Jaarrapportage informatieveiligheid 2025 Gemeente Waterland

Gemeente Waterland

Inhoud

Overige bijlagen:

(separaat vastgesteld door het college en daarna als bijlage bij de Jaarrekening op te nemen)
Verantwoordingsrapportage BAG, BGT en BRO 2025.

1. Inleiding

De gemeente streeft naar continue en betrouwbare dienstverlening, het zorgvuldig omgaan met informatie en het beheersen van risico's. Met de ambitie te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) met de focus op BIO 2.0. (vanaf september 2025 is de BIO versie 2 van kracht). Over het jaar 2025 verantwoord de gemeente zich nog over de versie 1.4 van de BIO vanaf 2026 vindt de verantwoording plaats op basis van versie 2. Dit omdat de verantwoording over een versie altijd over een volledig kalander jaar gebeurt. Naast de BIO committeert de gemeente zich om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en het nakomen van het eigen informatiebeveiligings- en privacy beleid.

Deze rapportage geeft op hoofdlijnen de uitkomsten weer van de gemeentebreed uitgevoerde zelfevaluatie
informatieveiligheid over het jaar 2025. Deze zelfevaluatie is gebaseerd op de BIO. De gemeente Waterland rapporteert op één moment in het jaar over de status van onze informatieveiligheid. De methodiek daarvoor is de 'Eenduidige Normatiek Single Information Audit' (ENSIA). Via ENSIA wordt verticaal verantwoording afgelegd aan de toezichthouders van de rijksoverheid en horizontaal aan de gemeenteraad. Voor de verantwoording aan de gemeenteraad sluit ENSIA middels deze jaarrapportage aan op de gemeentelijke Planning & Control (P&C)-cyclus als onderdeel (bijlage) van de Jaarrekening.
Verantwoording wordt afgelegd over de Basisregistratie Personen (BRP), de wetgeving voor Reisdocumenten (Paspoortuitvoeringsregeling Nederland/PUN), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Basisregistratie Ondergrond (BRO), Digitale persoonsidentificatie (DigiD) en de Gezamenlijke elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet). Daarnaast wordt de status van informatieveiligheid in brede zin conform de BIO verantwoord inclusief enkele maatregelen en verplichtingen op grond van de AVG.

In verband met het openbare karakter van deze jaarrapportage is geen detailinformatie opgenomen.

IT audit over DigiD en Suwinet

Voor 2025 geldt dat de verantwoording over DigiD en Suwinet aan de stelselhouders BZK/Logius en het ministerie SZW wordt verantwoord door middel van een Collegeverklaring. Deze Collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluatie en onderbouwende bewijsstukken. De Collegeverklaring is getoetst door een onafhankelijke IT auditor. Deze neemt de bevindingen op in een assurance rapport. Met de vastgestelde Collegeverklaring en het assurance rapport voldoen wij aan de verantwoordingsplicht voor DigiD en Suwinet.
Voor DigiD is aan één norm (identificatie en authenticatie) niet voldaan. Dit betreft het niet juist volgen van het uitdienst proces. Dit is geïdentificeerd als een hoog risico. Er moet een verbeterplan worden opgesteld
en dit moet ook worden gedeeld met de beheerder van DigiD (Logius) en binnen 6 maanden dient de gemeente te bewijzen te werken volgens het verbeterplan. Voor Suwinet heeft de gemeente zelf aan alle normen voldaan. De uitkomsten uit de zelfevaluatie zijn op hoofdlijnen in deze rapportage opgenomen (hoofdstuk 3). De tekst van de Collegeverklaring treft u aan in bijlage 1.

BRP en Reisdocumenten

De BRP scoorde op alle onderdelen op of boven de norm. De aanbevelingen zijn als actiepunt voor 2026 opgenomen. Voor de punten met betrekking tot informatiebeveiliging is er een informatiebeveiligingsjaarplan 2026 opgesteld, dit jaarplan is breder dan alleen de

bevindingen uit de ENSIA. Hierstaan alle technische en organisatorische plannen voor de gemeente in 2026 zo ook de bevindingen uit deze audit.

