Jaarrapportage informatieveiligheid en privacy 2017

Gemeente Waterland

Inhoud

1. Inleiding

Deze rapportage geeft op hoofdlijnen de uitkomsten weer van de gemeente-brede uitgevoerde zelfevaluatie informatieveiligheid over het jaar 2017. In verband met het openbare karakter van de rapportage is geen detailinformatie opgenomen.

De zelfevaluatie is gebaseerd op de Baseline Informatieveiligheid Gemeenten (BIG), hét gemeentelijk basisnormenkader voor informatieveiligheid, voortgekomen uit de VNG resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente'. 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 BIG en wet- en regelgeving, ook op het gebied van privacy.

Als gemeente Waterland kunnen we nu op één moment in het jaar rapporteren over de status van onze informatieveiligheid. De methodiek daarvoor is de 'Eenduidige Normatiek Single Information Audit' (ENSIA). Via ENSIA wordt horizontaal verantwoording afgelegd aan de gemeenteraad en verticaal aan de toezichthouders van de rijksoverheid. Verantwoording wordt afgelegd over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet). Daarnaast wordt de status van informatieveiligheid in brede zin conform de BIG verantwoord. De beantwoording van de zelfevaluatievragen is door bewijsdocumenten onderbouwd.

IT audit over DigiD en Suwinet

Voor het jaar 2017 geldt dat de verantwoording over DigiD en Suwinet aan de stelselhouders Logius en het ministerie van SZW wordt verantwoord door middel van een Collegeverklaring. De Collegeverklaring is opgesteld op basis van de bevindingen uit de zelfevaluatie en deze is getoetst door een onafhankelijke IT auditor. De uitkomsten uit de zelfevaluatie DigiD en Suwinet zijn op hoofdlijnen in deze jaarrapportage opgenomen. De tekst van de Collegeverklaring treft u aan in de bijlage.

Separate bestuurlijke verantwoording over BAG en BGT

De informatieveiligheidsvragen maken deel uit van de zelfevaluatie BIG (hoofdstuk 4).
De domein specifieke verantwoording is niet in deze jaarrapportage opgenomen. Door middel van de bestuurlijke verantwoordingsrapportage BAG en de bestuurlijke verantwoordingsrapportage BGT wordt hierover separaat verantwoording afgelegd aan de gemeenteraad.

Periode zelfevaluatie en verantwoording

Het verantwoordingsjaar is 2017. Voor 1 januari 2018 moest de zelfevaluatie via ENSIA worden ingeleverd en beschikbaar zijn voor de toezichthouders. De deadline voor de verantwoordingsrapportages BAG en BGT, de Collegeverklaring inzake DigiD en Suwinet en de Assurance-rapportage van de IT-auditor was 1 mei 2018.
De gemeente Waterland heeft daar ruim aan voldaan.

2. Uitkomsten IT audit DigiD en Suwinet

2.1 DigiD

De verantwoording over 2017 betreft DigiD aansluiting 999913 Digitaal Loket gemeente Waterland. De verantwoording aan de stelselhouder Logius vindt plaats door middel van de Collegeverklaring. Deze omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake DigiD. De beheersingsmaatregelen inzake DigiD 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 de gemeente Waterland niet aan alle geselecteerde normen voldaan. De op de uitzondering gerichte beheersmaatregel, waardoor aan één norm niet geheel werd voldaan, is in een verbeterplan opgenomen en belegd. De uitvoering van deze maatregel vindt plaats in het 2e kwartaal 2018.

Uit de verantwoording van de dienstverlener bleek dat niet aan alle geselecteerde normen werd voldaan. De uitbestede beheersmaatregelen vallen buiten de reikwijdte van de Collegeverklaring en de afwijking van de norm is dan ook niet opgenomen in het verbeterplan van de gemeente Waterland. Inmiddels is, na de IT audit, de verbetermaatregel door de dienstverlener uitgevoerd en wordt aan de norm voldaan.

2.2 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. De gemeente maakt hiernaast gebruik van Suwinet voor Burgerzaken.
De verantwoording over 2017 aan stelselhouder ministerie SZW vindt plaats door middel van de Collegeverklaring. Deze omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersmaatregelen aan de geselecteerde normen inzake Suwinet.

