BAG, BGT en BRO en gegevensbeheer: toezien op naleving van de Wet- en Regelgeving van deze basisregistraties.
- Applicatiebeheerder DigiD: een taak die bij de (web)applicatiebeheerder van de DigiD-aansluiting is belegd en verantwoordelijk is voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit de Basis beveiligingsrichtlijnen DigiD, zoals technische maatregelen bij de externe leverancier (infrastructuur, segmentering etc.) en de interne dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer die jaarlijks wordt getoetst (ENSIA). Denk daarbij ook aan de bescherming van persoonsgegevens, voor zover een softwareleverancier waaraan diensten zijn uitbesteed daar niet voor verantwoordelijk is. Ook rapporteert de beveiligingsbeheerder DigiD hierover periodiek aan zijn/haar afdelingshoofd.
- Security Officer Suwinet: De security officer Suwinet is verantwoordelijk voor de beveiliging van Suwinet en het toezien op de naleving van de maatregelen en procedures die voortvloeien uit het normenkader dat van toepassing is op Suwinet. Zoals: technische maatregelen bij de externe leverancier (infrastructuur, segmentering etc.) en de interne dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer die jaarlijks wordt getoetst (ENSIA). Denk daarbij ook aan de bescherming van persoonsgegevens, voor zover een softwareleverancier waaraan diensten zijn uitbesteed daar niet voor verantwoordelijk is. Ook rapporteert de Security Officer Suwinet hierover periodiek aan zijn/haar afdelingshoofd.
- Applicatiebeheerder BRP en Reisdocumenten en Rijbewijzen: de applicatiebeheerder BRP en reisdocumenten en rijbewijzen brengt verantwoordelijkheden met zich mee om toe te zien op naleving van de beveiligingsmaatregelen en –procedures op het gebied van Basisregistratie Personen (BRP) en op het treffen van maatregelen om reisdocumenten en rijbewijzen, apparatuur, programmatuur, opslagmedia, documentatie en overige materialen te beveiligen tegen ontvreemding dan wel vernietiging ten gevolge van inbraak, diefstal, verduistering, overvallen, brand of anderszins. Tevens verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations) en voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.

**Medewerkers**
Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatievoorziening. Ongewenste, onbewuste acties blijken een groter risico voor de privacy van inwoners en de veiligheid van informatie dan bewuste en gerichte aanvallen. Zij dienen zorgvuldig en gedisciplineerd om te gaan met informatie en (informatie)systemen en zich bewust te zijn van eisen ten aanzien van de betrouwbaarheid, de integriteit en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken. Mocht een medewerker iets signaleren m.b.t. informatieveiligheid of privacy neemt diegene contact op met de CISO, PO of FG.

**Chief Information Security Officer (CISO)**
De CISO is de belangrijkste adviseur op het gebied van informatiebeveiliging. De CISO is verantwoordelijk voor de controle op een juiste uitvoering van het informatiebeveiligingsbeleid, de realisatie van de veiligheidsmaatregelen en de classificatie, coördinatie en escalatie van beveiligingsincidenten. Hieronder valt ook het controleren van autorisatiematrices. De CISO kan hiertoe de interne controle opdracht geven. De CISO is door het college gemandateerd en heeft de volgende taken en bevoegdheden:

- Beleid en coördinatie: het opstellen en actualiseren van het informatiebeveiligingsbeleid; het opstellen van informatiebeveiligingsplannen voor afdelingen of deelgebieden. Het coördineren van de werkzaamheden van collega's, afdelingen en instanties die betrokken zijn bij de uitvoering van het informatiebeveiligingsbeleid en -plan en het ondersteunen van college of gemeentesecretaris en de leidinggevenden met kennis over informatiebeveiliging. Treedt op als adviseur voor informatiebeveiliging bij een ICT-crisis.
- Controle en registratie: het toezicht houden op de implementatie en naleving van het informatiebeveiligingsbeleid.
- Het beheersen van de risicoanalyses en toezicht houden op de processen en beveiligingsmaatregelen.
- Het bijhouden van de registratie van informatiebeveiligingsincidenten en het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.
- Stelt controleplannen op en voert risicoanalyses en interne audits uit of initieert deze.
- Communicatie en voorlichting: het onderhouden van externe en interne contacten op alle niveaus over informatiebeveiliging en deelname aan (bewustwordings)activiteiten met betrekking tot informatiebeveiliging.
- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn.
- Aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatiebeveiliging en contactpersoon van de gemeente voor de Informatie Beveiligingsdienst (IBD).
- Advies en rapportage en uitvoering: het opstellen en uitwerken van beveiligingsplannen ten aanzien van de maatregelen, evenals het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen, waarbij ook afgestemd wordt met lopende projecten binnen de organisatie. Overleg en rapportage o.a. via de P&C cyclus over het aspect informatiebeveiliging aan management, College en Raad. Adviseert over en voert maatregelen in op basis van wet- en regelgeving.

**Functionaris Gegevensbescherming (FG)**
De FG heeft ondermeer de volgende wettelijke taken (AVG Art 39). Iedere gemeente kan aanvullend nog een eigen reglement hebben vastgesteld over de taken en bevoegdheden van de FG.

- Gevraagd en ongevraagd signaleren, adviseren en informeren van alle bestuursorganen binnen de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen aangaande de AVG, Wpg, andere EU wet- en regeling en nationale bepalingen omtrent gegevens-bescherming en overige onderwerpen die de privacy betreffen;
- Het communiceren met de gemeentelijke diensten en medewerkers over alle ontwikkelingen op het gebied van techniek en wetgeving die relevant zijn voor het gemeentelijk privacy- en beveiligingsbeleid; is daarmee het aanspreekpunt en de contactpersoon aangaande privacy, voor zowel de Autoriteit Persoonsgegevens, de interne organisatie als externe organisaties;
- Toezicht houden op de naleving van zowel de AVG en Wpg, als alle andere wet- en regelgeving met betrekking tot persoonsgegevens. Hierbij hoort tevens het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van een zwaarwegend advies met betrekking tot een gegevensbescherming effectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, en toezien op de uitvoering daarvan en het ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen;
- Zorgdragen voor de juiste en correcte melding en registratie van de afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en op het melden van een datalek bij de Autoriteit en Persoonsgegevens en bij de betrokkenen.
- Brengt verslag uit aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen de gemeentesecretaris, het college of de burgemeester en in sommige gevallen de gemeenteraad.

**Concerncontroller**
De concerncontroller is gemachtigd om op eigen initiatief, steekproefsgewijs, controles uit te voeren op een juiste uitvoering van het beleid door de gemeente. Dit kan bijvoorbeeld betrekking hebben op de controle op de voortgang van het uitvoeren van de maatregelen uit het informatiebeveiligingsbeleid of jaarplan.

## Bijlage 2 – Uitwerking beleidsuitgangspunten

Op deze bijlage van het informatiebeveiligingsbeleid OWO-gemeenten is geheimhouding opgelegd door het college van burgemeester en wethouders op 20 januari 2026. De geheimhouding is opgelegd in verband met de bedrijfsgevoelige aard van de informatie in de bijlage.