Bestuurlijke verantwoording over de BAG, BGT en BRO

Voor de BAG, BGT en BRO zijn over 2025 separate zelfevaluaties in ENSIA uitgevoerd.
De BRO scoort ruim boven de streefnorm. Gelet op de aard en omvang van de organisatie zijn er geen ontwikkelingen en onderzoeken uitgevoerd die moesten worden aangeleverd of terugmeldingen ontvangen.
De BAG en BGT scoren ruim onder de norm, maar wel een flinke progressie t.o.v. voorgaande jaren. Dit betreft met name de kwaliteit van de gegevens. Dit wordt veroorzaakt door het niet structureel opvolgen van processtappen en slechte onderlinge samenwerking tussen de betrokken clusters (BAG) en onvoldoende capaciteit en middelen en de inhaalslag die nodig is voor het wegwerken van achterstanden (BGT). Voor deze registraties is een verbeterplan opgesteld. Dit verbeterplan wordt sinds 2025 opgepakt en dat laten de resultaten ook zien. Het verbeterplan is een meerjarig plan dus ook in 2026 en daarna wordt hieraan gewerkt. De rapportage BAG, BGT en BRO zijn als bijlage bij deze jaarrapportage opgenomen. De scores zijn opgenomen in de samenvatting resultaten zelfevaluatie 2025 (hoofdstuk 2).

Baseline Informatiebeveiliging Overheid (BIO)

Naast opzet en verantwoording is de BIO opgedeeld in de categorieën beleid en organisatie, personeel en toegang, continuïteit en incidenten, informatiesystemen en databescherming met elk meerdere vereiste beheersingsmaatregelen, in totaal 206 maatregelen variërend van 31 tot 59 per categorie. Binnen elke categorie wordt aan enkele maatregelen niet voldaan, in totaal 48 van de 206. Dit is er één minder dan vorig jaar.
De openstaande technische maatregelen, waar nu nog geen oplossing voor is, worden in het jaarplan 2026 meegenomen. Voor de technische maatregelen zijn dit vooral restanten uit het project de Digitale Moderne Werkplek die nog niet zijn opgeleverd 2025 en die in 2026 wel worden opgeleverd. Wanneer het project de Digitale Moderne Werkplek is afgerond heeft de gemeente een groot deel van de technische middelen in huis om te voldoen aan de BIO2.

De overige maatregelen worden als activiteit opgenomen in het jaarlijkse, niet openbare, informatiebeveiligingsplan. Dit betreft onder meer het verder opstellen van voor bepaalde systemen ontbrekende autorisatiematrixen (beleid en organisatie) en de periodieke controle hiervan (personeel en toegang), kennisdeling van incidenten dat wel is ingericht, maar niet expliciet wordt gepubliceerd (continuïteit en incidenten). Een aantal van deze procedures zijn in 2024/2025 opgesteld maar nog niet in gebruik genomen, om deze reden is aangegeven dat er niet nog niet aan de eisen is voldaan.

In 2026 is het doel om zoveel mogelijk te voldoen aan de BIO2. De progressie van 2024 naar 2025 lijkt op papier minder significant dan dat hij daadwerkelijk is. De gemeente heeft de BIO v1.4 volledig losgelaten en heeft zich volledig gefocust op de BIO 2.0 hiermee valt de score lager uit omdat bepaalde maatregelen die in de BIO 1.4 vereist worden en in de BIO 2.0 worden losgelaten het afgelopen jaar niet zijn uitgevoerd. Dit geeft een vertekenend beeld van de status van de implementatie van de BIO 2. In 2026 hoopt de gemeente een positief beeld te laten zien van de status van implementatie van de BIO 2. Bij de implementatie van de nieuwe werkplek is dan ook de waar nodig (mogelijk) de focus gelegd op het implementeren van de BIO 2. Vanaf 2026 evalueert de gemeente ook samen met de leverancier van de werkplek elk kwartaal of de werkplek nog voldoet aan de BIO 2 en op welke vlakken we kunnen verbeteren.

