Informatieveiligheid in Weststellingwerf: Tussen ambitie en uitvoering

Rekenkameronderzoek naar beleid, uitvoering en bestuurlijke grip op digitale veiligheid

WESTSTELLINGWERF

Inhoudsopgave

Bestuurlijke nota

Samenvatting

Gemeenten zijn steeds afhankelijker geworden van digitalisering; elk gemeentelijk proces kent wel een digitaal component. Daarom neemt ook het belang van informatieveiligheid toe. De Rijksoverheid en Europa dringen met Richtlijnen en wetgeving aan op digitaal veilige gemeenten. De Europese 'Network and Information Security-directive' (NIS2 richtlijn) is bedoeld om de cyberbeveiliging en de weerbaarheid van 'essentiële diensten', waaronder lokale overheden, in de EU-lidstaten te verbeteren. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in de Cyberbeveiligingswet. Dit houdt in dat digitale veiligheid een plicht wordt voor gemeenten. Vanwege het toegenomen belang van digitale veiligheid en de aanvullende verplichtingen voor gemeenten, hebben de rekenkamers van de gemeenten Opsterland, Weststellingwerf en Ooststellingwerf hier onderzoek naar gedaan. Dit onderzoek is uitgevoerd van oktober 2024 tot januari 2025.

Het doel van het onderzoek is om in beeld te brengen of de informatiebeveiliging adequaat is georganiseerd en geborgd bij de OWO-gemeenten en in hoeverre de gemeenteraden in positie zijn om hun taken uit te voeren. De volgende vraag staat centraal in dit onderzoek:
Is de informatiebeveiliging van de OWO-gemeenten adequaat georganiseerd en geborgd?

Beleid en uitvoering in Weststellingwerf
De gemeente Weststellingwerf werkt op het gebied van ICT en informatiebeveiliging samen met Ooststellingwerf en Opsterland in het samenwerkingsverband OWO. Binnen deze samenwerking is Team ICT verantwoordelijk voor de uitvoering van technische beveiligingsmaatregelen, zoals firewalls, monitoring, back-ups en het beheer van applicaties. Grote applicaties worden centraal beheerd, terwijl kleinere applicaties onder de verantwoordelijkheid van de afzonderlijke gemeenten vallen. De verdeling van taken en verantwoordelijkheden is nog niet volledig uitgewerkt, maar hier wordt aan gewerkt.

Weststellingwerf heeft een eigen strategisch informatiebeveiligings- en privacybeleid dat loopt tot 2026. Dit beleid is gebaseerd op de BIO-normen en de AVG, en richt zich op het verbeteren van digitale veiligheid, het verhogen van kennis en het versterken van de organisatie. De gemeente streeft ernaar om te voldoen aan de BIO2-norm en werkt met een meerjarenplan aan de implementatie. De volwassenheid van de organisatie wordt momenteel ingeschat op niveau 1 of 2, met als doel doorgroei naar niveau 4.

De gemeente voert jaarlijks een ENSIA-audit uit en stelt een jaarrapport op over informatieveiligheid en privacy. Incidenten worden geregistreerd in een speciaal systeem. In 2024 zijn tien incidenten gemeld, waarvan twee ernstig. De Functionaris Gegevensbescherming (FG) houdt toezicht op het register en de meldingen aan de Autoriteit Persoonsgegevens. Het verwerkingsregister is verouderd en wordt vernieuwd.

De gemeente gebruikt de PDCA-cyclus om continu te verbeteren, maar deze is nog niet volledig ingebed. Er worden audits en zelfevaluaties uitgevoerd, en verbeterpunten worden bijgehouden op een verbeterlijst. De opvolging van deze punten is echter niet altijd duidelijk vastgelegd. De CISO en FG geven advies en rapporteren via de concerncontroller aan de directie.

Binnen de organisatie zijn de rollen en verantwoordelijkheden beschreven, maar in de praktijk is het eigenaarschap nog niet overal duidelijk. De CISO en FG zijn niet volledig onafhankelijk gepositioneerd, wat niet in lijn is met de BIO2-normen. Op het gebied van bewustwording worden activiteiten georganiseerd zoals phishingtesten, e-learnings en bijeenkomsten. Deelname is niet verplicht en informatieveiligheid is nog geen vast onderdeel van het dagelijks werk.

Rol van de gemeenteraad

De gemeenteraad van Weststellingwerf ontvangt rapportages over informatieveiligheid, zoals de ENSIA-audit en het jaarrapport van de CISO en FG. De controlecommissie bespreekt deze stukken en koppelt terug aan de raad. Toch blijkt uit gesprekken dat raadsleden weinig vragen stellen over dit onderwerp en dat het thema weinig prioriteit krijgt. Raadsleden geven aan dat zij het onderwerp belangrijk vinden, maar het vaak te technisch vinden. Er is behoefte aan betere informatie en ondersteuning om de controlerende en kaderstellende rol goed te kunnen vervullen

Belangrijkste bevindingen

- **Beleid:** Weststellingwerf heeft een strategisch informatiebeveiligings- en privacybeleid dat gebaseerd is op de BIO-normen. De gemeente voldoet nog niet aan de BIO2-standaarden, maar werkt aan een meerjarenplan om deze te implementeren.
- **Uitvoering:** Team ICT voert technische taken uit zoals monitoring, firewalls, back-ups en pentesten. De verdeling van verantwoordelijkheden tussen Team ICT en de gemeenten is niet altijd duidelijk en structureel overleg ontbreekt.
- **Incidenten:** De gemeente registreert incidenten en datalekken in een eigen systeem. In 2024 zijn tien incidenten gemeld, waarvan twee ernstig. De FG houdt toezicht op het register en meldt indien nodig aan de Autoriteit Persoonsgegevens.
- **PDCA-cyclus:** Weststellingwerf werkt met een verbetercyclus, maar deze is nog niet volledig ingericht. Audits en evaluaties worden uitgevoerd, maar de opvolging van verbeterpunten is niet altijd aantoonbaar vastgelegd.
- **Bewustwording:** Er zijn bewustwordingsactiviteiten zoals phishingtesten, e-learnings en bijeenkomsten. Deelname is niet verplicht en informatieveiligheid is nog geen vast onderdeel van het dagelijks werk.
- **Crisisorganisatie:** Er is een procedure voor ernstige ICT-verstoringen, maar deze is verouderd. In 2024 is een gezamenlijke crisisoefening gehouden, maar de rolverdeling binnen het crisisteam is nog onduidelijk. Een strategisch crisisplan ontbreekt.
- **Rol van de raad:** De gemeenteraad ontvangt rapportages zoals de ENSIA-audit, maar stelt weinig vragen over informatieveiligheid. Raadsleden vinden het onderwerp vaak te technisch en geven aan onvoldoende kennis te hebben om hun rol goed te vervullen.

Conclusies en aanbevelingen

Hieronder presenteren wij de conclusies en aanbevelingen van dit onderzoek in de gemeente Weststellingwerf.

Conclusies

De gemeente Weststellingwerf is verantwoordelijk voor het informatiebeveiligingsbeleid, maar de uitvoering daarvan vindt sinds 2012 voor een belangrijk deel plaats in OWO verband. Deze samenwerking levert belangrijke schaalvoordelen op, maar de taakverdeling tussen het samenwerkingsverband en de gemeente Weststellingwerf is niet op alle onderdelen duidelijk. Zo ontbreekt de structurele afstemming tussen de CISO's van de drie OWO gemeenten en het samenwerkingsverband. Ook hebben de drie OWO gemeenten los van elkaar trainings- en bewustwordingsactiviteiten ingekocht en uitgevoerd. Dit komt de effectiviteit van de samenwerking niet ten goede. Direct na afloop van dit onderzoek zijn plannen voor uitbreiding van de samenwerking gepresenteerd om de doelmatigheid en doeltreffendheid van beleid en uitvoering te vergroten.

In Weststellingwerf is het strategisch informatiebeveiligingsbeleid recent herijkt en vastgesteld door de gemeenteraad. Dit beleid sluit aan op de gangbare normen voor de gemeentelijke overheid. Zo wordt de Baseline Informatieveiligheid Overheid (BIO) als uitgangspunt van het beleid genomen. Weststellingwerf voldoet nog niet aan deze norm, maar dit is wel een belangrijke doelstelling. De BIO norm wordt onder de Cyberbeveiligingswet vervangen door de BIO2 en verplicht gesteld. Weststellingwerf bereidt zich momenteel voor om te voldoen aan deze norm. Volgens deze nieuwe norm moet de volwassenheid van de digitale veiligheid in de gemeente naar niveau 4. Thans groeit de gemeente Weststellingwerf naar volwassenheidsniveau 2. Dit komt voor een belangrijk deel omdat de PCDA cyclus niet goed is ingericht.

De gemeente heeft het afgelopen jaar de ENSIA verklaring gekregen. Dit betekent dat een externe auditor heeft vastgesteld dat de gemeente voldoet aan de veiligheidseisen van stelselhouders bij de Rijksoverheid voor het gebruik van hun applicaties. Hier voldoet Weststellingwerf aan de gestelde norm.

Uit het onderzoek komt ook naar voren dat de medewerkers van de gemeente Weststellingwerf het belang van digitale veiligheid onderkennen. Het bewustzijn hiervoor is toegenomen. Maar ook op dit vlak is verbetering mogelijk. Op dit moment is de gemeente Weststellingwerf zelf verantwoordelijk voor de digitale weerbaarheid van de eigen medewerkers door middel van trainings- en bewustwordingsactiviteiten. Er worden incidenteel wel activiteiten aangeboden, maar deelname is vrijblijvend. Een gestructureerde aanpak van activiteiten en opleiding, voor zowel nieuwe als zittende medewerkers, inclusief raadsleden, zal de digitale veiligheid in de gemeente versterken. Als de drie OWO gemeenten dit gezamenlijk oppakken, zijn ook hier schaalvoordelen te halen.

In het strategisch beleid wordt risicomanagement genoemd als uitgangspunt voor sturing op digitale veiligheid door het gemeentebestuur. De gemeente heeft hiervoor een systeem aangeschaft, maar dat is nog in ontwikkeling. In de praktijk stuurt het college van b. en w. niet op veiligheidsrisico's. Ook de gemeenteraad stuurt onvoldoende op digitale veiligheid. De gemeenteraad wordt via de P&C cyclus op hoofdlijnen op de hoogte gebracht van ontwikkelingen op dit gebied, maar wordt door het college van b. en w. onvoldoende in stelling gebracht om de controlerende en kaderstellende rol in te vullen. Maar de raad kan zichzelf ook actiever opstellen; de afgelopen jaren heeft de raad van Weststellingwerf geen vragen gesteld over dit onderwerp.

Een laatste conclusie betreft de crisisorganisatie. Als er, ondanks alle preventieve maatregelen die de gemeente Weststellingwerf (individueel of

in OWO samenwerkingsverband) genomen heeft, toch een digitale verstoring plaatsvindt, moet er snel gehandeld worden om de schade te beperken. Bij majeure verstoringen wordt dan een crisisorganisatie ingericht. Dat gebeurt ook in Weststellingwerf. Er is een crisisprotocol, maar aan de crisisorganisatie wordt nog gewerkt. Bovendien vinden er geen periodieke digitale crisisoefeningen plaats.

Aanbevelingen

Beleid en Uitvoering:

1. ***Intensiveer de samenwerking in OWO verband en breid deze uit door niet alleen de uitvoering gezamenlijk op te pakken, maar ook op korte termijn gezamenlijk beleid te formuleren.*** Maak hiermee een einde aan onduidelijkheid in taakverdeling tussen de OWO samenwerking en de gemeente Weststellingwerf en draag zorg voor een duidelijke aansturing.

2. ***Werk aan de implementatie van de BIO2-normen en verhoog het volwassenheidsniveau van de organisatie door de PDCA-cyclus volledig in te richten.***
   De gemeente Weststellingwerf heeft een meerjarenplan opgesteld voor de implementatie van de BIO-normen. Een versnelde uitrol en strikte naleving van de geplande mijlpalen kunnen bijdragen aan structurele verbetering van de informatieveiligheid. Om aan de verplichtingen van de Cyberbeveiligingswet te voldoen moet de gemeente doorgroeien naar volwassenheidsniveau 4 (voorspelbaar en geoptimaliseerd). Dit niveau kan worden bereikt door een systematische monitoring van beveiligingsmaatregelen en het verbeteren van de interne evaluatieprocessen.

