Jaarrapportage informatieveiligheid 2024 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 2024, kenmerk 7949-2025)

1. Inleiding

De gemeente streeft naar continue en betrouwbare dienstverlening, het zorgvuldig omgaan met informatie en het beheersen van risico's. De gemeente heeft de ambitie om te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO), met volgend jaar de focus op de invoering van BIO 2.0., het basisnormenkader voor informatieveiligheid en wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), evenals het eigen informatiebeveiligings- en privacybeleid. Hierbij is het wel belangrijk om te vermelden over het jaar 2025 wordt de gemeente nog geaudit over BIO versie v1.4.

Deze rapportage geeft op hoofdlijnen de uitkomsten weer van de gemeente-brede uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2024. Deze zelfevaluatie is gebaseerd op de BIO en is uitgevoerd in de periode juli t/m december 2024. Wij rapporteren als gemeente Waterland 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 dit verslag 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 2024 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 zowel DigiD als Suwinet heeft de gemeente 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

Alle onderdelen scoorden op of boven de norm. De aanbevelingen zijn als actiepunt voor 2025 opgenomen. De aanbeveling om het AVG Register van Verwerkingen aan te vullen speelt organisatiebreed en wordt via het management geïnitieerd. Hier is een project plan reeds voor opgesteld en deze zal medio 2025 worden uitgevoerd en hopelijk Q4 2025 met uitloop naar Q1 2026 worden afgeronde. In totaal scoorde Reisdocumenten boven de norm. Voor het onderdeel naleving (net onder de norm) zijn aanbevelingen gedaan.

Openstaande technische maatregelen vanuit de BIO worden meegenomen in de implementatie voor de Digitale Moderne Werkplek (Het Nieuwe Werken) in 2025, als gemeente zijn we hier eind 2024 mee begonnen en verwachten dit Q3/Q4 2025 af te ronden.

Bestuurlijke verantwoording over de BAG, BGT en BRO

Voor de BAG, BGT en BRO zijn over 2024 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. 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.
De rapportage BAG, BGT en BRO zijn als bijlage bij deze jaarrapportage opgenomen. De scores zijn opgenomen in de samenvatting resultaten zelfevaluatie 2024 (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 49 van de 206.
De openstaande technische maatregelen, waarvoor nu nog geen oplossing is, worden in 2025 meegenomen in de implementatie voor de Digitale Moderne Werkplek (Het Nieuwe Werken) met als doel deze in 2025 ook af te ronden zoals eerder aangegeven. Veel technische eisen vanuit de BIO kan de gemeente met de huidige werkplek niet voldoen en met de implementatie van de nieuwe werkplek zijn deze technische middelen er wel. 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) en het opstellen van een procedure voor wijzigingenbeheer en het downloaden of installeren van software (informatiesystemen). Een aantal van deze procedures zijn in 2024 opgesteld maar nog niet in gebruik genomen, om deze reden is aangegeven dat er niet nog niet aan de eisen is voldaan.

In 2025 is het doel om volledig te voldoen aan de BIO. Echter met ook de implementatie van de BIO 2.0 (huidige versie is BIO 1.4) kan het zijn dat dit niet gaat lukken. Hierin wil de gemeente in ieder geval significante vooruitgang laten zien.

2. Samenvatting resultaten zelfevaluatie 2024

Zelfevaluatie	Audit	Bevindingen Gemeente Waterland
DigiD (IT audit) Resultaat 2024 *Resultaat 2023*	Conform college-verklaring/ bevindingen	Aan alle normen voldaan *Aan 1 norm niet voldaan*
Suwinet (IT audit) Resultaat 2024 *Resultaat 2023*	Conform college-verklaring/ bevindingen	Aan alle normen voldaan *Aan alle normen voldaan*

Zelfevaluatie	Norm	Score Gemeente Waterland
BRP domeinvragen Kwaliteitsmonitor RvIG BRP informatiebeveiligingsvragen ENSIA Samengevoegd resultaat 2024 *Samengevoegd resultaat 2023*	 90% *90%*	693 punten van 800 (84,6%) 1.170 punten van 1.200 (91,2%) *1.863 punten van 2.000 (93,15%)* *1.772 punten van 2.000 (88,6%)*
Reisdocumenten domeinvragen Kwaliteitsmonitor RvIG Reisdocumenten informatiebeveiligingsvragen ENSIA Samengevoegd resultaat 2024 *Samengevoegd resultaat 2023*	 90% *90%*	781 punten van 800 (97%) 1065 punten van 1.200 (88,3%) *1.846 punten van 2.000 (92,3%)* *1.836 punten van 2.000 (91,8%)*
BAG	75%	35% *2023 35%*
BGT	75%	28% *2023 40%*
BRO	60%	85% *2023 89%*

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 49 maatregelen niet voldaan (percentage voldaan 76,2%, 2023: 75,2%).

