Jaarrapportage informatieveiligheid en privacy 2020 Gemeente Waterland



Gemeente Waterland

Inhoud

1. Inleiding 3
2. Samenvatting resultaten zelfevaluatie 2020 4
3. Uitkomsten IT audit DigiD en Suwinet 6
3.1. DigiD 6
3.2. Suwinet 6
3.3. Collegeverklaring DigiD en Suwinet en assurancerapport IT auditor 7
4. Uitkomsten BRP en Reisdocumenten..... 7
4.1. Inleiding 7
4.2. BRP 7
4.3. Reisdocumenten..... 7
5. Status BIO 7
5.1. BIO hoofdstuk 2: Opzet van de BIO 8
5.2. BIO hoofdstuk 4: Verantwoording over de BIO 8
5.3. BIO hoofdstuk 5: Informatiebeveiligingsbeleid 9
5.4. BIO hoofdstuk 6: Organiseren van informatiebeveiliging 9
5.5. BIO hoofdstuk 7: Veilig personeel 9
5.6. BIO hoofdstuk 8: Beheer van bedrijfsmiddelen 10
5.7. BIO hoofdstuk 9: Toegangsbeveiliging 10
5.8. BIO hoofdstuk 10: Cryptografie 11
5.9. BIO hoofdstuk 11: Fysieke beveiliging en beveiliging van de omgeving 11
5.10. BIO hoofdstuk 12: Beveiliging bedrijfsvoering 11
5.11. BIO hoofdstuk 13: Communicatiebeveiliging 12
5.12. BIO hoofdstuk 14: Acquisitie, ontwikkeling en onderhoud van informatiesystemen 12
5.13. BIO hoofdstuk 15: Leveranciersrelaties 13
5.14. BIO hoofdstuk 16: Beheer van informatiebeveiligingsincidenten 13
5.15. BIO hoofdstuk 17: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 14
5.16. BIO hoofdstuk 18: Naleving 14
6. Algemene Verordening Gegevensbescherming (AVG) 14
7. Incidenten 15

Bijlagen:

1. Tekst Collegeverklaring ENSIA 2020 16

Overige bijlagen:

(separaat vastgesteld door het college en daarna als bijlage bij de Jaarrekening op te nemen)

Verantwoordingsrapportage BAG 2020, kenmerk 18941-2020: 691127

Verantwoordingsrapportage BGT 2020, kenmerk 18941-2020: 724643

Verantwoordingsrapportage BRO 2020, kenmerk 18941-2020: 202692

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), hét basisnormenkader voor informatieveiligheid en wet- en regelgeving, waaronder 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 gemeente-brede uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2020. Deze zelfevaluatie is dat jaar voor het eerst gebaseerd op de BIO en is uitgevoerd in de periode juli t/m december 2020. 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 deze jaarrapportage aan op de gemeentelijke 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 en de status van maatregelen en verplichtingen op grond van de AVG.

In verband met het openbare karakter van de rapportage is geen detailinformatie opgenomen.

IT audit over DigiD en Suwinet

Voor 2020 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 assurancerapport. Met de vastgestelde Collegeverklaring en het assurancerapport voldoen wij aan de verantwoordingsplicht voor DigiD en Suwinet. 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.

Bestuurlijke verantwoording over de BAG, BGT en BRO

Voor de BAG, BGT en BRO zijn over 2020 separate zelfevaluaties in ENSIA uitgevoerd. De domein specifieke verantwoordingsrapportages BAG, BGT en BRO zijn als bijlage bij deze jaarrapportage opgenomen. De scores zijn opgenomen in de samenvatting resultaten zelfevaluatie 2020 (hoofdstuk 2).

2. Samenvatting resultaten zelfevaluatie 2020

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

Zelfevaluatie	Norm	Score Gemeente Waterland
BRP domeinvragen Kwaliteitsmonitor RvIG BRP informatiebeveiligingsvragen ENSIA Samengevoegd resultaat 2020 *Samengevoegd resultaat 2019*	 90% *90%*	791 punten van 800 (98,9%) 1.145 punten van 1.200 (95%) 1.936 punten van 2.000 (96,8%) *1.796 punten van 2.000 (89,8%)*
Reisdocumenten domeinvragen Kwaliteitsmonitor RvIG Reisdocumenten informatiebeveiligingsvragen ENSIA Samengevoegd resultaat *Samengevoegd resultaat 2019*	 90% *90%*	1.283 punten van 1.350 (95%) 620 punten van 650 (95%) 1903 punten van 2.000 (95,1%) *1.827 punten van 2.000 (91,3%)*
BAG	75%	59% *2019 83%*
BGT	75%	57% *2019 60%*
BRO	60%	92% *2019 54,2%*