PDCA-cyclus:

3. ***Versterk de PDCA cyclus door de uitvoering van verbeterplannen aantoonbaar uit te voeren en in rapportages vast te leggen.***
   De gemeente voert audits uit en stelt verbeterplannen op, maar het is niet duidelijk of verbeterplannen daadwerkelijk worden uitgevoerd. Om door te kunnen groeien naar volwassenheidsniveau vier is het belangrijk dat de PDCA-cyclus volledig wordt doorlopen.

Versterking van authenticatie- en toegangsbeheer:

4. ***Versterk het authenticatie- en toegangsbeheer van de organisatie.*** Zorg voor twee factor authenticatie voor raadsleden om beveiligingsrisico te verminderen en scherp het toegangsbeheer (de controle op de gebruikersrechten van medewerkers) in de ambtelijke organisatie verder aan. Het is van belang deze beveiligingsmaatregel op korte termijn te implementeren.

Weerbaarheid:

5. ***Maak bewustwordingsactiviteiten verplicht voor* medewerkers, bestuurders en raadsleden *en zorg voor een gestructureerde aanpak voor opleiding en training*.**
   Vrijblijvende activiteiten kunnen leiden tot lage deelname en onvoldoende kennis en vaardigheden ten aanzien van digitale veiligheid. Verplichte en periodieke trainingen zorgen voor een structureel hoger kennisniveau en betere naleving van veiligheidsprotocollen.

Crisisorganisatie:

7. ***Organiseer periodieke crisisoefeningen en borg de effectiviteit ervan binnen een PDCA-cyclus.*** Hierbij is het van belang de betrokken rollen en verantwoordelijkheden helder vast te leggen en te evalueren. Zonder een duidelijk crisisprotocol en regelmatige oefeningen is de gemeente niet goed voorbereid op daadwerkelijke crisissituaties. Periodieke oefeningen helpen om de respons te verbeteren en de effectiviteit van het crisismanagement te verhogen

Rol van de Gemeenteraad:

8. ***Informeer de gemeenteraad zodanig dat zij haar controlerende en kaderstellende rol op het gebied van digitale veiligheid kan vervullen.***
   Geef de raad periodiek inzicht in de voortgang van het digitaal veiligheidsbeleid. Hierbij dient minimaal aandacht besteed te worden aan:
   - De mate waarin de gemeente voldoet aan de BIO norm;
   - Ontwikkeling in het volwassenheidsniveau;
   - Risicomanagement en crisisbeheersing.

Bestuurlijke reactie

Rekenkamercommissie Weststellingwerf

t.a.v. Mevrouw J.P.M Vervoort

gemeente Weststellingwerf

Weststellingwerf, 01-07-2025

Betreft: Bestuurlijke reactie onderzoek rekenkamerrapport 2025

Geachte leden van de rekenkamer,

Allereerst willen wij u bedanken voor het rapport informatiebeveiliging Weststellingwerf. Onze eerste reactie na het lezen van het rapport is dat wij ons grotendeels kunnen vinden in de gegeven conclusie en aanbevelingen.

Inhoudelijke reactie

We delen de conclusies en aanbevelingen die zijn gegeven in uw rapport. Wel willen wij graag een toelichting geven op uw stelling dat de functies van de FG en de CISO niet onafhankelijk zijn. Beide functies hebben functioneel een eigen verantwoordelijkheid en kunnen rechtstreeks rapporteren aan de gemeentesecretaris en de Autoriteit Persoonsgegevens en de Informatiebeveiligingsdienst (IBD).

Aanbevelingen

Hieronder kunt u onze inhoudelijke reactie op de aanbevelingen lezen:

1) ***Beleid en Uitvoering**: Intensiveer de samenwerking in OWO verband en breid deze uit door niet alleen de uitvoering gezamenlijk op te pakken, maar ook op korte termijn gezamenlijk beleid te formuleren. Maak hiermee een einde aan onduidelijkheid in taakverdeling tussen de OWO samenwerking en de gemeente Weststellingwerf en draag zorg voor een duidelijke aansturing.*

   Wij onderschrijven de aanbeveling om nauwer te gaan samenwerking in OWO-verband. Daarin zijn al stappen gemaakt. We zoeken elkaar vaker fysiek op en begin 2025 is ons

afwegingskader vastgesteld. In dit afwegingskader is besloten om de beleidsmatige kant van informatiebeveiliging in OWO verband op te pakken.

Onze wens is om de OWO samenwerking verder te intensiveren en dichterbij elkaar te komen, zowel ambtelijk als bestuurlijk. Echter, dit kunnen wij als gemeente Weststellingwerf niet alleen. We zijn voornemens om dit zowel ambtelijk als bestuurlijk samen op te pakken met de gemeenten Ooststellingwerf en de gemeente Opsterland.

2) ***Beleid en Uitvoering****: Werk aan de implementatie van de BIO2-normen en verhoog het volwassenheidsniveau van de organisatie door de PDCA-cyclus volledig in te richten. De gemeente Weststellingwerf heeft een meerjarenplan opgesteld voor de implementatie van de BIO-normen. Een versnelde uitrol en strikte naleving van de geplande mijlpalen kunnen bijdragen aan structurele verbetering van de informatieveiligheid. Om aan de verplichtingen van de Cyberbeveiligingswet te voldoen moet de gemeente doorgroeien naar volwassenheidsniveau 4 (voorspelbaar en geoptimaliseerd). Dit niveau kan worden bereikt door een systematische monitoring van beveiligingsmaatregelen en het verbeteren van de interne evaluatieprocessen.*

Op korte termijn, derde kwartaal 2025 kunnen wij een plan aan de OWO-directie presenteren dat gaat over de implementatie van BIO 2. Dit plan is in goed overleg tussen de drie gemeenten (ambtelijk) en afdeling bedrijfsvoering tot stand gekomen. In dit plan richten wij ons op volwassenheidsniveau 3 voor de aankomende twee jaren. Dit is gebaseerd op basis van de huidige beschikbare middelen en budget. Hiermee kunnen wij doorgroeien naar niveau 3. Na deze twee jaren maken we de balans op en gaan we gezamenlijk kijken in hoeverre we kunnen doorgroeien naar volwassenheidsniveau 4.

3) ***PDCA-cyclus****: Versterk de PDCA cyclus door de uitvoering van verbeterplannen aantoonbaar uit te voeren en in rapportages vast te leggen. De gemeente voert audits uit en stelt verbeterplannen op, maar het is niet duidelijk of verbeterplannen daadwerkelijk worden uitgevoerd. Om door te kunnen groeien naar volwassenheidsniveau vier is het belangrijk dat de PDCA-cyclus volledig wordt doorlopen.*

De PDCA-cyclus is een onderdeel van de implementatie van de BIO 2. Dit wordt in ons plan (zoals hierboven genoemd onder punt 2) meegenomen. Wij kunnen ons dan ook vinden in de genoemde aanbeveling en gaan de PDCA cyclus versterken.

4) ***Versterking van authenticatie- en toegangsbeheer****: Versterk het authenticatie- en toegangsbeheer van de organisatie. Zorg voor twee factor authenticatie voor raadsleden om beveiligingsrisico te verminderen en scherp het toegangsbeheer (de controle op de gebruikersrechten van medewerkers) in de ambtelijke organisatie verder aan. Het is van belang deze beveiligingsmaatregel op korte termijn te implementeren.*

Wij onderschrijven de genoemde aanbeveling. Het invoeren van 2 factor heeft het gebruiksgemak negatief beïnvloed en zorgde voor problemen om de werkzaamheden te kunnen uitvoeren. We beseffen de noodzaak van de twee factor authenticatie voor

raadsleden en dit gaan wij dan aankomend jaar, op korte termijn, opnieuw inzetten om alsnog te realiseren. Daarnaast gaan wij ook in OWO verband bezig met de controle op de gebruikersrechten van onze organisatie.

5) ***Weerbaarheid**: Maak bewustwordingsactiviteiten verplicht voor medewerkers, bestuurders en raadsleden en zorg voor een gestructureerde aanpak voor opleiding en training. Vrijblijvende activiteiten kunnen leiden tot lage deelname en onvoldoende kennis en vaardigheden ten aanzien van digitale veiligheid. Verplichte en periodieke trainingen zorgen voor een structureel hoger kennisniveau en betere naleving van veiligheidsprotocollen.*

   Voor de ambtelijke organisatie nemen wij deze aanbeveling ter harte. Intern willen wij onderzoeken wat nodig is om (een aantal) bewustwordingsactiviteiten/trainingen verplicht te laten worden voor de medewerkers en collegeleden. Wij onderschrijven ook het belang om dit verplicht te stellen voor de raadsleden maar dit is aan de gemeenteraad zelf en niet aan het college.

   Momenteel zijn de bewustwordingsactiviteiten nog niet verplicht, maar zijn we druk bezig om hier meer aandacht aan te schenken bij het onboardingsproces, en moeten collega's die recentelijk in dienst zijn de "nieuwe medewerkerstraining privacy en informatiebeveiliging" volgen. Daarnaast hebben we meerdere keren een interactieve spreker uitgenodigd, waarbij de opkomst, ondanks het niet verplichte karakter, wel hoog was.

6) ***Crisisorganisatie**: Organiseer periodieke crisisoefeningen en borg de effectiviteit ervan binnen een PDCA-cyclus. Hierbij is het van belang de betrokken rollen en verantwoordelijkheden helder vast te leggen en te evalueren. Zonder een duidelijk crisisprotocol en regelmatige oefeningen is de gemeente niet goed voorbereid op daadwerkelijke crisissituaties. Periodieke oefeningen helpen om de respons te verbeteren en de effectiviteit van het crisismanagement te verhogen.*

   We onderschrijven het belang van het organiseren van periodieke crisisoefeningen. Om dergelijke oefeningen periodiek terug te laten komen vereist deze aanpak nadere afstemming binnen OWO verband. Vanuit Weststellingwerf zetten we in op dit in OWO verband op te gaan pakken. Om dit te realiseren dient een bedrijfscontinuiteitsplan te worden geschreven aan de OWO-directie/college's, waarin de rollen, taken en verantwoordelijkheden van iedere gemeente duidelijk worden vastgelegd.

7) ***Rol van de Gemeenteraad**: Informeer de gemeenteraad zodanig dat zij haar controlerende en kaderstellende rol op het gebied van digitale veiligheid kan vervullen. Geef de raad periodiek inzicht in de voortgang van het digitaal veiligheidsbeleid. Hierbij dient minimaal aandacht besteed te worden aan:*

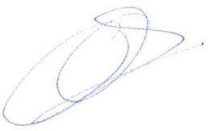
   - *De mate waarin de gemeente voldoet aan de BIO norm;*

- *Ontwikkeling in het volwassenheidsniveau;*
- *Risicomanagement en crisisbeheersing*

Tenslotte kunnen wij ons vinden in deze aanbeveling. Wij zullen als organisatie een actieve rol innemen om de raad mee te nemen op het gebied van digitale veiligheid. Jaarlijks leggen wij door middel van het jaarverslag verantwoording af. Dit jaarverslag wordt met de controlecommissie gedeeld en tijdens de vergadering van een toelichting voorzien. Tijdens de controlecommissies hebben de leden de mogelijkheid om vragen te stellen. Met het plan, dat in het derde kwartaal 2025 wordt gedeeld en ziet op de implementatie van de BIO 2, kunnen we gaan monitoren en rapporteren. Ook kunnen we de voortgang van de BIO 2 aan de raadsleden in de controlecommissie laten zien. Aan de hand van deze rapportages gaan we samen met de controlecommissie in gesprek wat zij nodig hebben om haar controlerende en kaderstellende rol op het gebied van digitale veiligheid goed inhoud te kunnen geven. We willen samen met de controlecommissie kijken hoe we de raadsleden in positie kunnen krijgen op het gebied van informatiebeveiliging.

Met vriendelijke groet,

Burgemeester en wethouders van Weststellingwerf,
de secretaris, de burgemeester,



Nota van bevindingen

1. Inleiding

1.1 Aanleiding

Gemeenten zijn steeds afhankelijker geworden van digitalisering; elk gemeentelijk proces kent wel een digitale component. Daarom neemt ook het belang van informatieveiligheid toe. Dit belang wordt onderkend door de VNG die met en voor haar leden de Agenda Digitale Veiligheid heeft opgesteld. In deze agenda wordt gepleit voor meer bestuurlijke aandacht voor dit thema. Deze aandacht behelst niet alleen die van de burgemeester of het college van b. en w. , maar ook van de gemeenteraad. De VNG adviseert de colleges dan ook om periodiek het gesprek met de raad aan te gaan over digitale veiligheid.[1]

Ook de Rijksoverheid en Europa dringen met Richtlijnen en wetgeving aan op digitaal veilige gemeenten. De Europese 'Network and Information Security-directive' ofwel de NIS2 richtlijn is bedoeld om de cyberbeveiliging en de weerbaarheid van 'essentiële diensten', waaronder lokale overheden, in de EU lidstaten te verbeteren. Op dit moment wordt de richtlijn naar Nederlandse wetgeving vertaald. De bepalingen worden opgenomen in de Cyberbeveiligingswet. Dit houdt in dat digitale veiligheid een plicht wordt voor gemeenten; de vrijblijvendheid gaat er vanaf. De Cyberbeveiligingswet treedt naar verwachting in oktober 2025 in werking.