Bevindingen

Voor Suwinet en Suwinet/Burgerzaken voldoen de interne beheersmaatregelen in opzet en bestaan aan alle geselecteerde normen inzake Suwinet.

2.3 Collegeverklaring DigiD en Suwinet en Assurance-rapportage IT auditor

De Collegeverklaring informatiebeveiliging DigiD en Suwinet is vastgesteld op 27 maart 2018. De onafhankelijke IT auditor heeft de Collegeverklaring getoetst en een Assurance-rapportage afgegeven. Naar het oordeel van de IT auditor is de Collegeverklaring ENSIA 2017 inzake informatiebeveiliging van DigiD en Suwinet van de gemeente Waterland, in alle van materieel belang zijnde aspecten, juist. De tekst van de Collegeverklaring treft u aan in de bijlage.

3. Uitkomsten BRP en PUN

3.1 Inleiding

Het resultaat van de toetsing BRP en PUN is in 2017 voor het eerst bepaald door samenvoeging van de resultaten van de ENSIA-verantwoording informatieveiligheid BRP en PUN en de resultaten van de domein specifieke zelfevaluatie via de 'Kwaliteitsmonitor' van de Rijksdienst voor Identiteitsgegevens (RvIG).
In de managementrapportages BRP en PUN zijn de resultaten samengevoegd.

3.2 BRP

De normering die is gekoppeld schets een beeld van de toepassing van de beveiligingsmaatregelen en overige aspecten van processen rondom de BRP. Uit de zelfevaluatie blijkt dat de gemeente Waterland 'goed' scoort op de inrichting, de werking en de beveiliging van de basisregistratie. De gemeente bereikt namelijk 95,7 % (normpercentage is 90%).

De gemeente Waterland scoort goed. De 100% wordt niet behaald omdat in een enkel geval van een maatregel of aanbeveling die geen risico vormt bewust en beargumenteerd wordt afgeweken.

3.3 PUN

De normering die is gekoppeld schets een beeld van de toepassing van de 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.
De gemeente bereikt namelijk 95,5 % (normpercentage is 90%).

De gemeente Waterland scoort goed. De 100% wordt niet behaald omdat in een enkel geval van een maatregel of aanbeveling die geen risico vormt bewust en beargumenteerd wordt afgeweken.

4. Uitkomsten en status BIG

4.1 BIG hoofdstuk 3: Implementatie van de Tactische Baseline

Voor het voldoen aan de BIG worden normen gesteld aan de wijze waarop de BIG is geïmplementeerd in de gemeentelijke organisatie. Dit is bijvoorbeeld vertaald naar het benoemen van verantwoordelijken, het samenstellen van een implementatieplan en rapporteren over de voortgang.

Bevindingen

Aan deze normen is voldaan. In 2017 is ter ondersteuning voor het implementeren van de BIG en het beheren en monitoren van beveiligingsmaatregelen een 'Information Security Management System' (ISMS) in gebruik genomen. In het ISMS zijn de normenkaders, ENSIA vragen en andere beheermaatregelen opgenomen en zijn onderbouwende documenten (bewijsstukken) beschikbaar. De ingevoerde gegevens in het ISMS hebben als basis gediend voor de zelfevaluatie via ENSIA.

4.2 BIG hoofdstuk 4: Samenwerkingsverbanden

In dit hoofdstuk gaat het over het beoordelen en afwegen van risico's om te komen tot een goede inschatting van het benodigde beveiligingsniveau vanuit het perspectief van samenwerkingsverbanden. Door afspraken over informatiebeveiliging vast te leggen maken deze integraal onderdeel uit van de samenwerking.

Bevindingen

In oudere overeenkomsten is dit niet altijd goed geregeld. Bij nieuwe samenwerkingsovereenkomsten of bij wijziging worden afspraken en voorwaarden om BIG en AVG (Algemene Verordening Gegevensbescherming) compliant te werken en afspraken over de manier waarop verantwoording plaatsvindt vastgelegd.

4.3 BIG hoofdstuk 5: Beveiligingsbeleid

Doelstelling is het realiseren van een aantoonbaar niveau van informatiebeveiliging op basis van relevante wetgeving. Als fundament voor betrouwbare dienstverlening en het door kunnen gaan van kritische processen bij een calamiteit of incident. Daarnaast moet het informatiebeveiligingsbeleid periodiek worden beoordeeld.