De BIO omvat verdeeld over de hoofdstukken in totaal 167 maatregelen en 107 sub-vragen of deze maatregelen (ook) toegepast worden op de BRP, reisdocumenten en Suwinet.
Van de 167 maatregelen is aan 24 maatregelen niet voldaan.

BIO (hoofdstuk) – Maatregelen per januari 2020:	Aantal maatregelen	Maatregelen waaraan niet is voldaan	Conclusie Gemeente Waterland
BIO (h2) – Opzet van de BIO	4	4	Voldoet niet
BIO (h4) – Verantwoording over de BIO	3	1	Voldoet niet
BIO (h5) – Informatiebeveiligingsbeleid	1	1	Voldoet niet
BIO (h6) – Organiseren van informatiebeveiliging	16	-	Voldoet
BIO (h7) – Veilig personeel	7	1	Voldoet niet
BIO (h8) – Beheer van bedrijfsmiddelen	9	1	Voldoet niet
BIO (h9) – Toegangsbeveiliging	28	2	Voldoet niet
BIO (h10) – Cryptografie	5	1	Voldoet niet
BIO (h11) – Fysieke beveiliging en beveiliging van de omgeving	13	-	Voldoet
BIO (h12) – Beveiliging bedrijfsvoering	26	6	Voldoet niet
BIO (h13) - Communicatiebeveiliging	10	-	Voldoet
BIO (h14) – Acquisitie, ontwikkeling en onderhoud van informatiesystemen	7	2	Voldoet niet
BIO (h15) – Leveranciersrelaties	12	3	Voldoet niet
BIO (h16) – Beheer van informatiebeveiligingsincidenten	12	-	Voldoet
BIO (h17) – Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	4	-	Voldoet
BIO (h18) – Naleving	10	2	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 999913 Digitaal Loket gemeente Waterland. De verantwoording aan de stelselhouder BZK/Logius vindt plaats door middel van de Collegeverklaring. Deze omvat het op 31 december 2020 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.

Bevindingen

Voor DigiD aansluitnummer 999913 wordt door gemeente Waterland aan één van de geselecteerde normen niet voldaan. De tekortkoming betreft het Informatiebeveiligingsplan dat in 2020 niet is geactualiseerd. Hiervoor is een verbeterplan opgesteld en de verbetermaatregel is belegd en wordt gemonitord.

Uit de verantwoording van de dienstverlener bleek dat ook voor de beheersingsmaatregelen die zijn uitbesteed niet aan alle normen wordt voldaan. De verbetermaatregelen zijn belegd bij de dienstverlener en worden door de gemeente Waterland gemonitord.

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 Halte Werk (Zelfstandigenloket). De Collegeverklaring omvat het op 31 december 2020 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake Suwinet.

Bevindingen

Voor zowel de Suwinet-taken als niet Suwi-taken wordt aan één van de geselecteerde normen inzake Suwinet niet voldaan. De tekortkoming betreft het ontbreken van een procedure voor het bevorderen en adequaat houden van i-bewustzijn. Er is in 2020 organisatie breed aandacht besteed aan het bevorderen van het bewustzijn, maar een procedure ontbreekt. Hiervoor is een verbeterplan opgesteld. De verbetermaatregel is belegd, inmiddels opgepakt en wordt gemonitord.

3.3. Collegeverklaring DigiD en Suwinet en assurancerapport IT auditor

De onafhankelijke IT auditor heeft op basis van de Collegeverklaring een voorlopig assurancerapport afgegeven. Naar oordeel van de IT auditor is de Collegeverklaring ENSIA 2020 inzake informatiebeveiliging van DigiD en Suwinet in alle van materieel belang zijnde aspecten juist. De Collegeverklaring informatiebeveiliging DigiD en Suwinet is vastgesteld op 20 april 2021, waarna de definitieve assurance van de IT auditor volgt. De tekst van de Collegeverklaring treft u aan in bijlage 1.