Het gemeentelijk beleidsdomein van informatieveiligheid is dus, ook in de OWO-gemeenten, volop in beweging. Gelet op de toegenomen cyberdreigingen en de (op handen zijnde) wettelijke verplichting op het gebied van informatieveiligheid is het van belang dat de gemeenteraad zijn kaderstellende en controlerende rol op dit domein goed kan invullen. De Rekenkamer van de OWO-gemeenten (Ooststellingwerf, Weststellingwerf en Opsterland) heeft daarom een onderzoek uitgevoerd naar de informatieveiligheid bij deze gemeenten.

1.2 Doel- en vraagstelling

Het doel van het onderzoek is het in beeld brengen of de informatiebeveiliging adequaat is georganiseerd en geborgd bij de OWO-gemeenten en in hoeverre de gemeenteraden in hun positie zijn om hun taken uit te voeren.

De centrale vraag van dit onderzoek luidt als volgt:
Is de informatiebeveiliging van de OWO-gemeenten adequaat georganiseerd en geborgd?

Deze centrale vraag is opgesplitst in de volgende deelvragen:

1. Wat is het beleid op het gebied van informatieveiligheid; voldoet dit aan actuele standaarden (als de BIO en ENSIA) en zijn de gemeenten voorbereid op de BIO2 en ENSIA?
2. Hoe wordt het Informatieveiligheidsbeleid uitgevoerd op bestuurlijk, organisatorisch, technisch, proces- en medewerkersniveau? Worden hierbij pentesten ingezet, zo ja, welke?
3. Zijn gegevens voldoende beschermd tegen toegang door onbevoegden? In hoeverre wordt getoetst of de organisatie 'in control' is op het gebied van informatiebeveiliging en welke instrumenten worden hierbij gebruikt?
4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident, hoe ziet het incidentmanagementproces eruit en wordt dit in de praktijk geoefend?
5. Hoe wordt omgegaan met risico's en incidenten op het gebied van informatieveiligheid en in hoeverre toont de organisatie lerend vermogen (PDCA cyclus)?

[1] Digitale veiligheid en privacy | VNG

6. Hoe wordt gezorgd voor bewustwording voor informatiebeveiliging bij medewerkers, bestuur, raad en samenwerkingspartners?
7. Zijn de rollen en taken op het gebied van informatiebeveiliging voor medewerkers en het management duidelijk en hoe wordt er gestuurd in de gemeentelijke organisatie?
8. Hoe is de raad betrokken bij het informatieveiligheidsbeleid en is dit voldoende om de kaderstellende en controlerende rol te kunnen vervullen?

1.3 Normenkader

Op basis van bovenstaande vragen is een normenkader uitgewerkt. Onderstaand normenkader, dat normen bevat over het gemeentelijk beleid, de uitvoeringspraktijk en de cultuur is toegepast in dit onderzoek.

Normen ten aanzien van het gemeentelijk beleid

- De gemeente heeft BIO- conform informatiebeveiligingsbeleid.
- De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad.
- In het beleid wordt o.a. ingegaan op:
    - Strategische uitgangspunten
    - Risicomanagement
    - Governance (waaronder rollen en verantwoordelijkheden)
    - De PDCA-cyclus van de gemeente
- In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging.
- In programma's en projecten wordt expliciet aandacht besteed aan informatiebeveiliging.
- Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol.
- De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers.

Normen ten aanzien van de uitvoeringspraktijk

- In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren van burgers en het vragen van toestemming.
- De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).
- De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen.
- Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld.
- De vastgelegde controles en rapportages worden in de praktijk uitgevoerd.
- De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen.
- De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers.
- De raad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.

Normen ten aanzien van de organisatiecultuur

- De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden.
- In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.
- In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging.

1.4 Werkwijze

Voorafgaand aan dit onderzoek heeft de rekenkamer een vooronderzoek gedaan bij de drie gemeenten, waarin gesprekken zijn gevoerd en documentatie is verzameld. Het onderzoek bestond uit verschillende fasen. Het onderzoek is gestart met een startbijeenkomst voor betrokken medewerkers van de drie gemeenten. Vervolgens is een documentstudie uitgevoerd en zijn verdiepende interviews gehouden. Om te onderzoeken hoe in de OWO-gemeenten het beleid in praktijk wordt gebracht, zijn voor elke gemeente bijeenkomsten met een focusgroep en raadsbijeenkomst georganiseerd. Om te toetsen of de onderzoeksbevindingen correct waren, is voor aanvang van het schrijven van het rapport een convergentiesessie uitgevoerd met ambtelijk betrokkenenvan de drie OWO-gemeenten. Op basis van de verkregen informatie is onze analyse uitgevoerd en deze rapportage geschreven.

1.5 Leeswijzer

Het rapport begint met een uitleg over de wettelijke kaders en normen voor het gemeentelijk digitale veiligheidsbeleid. In dit hoofdstuk wordt dieper ingegaan op (veranderingen in) de wet- en regelgeving zoals de NIS2 richtlijn, de Cyberbeveiligingswet, de BIO2 en ENSIA.

Vervolgens behandelen wij in hoofdstuk drie de OWO-samenwerking en het beleid en de uitvoering in Weststellingwerf. Dit hoofdstuk bevat een belangrijk deel van de bevindingen van ons onderzoek. In hoofdstuk vier zetten we de rol van de raad uiteen, door eerst te benoemen welke informatievoorziening zij ontvangen en daarna in te gaan op het perspectief van de raad.

De beantwoording van de onderzoeksvragen en de toetsing aan het normenkader is opgenomen in hoofdstuk 5.

In de bijlagen treft u ten slotte een overzicht van de functionarissen waarmee in het kader van dit onderzoek is gesproken plus een overzicht van de documenten die zijn geraadpleegd. Ook is hier een overzicht opgenomen van de gebruikte afkortingen.

2. Speelveld digitale veiligheid

Dit hoofdstuk is een algemene beschrijving van de context en organisatie van digitale veiligheid in gemeentelijke organisaties en de sturing daarop door college en gemeenteraad.

2.1 Belangrijke elementen digitale veiligheid

Digitale veiligheid gaat over veel meer dan bedrijfsvoering. De gemeentelijke dienstverlening is van digitalisering afhankelijk. Bovendien beschikken gemeenten over steeds meer persoonsgegevens van hun inwoners. Deze inwoners mogen van hun gemeente verwachten dat deze gegevens veilig zijn en dus niet op straat komen te liggen. Als dat toch gebeurt, dan schaadt dit het vertrouwen in de gemeentelijke overheid, en brengt mogelijk zelfs (directe) schade toe aan de getroffen inwoners.

Elke gemeente moet maatregelen nemen om ervoor te zorgen dat persoonsgegevens veilig zijn en de continuïteit van dienstverlening wordt geborgd. 100% Veilig bestaat echter niet; er is altijd een risico dat er iets misgaat, bijvoorbeeld dat een hacker inbreekt in een gemeentelijk informatiesysteem. Deze dreiging komt niet alleen van buiten, ook een slordigheidje van een van de eigen medewerkers kan leiden tot bijvoorbeeld een datalek (zie ook de voorbeelden uit de fictieve gemeente Fonkelveen in de kaders).

Daarnaast is informatiebeveiliging ook in het belang van de gemeente zelf, denk bijvoorbeeld aan informatie over voorbereidingen op strategische aankopen. Dergelijke informatie is niet per se door wetgeving beschermd, echter iedere gemeente realiseert zich dat dergelijke informatie niet moet lekken.

Een hack met gevolgen

Fractievoorzitter Jouke Drenth van oppositiepartij ***Voorwaarts Fonkelveen*** *was net thuis van een crisisberaad met het presidium. Dit was zijn derde raadsperiode, maar zo zout had hij het nog niet eerder gegeten. De burgemeester vertelde dat hackers hadden ingebroken in de gemeentelijke informatiesystemen. Er was vertrouwelijke informatie buitgemaakt; persoonsgegevens van inwoners die bij de gemeente vanwege de jeugdzorg geregistreerd waren. Het ging hierbij niet alleen om namen, adressen en BSN nummers, maar ook om behandeldossiers van jongeren. De hackers eisten 5 Bitcoin losgeld van de gemeente, dan zou de gemeente weer toegang krijgen tot de eigen bestanden. Dat kwam neer op € 450.000,-! Waar moest je als kleine gemeente dat geld vandaan halen? Niet ingaan op deze eis ging misschien nog wel meer kosten. De hackers dreigden om de buitgemaakte informatie op het dark web te plaatsen en, zo gaf de burgemeester aan, Fonkelveen zou de hele IT-omgeving opnieuw moeten opbouwen. Dat kon wel een paar miljoen kosten. Het was een duivels dilemma; zakendoen met criminelen of een financiële strop die de gemeente wel eens de kop kon kosten. Binnen twee dagen moest de burgemeester beslissen. Tot die tijd werd er nog naar een oplossing gezocht. Als de back-up bestanden niet aangetast waren, kon de (financiële) schade nog beperkt worden. Maar wat zouden de inwoners van hun gemeente vinden als hun persoonsgegevens op het web gepubliceerd zouden worden? Drenth had er geen goed gevoel bij. Digitale veiligheid was altijd een hamerstuk geweest op de raadsagenda, maar na deze wake-up call vast niet meer*.

In het algemeen leggen gemeenten hun doelstellingen, processen en rolverdeling vast in een beleidsdocument. Hierbij maken veel gemeenten gebruik van het format van de Informatiebeveiligingsdienst (IBD) van de VNG. Dit format gaat ervan uit dat een beleidsplan voor een periode van meestal vier jaar wordt vastgesteld. Op tactisch niveau wordt het beleid uitgewerkt in jaarplannen. Die plannen worden aan de hand van de Plan-Do-Check-Act (PDCA) cyclus gemonitord met als doel om permanente verbetering door te voeren.

2.2 Wetten & regels

Bij de uitvoering van het informatieveiligheidsbeleid moeten gemeenten voldoen aan verschillende wetten en regels. De belangrijkste zijn de Europese Network- and Information Security 2 directive (NIS2), de Cyberbeveiligingswet (Cbw), de Algemene Verordening Gegevensbescherming (AVG), de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA).

De NIS2 richtlijn van de Europese Unie heeft als doel om de informatiebeveiliging van essentiële diensten, waaronder die van gemeenten, in de EU-lidstaten te verbeteren. In de richtlijn is hiertoe onder meer een zorgplicht en een meldplicht opgenomen, en wordt ook het toezicht op informatiebeveiliging geregeld. De NIS2 richtlijn is niet rechtstreeks van toepassing op gemeenten, maar wordt uitgewerkt in de Cyberbeveiligingswet, waar gemeenten wel aan moeten voldoen. Naar verwachting wordt de wet in het derde kwartaal van 2025 ingevoerd. Vanaf het moment dat de wet ingaat, moet de gemeentelijke digitale veiligheid voldoen aan de eisen die in deze wet staan. De invoering van de Cyberbeveiligingswet leidt tot een taakverzwaring en extra kosten voor gemeenten. De VNG heeft in een reactie op deze wet gevraagd om compensatie van het Rijk voor deze kosten.[2]

De maatregelen die de Cyberbeveiligingswet voorschrijft om de informatiebeveiliging te verbeteren, de zorgplicht, zijn grotendeels opgenomen in de BIO2. In de Cyberbeveiligingswet gaat het naast de beveiliging van kantoorautomatisering (KA) ook over de beveiliging van operationele technologie (OT). Deze OT betreft bijvoorbeeld gemeentelijke bruggen en sluizen die op afstand worden bediend, en camera's in de openbare ruimte. Nieuw met de komst van de Cyberbeveiligingswet is ook dat er naast ad hoc toezicht (achteraf, via rapportage aan de raad en de stelselhouders bij het Rijk) ook proactief toezicht zal worden gehouden op de informatiebeveiliging van gemeenten. De Rijksinspectie Digitale Infrastructuur (RDI) is daarvoor aangewezen als toezichthouder voor de gemeenten en andere overheidsorganisaties.