2. Samenvatting resultaten zelfevaluatie 2025

Zelfevaluatie	Audit	Bevindingen Gemeente Waterland
DigiD (IT audit) *Resultaat 2025*	Conform college-verklaring/ bevindingen	Aan 1 norm niet voldaan *Aan alle normen voldaan*
Suwinet (IT audit) *Resultaat 2025*	Conform college-verklaring/ bevindingen	Aan alle normen voldaan *Aan alle normen voldaan*

Zelfevaluatie	Norm	Score Gemeente Waterland
BRP domeinvragen Kwaliteitsmonitor RvIG BRP informatiebeveiligingsvragen ENSIA Samengevoegde resultaat 2025 *Samengevoegde resultaat 2024*	 90% *90%*	733 punten van 800 (91,6%) 1130 punten van 1.200 (94,2%) *1863 punten van 2.000 (93,15%)* *1.863 punten van 2.000 (93,15%)*
Reisdocumenten domeinvragen Kwaliteitsmonitor RvIG Reisdocumenten informatiebeveiligingsvragen ENSIA Samengevoegde resultaat 2025 *Samengevoegde resultaat 2024*	 90% *90%*	767 punten van 800 (95,9%) 1095 punten van 1.200 (91,3%) *1862 punten van 2.000 (93,1%)* *1.846 punten van 2.000 (92,3%)*
BAG	75%	68% *2024 35%*
BGT	75%	50% *2024 28%*
BRO	60%	80% *2024 85%*

Naast opzet van en verantwoording over de BIO is de BIO onderverdeeld in 5 categorieën (bouwstenen) en omvat in totaal 206 maatregelen. Als aan één BIO-maatregel niet is voldaan is de conclusie ‘voldoet niet’.
Van de 206 maatregelen is aan 48 maatregelen niet voldaan* (percentage voldaan 76,7%, 2024: 76,2%).

BIO	Aantal maatregelen	Maatregelen waaraan niet is voldaan	Conclusie Gemeente Waterland
Achtergrond BIO *(hoofdstuk 2 opzet BIO en hoofdstuk 4 verantwoording over de BIO)*	7	2 *2024: 1*	Voldoet niet
Categorie 1: Beleid en organisatie *(hoofdstuk 5 informatiebeveiligingsbeleid, hoofdstuk 6 organiseren van informatiebeveiliging en hoofdstuk 18 naleving)*	31	4 *2024: 5*	Voldoet niet
Categorie 2: Personeel en toegang *(hoofdstuk 7 veilig personeel, hoofdstuk 9 toegangsbeveiliging en hoofdstuk 11 fysieke beveiliging en beveiliging van de omgeving)*	59	11 *2024: 8*	Voldoet niet
Categorie 3: Continuïteit en incidenten *(hoofdstuk 16 beheer van informatie-beveiligingsincidenten en hoofdstuk 17 informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer)*	20	10 *2024: 7*	Voldoet niet
Categorie 4: Informatiesystemen *(hoofdstuk 12 beveiliging bedrijfsvoering, hoofdstuk 14 acquisitie, ontwikkeling en onderhoud van informatiesystemen en hoofdstuk 15 leveranciersrelaties)*	57	17 *2024: 24*	Voldoet niet
Categorie 5: Databescherming *(hoofdstuk 8 beheer van bedrijfsmiddelen, hoofdstuk 10 cryptografie en hoofdstuk 13 communicatiebeveiliging)*	32	4 *2024: 4*	Voldoet niet

*van het totaal niet behaalde maatregels zijn er 10 die betrekking hebben op de basisbeveiligingsniveaus
die komen te vervallen in de controle van volgend jaar en hierdoor ook geen acties op zijn uitgevoerd in 2025.

3. Uitkomsten IT audit DigiD en Suwinet

3.1. DigiD

DigiD is het authenticatiemiddel voor onze online dienstverlening. De gemeente Waterland heeft twee DigiD aansluitingen. Eén voor het zaaksystemen (refentie nummer 1005565) en één voor de eDiensten van Burgerzaken (referentie nummer 1005997). Jaarlijks dient de gemeente verantwoording af te leggen aan de stelselhouder BZK/Logius vindt plaats door middel van een externe audit. Deze omvat het op 31 december 2025 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake DigiD. De beheersingsmaatregelen die zijn uitbesteed vallen buiten de reikwijdte van de externe audit. De audit bij Waterland en de verantwoording van de dienstverleners dekken tezamen alle geselecteerde normen inzake DigiD af.

Bevindingen

Voor DigiD aansluitnummer 1005565 en 1005997 wordt door gemeente Waterland aan één van alle geselecteerde normen niet voldaan. De tekortkoming betreft het uit dienst proces, waarbij in één specifiek geval de uitdienstreding proces niet correct is gevolgd. De beveiligingsrisico’s waren hiervan hoog en is intern ook aangegeven.