4. Uitkomsten BRP en Reisdocumenten

4.1. Inleiding

Over 2020 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 in februari 2021 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 1.936 punten van de maximaal 2.000 punten. Dat geeft een percentage van 96,8%.

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 goed scoort op de beveiliging en overige aspecten van het aanvraag- en uitgifteproces. Het samengevoegd resultaat van de domein- en informatiebeveiligingsvragen is 1.903 punten van de maximaal 2.000 punten. Dat geeft een percentage van 95,1%.

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. De vragen over de BIO-maatregelen zijn verdeeld over een aantal hoofdstukken. Als van een hoofdstuk aan één 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.

5.1. BIO hoofdstuk 2: Opzet 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 2020 zijn processen grotendeels vastgelegd. In 2021 worden rondom deze processen de risico's, controls, maatregelen en verantwoordelijkheden vastgelegd.

5.2. BIO hoofdstuk 4: Verantwoording over de BIO

De verantwoording over de toepassing van de BIO maakt onderdeel uit van de bestuurlijke verantwoording over informatiebeveiliging. De BIO kent drie basisbeveiligingsniveaus met bijbehorende beveiligingseisen voor de overheid. BBN 1 is wat minimaal verwacht mag worden. BBN 2 valt onder goed huisvaderschap, de betrouwbare overheid en is vergelijkbaar met voorheen de Baseline Informatiebeveiliging Gemeenten BIG). Voor BBN 3 (departementaal vertrouwelijk) geldt dat vooraf toestemming voor het verwerken van bijzondere informatie verleend moet worden door de gemeentesecretaris/algemeen directeur. Voor de gemeente Waterland is BBN 3 niet van toepassing.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

Waterland heeft nog geen registratie van maatregelen waaraan niet of nog niet geheel kan worden voldaan. Deze Zelfevaluatie BIO vormt daartoe een nulmeting, maar is geen feitelijke registratie vanuit het 'pas toe of leg uit' principe met vermelding van de risico's.

Verbetermaatregel

In 2021 worden de controls en maatregelen vastgelegd, integraal in het kennisplatform Mavim.

5.3. BIO hoofdstuk 5: Informatiebeveiligingsbeleid

Voor informatiebeveiliging behoort een beleidsregels te worden gedefinieerd, goedgekeurd, gepubliceerd, gecommuniceerd aan medewerkers en relevante externe partijen en periodiek te worden geëvalueerd.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

Voor Suwinet, BRP en Reisdocumenten zijn het beveiligingsplan en -procedures in 2020 geactualiseerd. Het Privacy beleid was nog actueel. Het (algemene) Informatiebeveiligingsbeleid/-plan is niet meer actueel.

Verbetermaatregel

Actualisatie van het informatiebeveiligingsbeleid/-plan is in behandeling en vaststelling vindt plaats in 2021.

5.4. BIO hoofdstuk 6: Organiseren van informatiebeveiliging

Alle rollen en verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen, waarbij conflicterende taken en verantwoordelijkheden zijn gescheiden. Met relevante overheidsorganisaties worden passende contacten onderhouden. Beleid en ondersteunende maatregelen ter beveiliging van informatie vanaf telewerklocaties en het beheren van risico's ten aanzien van het gebruik van mobiele apparatuur behoren te zijn geïmplementeerd.

Bevindingen

Aan deze maatregelen is voldaan.

5.5. BIO hoofdstuk 7: Veilig personeel

Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en in verhouding te staan tot de organisatie-eisen en informatie waartoe toegang wordt verleend. De verantwoordelijkheden voor en toepassing van informatiebeveiliging in overeenstemming met de beleidsregels en procedures behoren in een overeenkomst te worden vastgelegd. Alle medewerkers behoren een passende bewustzijnsopleiding/-training te krijgen, nieuwe medewerkers binnen drie maanden na indiensttreding, en regelmatige bijscholing van beleidsregels en procedures voor zover relevant voor hun functie.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

Jaarlijks is er organisatie breed aandacht voor bewustzijn. Nieuwe medewerkers ontvangen een instructie inclusief het zorgvuldig omgaan met (persoons)gegevens. Het binnen drie maanden na indiensttreding volgen van een training i-bewustzijn is nog niet geregeld.

Verbetermaatregel

Dit wordt in 2021 in samenwerking met HR opgepakt.