Bevindingen

Aan deze normen is voldaan. Beveiligingsmaatregelen en –processen worden jaarlijks geëvalueerd en geactualiseerd vastgesteld. In 2017 zijn het ICT-Beveiligingshandboek, het handboek beveiliging Suwinet en het Informatiebeveiligingsplan (BRP en PUN), inclusief procedures, geactualiseerd en opnieuw vastgesteld.

4.4 BIG hoofdstuk 6: Organisatie van de informatiebeveiliging

Een adequate organisatie van de informatiebeveiliging is onderdeel van de BIG. In de gemeente Waterland zijn de verantwoordelijkheden, functies en rollen belegd. Dit wordt gemonitord en geactualiseerd. Medewerkers worden conform een autorisatieprocedure voor systemen, rollen en rechten geautoriseerd. Voor aanstelling wordt een VOG overlegd en een geheimhoudingsverklaring getekend. In contracten met externe partijen worden vereiste beveiligingsmaatregelen opgenomen in een (Verwerkers)overeenkomst.

Bevindingen

Aan deze normen is grotendeels voldaan. Met externe partijen worden, binnen de scope van de Collegeverklaring DigiD en Suwinet, de opgelegde beveiligingsmaatregelen jaarlijks getoetst. Het, door middel van het uit (laten) voeren van een audit, steekproefsgewijs toetsen of overige derde partijen zich aan de overeengekomen afspraken houden is een verbeterpunt. Voor 2018 is dit in de begroting opgenomen.

4.5 BIG hoofdstuk 7: Beheer van bedrijfsmiddelen

De bedrijfsmiddelen zijn actueel geregistreerd en er zijn regels voor een juist gebruik van ICT-middelen. De risico's en maatregelen zijn geclassificeerd. Op basis van een actuele 'ICT-foto' wordt de gemeente gericht geïnformeerd over mogelijke kwetsbaarheden door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Bevindingen

Aan deze normen is voldaan.

4.6 BIG hoofdstuk 8: Personele beveiliging

Doelstelling is het bewerkstelligen dat medewerkers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, geschikt zijn voor hun rollen en om risico's te vermijden.

Bevindingen

Verantwoordelijkheden, rollen en rechten zijn vastgelegd. Voor aanstelling wordt de achtergrond van kandidaten onderzocht, een VOG gevraagd en een geheimhoudingsverklaring getekend. Er is aandacht voor voldoende kennis en bewustzijn ten aanzien van informatieveiligheid. Uitzonderingen op de normen betreft het periodiek herhalen van achtergrondonderzoek en sanctiebeleid. Er is (nog) geen aanleiding achtergrond onderzoek periodiek te herhalen. De gemeente Waterland heeft geen specifiek disciplinair proces (sanctiebeleid). Bij inbreuken op het informatiebeveiligingsbeleid wordt waar nodig de CAR/UWO toegepast.

4.7 BIG hoofdstuk 9: Fysieke beveiliging en beveiliging van de omgeving

Doelstelling is het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

Bevindingen

Aan deze normen is voldaan. Er zijn voldoende maatregelen genomen voor de plaatsing en bescherming van bedrijfsmiddelen. Toegangsbeveiliging is ingericht met publiektoegankelijke ruimten en afgeschermde ruimten, met specifieke aandacht voor de kritische ruimten en processen.

4.8 BIG hoofdstuk 10: Beheer van communicatie- en bedieningsprocessen

Doelstelling is het waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

Bevindingen

Taken en verantwoordelijkheden voor het gebruik en beheer zijn gescheiden belegd. Bedieningsprocedures zijn beschreven en er is een vastgestelde procedure voor wijzigingenbeheer op ICT-voorzieningen. In 2018 wordt het functioneel- en systeembeheer heringericht. De verslaglegging van het wijzigingenbeheer wordt daarin verankerd. Bij externe dienstverlening worden relevante beveiligingsmaatregelen opgenomen in een (Verwerkers)overeenkomst. Aandachtspunt is om periodiek met externe partijen waaraan IT-diensten zijn uitbesteed overleg te voeren over het bestaan en de actualiteit van IB-maatregelen.

4.9 BIG hoofdstuk 11: Toegangsbeveiliging

Doelstelling is het beheersen van de toegang tot informatie.