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	1 2023: 1	Voldoet niet
Categorie 1: Beleid en organisatie *(hoofdstuk 5 informatiebeveiligingsbeleid, hoofdstuk 6 organiseren van informatiebeveiliging en hoofdstuk 18 naleving)*	31	5 2023: 4	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	8 2023: 10	Voldoet niet
Categorie 3: Continuïteit en incidenten *(hoofdstuk 16 beheer van informatie-beveiligingsincidenten en hoofdstuk 17 informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer)*	20	7 2023: 9	Voldoet niet
Categorie 4: Informatiesystemen *(hoofdstuk 12 beveiliging bedrijfsvoering, hoofdstuk 14 acquisitie, ontwikkeling en onderhoud van informatiesystemen en hoofdstuk 15 leveranciersrelaties)*	57	24 2023: 23	Voldoet niet
Categorie 5: Databescherming *(hoofdstuk 8 beheer van bedrijfsmiddelen, hoofdstuk 10 cryptografie en hoofdstuk 13 communicatiebeveiliging)*	32	4 2023: 4	Voldoet niet

3. Uitkomsten IT audit DigiD en Suwinet

3.1. DigiD

DigiD is het authenticatiemiddel voor onze online dienstverlening. Het object van onderzoek was de webomgeving van DigiD aansluiting 1005565 Digitaal Loket gemeente Waterland. De verantwoording aan de stelselhouder BZK/Logius vindt plaats door middel van de Collegeverklaring. Deze omvat het op 31 december 2024 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 Collegeverklaring. De Collegeverklaring en de verantwoording van de dienstverlener dekken tezamen alle geselecteerde normen inzake DigiD af. De gemeente dient per DigiD aansluiting verantwoording af te leggen vanaf 2025 zijn dit er minimaal twee plus eventuele extra DigiD aansluitingen die erbij komen.

Bevindingen

Er zijn geen bevindingen uit de DigiD en Suwinet audit.

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 2024 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 voorlopig assurance rapport opgesteld voor het college. Volgens de IT auditor is de Collegeverklaring ENSIA 2024, inzake informatiebeveiliging van DigiD en Suwinet, in alle van materieel belang zijnde aspecten correct. Zodra dit stuk naar de raad gaat, wordt het assurance rapport definitief. De definitieve tekst van de Collegeverklaring zal in april 2025 worden vastgesteld en uitgegeven door de IT auditor. De tekst van de Collegeverklaring treft u aan in bijlage 1.

4. Uitkomsten BRP en Reisdocumenten

4.1. Inleiding

Over 2024 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 '24 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 schets 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 samengevoegd resultaat van de domeinvragen en informatiebeveiligingsvragen is 1.863 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 samengevoegd resultaat van de domein- en informatiebeveiligingsvragen is 1. 846 punten van de maximaal 2.000 punten. Dat geeft een percentage van 92,3%.

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 2025 opgepakt door de organisatie. Voor de BRP moet het bedrijfscontinuïteitsplan worden afgerond en in 2025 worden getest. Hierbij wordt een PDCA-cyclus gehanteerd. Verder ontwikkelt de organisatie het beleid door voor de verbetering van de kwaliteit van de BRP. In 2024 is een werkprocedure opgevolgd en deze periodieke gecontroleerd in 2025.

Voor 2025 zijn de verbeterpunten voor de BRP: het AVG- verwerkingenregister verder aanvullen en de werkprocedure omtrent het aanschrijven van de inwoner voor het inleveren van sterkere brondocumenten moet worden aangescherpt om te voldoen aan de eisen uit 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 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 2025 zal de BIO 2.0 van in treedt in werking in samenhang met de Cyberbeveiligingswet. 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 start de gemeente ook 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 2026 actief ge-audit kan worden en dat het voldoen aan de BIO 2.0 een wettelijke verplichting wordt. Eigenlijk zoals dit ook de bij AVG-wetgeving is, wanneer er niet wordt voldaan kan er onder andere een boete worden uitgeschreven.