IT leverancier vliegt uit de bocht

*Eind november krijgt raadslid Elke Schrijver van coalitiepartij **Fonkelveen Vooruit** een telefoontje van een alleenstaande ouder die in haar straat woont. Haar bijstandsuitkering was niet op haar rekening gestort, misschien zou Elke eens navraag kunnen doen of er iets aan de hand was. Schrijver besluit op onderzoek uit te gaan en neemt contact op met de verantwoordelijk wethouder. Het blijkt om een serieus probleem te gaan: geen enkele uitkeringsgerechtigde in Fonkelveen heeft zijn of haar uitkering gekregen en de telefoon van het klantcontactcentrum staat roodgloeiend. Sommige bellers zijn acuut in de problemen gekomen en moeten geld lenen om boodschappen te doen.*

Sinds jaar en dag neemt de gemeente Fonkelveen het ICT-systeem van de firma Rik de Zand IT Solutions af voor de uitkeringsadministratie. Uit onderzoek van de beheerders van Fonkelveen bleek dat er enkele dagen geleden een nieuwe versie van deze cloudapplicatie draait die een fout betaalbestand genereert. Geen enkele uitkeringen is daarom betaald. Fonkelveen lijkt overvallen door de nieuwe versie en heeft deze, omdat het om een cloudapplicatie gaat, zelf niet getest. De leverancier probeert de fout op te lossen, maar weet nog niet wanneer dat gaat lukken. Ondertussen is het advies om de betaaltape van vorige maand te gebruiken. Maar die is niet accuraat. De portefeuillehouder weet nog even niet hoe dit op te lossen. Ondertussen stromen de klachten binnen bij het KCC en vraagt Schrijver zich af wat zij haar buurvrouw kan melden.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze verordening betreft een uitwerking van Europese regelgeving die bedoeld is om de privacy van alle inwoners (beter) te beschermen. De Autoriteit Persoonsgegevens houdt toezicht op de uitvoering van

[2] zie VNG-reactie consultatie Cyberbeveiligingswet (NIS2) | VNG voor meer informatie

de AVG in Nederland. Wanneer gemeenten de bescherming van persoonsgegevens niet op orde hebben, riskeren zij een boete van de Autoriteit Persoonsgegevens. Het maatschappelijk en financieel belang van een adequaat privacybeleid is groot. Gemeenten hebben echter niet alleen een goed privacybeleid nodig, maar ook een goede uitvoering daarvan. Beiden zijn verplicht op grond van de AVG. Omdat de beveiliging van persoonsgegevens veel raakvlak heeft met de beveiliging van informatie in het algemeen, zijn de verplichtingen die voortvloeien uit de AVG ook meegenomen in dit onderzoek.

De BIO is sinds 2019 het verplichte basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (en dus ook gemeenten). De BIO is gebaseerd op de informatiebeveiligingsstandaarden ISO 27001 en ISO 27002 en omvat een minimum aan maatregelen die getroffen moeten worden op het gebied van informatiebeveiliging. Gemeenten baseren hun informatiebeveiligingsbeleid en hun verantwoording aan de gemeenteraad en de toezichthouders vanuit het Rijk in belangrijke mate op deze BIO. De BIO wordt op dit moment doorontwikkeld naar de BIO2 en wordt wettelijk verplicht onder de Cyberbeveiligingswet. In de BIO2 is mede naar aanleiding van de komst van de Cyberbeveiligingswet de verantwoordelijkheid van het hogere management in de gemeentelijke informatiebeveiliging vastgelegd. Ook het toewijzen van benodigde middelen, het verhogen van veiligheidsbewustzijn en het uitvoeren van controles maken onderdeel uit van de BIO2.

ENSIA is ontstaan uit een gezamenlijk initiatief van een aantal departementen en de VNG. Het doel van ENSIA is om tot een effectief en efficiënt ingericht verantwoordingsstelsel voor informatieveiligheid te komen. De ENSIA is een jaarlijkse audit die gebaseerd is op de BIO. Uitgangspunt voor ENSIA is het horizontale verantwoordingsproces waarin het college van b. en w. zich over de informatieveiligheid verantwoordt aan de gemeenteraad. Deze verantwoording vormt de basis voor de verantwoording aan de stelselhouder (bijvoorbeeld het ministerie van BZK of SZW). Er wordt dus jaarlijks één audit uitgevoerd waarvan (een deel van) de resultaten zowel naar de gemeenteraad als de stelselhouder gaan. Net als de BIO, wordt ook de ENSIA op dit moment doorontwikkeld naar een nieuwe versie. Deze moet vooral gebruikersvriendelijker worden, zowel voor de ambtelijke organisatie als het gemeentebestuur.

2.3 Bestuur & organisatie

Informatieveiligheid is van de hele gemeentelijke organisatie. Vaak is in beleidsdocumenten vastgelegd dat het lijnmanagement hier verantwoordelijkheid voor draagt. Managers moeten erop toezien dat richtlijnen bij medewerkers bekend zijn en worden nageleefd. Vanuit wet- en regelgeving is een aantal functies verplicht gesteld. Zo verplicht de AVG gemeenten om een Functionaris Gegevensbescherming (FG) in dienst te hebben en dient de Chief Information Security Officer (CISO) volgens de BIO2 zo gepositioneerd te zijn binnen de organisatie dat hij onafhankelijk van de lijn kan adviseren over informatieveiligheid[3].

Het college is eindverantwoordelijk voor de informatieveiligheid van de organisatie. Het College stelt beleid vast en ziet erop toe dat onbevoegden zich geen toegang kunnen verschaffen tot

[3] CISO (Chief Information Security Officer): Verantwoordelijk voor het ontwikkelen en implementeren van het informatiebeveiligingsbeleid binnen een organisatie. Houdt toezicht op de beveiliging van informatie en zorgt ervoor dat de organisatie voldoet aan relevante wet- en regelgeving. Heeft kennis van informatiebeveiliging, risicoanalyse en beveiligingstechnieken.
FG (Functionaris Gegevensbescherming) of DPO (Data Protection Officer): Houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) binnen een organisatie. Adviseert en rapporteert aan het hoogste managementniveau over privacykwesties. Is verplicht voor overheidsinstanties en organisaties die op grote schaal bijzondere persoonsgegevens verwerken.
PO (Privacy Officer): Ontwikkelt en voert het privacybeleid uit binnen een organisatie. Ondersteunt de FG en fungeert als juridisch adviseur op het gebied van privacy. Is niet verplicht zoals de FG, maar speelt een belangrijke rol in het waarborgen van privacy binnen de organisatie.

gemeentelijke informatiesystemen. Mocht dit toch gebeuren, dan kan het nodig zijn om een crisisorganisatie in te richten.

De gemeenteraad is bevoegd de kaders te stellen en het college te controleren. Allereerst wordt van de gemeenteraad verwacht dat hij voldoende middelen beschikbaar stelt, zodat de gemeente aan wet- en regelgeving kan voldoen. In de praktijk blijkt vaak dat raden het lastig vinden om hun controlerende rol goed in te vullen omdat informatieveiligheid als een technisch onderwerp wordt beschouwd. Maar net als bij andere beleidsterreinen is ook hier het de rol van de gemeenteraad om kaders te stellen en te controleren of de gemeente recht- en doelmatig handelt. Zo is het belangrijk dat de raad controleert of de gemeente voldoet aan de BIO. Maar ook over de andere vlakken van het speelveld kan de raad het college bevragen.

2.4 Weerbaarheid

Weerbaarheid is het volgende belangrijke onderdeel van digitale veiligheid. Elke gemeente neemt maatregelen om onbevoegd gebruik van data en informatiesystemen tegen te gaan. Maar 100% veilig bestaat niet; er is altijd een kans dat het mis gaat. Het gaat hierbij niet alleen om het risico op een hack, maar ook onbedoeld verlies van geclassificeerde informatie, of een IT- leverancier van de gemeente die een fout maakt, waardoor de continuïteit van de gemeentelijke dienstverlening in gevaar komt.

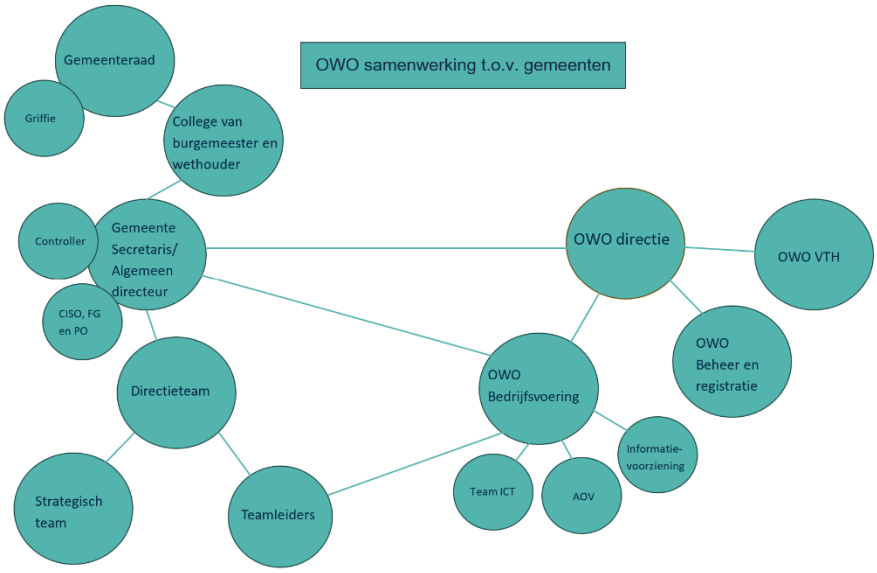
Bij weerbaarheid gaat het in eerste instantie om preventieve maatregelen die worden genomen om digitale verstoringen te voorkomen. Voorbeelden van deze maatregelen zijn het autorisatiebeleid en de toegang van medewerkers tot de verschillende informatiesystemen. Ook bewustwordingsactiviteiten als (online) opleidingen en pentesten zijn belangrijke preventieve maatregelen om verstoringen te voorkomen. Bij opleidingen gaat het niet alleen over de vraag of er voldoende wordt aangeboden, maar ook over de mate waarin opleidingen, al dan niet verplicht worden gevolgd en de wijze waarop hierop wordt gemonitord en gestuurd. Pentesten kunnen zowel betrekking hebben op de technische beveiliging van informatiesystemen als op de medewerkers (human factor pentesten). Voorbeelden van deze laatste categorie zijn ‘phishing mails’ en mystery guests, die proberen om fysiek het gemeentehuis binnen te komen en toegang te krijgen tot informatiesystemen.

Weerbaarheid gaat ook over de respons van de gemeente als een digitale verstoring zich voordoet. Reageert de gemeente adequaat? Wordt er tijdig een crisisorganisatie ingericht en worden hier de juiste beslissingen genomen? Met oefeningen en simulaties van digitale verstoringen kan de gemeente inzicht krijgen in de respons van de organisatie op een digitale verstoring. Zeker als gemeenten samenwerken op het gebied van digitalisering en informatieveiligheid is het van belang om periodiek te oefenen met een digitale verstoring, zodat duidelijk wordt of de juiste afspraken zijn gemaakt ten aanzien van mandaten en bevoegdheden.

3. Beleid en uitvoering

3.1 OWO-samenwerking

De colleges van b. en w. van de gemeente Ooststellingwerf, Weststellingwerf en Opsterland zijn in 2011 een intergemeentelijke samenwerking aangegaan voor verschillende diensten, waaronder bedrijfsvoering, de OWO-samenwerking. Ter aanvulling is er tussen de drie samenwerkende gemeenten de regeling 'gezamenlijke verantwoordelijkheid' opgesteld in 2015 en door de afzonderlijke colleges vastgesteld[4]. De OWO samenwerking beslaat verschillende onderdelen, waaronder een afdeling die verantwoordelijk is voor de bedrijfsvoering van de drie gemeenten (OWO bedrijfsvoering). OWO bedrijfsvoering bestaat uit verschillende teams. Een van de teams die onderdeel zijn van OWO bedrijfsvoering is Team ICT. De schematische weergave van de OWO-samenwerking biedt een globaal overzicht van de onderlinge verbanden tussen individuele OWO gemeenten en de OWO organisatie. Deze weergave is gebaseerd op de PowerPoint-presentatie van de themabijeenkomst ICT voor raadsleden van de OWO-gemeenten en op informatie verkregen uit interviews.