Bevindingen

Aan deze normen is grotendeels voldaan. Wachtwoordbeheer, inlogprocedures, time-outsessies/clear screen en authenticatie zijn goed ingericht. Er zijn actueel vastgestelde autorisatieprocedures voor het toekennen van accounts en toegangsrechten. Zowel het correct uitvoeren van de procedures als het toekennen van de juiste autorisaties wordt stelselmatig gecontroleerd. Medewerkers worden geïnformeerd over het veilig omgaan met wachtwoorden. Verbeterpunt is om dit, meer dan nu het geval is, periodiek te herhalen.

4.10 BIG hoofdstuk 12: Verwerving, ontwikkeling en onderhoud van informatiesystemen

Doelstelling is het bewerkstelligen dat beveiliging integraal deel uitmaakt van de gemeentelijke informatiesystemen.

Bevindingen

Wordt grotendeels aan voldaan. De gemeente Waterland ontwikkelt zelf geen software en heeft daarom geen beleid of richtlijnen voor validatiecontroles bij de ontwikkeling van (web)applicaties. Als verbeterpunt wordt in het testproces voor het testen van software een procedure opgenomen voor het zorgvuldig gebruik van geanonimiseerde testdata. Maatregelen zijn getroffen voor de beheersing van en regelmatige controle op technische kwetsbaarheden.

4.11 BIG hoofdstuk 13: Beheer van informatiebeveiligingsincidenten

Doelstelling is het bewerkstelligen dat informatiebeveiligingsincidenten en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Bevindingen

Aan deze normen is voldaan. De gemeente Waterland heeft een incidentmanagementprocedure en registreert mogelijke kwetsbaarheden en incidenten. De Informatiebeveiligingsdienst voor gemeenten (IBD) informeert de gemeente gericht over mogelijke kwetsbaarheden en incidenten.

4.12 BIG hoofdstuk 14: Bedrijfscontinuïteitsbeheer

Doelstelling is het tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of om tijdig herstel te bewerkstelligen.

Bevindingen

Voor alle primaire processen is er een calamiteiten- en continuïteitsplan. Op dit moment is nog niet voor alle processen een 'Beveiliging Impact Assessment' uitgevoerd, dat inzicht geeft in de afhankelijkheden van diensten of processen. Dit wordt in 2018 ingericht.

4.13 BIG hoofdstuk 15: Naleving

Doelstelling is het voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen en van enige beveiligingseisen.

Bevindingen

Wettelijke- en contractuele voorschriften en het beveiligingsbeleid worden nageleefd. Controle op de technische naleving door penetratietesten vindt nog niet jaarlijks plaats.

5. 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 mogelijke nadelige gevolgen van het lekken van persoonsgegevens te beperken en om de kans op uitval van systemen en bedrijfsvoeringprocessen of schade te minimaliseren of te voorkomen. De gemeente Waterland heeft een procedure voor het melden van mogelijke beveiligingsincidenten en datalekken en wordt specifiek en gericht geïnformeerd over kwetsbaarheden en incidenten door de IBD.

In 2017 zijn 26 meldingen van mogelijke beveiligingsincidenten ontvangen en opgenomen in het meldingenregister:

- 12 meldingen die informatief waren of na controle niet van toepassing zijn gebleken;
- 4 meldingen van een technische kwetsbaarheid, die vrijwel direct zijn opgelost en waarvan geen nadelige gevolgen zijn ondervonden;
- 7 meldingen van een incident waarbij persoonsgegevens waren betrokken (datalekken). Deze zijn direct na het ontdekken er van hersteld. Vanwege de aard van de datalekken, deze direct zijn hersteld, geen gegevens naar buiten zijn gelekt en geen indicaties van nadelige gevolgen waren is hiervan geen melding gedaan aan de Autoriteit Persoonsgegevens (AP).
- 3 meldingen waarbij persoonsgegevens waren betrokken zijn, gelet op de aard van de gegevens en afhankelijkheid van derde partijen, gemeld bij de AP. De incidenten zijn hersteld en er zijn geen indicaties van nadelige gevolgen.

Bijlage: Tekst Collegeverklaring ENSIA 2017

Vanwege het openbare karakter van deze jaarrapportage is de in de originele verklaring specifiek benoemde norm en (inmiddels herstelde) tekortkoming van de dienstverlener niet opgenomen. Om die reden zijn ook de bijlagen met detailinformatie over DigiD en Suwinet niet bijgevoegd. De verantwoording op hoofdlijnen over DigiD en Suwinet is opgenomen in hoofdstuk 2 van deze rapportage.