Het doel van het project is om in 2025 de basis neer te leggen om te voldoen aan de BIO 2.0 mogelijk kan het zijn dat er eind 2025 nog niet volledig wordt voldaan aan de BIO 2.0 omdat er ook eisen in zitten of de controle en effectiviteit van genomen maatregelen voldoen voor de organisatie. Op deze punten kan het mogelijk zijn dat we nog niet lang genoeg de maatregelingen hebben geïmplementeerd of we ook weten of het gewenste effect is bereikt.

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.

Verbetermaatregel

- In 2024 hebben we hier voor de primaire processen al aan voldaan maar nog niet voor alle processen. Het is reeds bekend dat in de BIO 2.0 de BBN's komen te vervallen en er op basis van een risicoanalyse gestuurd moet worden op maatregelen. Hier is dan ook meer de focus op gelegd als organisatie om alvast te sturen richting de BIO 2.0 en niet alsnog aan alle processen een BBN te gaan toekennen.

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

- De ondersteunende maatregelen voor het beheren van risico's ten aanzien van het gebruik van mobiele apparatuur zijn onvoldoende.
- Het zero footprint-principe is niet toegepast (er wordt geen informatie onbewust lokaal opgeslagen).
- De Plan-Do-Act-Check methodiek wordt toegepast op alle onderdelen van informatiebeveiliging

Verbetermaatregelen

- In 2025 wordt een Mobile Device Management (MDM) en Mobile Application Management Systeem (MAM) systeem geïmplementeerd door het project De Moderne Werkplek.
- Het project De Moderne Werkplek gaat ook het principe zero footprint principe toepassen. Hiermee wordt data alleen nog opgeslagen op de door Waterland beheerde plekken.
- Dit is onderdeel van het Cyberbeveiligingswet/ BIO 2.0 project wat in 2025 wordt gestart. Oorspronkelijk zou dit al in 2024 starten, maar door het uitstellen van de cyberbeveiligingswet van 2024 naar 2025 (mogelijk zelfs Q1 2026) was het niet mogelijk eerder te starten.

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

- Maatregelen ten aanzien van de toegang van eigen en geauthenticeerde apparatuur tot (netwerk) omgevingen.
- De frequentie van het beoordelen van toegangsrechten voor systemen.
- De (genomen) maatregelen voor bedreigingen van buitenaf zijn nog niet gebaseerd op een expliciete risicoafweging.

Verbetermaatregelen

- Dit punt wordt opgepakt met het project de Moderne Werkplek. Met dit project wordt er een netwerk opgezet waar alleen door Waterland beheerde apparaten bij kunnen. Alle niet beheerde apparaten krijgen hun eigen netwerk.
- De controle op autorisatiematrixen is opgevoerd, maar er is nog een te beperkt overzicht van de speciale rechten/extra rechten die door de tijd zijn verkregen. Hier zal het project de moderne werkplek een nieuwe start in maken.
- Hiervoor zijn in 2024 voldoende maatregelen genomen en ook op basis van expliciete risico afwegingen en deze risico's zijn voorgelegd aan het MT en in een specifiek geval zelf aan het college. Dit is het enige punt dat wel is behaald, maar niet op deze manier is verantwoord.

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

- Kennisdeling over kwetsbaarheden is ingericht, maar wordt niet gepubliceerd.
- Proceseigenaren zijn verantwoordelijk voor oplossing informatiebeveiligingsincidenten.
- Een continuïteitsplan is aanwezig, maar wordt niet jaarlijks getest.
- Bedrijf kritische procesonderdelen zijn geïdentificeerd maar niet op basis van een specifieke risicoafweging.
- Coordinated Vulnerability Disclosure-procedure ontbreekt.