De operationele taken en verantwoordelijkheden met betrekking tot de ICT-informatiebeveiliging liggen bij Team ICT van de afdeling OWO-Bedrijfsvoering. De medewerkers van het team ICT dragen zorg voor de uitvoering van alle beveiligingsmaatregelen die in het Informatiebeveiligingsplan ICT 2020 zijn benoemd. Team ICT is verantwoordelijk voor de centrale ICT-infrastructuur van de drie OWO gemeenten, waaronder data, applicaties en telefonievoorzieningen. Daarnaast is Team ICT verantwoordelijk voor de operationele activiteiten op gebied van informatieveiligheid, dit omvat bijvoorbeeld tooling, logging, firewalls en monitoring. Het leveranciersmanagement voor de drie gemeenten wordt deels door Team ICT uitgevoerd. Leveranciersmanagement is belegd bij team ICT van OWO-bedrijfsvoering en bij de afdeling Inkoop, de toetsing of leveranciers voldoen aan contractuele eisen is niet duidelijk belegd. Daarnaast is Team ICT ook verantwoordelijk voor de uitvoering van de back-ups en restores. Ook is Team ICT betrokken bij een monitoring- en responsproject van de VNG, daar is verder geen aanvullende informatie over opgevraagd.

Alle grotere applicaties staan onder verantwoordelijkheid van Team ICT, kleinere applicaties staan onder verantwoordelijkheid van de individuele OWO-gemeenten zelf. Grote applicaties zijn applicaties die in OWO-verband worden gebruikt, te denken valt aan VTH (Vergunning, Toezicht en Handhaving), I-zaak (archivering), Teams, I-Babs, csam en isam. Tijdens het onderzoek is gebleken dat iedere applicatie een eigenaar behoort te hebben en hieraan wordt gewerkt, maar dit nog niet bij elke applicatie al het geval is.

4 Deze Regeling Gezamenlijke verantwoordelijkheid is onder de herziende bestuursovereenkomst OWO-samenwerking in 2024 vernieuwd. Deze zijn tijdens de onderzoeksperiode niet ontvangen.

Er is geen documentatie ontvangen over de precieze verdeling van verantwoordelijkheden rondom applicaties. Medewerkers vertelden in het kader van het onderzoek dat de CISO's van de individuele gemeenten in samenwerking met Team ICT op dit moment bezig zijn hun applicaties en de bijbehorende taken, rollen en verantwoordelijkheden in kaart te brengen.

De OWO-gemeenten hebben een gezamenlijke aanpak voor de levering en het beheer van ICT-voorzieningen. Apparatuur en applicaties worden door Team ICT centraal verstrekt aan de medewerkers van de gemeente. Medewerkers hebben op laptops geen mogelijkheid om zelf applicaties te downloaden. Dat geeft enige mate van controle over de gebruikte software. Voor mobiele telefoons ontbreekt echter een vergelijkbare mate van beleid; zo blijkt uit de focusgroepen dat er geen richtlijnen zijn voor wachtwoordbeheer en het downloaden van applicaties op mobiele werktelefoons, afgezien van de standaard wachtwoord vereisten, en het downloaden van applicaties op mobiele werktelefoons.

Het proces van in- en uitdiensttreding op gebied van apparatuur start en eindigt bij voor medewerkers bij de eigen teamleider. Zo leveren medewerkers hun apparatuur in bij de teamleider in het geval van een uitdiensttreding. Het verdere proces is belegd bij Team ICT. Dit proces omvat bijvoorbeeld het resetten van apparatuur, tijdig afmelden van medewerkers bij systemen en het toekennen van toegang van nieuwe werknemers tot systemen. Team ICT kent de juiste toegangsrechten tot het systeem toe aan de juiste medewerkers van de individuele OWO gemeenten. De informatie over de juiste toegangsrechten per medewerker ontvangt Team ICT van de drie HR afdelingen van de OWO gemeenten zelf. Het HR-beleid is de verantwoordelijkheid van de drie individuele OWO-gemeenten zelf. Uit interviews blijkt dat het beheer op de juiste toegangsrechten tot systemenvolgens Team ICT nog niet sluitend is geregeld binnen de gemeenten. Hier zit een risico dat onbevoegden toegang kunnen krijgen tot gevoelige informatie en systemen.

De colleges van b. en w. van de drie individuele gemeenten zijn eindverantwoordelijk voor het informatiebeveiligingsbeleid. De drie OWO-gemeenten hebben daarom tot nu toe eigen strategisch informatieveiligheidsbeleid. Dit beleid is gebaseerd op de ISO 27001- en ISO 27002-standaarden. Uit gesprekken met medewerkers is gebleken dat Team ICT van OWO-bedrijfsvoering niet structureel bij het opstellen van het strategisch informatieveiligheidsbeleid van alle gemeenten betrokken is. De CISO van de gemeente Weststellingwerf heeft advies gevraagd aan Team ICT over het strategisch informatieveiligheidsbeleid, de CISO van gemeente Ooststellingwerf heeft het strategisch informatieveiligheidsbeleid ter informatie opgestuurd en de CISO van gemeente Opsterland heeft enkel gesprekken gehad met OWO ICT over het strategisch informatieveiligheidsbeleid. De drie gemeenten zijn momenteel met elkaar in gesprek om gezamenlijk informatiebeveiligingsbeleid op te stellen. Ten tijde van de onderzoeksactiviteiten was dit echter nog niet uitgewerkt.

Naast het strategisch informatieveiligheidsbeleid van de drie OWO gemeenten zelf zijn door Team ICT de veiligheidsstandaarden van het informatieveiligheidsbeleid aangevuld met richtlijnen die voor alle OWO-gemeenten gelden. Een van de documenten waar veiligheidsstandaarden voor de drie OWO- gemeenten zijn beschreven, is het Informatiebeveiligingsplan ICT 2020. Hiermee wordt nadere invulling gegeven aan het strategisch informatiebeveiligingsbeleid van de OWO-gemeenten. Het informatiebeveiligingsplan ICT 2020 benoemt de beveiligingsobjecten op het gebied van de ICT en de getroffen maatregelen ten behoeve van het gevraagde beveiligingsniveau.

Team ICT heeft daarnaast een werkinstructie opgesteld voor het omgaan met ernstige verstoringen die voor alle drie de OWO-gemeenten geldt en de verschillende directies van de gemeenten hebben hier op kunnen reageren. De werkinstructie 'procedure ernstige verstoring ICT' is in 2024 vernieuwd naar aanleiding van de gezamenlijke crisisoefening van de drie OWO gemeenten in april 2024 hebben uitgevoerd. Dit blijkt uit de memo "terugkoppeling OWO colleges bijeenkomst 2 april."

De werkinstructie ernstige verstoring ICT bevat een standaardprocedure die gevolgd moet worden zodat er op toegezien kan worden dat de verstoring met de juiste aandacht en op een gestructureerde wijze wordt behandeld. Een ernstige ICT verstoring wordt in deze werkinstructie beschreven als een incident waarbij meerdere personen niet verder kunnen werken omdat het kritische werkproces niet beschikbaar is of ernstig beïnvloed wordt door het probleem. Het doel van de procedure ernstige verstoringen is het gestructureerd oplossen van het probleem en een juiste prioritering bepalen om de dienstverlening te kunnen herstellen.

In de werkinstructie ‘ernstige verstoring ICT’ staat beschreven wie de crisiscoördinatoren zijn, wat een ernstige verstoring is, hoe prioriteiten aan verstoringen worden toebedeeld en een stappenplan om een ernstige ICT verstoring op te lossen. In het stappenplan staat beschreven wat er gedaan moet worden door de verschillende actoren en in welke volgorde. Het proces start met een melding van een verstoring die wordt beoordeeld door een securitymedewerker van Team ICT. Vervolgens beoordeelt de crisiscoördinator of er sprake is van een ernstig of major incident. Als dit het geval is dan stelt de crisiscoördinator een oplosteam samen en wordt er naar aanleiding van een eerste analyse een oplossingsrichting bepaald. Het oplosteam geeft prioriteit aan de herstelwerkzaamheden. Vervolgens wordt gestart met het herstellen van de dienstverlening en vindt er indien nodig regelmatig contact plaats met de CISO van de desbetreffende gemeente. Als laatste stap wordt onder verantwoordelijkheid van de crisiscoördinator een major incident rapport opgesteld dat naar de CISO’s van de OWO gemeenten wordt gestuurd. De betreffende medewerkers coördineren waar mogelijk de verbetervoorstellen.

Oefenen met crisissituaties is cruciaal om adequaat te kunnen handelen in het geval van een crisis. In april 2024 vond een oefening plaats met de colleges en gemeentesecretarissen van de drie gemeenten. Uit gesprekken met medewerkers bleek dat er binnen de OWO-samenwerking redelijk veel afspraken duidelijk zijn door de procedure ernstige verstoringen, maar dat er ook onderdelen zijn waar aanvullende afspraken over gemaakt moeten worden, zoals een gezamenlijk standpunt op ransomware[5].

De PDCA-cyclus op informatiebeveiliging is voor een groot deel bij de individuele gemeenten zelf belegd. Zo worden jaarlijks audits uitgevoerd volgens de ENSIA systematiek. Hiervoor levert Weststellingwerf voor Ooststellingwerf en Opsterland de gegevens op gebied van ICT aan. Ooststellingwerf levert de gegevens aan voor BAG en BGT rapportage. Op operationeel gebied worden technische verbeterplannen uitgevoerd door Team ICT van OWO bedrijfsvoering. Uit interviews is gebleken dat niet bij alle acties duidelijk is waar de verantwoordelijkheid ligt op het vervolg. Team ICT wordt daarnaast niet structureel betrokken bij de opstart en uitvoering van risicoanalyses door de individuele gemeenten.

Er is geen structureel overleg tussen de CISO’s van de drie gemeenten en Team ICT van OWO bedrijfsvoering. Uit gesprekken met medewerkers blijkt dat Team ICT niet altijd op de hoogte is van informatiebeveiligingsplannen van de gemeenten en dat de effectiviteit van advies en samenwerking daardoor beperkt wordt. Deze medewerkers geven aan dat er wel regelmatig contact is met de CISO van de gemeente Weststellingwerf en enig contact met de CISO van Opsterland. Echter, met de CISO van de gemeente Ooststellingwerf is minder vaak contact. De CISO's hebben onderlinge werkafspraken gemaakt. Eén van de werkafspraken is dat de CISO van West als contactpersoon optreedt bij I&A aangelegenheden (waaronder de ICT gerelateerde vragen vanuit ENSIA) en van daaruit doorschakelt naar de CISO's van Oost en Opsterland. De CISO van Oost is contactpersoon voor wat betreft de OWO-onderdelen BVI en Backoffice Sociaal Domein. Uit gesprekken is ook

[5] Informatiebeveiligingsdienst (IBD) De IBD is het Computer Emergency Response Team, of Computer Security Incident Response Team (CERT/CSIRT) voor alle Nederlandse gemeenten, en onderdeel van de Vereniging van Nederlandse Gemeenten.

gebleken dat enige tijd terug een CITSO (Chief Information Technical Security Officer) is aangenomen door OWO bedrijfsvoering. Deze CITSO dient als tussenpersoon tussen Team ICT van OWO bedrijfsvoering en de drie CISO's van de individuele OWO-gemeenten en adviseert op de technische infrastructuur. Ook blijkt uit de interviews dat de CITSO vanuit team ICT het nieuwe gezamenlijke strategische informatieveiligheidsbeleid coördineert en voor de drie OWO-gemeenten technische vraagstukken afstemt.

3.2 Weststellingwerf

Het strategisch beleid voor informatiebeveiliging en privacy is bij de gemeente Weststellingwerf vastgelegd in het document 'Strategisch informatiebeveiliging en privacy-plan.' Het beleid is recent herijkt en geldt tot 2026. Hiervoor heeft de gemeente het format van de Informatie Beveiligingsdienst (IBD, een onderdeel van de VNG) overgenomen. De basis voor dit beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO) en het VNG Borgingsproduct AVG versie 3.0.

In het strategisch beleid zijn vier concrete ambities geformuleerd.