Tekst Collegeverklaring

Het college van burgemeester en wethouders van de gemeente Waterland legt met deze verklaring verantwoording af over geselecteerde informatiebeveiligingsnormen inzake DigiD en Suwinet op basis van de Eenduidige Normatiek Single Information Audit (ENSIA) systematiek.

Het doel van ENSIA is om verantwoording over informatieveiligheid af te leggen aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en control cyclus voor informatiebeveiliging, neemt de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt en maakt gebruik van een daarop ingerichte zelfevaluatie. Hierdoor heeft het gemeentebestuur meer overzicht over de informatiebeveiliging van de gemeente en kan het bestuur beter sturen en verantwoording afleggen aan de gemeenteraad en andere belanghebbenden.

Zo structureert ENSIA ook de verticale verantwoording van gemeenten richting de rijksoverheid over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling Nederland (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet).

Reikwijdte verklaring

Deze verklaring betreft de onderdelen van de ENSIA systematiek waarover assurance wordt gevraagd van een onafhankelijke IT auditor. Voor het jaar 2017 betreft dit DigID (aansluitnummer 999913 Digitaal Loket Gemeente Waterland) en Suwinet. De verklaring omvat het op 31 december 2017 in opzet en bestaan voldoen van de beheersingsmaatregelen aan de geselecteerde normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD versie 2.0, op het openbare deel van de websites van het ministerie van BZK[1]) en Suwinet (Specifiek Suwinet normenkader Afnemers, versie 1.01 op website BKWI[2] en bijlage 1 van de notitie Verantwoordingsstelsel op website ENSIA[3] voor de selectie van normen). De normen vinden hun basis in internationale standaarden en zijn geschikt voor het doel van deze Collegeverklaring. De Collegeverklaring omvat niet de werking van de maatregelen over 2017.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze Collegeverklaring. Uit de bijlage bij de Collegeverklaring “bijlage 1 DigiD” blijkt over welke beheersmaatregelen en DigiD-normen door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed verantwoording wordt afgelegd. Deze Collegeverklaring en de verantwoording van de dienstverlener dekken tezamen de geselecteerde normen inzake DigiD af.

1 https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/normenkader-v20-voor-2017/
2 https://www.bkwi.nl/nieuws/nieuw-normenkader-voor-gemeenten
3 https://www.ensia.nl/

Deze Collegeverklaring is opgesteld voor de gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet. De gemeenteraad en de departementen die toezien op de veiligheid van DigiD en Suwinet zijn via bij deze Collegeverklaring behorende afzonderlijke bijlagen voor DigiD (bijlage 1 DigiD met kenmerk IT18.00545) en Suwinet (bijlage 2 Suwinet met kenmerk IT18.01049) geïnformeerd over de afwijkingen van de normen.

Verklaring college

Het college verklaart dat bij gemeente Waterland op 31 december 2017 de interne beheersingsmaatregelen in opzet en bestaan voldoen aan de geselecteerde normen inzake Suwinet.

Voor DigiD-aansluitnummer 999913 wordt niet aan alle geselecteerde normen voldaan. De op de uitzonderingen gerichte beheersmaatregelen zijn in een verbeterplan (bijalge 3 Verbeterplan DigiD met kenmerk IT18.01171) opgenomen, zijn belegd en worden gemonitord.

Afwijking van de norm bij de dienstverlener

Uit de bijlage bij de collegeverklaring “bijlage 1 DigiD” blijkt dat voor DigiD-aansluitnummer 999913 door de dienstverlener aan wie de beheersmaatregelen zijn uitbesteed niet aan alle geselecteerde normen wordt voldaan.

De beheersingsmaatregelen inzake DigiD die zijn uitbesteed vallen buiten de reikwijdte van deze collegeverklaring. De afwijking van deze norm is dan ook niet opgenomen in het verbeterplan van de gemeente Waterland. Wel wordt door de gemeente gemonitord dat de dienstverlener de op deze uitzondering gerichte beheersmaatregelen neemt

Monnickendam, 27 maart 2018
College van burgemeester en wethouders gemeente Waterland