Verbetermaatregelen

- Niet van toepassing, aangezien dit betrekking heeft op software die door de gemeente zelf is ontwikkeld, wat niet het geval is voor de gemeente. De gemeente ontwikkeld zelf geen software.
- Op dit moment worden proceseigenaren betrokken bij beveiligingsincidenten en handelen daar ook naar maar het enige wat nog ontbreekt is een formeel proces. Om deze reden dit punt op niet voldaan gezet.
- In 2023 zouden de continuïteitsplannen worden herzien maar dit is pas in 2024 gebeurd. Doel is om in 2025 een test uit te voeren. Dit valt onder het cyberbeveiligingswet/ BIO 2.0 project.
- Dit valt onder het cyberbeveiligingswet/ BIO 2.0 project, als organisatie moeten we risico gestuurd te werk gaan.
- Dit valt onder het cyberbeveiligingswet/ BIO 2.0 project

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

- De procedure voor wijzigingenbeheer is niet actueel en er zijn geen aanvullende maatregelen gedefinieerd voor transacties, wijzigingsbeheer en testen.
- Back-ups en restore worden uitgevoerd, maar er is geen actueel vastgesteld back-up beleid.
- Een procedure voor het installeren van software en een risicoafweging voor het downloaden van bestanden ontbreken.
- De organisatie beschikt, met uitzondering van een aantal kritische processen, nog niet over een volledig overzicht van logbestanden.
- In de afspraken met leveranciers zijn beveiligingseisen en prestatie-indicatoren opgenomen, maar niet op basis van een expliciete risicoafweging bepaald.
- Er zijn geen duidelijke afspraken met leveranciers over hoe de volledige keten van leveranciers wordt beveiligd.
- In de productieomgeving wordt niet getest. Echter, de afwijkende procedure is niet goed ingericht.
- Binnen de organisatie is geen overzicht van logbestanden die gegeneerd worden.
- In het inkoopproces is informatiebeveiliging nog niet op de juiste manier geborgd.

Verbetermaatregelen

- 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.
- Eind 2024 is er een back-up beleid vastgesteld, deze was voor eind 2024 nog niet getoetst op alle applicaties.
- De implementatie was gepland voor 2024, maar vanwege het ontbreken van technische middelen is dit uitgesteld. Hierdoor wordt dit meegenomen in het project de moderne werkplek.

- Dit punt was buiten scope voor 2024 en wordt opgepakt in 2025 in het project Cyberbeveiligingswet/ BIO 2.0. De verwachting is om dit in 2026 compleet te hebben.
- Wordt in 2025 meegenomen in het project Cyberbeveiligingswet/ BIO 2.0. Hiervoor wordt een procedure opgesteld voor nieuwe overeenkomsten, de huidige overeenkomsten zijn buiten scope.
- Wordt meegenomen in het project Cyberbeveiligingswet/ BIO 2.0.
- Dit wordt meegenomen in de procedures vanuit informatievoorzieningen over wijzigingen en testen.
- In 2025 wordt er op basis van een risico afweging een lijst gemaakt en deze wordt daarna langzamerhand aangevuld.
- Dit wordt meegenomen in het project Cyberbeveiligingswet/ BIO 2.0.

Kanttekening

- In 2023 / 2024 zijn bepaalde beleidsstukken vastgesteld maar er zijn op dit moment niet de technische middelen om ze in werking te stellen. Hierdoor is het opstaande tekortkoming niet opgelost. Dit wordt opgepakt in het project De Moderne Werkplek
- In 2023 zou er een procedure voor installeren/downloaden van software worden opgesteld, dit is doorgeschoven naar 2024. Door ontbreken technische middelen is dit verplaatst naar 2025. Beleid opstellen maar het niet afdwingen waar mogelijk heeft niet de voorkeur van de organisatie.

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.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

- Informatie is geclassificeerd op basis van een risicoafweging, maar is niet gelabeld.
- Er wordt alleen gebruikgemaakt van PKI Overheidscertificaten. Er zijn geen afspraken met andere leveranciers over reservecertificaten.
- Er is geen beleid of procedure voor informatietransport.

Verbetermaatregelen

- Eind 2024 is hiervoor het beleid vastgesteld, het informatieclassificatie beleid binnen de gemeente. Echter is dit beleid nog niet volledig doorgevoerd en daarmee is hier ook niet aan voldaan. In 2025 zal dit wel gebeuren.
- Begin 2025 is er een cryptografiebeleid vastgesteld, hierin is het standpunt over reserve certificaten vastgelegd, dit is nog niet (volledig) getoetst op de huidige situatie.
- Er is begin 2025 een beleid vastgesteld over informatietransport.