5.6. BIO hoofdstuk 8: Beheer van bedrijfsmiddelen

Voor het aanvaardbaar gebruik van informatie en bedrijfsmiddelen behoren regels te worden geïmplementeerd. Informatie moet worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid. Media behoren te worden beschermd tegen onbevoegde toegang, misbruik en corruptie tijdens transport en op een veilige manier te worden verwijderd.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

Media is beschermd en op media wordt alle data door de Servicedesk zorgvuldig verwijderd, maar niet door deze eerst een aantal keren te overschrijven met data.

Verbetermaatregel

Voor 2021 is dit in de werkinstructie opgenomen.

5.7. BIO hoofdstuk 9: Toegangsbeveiliging

Beleid voor toegangsbeveiliging behoort te worden vastgesteld en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. Gebruikers behoren alleen toegang te krijgen tot het netwerk en de informatie waarvoor zij specifiek bevoegd zijn. Voor de toegang van gebruikers en de toewijzing van toegangsrechten is een formele registratie- en afmeldingsprocedure geïmplementeerd. Speciale toegangsrechten worden beperkt en beheerst. De toegangsrechten worden regelmatig beoordeeld.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

Speciale bevoegdheden en toegangsrechten voor systemen worden regelmatig gecontroleerd. Speciale bevoegdheden echter nog niet minimaal ieder kwartaal en niet voor alle systemen worden de toegangsrechten minimaal één keer per half jaar beoordeeld.

Verbetermaatregel

Op onderdelen wordt de frequentie van de controles in 2021 aangescherpt.

5.8. BIO hoofdstuk 10: Cryptografie

Ter bescherming van informatie behoort beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd. Inclusief beleid met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

De gemeente Waterland hanteert de beveiligingsstandaarden conform de normen van Forum voor Standaardisatie (beveiligingsstandaarden ten aanzien van de website(s) en e-mail) en hanteert de PKI Overheid-eisen voor het beheer van cryptografische sleutels. Er zijn echter geen afspraken gemaakt over reserve-certificaten met een tweede leverancier.

Verbetermaatregel

Dit wordt in 2021 afgestemd met de dienstverlener ICT-infrastructuur.

5.9. BIO hoofdstuk 11: Fysieke beveiliging en beveiliging van de omgeving

Beveiligingszones behoren te worden gebruikt om gebieden te beschermen die gevoelige of essentiële informatie(faciliteiten) bevatten. De gebieden moeten worden beschermd door passende toegangsbeveiliging om er voor te zorgen dat alleen bevoegd personeel toegang krijgt, fysieke beveiliging dient te zijn toegepast als ook bescherming tegen bedreigingen van buitenaf. Apparatuur en informatie mogen niet zonder voorafgaande goedkeuring van de locatie worden meegenomen en de bedrijfsmiddelen die zich buiten het terrein bevinden behoren te worden beveiligd. Er behoort een ‘Clear desk’ en ‘Clear Screen’-beleid te worden ingesteld.

Bevindingen

Aan deze maatregelen is voldaan.

5.10. BIO hoofdstuk 12: Beveiliging bedrijfsvoering

Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben. Veranderingen in de organisatie, processen en informatie verwerkende systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst. Ontwikkel-, test- en productieomgevingen moeten zijn gescheiden. Ter bescherming van malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd in combinatie met een passend bewustzijn van gebruikers. Regelmatig behoren back-ups te worden gemaakt en getest overeenkomst een overeengekomen back-upbeleid. Logbestanden van (informatiebeveiliging)gebeurtenissen behoren te worden gemaakt, beschermd en regelmatig te worden beoordeeld. Informatie over technische kwetsbaarheden behoort tijdig te worden verkregen. De blootstelling aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en passende maatregelen te worden genomen.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

Het back-upbeleid en de procedure voor wijzigingenbeheer moeten in 2021 nog worden geactualiseerd naar de situatie van de uitbesteding van de ICT-infrastructuur- en beheerdiensten. Voor het downloaden van bestanden zijn maatregelen genomen, echter niet op basis van een specifieke risicoanalyse. De organisatie beschikt, met uitzondering van een aantal kritische processen, nog niet over een volledig overzicht van logbestanden die worden gegenereerd.

Verbetermaatregel

Deze maatregelen en procedures worden meegenomen bij het actualiseren dan wel nieuw op te stellen informatiebeveiligingsbeleid/-plan in 2021.