3.2. Suwinet

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. De gemeente Waterland maakt gebruik van Suwinet voor de uitvoering van de Participatiewet, IOAZ en IOAW. Daarnaast maakt de gemeente gebruik van Suwinet voor niet Suwi-taken. Dit betreft Suwinet/Burgerzaken voor adresonderzoek. De verantwoording aan stelselhouder ministerie SZW vindt plaats door middel van de Collegeverklaring. Inzake Suwinet heeft de Collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan GR-BVO Zaffier (Zelfstandigenloket). De Collegeverklaring omvat het op 31 december 2025 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake Suwinet.

Bevindingen

Voor de Suwinet-taken zijn geen bevindingen gevonden. Hiermee hebben wij aan de audit voldaan.

3.3. Collegeverklaring DigiD en Suwinet en assurance rapport IT auditor

De onafhankelijke IT-auditor heeft op basis van de Collegeverklaring een assurance rapport opgesteld. De auditor geeft aan dat de Collegeverklaring ENSIA 2025 over de informatiebeveiliging van DigiD en Suwinet op alle belangrijke punten juist is. De Collegeverklaring voor DigiD en Suwinet is in april 2026 vastgesteld. Het definitieve assurance rapport van de IT-auditor werd daarna gedeeld met de betrokken ministeries.

4. Uitkomsten BRP en Reisdocumenten

4.1. Inleiding

Over 2025 is de zelfevaluatie BRP en Reisdocumenten gescheiden uitgevoerd. De domein specifieke vragen zijn beantwoord via de ‘Kwaliteitsmonitor’ van de Rijksdienst voor Identiteitsgegevens (RvIG) en de informatiebeveiligingsvragen via ENSIA. De resultaten worden verstrekt in de vorm van uittreksels en zijn weergegeven in een puntenaantal.
De managementrapportages en uittreksels BRP en Reisdocumenten zijn februari 2026 separaat voorgelegd aan het college van burgemeester en wethouders voor de verantwoording aan de stelselhouders. Alle actiepunten en aanbevelingen die in de managementrapportages zijn benoemd worden opgevolgd.

4.2. BRP

De normering die is gekoppeld schetst een beeld van de toepassing van technische en organisatorische beveiligingsmaatregelen en overige aspecten van processen rondom de BRP. Uit de zelfevaluaties blijkt dat de gemeente Waterland goed scoort op de inrichting, de werking en de beveiliging van de basisregistratie. Het samengevoegde resultaat van de domeinvragen en informatiebeveiligingsvragen is *1863* punten van de maximaal 2.000 punten. Dat geeft een percentage van *93,15%.*

4.3. Reisdocumenten

De normering die is gekoppeld schets een beeld van de toepassing van technische en organisatorische beveiligingsmaatregelen en overige aspecten van het aanvraag- en uitgifteproces paspoorten en NIK. Uit de zelfevaluatie blijkt dat de gemeente Waterland op de beveiliging en overige aspecten van het aanvraag- en uitgifteproces net onder de norm scoort. Het samengevoegde resultaat van de domein- en informatiebeveiligingsvragen is *1862* punten van de maximaal 2.000 punten. Dat geeft een percentage van *93,1%.*

4.4. Verbeterpunten BRP en Reisdocumenten

Een verbeterpunt voor Reisdocumenten is het uitbreiden van de bestaande in dienst procedure voor publiekszakenmedewerkers, dit wordt naar verwachting in 2026 opgepakt door de organisatie. Voor de BRP is het bedrijfscontinuïteitplan af en moet deze worden getest daarnaast wordt hierop een PDCA-cyclus gehanteerd. Verder ontwikkelt de organisatie het beleid door voor de verbetering van de kwaliteit van de BRP.

Voor 2026 zijn de verbeterpunten voor de BRP: het AVG- verwerkinsregister verder aanvullen (was in 2025 ook een verbeterpunt) en de werkprocedure omtrent het aanschrijven van de inwoner voor het inleveren van sterkere brondocumenten moet verder worden aangescherpt om aan de punten te voldoen van de zelfevaluatie van de RVIG.