Kanttekening

- Er is in 2025 een leverancier aangetrokken die het certificaat beheer voor de gemeente Waterland gaat doen. De gemeente is enkel nog verantwoordelijk voor de regie op het certificatenbeheer..

5.7. Algemene verbetermaatregelen.

In 2024 heeft de gemeente vooral de focus gelegd op het voorbereiden van de aanbesteding en uitvoering voor de Digitale Moderne Werkplek, ook wel ‘Het nieuwe werken’ genoemd. In september 2024 is deze aanbesteding succesvol afgerond en per oktober 2024 is de gemeente begonnen met de inventarisatie die nodig is voor het aanpakken van dit grote project. In 2025 zal dit project worden afgerond. In dit project worden een hoop BIO maatregelen meegenomen waaraan nu nog niet wordt voldaan, waaronder ook maatregelen die in BIO 1.4 nog niet waren opgenomen.

Daarnaast start de gemeente tegelijkertijd een project Cyberbeveiligingswet/ BIO 2.0 om hiermee eind 2025 zo veel mogelijk te voldoen aan de BIO 2 en aan de Cyberbeveiligingswet. De verwachting is dat de gemeente eind 2025 nog niet volledig voldoet maar wel indien nodig aan een toezichthouder kan laten zien welke stappen er reeds zijn genomen en welke de gemeente nog gaat nemen. Op deze manier kan de gemeente aantonen dat het zo genoemd ‘in control is’ over de transitie naar de Cyberbeveiligingswet en de daarbij behorende BIO 2.0.

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 IBD.

Meldingen 2024

In 2024 zijn meerdere meldingen geweest waarvan er 20 meldingen zijn geclassificeerd (wat een verdubbeling is ten opzichte van vorig jaar) als mogelijke beveiligingsincident/datalek en opgenomen in het meldingenregister.

Het grootste risico waar de gemeente dit jaar drie keer mee te maken heeft gehad, is dat een bekende/ betrouwbare leverancier gehackt is en dat vanuit deze leverancier een phishingmail gestuurd is. Deze phishing mail was ook wel het zo bekende Man In the Middle Attack (MitMA) waarbij er een mail met een offerte, factuur etc. wordt verstuurd waarbij de ontvanger eerst moet inloggen via het Microsoft-account. Deze aanval steelt dan de inlog gegevens van de ontvanger. In één van de gevallen is dit binnen de gemeente ook fout gegaan en zijn er inlog gegevens gelekt. Mede door adequaat reageren van de desbetreffende medewerker en het securityteam is verdere schade voorkomen. Om dit met zekerheid uit te sluiten is er in dit specifieke geval ook een specialistische partij ingehuurd die onderzoek heeft gedaan of dat hacker ook gegevens heeft gestolen en dit was niet het geval. De gemeente is bij dit incident uiteindelijk ternauwernood aan schade ontsnapt.

Verder heeft de gemeente veelal last gehad van een phishing techniek die Whaling genoemd wordt. Hierbij wordt er door de aanvaller zich voorgedaan als een hooggeplaatste persoon binnen de organisatie. De meest voorkomende functie die hiervoor is gekozen is de CISO. Nieuwe medewerkers zijn het doelwit van deze campagnes met het idee dat zij de organisatie nog niet zo goed kennen en daardoor eerder vatbaar zijn voor dit soort aanvallen. Deze aanvallen zijn tot nu toe altijd nog tijdig onderschept mede door de SIEM/SOC-partij die sinds Q3 2024 voor Waterland actief is. Deze partij monitort het netwerk van de gemeente 24/7.

- Er zijn meerdere meldingen van phishing/ CEO-fraude (phishing voor financieel gewin) geweest. Hier is adequaat op gehandeld zonder nadelige gevolgen. Daarnaast zijn de procedures nogmaals doorsproken met de desbetreffende afdelingen.
- Er komen periodiek meldingen van (technische) kwetsbaarheden binnen bij de gemeente waarvan de meeste niet van toepassing zijn of direct met onze leveranciers gedeeld worden. Er waren meerdere technische kwetsbaarheden die snel en adequaat opgelost moesten worden. Er zijn (voor zover bekend) geen nadelige gevolgen van ondervonden; Vaak worden deze direct door een leverancier opgelost zonder tussenkomst van de gemeente.