5.11. BIO hoofdstuk 13: Communicatiebeveiliging

Beveiligingseisen voor netwerkdiensten en dienstverleningsniveaus worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Diensten, systemen en gebruikers behoren in netwerken te worden gescheiden. Informatie opgenomen in elektronische berichten behoren passend te zijn beschermd. Hiervoor wordt gebruik gemaakt van de vaste open standaarden van het Forum Standaardisatie en de PKI Overheid-certificaten. Voor het signaleren en reageren op aanvallen die de beschikbaarheid negatief beïnvloeden zijn maatregelen getroffen. Ontdekte nieuwe dreigingen worden, rekening houdend met geldende juridische kaders, gedeeld binnen de overheid.
Er wordt gebruik gemaakt van geheimhoudingsovereenkomsten conform de Ambtenarenwet.

Bevindingen

Aan deze maatregelen is voldaan.

5.12. BIO hoofdstuk 14: Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Eisen voor informatiebeveiliging behoren te worden opgenomen in eisen voor nieuwe of uitbreiding van bestaande informatiesystemen. Voor de ontwikkeling van software en systemen behoren regels te worden vastgesteld en toegepast. Wijzigingen behoren te worden beheerst door gebruik van formele procedures voor wijzigingsbeheer. Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie. Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

Bij nieuwe of wijziging op bestaande informatiesysteem vindt niet altijd een expliciete risicoafweging plaats. Niet van alle acceptatietesten worden verslagen gemaakt.

Verbetermaatregel

In 2021 worden processen, risico's en controls/maatregelen op basis van risicoanalyses vastgelegd.

5.13. BIO hoofdstuk 15: Leveranciersrelaties

Met leveranciers behoren informatiebeveiligingseisen te worden overeengekomen en vastgelegd om risico's te verlagen die verband houden met de toegang van leveranciers tot de bedrijfsmiddelen van de organisatie. Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met leveranciers en organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkoming

Bij offerteaanvragen waar informatievoorziening een rol speelt worden beveiligingseisen ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie expliciet benoemd. Dit gebeurt echter nog niet in alle gevallen op basis van een expliciete risicoafweging.

Verbetermaatregel

In 2021 worden processen, risico's en controls/maatregelen op basis van risicoanalyses vastgelegd.

5.14. BIO hoofdstuk 16: Beheer van informatiebeveiligingsincidenten

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. Medewerkers en contractanten die gebruik maken van de informatiesystemen van de organisatie behoren waargenomen of vermeende zwakke plekken in de informatiebeveiliging te registreren en rapporteren. Incidenten behoren te worden beoordeeld en kennis die is verkregen door incidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid en impact van toekomstige incidenten te verkleinen. Informatie die als bewijs kan dienen wordt verzameld en bewaard.

Bevindingen

Aan deze maatregelen is voldaan.

5.15. BIO hoofdstuk 17: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

De organisatie behoort haar eisen voor informatiebeveiliging en continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijvoorbeeld een crisis of ramp, vast te stellen. De ten behoeve van de continuïteit vastgestelde en geïmplementeerde beheersmaatregelen behoren regelmatig te worden geverifieerd om te waarborgen dat ze deugdelijk en doeltreffend zijn.

Bevindingen

Aan deze maatregelen is voldaan.

5.16. BIO hoofdstuk 18: Naleving

Alle relevante wetgeving en contractuele eisen en de aanpak van de organisatie om daaraan te voldoen behoren voor elk informatiesysteem van de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden. Registraties behoren in overeenstemming hiermee te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave. De privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, behoren onafhankelijk en met geplande tussenpozen of bij belangrijke veranderingen te worden beoordeeld. De directie behoort regelmatig de naleving van informatieverwerking en -procedures te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen.

Bevindingen

Aan deze maatregelen is niet voldaan.

Tekortkomingen

De organisatie beschikt nog niet over goed ingericht Information Security Management System (ISMS). Het beschikbare ISMS voldeed niet aan de verwachtingen en was onvoldoende ingericht.

Verbetermaatregel

In 2021 wordt een ISMS tool, waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt, ingericht in het Management Control Framework in Mavim.