1. Allereerst heeft de gemeente Weststellingwerf de ambitie om de maatregelen uit de BIO volledig te implementeren.
2. Tevens wil de gemeentelijke organisatie de verdeling van werkzaamheden op orde krijgen.
3. Ook is het de ambitie van de gemeente Weststellingwerf om kennis en vaardigheden van privacy en informatiebeveiliging in de ambtelijke organisatie te verbeteren en borgen.
4. Verder wil de gemeente Weststellingwerf in dat kader inzetten op duidelijker eigenaarschap voor verbeteracties en het opzetten van een beter proces voor het doorlopen van de Plan, Do, Check, Act cyclus (PDCA). In het onderdeel belangrijkste uitgangspunten wordt dit continue verbeterproces van de PDCA cyclus nogmaals benadrukt, alleen zijn de bijbehorende rapportages nog niet benoemd.

Het strategisch beleid wordt nader uitgewerkt in concrete jaarplannen informatiebeveiliging en privacy. In deze jaarplannen wordt richting gegeven aan de uitvoering van digitale veiligheid op tactisch en operationeel niveau. Hieronder gaan we nader in op de uitwerking van de aspecten van het strategische informatieveiligheidsbeleid, waarbij we kijken naar de documenten die onder het strategisch beleid hangen. Hierbij zullen we telkens de verbinding maken tussen die documenten en het strategische beleid dat als basis dient.

3.2.1 BIO

In het Strategisch informatiebeveiliging en privacy-plan is de BIO als normenkader opgenomen. Deze richtlijn bevat het totaalpakket aan informatiebeveiligingsmaatregelen die gelden voor elke gemeente, dus ook voor gemeente Weststellingwerf. Een van de maatregelen die de gemeentelijke organisatie neemt is het uitvoeren van zelfevaluaties.

Uit gesprekken met medewerkers blijkt dat de gemeente Weststellingwerf zich op dit moment aan het voorbereiden is op het BIO2 normenkader dat onder de Cyberbeveiligingswet verplicht wordt. De CISO van de gemeente Weststellingwerf stelt dat de gemeentelijke organisatie van Weststellingwerf op dit moment op niveau 1 of 2 van volwassenheidsniveau zit en dat een organisatie brede opdracht nodig is om naar niveau 4 te groeien. In het jaarverslag van 2023 stelt de gemeente Weststellingwerf dat in 2024 de volgende stap gezet wordt naar de implementatie van de BIO en jaarlijkse controles op basis van risicomanagement worden gestart. Met hulp van de Team ICT van de OWO bedrijfsvoering wordt een (meerjarig) geïntegreerd plan met mijlpalen en concrete planning opgesteld om te komen tot BIO2 implementatie in 2026. In het jaarplan 2024 privacy en informatieveiligheid stelt de gemeente

Weststellingwerf in 2024 te willen starten met het opstellen van een continuïteitsplan en het in kaart brengen van verwerkingen en mogelijk gekoppelde risico's.

3.2.2 Incidenten(afhandeling)

De gemeente Weststellingwerf beschrijft in het Strategisch informatiebeveiliging en privacy-plan dat een van de strategische doelen van de gemeentelijke organisatie van Weststellingwerf het adequaat reageren op incidenten is. De gemeentelijke organisatie heeft een eigen register en procedure voor het vastleggen van incidenten. Er is een eigen systeem waarin incidenten worden vastgelegd: het register "beveiligingsincidenten en datalekken". In dit register wordt bijgehouden hoeveel bijna incidenten, beveiligingsincidenten, ernstige en niet ernstige datalekken er per jaar voorkomen binnen de gemeente. Ook staat er bij de incidenten of deze zijn gemeld aan de Autoriteit Persoonsgegevens (AP). Uit het "register beveiligingsincidenten en datalekken – overzicht" blijkt dat er ten tijde van het onderzoek in 2024 in totaal tien incidenten en datalekken hebben plaatsgevonden, waarvan twee ernstig. Er is geen sprake geweest van beveiligingsincidenten of bijna incidenten.

De taken en rollen die van belang zijn bij een datalek worden beschreven in het Strategisch informatiebeveiliging en privacy-plan. Volgens dit document is de privacy officer (PO) verantwoordelijk voor het coördineren en afhandelen van beveiligingsincidenten en datalekken, inclusief het beheren en registreren hiervan. De Functionaris Gegevensbescherming (FG) ziet toe op het register van datalekken en het melden van datalekken aan de toezichthouder. Verder zijn teamleiders volgens het strategisch informatieveiligheidsbeleid verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten.

Uit het jaarplan 2024 privacy en informatiebeveiliging blijkt dat het verwerkingsregister is verouderd. De CISO en FG van Weststellingwerf hebben de ambitie om risicogericht de verwerkingen in kaart te brengen en het register te vernieuwen. Hierbij wordt onderzocht welke verwerkingen de hoogste impact hebben voor de bescherming van persoonsgegevens. De gemeentelijke organisatie van Weststellingwerf heeft in 2023 drie DPIA's (Data Protection Impact Assessment) laten uitvoeren en heeft de ambitie om in 2024 het protocol voor de uitvoering van DPIA's te vernieuwen, blijkt uit het jaarverslag 2023 en jaarplan privacy en informatiebeveiliging 2024.

3.2.3 PDCA-cyclus

In het Strategisch informatiebeveiliging en privacy-plan staat dat informatieveiligheid een continu proces is. Daarnaast stelt het college van b. en w. van de gemeente Weststellingwerf in dit document dat het wil inzetten op duidelijker eigenaarschap voor verbeteracties en het opzetten van een beter proces voor het doorlopen van de kwaliteitscyclus, de Plan, Do, Check, Act cyclus (PDCA). Ook wordt beschreven dat de cyclus structureel geborgd en verder geautomatiseerd gaat worden.

De gemeentelijke organisatie verantwoordt zich middels de ENSIA rapportage, audits en interim controles. Het College van b. en w. jaarlijks verantwoording af aan de gemeenteraad met een door een externe auditor ondertekende verklaring. De ENSIA rapportages zijn onderdeel van de jaarlijkse cyclus. In het jaarplan 2024 staan de bevindingen van de ENSIA rapportage beschreven. Ook staat beschreven welke maatregelen zijn getroffen voor de zaken waar de gemeentelijke organisatie Weststellingwerf niet aan voldeed. Resultaten van aanvullende audits en interim controles hebben de onderzoekers niet in de jaarplannen terug kunnen vinden. In het jaarplan 2024 worden wel de verbeterplannen genoemd die worden doorgevoerd in 2024. Uit gesprekken met raadsleden van de gemeente Weststellingwerf blijkt dat er een controlecommissie bestaande uit raadsleden ook op de hoogte wordt gehouden van jaarplannen en uitkomsten van evaluaties. Buiten het jaarplan en de ENSIA rapportage heeft het onderzoeksteam geen verbeterplannen gezien of andere documentatie die wijzen op een volledige PDCA-cyclus.

Vanuit de controlerende functie van de CISO van Weststellingwerf wordt er in samenwerking met de FG en Internal Controle (VIC) van Weststellingwerf wordt er getoetst en advies gegeven over geconstateerde feiten, risico's en verbetermaatregelen. Uit het jaarplan van 2024 blijkt dat de focus van de audit van 2024 op het thema In- door en uitstroom (IDU) ligt en in de tweede helft van 2024 op het sociaal domein. In OWO-verband worden door Team ICT daarnaast ook pentesten uitgevoerd, de vervolgacties worden indien nodig door de CISO van de gemeente Weststellingwerf opgepakt. Twee keer per jaar wordt er vanuit de organisatie gerapporteerd over de voortgang en afhandeling van de openstaande aanbevelingen. Deze rapportage gaat achtereenvolgens naar de directie, het college en de controlecommissie. Uit gesprekken is gebleken dat de voortgang op aanbevelingen uit evaluaties en audits wordt gemonitord. De bevindingen en gekoppelde aanbevelingen worden op een verbeterlijst geplaatst. Op de verbeterlijst staat een termijn waarbinnen aanbevelingen opvolging dienen te krijgen. krijgen.

3.3.4 Bestuur & organisatie

In het Strategisch informatiebeveiliging en privacy-plan zijn de rollen en verantwoordelijkheden ten aanzien van informatieveiligheid beschreven. De rol van het college van b. en w., de gemeenteraad, de directie, teammanagers, controllers en Team ICT van OWO bedrijfsvoering worden beschreven in het onderdeel IB&P governance. Bij het onderdeel belangrijkste uitgangspunten worden ook de verantwoordelijkheden van het lijnmanagement uiteengezet.

Het college van b. en w. van gemeente Weststellingwerf is eindverantwoordelijk voor het beleidsveld informatiebeveiliging en stelt in die rol het strategisch informatieveiligheidsbeleid vast. De directie is volgens het strategisch veiligheidsbeleid verantwoordelijk voor het laten uitwerken en uitvoeren van beleidsregels. Daarnaast is de directie verantwoordelijk voor het opvragen van informatie bij teamleiders en het toezien dat de juiste maatregelen genomen worden voor de bescherming van gegevens, informatiesystemen en procesautomatisering.

Volgens het strategisch informatieveiligheidsbeleid ondersteunt de Chief Information Security Officer (CISO) vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover aan de directie. De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van b. en w. over de juiste en zorgvuldige omgang met persoonsgegevens. De Privacy Officer (PO) is als eerste aanspreekpunt voor de gemeente over privacy gerelateerde vraagstukken aangemerkt. Daarnaast monitort en ondersteunt de PO het naleven en uitvoeren van het privacy beleid.

Het lijnmanagement draagt verantwoordelijkheid voor de uitvoering van de informatiebeveiliging en privacybescherming. Daarnaast is de rol van teamleiders beschreven in het strategisch informatieveiligheidsbeleid. Teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn. Daarnaast zijn teamleiders verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit. Ook dienen teamleiders regelmatig controles uit te voeren op het verwerken van persoonsgegevens. In de praktijk is gebleken dat veel taken binnen informatieveiligheid bij teamleiders zijn belegd. Echter, uit de focusgroepen is gebleken dat het eigenaarschap en de bijbehorende taken nog niet overal in de organisatie gevoeld wordt. Uit gesprekken met medewerkers blijkt dat het bestendigen van eigenaarschap een van de verbeterpunten is van de gemeentelijke organisatie Weststellingwerf.

Uit het jaarverslag 2024 privacy en informatieveiligheid blijkt dat er een vaste formatie is voor de onderwerpen privacy en informatieveiligheid, te weten de CISO, de PO en de FG. Ook zijn de drie rollen in de organisatie kenbaar gemaakt. Volgens het normenkader van de BIO2 dient de CISO zo

gepositioneerd te zijn binnen de organisatie dat hij onafhankelijk van de lijn kan adviseren over informatieveiligheid.

De CISO en FG zijn onderdeel van het team Advies en Ondersteuning. Het eerste aanspreekpunt van de CISO en FG is hun teamleider die ook de functie concern controller bekleedt. Rapportages van de CISO en FG gaan via de concern controller naar de directie. Uit gesprekken is gebleken dat er geen structurele overleggen zijn of direct contact is tussen de CISO, FG en de directie. Er zijn wel periodieke overleggen tussen de CISO, FG en portefeuillehouder.

In de AVG zijn er waarborgen opgenomen om de FG onafhankelijk te laten werken. Er mag geen belangenverstrengeling zijn tussen de FG-taken en andere taken of functies van de FG en er mag geen positie zijn waarin de FG het doel en de middelen van gegevensbewerking bepaalt. Geen directe communicatielijn of rapportagelijn naar de directie is in strijd met deze onafhankelijkheid en de aankomende BIO2.[6] Daarnaast mag de FG geen instructies ontvangen over het uit te voeren werk. Hier ligt een aandachtspunt aangezien de FG wordt aangestuurd door het hoofd concerncontrol.

Uit de gesprekken is gebleken dat informatiebeveiliging en privacy nog niet overal in de organisatie duidelijk belegd zijn. In het jaarplan privacy en informatiebeveiliging van 2024 wordt daarom de ambitie uitgesproken om het gesprek met teamleiders en de directie hierover te voeren en deze dialoog periodiek te blijven voeren.

3.3.5 Weerbaarheid

Het Strategisch informatiebeveiliging en privacy-plan van Weststellingwerf beschrijft dat het minimaliseren van risico's van menselijk gedrag een strategisch doel is voor de gemeente. Nieuwe medewerkers tekenen bij indiensttreding en bij de start van een nieuwe functie een Verklaring Omtrent het Gedrag (VOG). Ook moeten medewerkers getraind worden in het gebruik van beveiligingsprocedures en horen medewerkers een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk. Daarnaast staat in het strategisch informatieveiligheidsbeleid dat een bewustwordingsprogramma hiertoe bijdraagt.