5. Status BIO

In dit hoofdstuk is een uitwerking per onderdeel uit de ENSIA-zelfevaluatie opgenomen. De vragenlijst informatiebeveiliging BIO betreft BIO-maatregelen voor informatieveiligheid in brede zin, zowel de fysieke- als logische beveiliging, en maatregelen ten aanzien van de Algemene Verordening Gegevensbescherming (AVG).
De BIO is met ingang van 1 januari 2020 van kracht. In september 2025 is de BIO 2.0 ingegaan. De BIO 2.0 is nog niet wettelijk verplicht, dit gebeurt pas bij de inwerkingtreding van de Cyberbeveiligingswet. Naar verwachting wordt deze wet in 2026 aangenomen. Dit betekent dat de gemeente een wettelijke verplichting voor BIO 2.0 heeft vanaf 2027.

De vragen over de BIO-maatregelen zijn verdeeld over een aantal categorieën. Als aan één BIO-maatregel niet is voldaan is de conclusie ‘voldoet niet’. De beantwoording, die is onderbouwd met bewijsstukken, geeft aan of wel of niet aan de maatregelen wordt voldaan, maar leidt niet tot een score. Onderstaand zijn de bevindingen en op hoofdlijnen de tekortkomingen en verbetermaatregelen aangegeven.

In 2025 is de gemeente gestart met een project om te voldoen aan de Cyberbeveiligingswet en daarmee ook aan de BIO 2.0. Onder de Cyberbeveiligingswet is de gemeente per 2025 een zo genoemde ‘essentiële’ organisatie waarmee de gemeente per 2027 actief ge-audit kan worden en dat het voldoen aan de BIO 2.0 een wettelijke verplichting wordt.

Het doel van het project in 2025 was om de basis neer te leggen om te voldoen aan de BIO 2.0. Dit project loopt nog voort in 2026. Daarna is het vooral belangrijk dat het project overgaat in de dagelijkse werkzaamheden van de gemeente zodat de gemeente continue blijft verbeteren en risico's die er zijn in kaart brengt. Het doel in 2026 is om in kaart brengen wat er nog moet gebeuren, wat nog moet verbeteren en wat er al is t.o.v. de BIO2.

5.1. Achtergrond van de BIO

Op basis van risicomanagement dient te worden bepaald hoe aan beveiligingsdoelstellingen voldaan kan worden. Op basis van risicoafwegingen worden basisbeveiligingsniveaus (BBN) toegekend door proceseigenaren. Vastgelegd moet worden welke controls en maatregelen niet van toepassing zijn. Alle controls en maatregelen die wel van toepassing zijn, moeten intern zijn toebedeeld aan een verantwoordelijke.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

- Er zijn door proceseigenaren nog geen BBN’s toegekend op basis van risicomanagement. In de BIO 2.0 de BBN’s komen te vervallen en er op basis van een risicoanalyse gestuurd moet worden op maatregelen.
- In de verantwoording over de BIO wordt ook verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt.

Verbetermaatregel

- In 2026 is de gemeente al begonnen met het in kaart brengen van de risico’s voor de primaire processen. Dit betekent dat de gemeente hiermee voldoet aan de eisen vanuit de BIO2. Het doel is om eind 2026 alle primaire processen een risicoanalyse te hebben gedaan.
- Op dit moment wordt er nog geen verantwoording over afspraken met ketenpartners afgelegd, dit zal wel gebeuren over het jaar 2026. In Q3 2026 staat ook

leveranciersmanagement op de planning en wordt de verantwoording hierover ook meegenomen. Dit zal nog doorlopen in 2027.

5.2. Categorie 1: Beleid en organisatie

Het bestuur en medewerkers zijn actief betrokken bij informatiebeveiliging. Er is een organisatie breed informatiebeveiligingsbeleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

1. Zero footprint principe is niet toegepast (er wordt geen informatie onbewust lokaal opgeslagen).
2. De Plan-Do-Check-Act (PDCA) methodiek wordt niet toegepast op alle onderdelen van informatiebeveiliging.
3. Bij projecten is informatiebeveiliging niet een structureel onderdeel. Het proces is juist ingebouwd maar de toepassing in de praktijk is nog niet volledig.
4. Aantal openstaande punten t.o.v. de basis beveiligingsniveau's (BBN)