6. Algemene Verordening Gegevensbescherming (AVG)

Voor de datum van inwerkingtreding van de AVG (25 mei 2018) had de gemeente Waterland al een proces ingericht in het kader van de Meldplicht Datalekken en een Functionaris Gegevensbescherming (FG) aangesteld. In 2019 heeft de gemeente Waterland haar Privacy beleid vastgesteld en gepubliceerd op Mijn Overheid.

Op de website is een digitaal formulier geplaatst dat is gekoppeld aan DigiD en waarmee inwoners verzoeken in kunnen dienen over de verwerking van hun persoonsgegevens.
In 2020 zijn drie inzageverzoeken behandeld.

Jaarlijks wordt organisatie breed aandacht besteed aan bewustwording over beveiliging en privacy. In het eerste kwartaal van 2020 is voor alle teams een presentatie 'Informatiebeveiliging en privacy' gehouden.

7. 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 2020

In 2020 zijn 24 meldingen van mogelijke beveiligingsincidenten/datalekken ontvangen en opgenomen in het meldingenregister:

- 3 meldingen van CEO-fraude (phishing voor financieel gewin). Daar is adequaat op gereageerd zonder nadelige gevolgen. Twee fraudepogingen zijn ter informatie gemeld aan de IBD;
- 17 meldingen van (technische) kwetsbaarheden waarvan 7 niet van toepassing bleken te zijn en 10 snel en adequaat zijn opgelost. Er zijn geen nadelige gevolgen van ondervonden;
- 4 mogelijke incidenten waarbij persoonsgegevens waren betrokken. Twee, niet zijnde datalekken, zijn direct bij ontdekking opgelost. Twee incidenten zijn als datalekken gemeld bij de Autoriteit Persoonsgegevens. Na onderzoek is één melding ingetrokken. Het andere incident was snel opgelost zonder nadelige gevolgen. Er zijn geen datalekken gemeld aan betrokkenen.

Daarnaast zijn 2 aanbevelingen en 3 kwetsbaarheidswaarschuwingen waar uiteindelijk geen hinder van is ondervonden, vermeld.

Bijlage 1: Tekst Collegeverklaring ENSIA 2020

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

Met deze verklaring geven wij, het college van burgemeester en wethouders, aan in welke mate de gemeente Waterland 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. De inhoud wordt getoetst door een onafhankelijke IT-auditor.

De verklaring is bestemd voor de stelselhouders van DigiD en Suwinet, te weten het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Sociale Zaken en Werkgelegenheid.

Reikwijdte en diepgang verklaring

De toetsing gaat over de opzet en het bestaan van de beheersingsmaatregelen om te kunnen voldoen aan de relevante beveiligingsnormen voor DigiD en Suwinet op 31 december 2020.

Inzake Suwinet heeft deze collegeverklaring zowel betrekking op de beheersingsmaatregelen van de gemeente als op die van de uitbestede diensten aan GR-BVO Halte Werk (Zelfstandigenloket).

De beheersingsmaatregelen inzake DigiD en Suwinet die zijn uitbesteed aan dienstverleners worden niet getoetst door de auditor. Deze collegeverklaring en de verantwoording van de dienstverleners dekken tezamen de normen inzake DigiD en Suwinet af. Het overzicht van normen, eventuele afwijkingen en waar deze belegd zijn, is opgenomen in de bijlagen:

bijlage 1 DigiD met kenmerk 18941-2020:063431

bijlage 2 Suwinet met kenmerk 18941-2020:912735

Verklaring college

Het college verklaart dat voor DigiD en Suwinet niet aan alle normen wordt voldaan. Wij hebben verbeterplannen opgesteld om aan de normen te voldoen, de acties zijn belegd en worden gemonitord.

(1) ENSIA ondersteunt de gemeente bij de verantwoording over informatiebeveiliging richting de gemeenteraad en de rijksoverheid. ENSIA gaat uit van de Baseline Informatiebeveiliging Overheid (BIO), alsmede van informatiebeveiligingsnormen vanuit Basisregistratie Personen (BRP), wet- en regelgeving reisdocumenten (PUN, PNIK), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Samenvattend beeld

Onderwerp	Wordt aan alle normen voldaan?	Zijn de uitzonderingen in verbeterplannen opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord?
Digid (1) 999913	Nee	Ja
Suwinet voor SUWI-taken	Nee	Ja
Suwinet voor niet-SUWI-taken	Nee	Ja

Monnickendam, 20 april 2021

College van burgemeester en wethouders gemeente Waterland,