In het jaarplan privacy en informatiebeveiliging van 2024 wordt beschreven dat het verhogen van de bewustwording van iedereen in de organisatie een speerpunt is voor de organisatie. Uit de gesprekken met medewerkers blijkt dat de verschillende interventies die gepland waren, ook zijn uitgevoerd. Zo zijn er in 2024 phishintesten in de organisatie verspreid. De phishingtesten zijn zowel naar medewerkers van de ambtelijke organisatie, naar het college van b. en w. en naar de gemeenteraad verstuurd. De gesproken medewerkers geven aan dat een e-learning digitale veiligheid onderdeel uitmaakt van hun onboarding. Daarnaast wordt er minimaal een keer per jaar een bijeenkomst over dit onderwerp georganiseerd. Zo is er in 2024 een gastspreker langsgekomen om meer te vertellen over informatiebeveiliging vanuit het perspectief van hackers. Ook krijgen medewerkers regelmatig via de mail een micro learning, over verschillende aspecten rondom informatieveiligheid. Deze activiteiten zijn echter niet verplicht. Uit gesprekken met medewerkers blijkt dat de aanwezigheid van medewerkers bij bewustwordingsbijeenkomsten wordt gemonitord. Ook wordt de deelname aan micro learnings bijgehouden. Medewerkers hebben tijdens de gesprekken aangegeven dat de opleidings- en bewueswordingsactiviteiten helpen bij de bekendheid van informatieveiligheid.

Uit de interviews en focusgroepen blijkt dat de ambities uit het strategisch beleid deels worden opgevolgd. Alle werknemers worden getraind in het gebruik van beveiligingsprocedures, al is dit met name gericht op nieuwe werknemers. Activiteiten rondom informatieveiligheid zijn echter niet verplicht voor medewerkers.

[6] Zie voor meer informatie De Autoriteit Persoonsgegevens.

Ook is informatieveiligheid nog geen onderwerp van gesprek in werkoverleggen en in het dagelijkse werk van medewerkers. Vanuit dat oogpunt wordt de ambitie om verantwoord om te gaan met gegevens en informatieveiligheid nog niet volledig gehaald.

3.3.6 Crisisorganisatie

Het adequaat reageren op incidenten wordt benoemd als strategisch doel van het informatieveiligheidsbeleid. Hieronder valt het oefenen met (cyber)crisissituaties. Volgens het strategisch informatieveiligheidsbeleid zijn de teammanagers verantwoordelijk voor het oefenen met informatiebeveiligings- en privacyincidenten.

In het jaarplan privacy en informatiebeveiliging van 2024 wordt de ambitie beschreven om in OWO-verband nadrukkelijk en intensiever samen te werken, zo ook over het thema bedrijfscontinuïteit. De drie OWO-gemeenten hebben de ambitie uitgesproken om een strategisch crisisplan te ontwikkelen ter voorbereiding op een eventuele verstoring op ICT infrastructuur en -dienstverlening. Dit crisisplan is echter nog niet opgesteld. In het jaarplan privacy en informatiebeveiliging van 2024 beschrijft het college van b. en w. van de gemeente Weststellingwerf dat de procedure ernstige verstoring aanwezig is, maar gedateerd. Daarom heeft het college van b. en w. van de gemeente Weststellingwerf ook de ambitie om een vernieuwde interne noodprocedure op te stellen. De procedure ernstige verstoring heeft het onderzoeksteam ontvangen, maar de vernieuwde noodprocedure niet.

Omgaan met een cybercrisis is in 2023 opgenomen in het integraal veiligheidsplan van de afdeling openbare orde en veiligheid. Naast plannen ontwikkelen is het oefenen met crisissituaties cruciaal om adequaat te kunnen handelen in het geval van een incident. Uit gesprekken met functionarissen van de gemeente Weststellingwerf is gebleken dat er in 2024 wel geoefend is met een cybercrisis binnen de gemeentelijke organisatie. Daarnaast is in april 2024 een gezamenlijke cybercrisis oefening in OWO-verband uitgevoerd. Er is geen documentatie gedeeld waarin het verloop van de crisisoefening en de behaalde resultaten worden beschreven. In het memo “Terugkoppeling OWO-colleges bijeenkomst 2 april 2024 – cyberaanval oefening” worden wel enkele genomen maatregelen beschreven. Tijdens de interviews kwam naar voren dat de verschillende rollen en taakverdeling van een cybercrisisteam op dit moment nog niet duidelijk zijn.

4. Rol van de Raad

De gemeenteraad speelt een belangrijke rol bij de digitale veiligheid van de gemeente. De raad controleert immers het college of de veiligheid voldoet aan de daaraan gestelde eisen. Ook stelt de raad de beleids- en financiële kaders vast. Deze belangrijke rol van de raad is expliciet meegenomen in dit onderzoek. In elk van de OWO-gemeenten is gesproken met een vertegenwoordiging van de gemeenteraad. Na een korte introductie over de status van het onderzoek is met de aanwezige raadsleden een casus over digitale veiligheid besproken. Deze casus speelde zich af in een fictieve gemeente die in karakteristiek vergelijkbaar is met de eigen gemeente. Na de behandeling van deze casus is het gesprek gevoerd over de wijze waarop de raad thans de controlerende en kaderstellende rol ten aanzien van digitale veiligheid vervult. Vervolgens is gesproken over mogelijke verbeteringen van deze rol.

4.1 Informatievoorziening

Er zijn verschillende manieren waarop de gemeenteraad geïnformeerd kan worden over informatieveiligheid. Allereerst zijn er raadsstukken die de situatie rondom informatieveiligheid uiteenzetten. Dit zijn bijvoorbeeld jaarrapportages en ENSIA-rapportages. Raadsleden kunnen daarnaast zelf ook vragen stellen over de actualiteiten rondom informatieveiligheid.

De CISO van Weststellingwerf stelt gezamenlijk met de FG een jaarlijkse rapportage op, deze wordt door het college van b. en w. aan de gemeenteraad aangeboden. Deze jaarrapportage biedt een overzicht van de stand van zaken rondom informatieveiligheid. Daarnaast krijgen de raadsleden informatie over de ENSIA-audit. In de controle commissie van de gemeente worden rapporten zoals ENSIA-audits besproken en incidentrapporten besproken. De leden van de controlecommissie koppelen deze informatie terug aan de (fracties van de) gemeenteraad.

Ook wordt de gemeenteraad van Weststellingwerf geïnformeerd over nieuwe informatiebeveiliging ontwikkelingen binnen de OWO-samenwerking. De raadsleden geven aan dat zij op gebied van ICT specifiek over de OWO-samenwerking worden geïnformeerd door middel van beleidsrapporten.

Er zijn door de raadsleden van de gemeente Weststellingwerf geen schriftelijke vragen gesteld over informatieveiligheid. Er is wel een enkele mondelinge vraag gesteld over het beleid omtrent de app TikTok door de raad. Hoewel zij het onderwerp informatieveiligheid wel belangrijk vinden, zijn zij van mening dat dit een bedrijfsvoeringsvraagstuk is. Medewerkers van de gemeente stellen dat de controlecommissie en de raad tot nog toe niet inhoudelijk reageert op de aangedragen stukken.

4.2 Perspectief raadsleden in Weststellingwerf

Uit de raadsbijeenkomst in Weststellingwerf kwam naar voren dat de gemeenteraadsleden een wisselend kennisniveau hebben ten aanzien van digitalisering en digitale veiligheid. Raadsleden geven aan dat zij geïnformeerd worden over digitale verstoringen of incidenten die hebben plaatsgevonden. Eventuele verbeterpunten die hieruit voorkomen worden echter niet gevolgd door de raad, waardoor er bij de raad geen inzicht is over structurele verbetering van de digitale veiligheid van de gemeentelijke organisatie.

Raadsleden hebben ook geen eenduidig beeld over de wijze waarop zij invulling kunnen geven aan hun controlerende en kaderstellende rol ten aanzien van digitale veiligheid. Zij zijn van mening dat dit onderwerp meer aandacht van de raad verdient, maar vragen zich af wanneer het genoeg is. Zo vinden zij het lastig om te vragen hoe het zit met het kennisniveau van ambtenaren op dit punt. Ook geven zij aan dat het sturen op technische aspecten van digitale veiligheid voor de raad geen reële optie is.

Dit vereist namelijk een kennisniveau waar niet alle raadsleden over beschikken.

De jaarlijkse ENSIA verklaring wordt besproken in de controlecommissie. De leden van de auditcommissie informeren vervolgens hun fracties. Raadsleden zijn hier tevreden over; zij waarderen de informatie die wordt gedeeld.

Raadsleden geven ook aan dat zij (nog) onvoldoende prioriteit aan digitale veiligheid toekennen. Zo was er enige tijd geleden een informatiebijeenkomst voor de drie gemeenteraden van de OWO-gemeenten, maar daarvoor was de opkomst zeer gering.

Beantwoording onderzoeksvragen

5.1 Beantwoording onderzoeksvragen

1. **Wat is het beleid op het gebied van informatieveiligheid; voldoet dit aan actuele standaarden (als de BIO en ENSIA) en zijn de gemeenten voorbereid op de BIO2 en ENSIA?**

De drie OWO-gemeenten stellen op dit moment hun eigen strategisch informatiebeveiligingsbeleid op. Team ICT werkt samen met de individuele OWO-gemeenten aan een gezamenlijk nieuw strategisch informatiebeveiligingsbeleid dat voor alle drie de gemeenten geldt. Individuele gemeenten bereiden zich voor op de BIO2, team ICT is hier via de Chief Information Technical Security Officer (CITSO) bij betrokken. Voor de drie individuele gemeenten geldt wel dat ze verschillen in volwassenheid en de mate waarin ze aan de BIO en ENSIA standaarden voldoen. De mate waarin de gemeente Weststellingwerf voldoet aan de normen van het BIO normenkader en scoort op de zelfevaluatie van de ENSIA is gelijk aan de gemeente Ooststellingwerf. De gemeente Opsterland voldoet in mindere mate aan de normen die in het BIO normenkader en de ENSIA zelfevaluatie.

Het college van B&W van de gemeente Weststellingwerf heeft aangegeven in OWO-verband het beleid gezamenlijk te actualiseren. De gemeente Weststellingwerf heeft in samenwerking met Team ICT van de OWO-samenwerking een plan opgesteld om in 2026 te komen tot BIO2 implementatie. De CISO van de gemeente Weststellingwerf stelt dat de gemeente Weststellingwerf op dit moment op niveau 1 of 2 van volwassenheidsniveau zit voor wat betreft de BIO en dat een organisatie brede opdracht nodig is om naar niveau 4 te groeien.

2. **Hoe wordt het Informatieveiligheidsbeleid uitgevoerd op bestuurlijk, organisatorisch, technisch, proces- en medewerkersniveau? Worden hierbij pentesten ingezet, zo ja, welke?**

Team ICT is verantwoordelijk voor de operationele activiteiten op gebied van informatieveiligheid. Op bestuurlijk niveau wordt Team ICT betrokken bij het nieuwe strategisch informatieveiligheidsbeleid dat door de drie gemeenten opgesteld wordt. Er is echter geen structureel bestuurlijk overleg tussen OWO en de portefeuillehouders van de individuele gemeenten. Daarnaast worden er periodiek pentesten en ENSIA audits uitgevoerd door Team ICT. De verantwoordelijkheid voor het vervolg op bevindingen van pentesten, interne audits en evaluaties zijn bij de desbetreffende OWO-gemeenten belegd. De opvolging daarvan is verschillend in uitvoering. Team ICT voert de technische en praktische bevindingen uit.

Het informatieveiligheidsbeleid van de gemeente Weststellingwerf wordt door middel van evaluaties en interne audits getoetst. De opvolging verbeteracties die voortkomen uit de evaluaties en audits worden door middel van een verbeterlijst in de gemeente gemonitord. Daarnaast worden er in OWO-verband technische pentesten uitgevoerd. De gemeente Weststellingwerf voert ook human focused pentesten uit, in de vorm van phishing testen.