Verbetermaatregelen

1. In 2025 is een Mobile Device Management (MDM) en Mobile Application Management Systeem (MAM) systeem geïmplementeerd door het project De Moderne Werkplek. Echter is dit nog niet toegepast op iPhones binnen de organisatie, dit zal in 2026 worden uitgerold en daarmee zal aan dit punt worden voldaan.
2. Voor aantoonbare PDAC-cyclus zijn in 2025 de eerste stappen gezet binnen de organisatie en daarnaast heeft de organisatie ook een nieuw systeem aangeschaft om hierbij te ondersteunen.
3. Het proces is in 2025 juist ingericht echter moet dit nu nog in de praktijk komen, hierbij ligt vooral een verantwoording bij de opdrachtgevers van projecten.
4. Met de komst van de BIO versie 2 zijn BBN's niet langer van toepassing daarom heeft de gemeente deze punten losgelaten in 2025 en is hier dan ook niet aan voldaan.

5.3. Categorie 2: Personeel en toegang

Alleen de juiste personen hebben toegang tot de gebouwen, systemen en gegevens van de gemeente. Er zijn passende organisatorische en technische maatregelen getroffen voor waarborgen rondom in- en externe medewerkers en de toegang tot gebouwen, omgeving en de (digitale) informatievoorziening.
Voor, tijdens en na het dienstverband is alles goed geregeld. Medewerkers gaan bewust om met informatie en hebben de juiste toegangsrechten.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

1. Er worden geen expliciete risicoafwegingen gemaakt voor informatiesystemen.
2. Geen actuele verwijderinstructie voor het waar nodig onherstelbaar verwijderen van informatie.
3. Geen periodieke controle op de uitgegeven toegangsbadges.
4. Maatregelen ten aanzien van de toegang van eigen en geauthenticeerde apparatuur tot (netwerk) omgevingen.

5. Voor niet alle applicaties zijn er autorisatiematrixen binnen de organisatie en daarom ook geen controle hierop.
6. De eisen voor wachtwoorden uit de BIO 1.4 komen niet overeen met het wachtwoordbeleid van Waterland.
7. De (genomen) maatregelen voor bedreigingen van buitenaf zijn nog niet gebaseerd op een expliciete risicoafweging.

Verbetermaatregelen

1. In 2026 is de gemeente Waterland gestart met het uitvoeren van risicoanalyses op de primaire processen en verwacht dit voor alle primaire processen te hebben afgerond in 2026.
2. De procedure die er is zal in 2026 worden ge-update zodat deze weer overeenkomt met de praktijk.
3. Er dient een eigenaar te komen voor de interne badges, deze dient een periodieke controle te doen over de uitgegeven toegangen en dit te rapporteren.
4. Een van de restant punten vanuit de Moderne Werkplek is het opnieuw oprichten van verschillende (wifi) netwerken voor beheerde en onbeheerde apparaten. Het plan hiervoor ligt al klaar en zal worden uitgevoerd in 2026.
5. Voor de primaire applicaties en de applicaties met een DigiD koppeling dienen per 2026 autorisatiematrixen te worden opgesteld en minimaal 2 (bij voorkeur 4) controles te worden uitgevoerd.
6. Het wachtwoordbeleid binnen de gemeente is conform de BIO 2.0 en voldoet daarmee niet aan de BIO 1.4. Dit vanwege het feit dat de wachtwoord eisen in de BIO 1.4 achterhaald zijn zoals elke 90 dagen wachtwoord wijzigen.
7. Dit punt verwijst ook naar verbeterpunt 1, er worden in 2026 risicoanalyses gemaakt voor de primaire processen.

5.4. Categorie 3: Continuïteit en incidenten

De diensten van de gemeente worden geleverd volgens de afspraken die de gemeente daarover maakt met de inwoners en bedrijven, ook bij incidenten. Incidenten worden altijd gemeld, geanalyseerd en beoordeeld. Continuïteitsplannen zijn actueel en worden getest.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

1. De incidenten procedure is op dit moment niet juist ingericht.
2. Een continuïteitsplannen zijn beperkt aanwezig, maar worden niet jaarlijks getest.

Verbetermaatregelen

1. De volledige procedure voor incidenten is herschreven en dient in 2026 ook in de praktijk te worden ingevoerd. Dit betrekt het eigenaarschap, het rapporteren op incidenten en het leren van incidenten.
2. Continuiteitsplannen zijn beperkt aanwezig binnen de gemeente en hier dient buiten informatiebeveiliging om eerst eigenaarschap en verantwoordelijkheid worden belegd op bestuurlijk niveau.