Bijlage 1: Tekst Collegeverklaring ENSIA 2024

Vanwege het openbare karakter van deze jaarrapportage is alleen de tekst van de Collegeverklaring, exclusief de bijlagen DigiD en Suwinet opgenomen omdat deze vertrouwelijke detailinformatie bevatten. De verantwoording over DigiD en Suwinet is op hoofdlijnen opgenomen in hoofdstuk 3 van deze jaarrapportage.

Doel en achtergrond verklaring

De aansluitingen die we als gemeente voor DigiD en Suwinet hebben, vereisen dat voorzieningen moeten zijn beveiligd en (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. De gemeente treft interne beheersingsmaatregelen om veilig gebruik te maken van deze aansluitingen.

Met deze verklaring geven wij, het College van Burgemeester en Wethouders, aan in welke mate de gemeente voldoet aan de informatiebeveiligingsnormen voor DigiD en Suwinet. Deze verklaring maakt onderdeel uit van de verantwoording over informatiebeveiliging middels ENSIA[1] en is tot stand gekomen door een zelfevaluatie over informatiebeveiligingsnormen gebaseerd op de door de toezichthouder geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv voor Suwinet en de 'Norm ICT-beveiligingsassessments DigiD versie 3.0' van Logius. De inhoud van deze collegeverklaring is getoetst door een onafhankelijke IT-auditor/RE.

Deze verklaring is bestemd voor de toezichthouders van DigiD en Suwinet, te weten Logius, en alsmede de stelselhouder: het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en de toezichthouder van Suwinet, te weten het Ministerie van Sociale Zaken en Werkgelegenheid via het Bureau Keteninformatie Werk en Inkomen (BKWI).

Reikwijdte en diepgang verklaring

De aansluitingen die we als gemeentelijke organisatie voor DigiD en Suwinet hebben, vereisen dat onze voorzieningen moeten zijn beveiligd en dat (privacygevoelige) data moet worden beschermd tegen onrechtmatig gebruik. Hiervoor stellen de stelselhouders een aantal informatiebeveiligingsnormen verplicht. De gemeentelijke organisatie moet interne beheersingsmaatregelen treffen om te voldoen aan deze gestelde normen teneinde gebruik te mogen (blijven) maken van deze aansluitingen.

De zelfevaluatie ENSIA gaat over de opzet en het bestaan van deze beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2024. Voor DigiD wordt het door Logius vastgestelde Norm ICT-beveiligingsassessments DigiD versie 3.0 gehanteerd. Daarbij zijn normen getoetst op werking.

Voor Suwinet de Verantwoordingsrichtlijn GeVS 2022 (tevens geldend voor het verslagjaar 2024) waarin zijn opgenomen de geselecteerde eisen uit de 'Baseline Informatiebeveiliging Overheid' versie 1.04zv. Deze Verantwoordingsrichtlijn betreft opzet, bestaan en werking van de interne beheersingsmaatregelen. In het kader van de zelfevaluatie ENSIA zijn geen werkzaamheden uitgevoerd met betrekking tot de werking van deze maatregelen.

Collegeverklaring en samenvattend beeld van de auditbevindingen

Verklaring / Conclusie

Het college van Burgemeester en Wethouders van de Gemeente Waterland verklaart dat de gemeentelijke organisatie op 31 december 2024 voldoet aan alle geselecteerde normen inzake DigiD en Suwinet.

Samenvattend beeld

Deze collegeverklaring betreffende de gemeentelijke organisatie en de serviceorganisaties dekt de geslecteerde normen inzake DigiD en Suwinet af. Het detailoverzicht van normen en of we hier als gemeente aan voldoen, is opgenomen in de volgende bijlagen:

- Bijlage 1 DigiD met kenmerk 7929-2025:992003
- Bijlage 2 Suwinet met kenmerk 7929-2025:346273

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
DigiD **1005565**	Ja	Niet van toepassing
Suwinet voor SUWI-taken	Ja	Niet van toepassing
Suwinet voor niet-SUWI-taken	Ja	Niet van toepassing

Namens het College van B&W Gemeente Waterland

drs. E.G.H. Dijk MPM
gemeentesecretaris/algemeen directeur

drs. M.C. van der Weele
burgemeester