3. **Zijn gegevens voldoende beschermd tegen toegang door onbevoegden? In hoeverre wordt getoetst of de organisatie ‘in control’ is op het gebied van informatiebeveiliging en welke instrumenten worden hierbij gebruikt?**

Team ICT voert het leveranciersmanagement uit voor de drie OWO-gemeenten. Alle grotere applicaties staan onder verantwoordelijkheid van team ICT van OWO, kleinere applicaties staan onder verantwoordelijkheid van de gemeenten zelf. De drie OWO-gemeenten werken gezamenlijk aan een overzicht van alle kernapplicaties en de bijbehorende regie verantwoordelijkheden. Het beheer op de juiste toegangsrechten voor applicaties is volgens team ICT van OWO nog niet sluitend geregeld binnen de gemeenten, waardoor onbevoegden mogelijk toegang kunnen krijgen tot gevoelige informatie en systemen. Team ICT van OWO maakt gebruik van tooling, logging, firewalls

en monitoring. Daarnaast is team ICT ook verantwoordelijk voor de uitvoering van de back-ups en restores van de OWO gemeenten.

Er is in de gemeente Weststellingwerf momenteel onvoldoende controle op de gebruikersrechten van medewerkers voor de juiste applicaties door in-, door- en uitstroom van medewerkers. De gemeentelijke organisatie van Weststellingwerf heeft in het jaarplan privacy en informatieveiligheid van 2024 beschreven dit te willen verbeteren. Ook het authenticatieproces voor raadsleden is ten tijde van het onderzoek nog niet sluitend geregeld. Daarnaast werkt de ambtelijke organisatie aan een vernieuwde versie van het verwerkingsregister waarna per werkproces de verwerkingen in kaart zullen worden gebracht.

4. Is de continuïteit van de gemeentelijke dienstverlening gewaarborgd in geval van grootschalige uitval of verstoring van ICT en hoe is dat geregeld? Weet de organisatie hoe te handelen bij een (ernstig) informatiebeveiligingsincident, hoe ziet het incidentmanagementproces eruit en wordt dit in de praktijk geoefend?

In OWO-verband is een procedure ernstige verstoringen waarin de volgorde en prioriteit van handelen tijdens een ernstige verstoring beschreven staat. Er wordt echter niet structureel geoefend met een uitgebreide verstoring zoals een cybercrisis. Ook zijn de taken en verantwoordelijkheden tijdens een cybercrisis tussen de individuele gemeenten en Team ICT momenteel niet geheel duidelijk.

Er is in de gemeente Weststellingwerf een procedure aanwezig voor incidenten en datalekken. De ambtelijke organisatie maakt jaarrapporten met een overzicht van alle incidenten. De gemeente Weststellingwerf heeft de ambitie beschreven om gezamenlijk met de andere OWO-gemeenten aan een nieuw plan voor ernstige verstoringen te schrijven. Er wordt momenteel niet structureel geoefend met grootschalige incidenten. Er is één keer gezamenlijk een crisisoefening uitgevoerd. De uitkomsten en opvolging van deze oefening zijn onduidelijk.

5. Hoe wordt omgegaan met risico's en incidenten op het gebied van informatieveiligheid en in hoeverre toont de organisatie lerend vermogen (PDCA cyclus)?

Er is geen gezamenlijke verbetercyclus voor de drie OWO-gemeenten. De risicoanalyses en incidentenprocedures worden bij de verschillende gemeenten verschillend uitgevoerd. Wel wordt binnen team ICT gewerkt aan monitoring en verbetering van zwakke punten in de informatiebeveiliging. Het verlenen en beheren van de juiste toegangsrechten voor gebruikers wordt door team ICT genoemd als een van die verbeterpunten. Een incident wordt vastgesteld bij de servicedesk van OWO door een gebruikersmelding van een medewerker van een van de OWO gemeenten of vanuit een van de monitoringstools. Team ICT monitort vervolgens of een incident een ernstige verstoring is en start de bijbehorende oplossingsmaatregel.

Weststellingwerf heeft de PDCA-cyclus nog niet volledig ingebed. In de jaarrapportage worden de ambities voor het aankomende jaar uiteengezet, maar er missen verbeterplannen. Bevindingen uit de ENSIA rapportage en zelfevaluaties worden op een verbeterlijst geplaatst, maar onduidelijk is met welke prioriteit en op welke termijn deze verbeteringen worden opgepakt. De bevindingen worden wel in de controlecommissie van de gemeenteraad besproken.

6. Hoe wordt gezorgd voor bewustwording voor informatiebeveiliging bij medewerkers, bestuur, raad en samenwerkingspartners?

Team ICT van OWO heeft geen rol in de bewustwording over informatiebeveiliging onder medewerkers van de individuele OWO-gemeenten. Er is geen gezamenlijke aanpak. De individuele gemeenten hebben hun eigen bewustwordingsprogramma. De intensiteit van dat programma verschilt per gemeente.

Er is een verplichte onboarding met een vast onderdeel over informatieveiligheid voor nieuwe medewerkers van de gemeente Weststellingwerf. De gemeentelijke organisatie organiseert eens per jaar een bijeenkomst rondom het thema, hier worden ook gemeenteraadsleden voor uitgenodigd. Daarnaast krijgen medewerkers regelmatig een microlearning. De bewustwordingsactiviteiten voor zittende medewerkers zijn echter niet verplicht waardoor medewerkers hier zich gemakkelijk aan kunnen onttrekken. Daarmee kan niet met zekerheid gezegd worden of medewerkers binnen de ambtelijke organisatie zich bewust zijn van het belang van informatieveiligheid. De leden van het college van b. en w. ontvangen ook de phishingtesten en worden uitgenodigd voor bewustwordingsactiviteiten. Binnen het college van b. en w. van de gemeente Weststellingwerf is informatieveiligheid onderwerp van gesprek. Het is onduidelijk of er verwerkersovereenkomsten worden gesloten met samenwerkingspartners en of door samenwerkingspartners bewust met informatieveiligheid wordt omgegaan.

7. **Zijn de rollen en taken op het gebied van informatiebeveiliging voor medewerkers en het management duidelijk en hoe wordt er gestuurd in de gemeentelijke organisatie?**

Er is geen structureel bestuurlijk overleg tussen Team ICT van OWO en de CISO's van de individuele gemeenten. Er is hierdoor nog weinig afstemming over het informatieveiligheidsbeleid en uitvoering tussen de gemeenten en Team ICT van OWO. De taken en verantwoordelijkheden binnen Team ICT liggen vooral op de technische en praktische uitvoering van ICT zoals het leveranciersmanagement en het beheer van de grotere applicaties. De drie OWO-gemeenten werken op dit moment gezamenlijk met Team ICT aan een overzicht autorisaties, rollen en taken van de kernapplicaties. Een CITSO dient als tussenpersoon tussen Team ICT van OWO bedrijfsvoering en de drie CISO's van de individuele OWO gemeenten en adviseert op de techniek.

De rollen en verantwoordelijkheden zijn in het beleid van Weststellingwerf duidelijk uiteengezet. In de praktijk hebben teammanagers in de gemeente Weststellingwerf veel taken en lijken de verantwoordelijkheden voor de informatiebeveiliging wat onder te sneeuwen door reguliere taken van hun functie. De FG en CISO vallen functioneel binnen het team concern control. De CISO en FG rapporteren aan de concerncontroller en zijn daarmee niet volledig onafhankelijk. De concerncontroller vervult door deze organisatorische invulling de facto beide rollen naar de directie vervuld. De CISO en FG werken eraan hun positie richting bestuur en de medewerkers van de ambtelijke organisatie duidelijker te beleggen.

8. **Hoe is de raad betrokken bij het informatieveiligheidsbeleid en is dit voldoende om de kaderstellende en controlerende rol te kunnen vervullen?**

Raadsleden ontvangen jaarlijks rapportages over informatieveiligheid. Er is echter een wisselend kennisniveau en er wordt volgens de raadsleden ook door hen zelf onvoldoende prioriteit toegekend aan het onderwerp. Een aantal raadsleden heeft zitting in de controlecommissie waarin zij ook op de hoogte worden gehouden van jaarplannen en uitkomsten van evaluaties op gebied van informatieveiligheid. Raadsleden stellen zelf dat zij meer werk kunnen maken van hun controlerende en kaderstellende rol, maar vragen zich daarbij ook af of zij wel voldoende kennis bezitten om dit ook goed te kunnen uitvoeren.

5.2 Toetsing aan het normenkader

5.2.1 Normen ten aanzien van het beleid

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
De gemeente heeft BIO- conform informatiebeveiligingsbeleid.				nvt
De algemene uitgangspunten en kaders zijn besproken in en vastgelegd door de gemeenteraad.				
In het beleid wordt o.a. ingegaan op: • Strategische uitgangspunten • Risicomanagement • Governance (waaronder rollen en verantwoordelijkheden) • De PDCA-cyclus van de gemeente				nvt
In (voortgangs)rapportages wordt ingegaan op informatiebeveiliging.				nvt
In programma's en projecten wordt expliciet aandacht besteed aan informatiebeveiliging.				nvt
Er is een procedure hoe wordt omgegaan met informatiebeveiligingsincidenten (waaronder cyberaanvallen) en een crisisprotocol.				
De gemeente heeft beleid voor informatiebeveiliging ten aanzien van samenwerkingspartners, gemeenschappelijke regelingen en leveranciers.				

5.2.2 Normen ten aanzien van digitale veiligheid in de praktijk

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
In de praktijk wordt gehandeld conform de wijze waarop informatie wordt beveiligd, waaronder in de relevante werkprocessen, de toewijzing van verantwoordelijkheden, de inrichting van informatiesystemen, de autorisaties, de afspraken voor de verwerking van gegevens en de afspraken over het informeren				

van burgers en het vragen van toestemming.				
De gemeente heeft een leer- en verbetercyclus (PDCA-cyclus).				nvt
De gemeente heeft inzicht in de belangrijkste verbeterplannen en –maatregelen.				
Er wordt in het geval van incidenten, calamiteiten en crisis volgens de vastgelegde procedures gehandeld.				
De vastgelegde controles en rapportages worden in de praktijk uitgevoerd.				
De gemeente test en toetst procedures regelmatig om de effectiviteit en werking te toetsen.				
De gemeente houdt toezicht op de afspraken ten aanzien van informatiebeveiliging met (samenwerkings)partners, regelingen en leveranciers.				
De gemeenteraad wordt geïnformeerd op een manier die hem in staat stelt te sturen en te controleren.				nvt

5.2.3 Normen ten aanzien van de organisatiecultuur

Norm	Ooststellingwerf	Weststellingwerf	Opsterland	OWO
De medewerkers van de gemeente zijn bekend met het gemeentelijk beleid met betrekking tot informatiebeveiliging en worden van aanpassingen op de hoogte gehouden.				
In hun dagelijks functioneren geven de medewerkers er blijk van het gemeentelijk informatiebeveiligingsbeleid na te leven.				
In de relatie met ketenpartners bewaken de medewerkers actief dat deze ketenpartners zich conformeren aan de regels, standaarden en procedures van de gemeente op het gebied van informatiebeveiliging.				

Bijlage 1- Geïnterviewde personen

Afdelingshoofd OWO bedrijfsvoering
Burgemeester Weststellingwerf
CISO Weststellingwerf
Concerncontroller Weststellingwerf
FG Weststellingwerf
Inkoopstrateeg OWO bedrijfsvoering
Teamleider ICT OWO bedrijfsvoering

Bijlage 2 - Documentatie

Documentnaam	Versie	Datum
Jaarverslag 2023 en jaarplanning 2024		2023
Jaarplan 2024 Informatiebeveiliging		
Strategisch informatiebeveiliging & privacyplan 2023		
Presentatie MT IBP		09-11-2023
Register beveiligingsincidenten en datalekken		
Register beveiligingsincidenten en datalekken - overzicht		
Register verwerkingen Weststellingwerf AVG		
Samenvatting AVG-procedures 2024		

Bijlage 3 - Lijst met afkortingen

Afkorting	Betekenis
AVG	Algemene Verordening Gegevensbescherming
Wpg	Wet politiegegevens
DPIA	Data Protection Impact Assessment
ENSIA	Eenduidige Normatiek Single Information Audit
IBP	Informatiebeveiliging en Privacy
FG	Functionaris Gegevensbescherming
CISO	Chief Information Security Officer
CITSO	Chief Information Technical Security Officer
PO	Privacy Officer
OWO	Ooststellingwerf, Weststellingwerf en Opsterland (samenwerkingsverband gemeenten)
PDCA	Plan-Do-Check-Act (kwaliteitscyclus)
BIO	Baseline Informatiebeveiliging Overheid
VNG	Vereniging van Nederlandse Gemeenten
KCC	Klant Contact Centrum
AP	Autoriteit Persoonsgegevens
b. en w.	Burgemeester en Wethouders
ICT	Informatie- en Communicatietechnologie
VTH	Vergunning Toezicht en Handhaving
I&A	Informatie en Automatisering
IBD	Informatie beveiligingsdienst