5.5. Categorie 4: Informatiesystemen

Informatiesystemen zijn een keten van mensen, processen en middelen. Het betreft zowel de interne als de externe informatiesystemen. Hierin zijn procedures en maatregelen beschikbaar ter bescherming van de omgeving. Afspraken met leveranciers zijn vastgelegd. Wijzigingen worden op een gecontroleerde manier doorgevoerd en back-ups volgens beleid uitgevoerd. Er is bescherming tegen malware.

Bevindingen
Aan deze maatregelen is niet voldaan.

Tekortkomingen
1. De procedure voor wijzigingenbeheer is niet actueel en er zijn geen aanvullende maatregelen gedefinieerd voor transacties, wijzigingsbeheer en testen.
    a. Hoe gaan we als organisatie om met productiegegevens in de test omgeving.
    b. Afwijkingsprocedure voor de test in de productieomgeving.
2. Back-ups en restore worden uitgevoerd, er is vastgesteld back-up beleid maar geen (goede) vastlegging dat de actie is voldaan.
3. Logging van (primaire) applicaties wordt niet actief getoetst aan het beleid.
    a. Binnen de organisatie is geen overzicht van logbestanden die gegeneerd worden.
4. Wordt geen expliciete risicoanalyse gemaakt bij aanschaf nieuwe software.
5. Een procedure voor het installeren van software en een risicoafweging voor het downloaden van bestanden ontbreken.
6. Leveranciers management moet worden verbeterd binnen de organisatie

Verbetermaatregelen
1. In 2025 gaat het Informatievoorzieningen team aan de slag met het opstellen van procedures voor wijzigingsbeheer en testen. Zodat dit vanaf dan op een eenduidige manier gebeurt binnen de organisatie.
2. Eind 2024 is er een back-up beleid vastgesteld, deze is in 2025 niet op alle (primaire) applicaties getoetst. Dit wordt in 2026 wel toegepast.
3. Het in kaart brengen van de loggen en deze toetsen van de normen van de BIO wordt waarschijnlijk niet behandeld in 2026 en daarmee verplaatst naar 2027.
4. De verplichting hiervoor wordt besproken met het IV-team en daar moet de verantwoording te komen liggen over de verplichtingen.
5. Deze procedure wordt opgesteld in 2026 en toegepast.
6. In het informatiebeveiligingsjaarplan 2026 is dit punt opgenomen in Q2 van 2026.

Kanttekening
- Sommige van de punten uit dit hoofdstuk zouden worden opgepakt in 2025. Echter door de extra tijd die het project de Moderne Werkplek vroeg in 2025 zijn sommige taken doorgeschoven naar 2026.

5.6. Categorie 5: Databescherming
Data wordt op de juiste manier beschermd. Gegevens van inwoners worden veilig opgeslagen en gecommuniceerd, binnen en buiten de gemeente. Met de nieuwe werkplek zijn op dit onderdeel de meeste stappen gezet t.o.v. 2024 en deze zullen worden voortgezet in 2025.

Bevindingen
Aan deze maatregelen is niet voldaan.

Tekortkomingen
- Risico analyses worden niet gedaan op systemen en informatie.
    - Informatie is geclassificeerd op basis van een risicoafweging, maar is niet gelabeld.
- Er zijn geen afspraken met leveranciers over reserve certificaten.
- Er is geen beleid of procedure voor informatietransport.

Verbetermaatregelen
- Zoals eerder vermeld is de gemeente al gestart met risicoanalyse en verwacht dit voor de primaire processen te hebben afgerond in 2026. Verder komt het label voort uit het

project de Moderne Werkplek en is dit onderdeel doorgeschoven naar 2025 in dit project.
- Er is begin 2024 een beleid vastgesteld over informatietransport echter is dit niet volledig doorgevoerd nog.

Kanttekening

- Met de aanbesteding van de moderne werkplekis er leverancier aangetrokken die het certificaat beheer voor de gemeente Waterland gaat doen. Als gemeente dienen we enkel nog regie te voeren op de certificaten van de gemeente.

5.7. Algemene verbetermaatregelen.

In het jaar 2025 lag de focus qua informatiebeveiliging op twee belangrijke punten. De eerste was de implementatie van de moderne werkplek. In oktober 2024 was de aanbesteding voor de moderne werkplek succesvol afgerond en daarna is overgegaan op de inrichting en implementatie. Tijdens dit project wordt er waar mogelijk ingericht volgens wettelijke kaders zoals de AVG en de BIO. Daarnaast is er in 2025 een start gemaakt met het interne project Cyberbeveiligingswet/ BIO 2.0. De eerste stap hiervoor was kijken naar de huidige processen en beleidsstukken. Zoals in 2024 al aangegeven voldoet de gemeente in 2025 nog niet aan de BIO 2.0 en dit zal in 2026 waarschijnlijk ook nog niet zomaar dan is de verwachting dat bepaalde onderdelen wel voldoen.
Tot slot ligt in de naast afronding van het project de moderne werkplek en het project Cyberbeveiligingswet/ BIO 2.0 de focus op de implementatie van een nieuwe GRC-tool (Gouvernance Risk Compliance). In deze tool wordt het ISMS (information security managementsysteem) verwerkt. Via het ISMS houdt de gemeente grip op informatiebeveiliging en legt de gemeente de bewijslast vast voor de wet- en regelgeving.

6. Incidenten

Een dreiging of tekortkoming in de beveiliging kan leiden tot een beveiligingsincident, een daadwerkelijke inbreuk op de beveiliging. Als daarbij persoonsgegevens zijn betrokken is er sprake van datalekken. Het is van groot belang dat (mogelijke) incidenten snel, adequaat gedetecteerd, gemeld en behandeld worden om de mogelijke nadelige gevolgen te voorkomen of te beperken. De gemeente Waterland heeft een procedure voor het melden van mogelijke incidenten en wordt specifiek en gericht geïnformeerd over kwetsbaarheden en incidenten door de Informatiebeveiligingsdienst (IBD).

Meldingen 2025

In 2025 zijn meerdere meldingen geweest maar is er vooral geconstateerd dat niet alle meldingen juist worden geregistreerd. Niet alle meldingen komen binnen via het ticket systeem dat de gemeente hanteert, sommige worden ook mondeling doorgegeven of telefonisch. Deze meldingen worden dan zo snel mogelijk opgelost maar niet altijd (alsnog) geregistreerd. Hierdoor is de conclusie voor 2025 vooral dat er geen duidelijk overzicht met alle meldingen. Daarnaast is met de overgang van de moderne werkplek een nieuwe methode in gebruik genomen zoals bijvoorbeeld het melden van phishing emails. Er is op dit moment nog geen overzichtelijke manier om alle gedane meldingen in te zien.

Hierdoor wordt er over 2025 geen aantallen weergegeven maar wel een globaal inzicht wat zich in de gemeente heeft afgespeeld qua incidenten.

Het meest voorkomende incident en wat ook direct burgers raaks is storingen in ICT-systemen van onze primaire diensten. Hier wordt dan direct over geschakeld met onze leveranciers en is in de meeste gevallen in korte tijd opgelost.

Verder heeft de gemeente nog steeds wekelijks last van phishing e-mails op verschillende gebieden. Voorbeelden zijn:

- Facturen die we niet betaald hebben
- E-mails namens de gemeentesecretaris dat er iets met spoed moet gebeuren
- E-mails namens de CISO dat er iets met spoed moet gebeuren
- Uitnodigingen voor niet bestaande evenementen.

Hierbij is het grootste risico wanneer een vertrouwd emailadres zoals die van een leverancier. Hiervan is zover bekend dit eenmalig voorgekomen in 2025. Deze is gelukkig tegengehouden door de technische beveiliging voordat er schade aangebracht kon worden.

Tot slot krijgt de gemeente minimaal wekelijks of bij een kwetsbaarheid met hoge prioriteit berichten vanuit de IBD. Deze meldingen worden beoordeeld binnen de gemeente en waar nodig opgepakt of gedeeld met leverancier om te laten oppakken. Er zijn (voor zover bekend) geen nadelige gevolgen geweest naar aanleiding van kwetsbaarheden.

De conclusie is dat de gemeente zover bekend is geen grote incidenten op het gebied van informatiebeveiliging heeft gehad.