# Jaarrapportage informatieveiligheid

## 2022

## 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 2022, kenmerk 25444-2022:687602

Verantwoordingsrapportage WOZ 2022, kenmerk 25444-2022:854599

# 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 2022. Deze zelfevaluatie is gebaseerd op de BIO en is uitgevoerd in de periode juli t/m december 2022. 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 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), Waardering Onroerende Zaken (WOZ), 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 2022 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. 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, BRO en de WOZ

Voor de BAG, BGT, BRO en WOZ zijn over 2022 separate zelfevaluaties in ENSIA uitgevoerd. De domein specifieke verantwoordingsrapportage BAG, BGT en BRO en de specifieke verantwoordingsrapportage WOZ zijn als bijlage bij deze jaarrapportage opgenomen. De scores zijn opgenomen in de samenvatting resultaten zelfevaluatie 2022 (hoofdstuk 2).

# 2. Samenvatting resultaten zelfevaluatie 2022

| Zelfevaluatie | Audit | Bevindingen Gemeente Waterland |
|---|---|---|
| DigiD (IT audit)<br><br>*Resultaat 2021* | Conform college-verklaring/ bevindingen | Aan alle normen voldaan<br><br>*Aan alle normen voldaan* |
| Suwinet (IT audit)<br><br>*Resultaat 2021* | Conform college-verklaring/ bevindingen | Aan alle normen voldaan<br><br>*Aan 2 normen niet voldaan* |

| Zelfevaluatie | Norm | Score Gemeente Waterland |
|---|---|---|
| BRP domeinvragen Kwaliteitsmonitor RvIG<br>BRP informatiebeveiligingsvragen ENSIA<br><br>Samengevoegd resultaat 2022<br>*Samengevoegd resultaat 2021* | <br><br><br>90%<br>*90%* | 791 punten van 800 (98,8%)<br>1.030 punten van 1.200 (85,8%)<br><br>1.821 punten van 2.000 (91%)<br>*1.843 punten van 2.000 (92%)* |
| Reisdocumenten domeinvragen Kwaliteitsmonitor RvIG<br>Reisdocumenten informatiebeveiligingsvragen ENSIA<br><br>Samengevoegd resultaat 2022<br>*Samengevoegd resultaat 2021* | <br><br><br>90%<br>*90%* | 780 punten van 800 (97,5%)<br>995 punten van 1.200 (82,9%)<br><br>1.775 punten van 2.000 (88,7%)<br>*1.820 punten van 2.000 (91%)* |
| BAG | 75% | 64%<br>*2021 82%* |
| BGT | 75% | 29%<br>*2021 31%* |
| BRO | 60% | 61%<br>*2021 88%* |
| WOZ | n.v.t. | 44,4%<br>*2021 42,8%* |

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%).

| BIO | Aantal maatregelen | Maatregelen waaraan niet is voldaan | Conclusie Gemeente Waterland |
|---|---|---|---|
| Achtergrond BIO<br><br>*(hoofdstuk 2 opzet BIO en hoofdstuk 4 verantwoording over de BIO)* | 7 | 1 | Voldoet niet |
| Categorie 1: Beleid en organisatie<br><br>*(hoofdstuk 5 informatiebeveiligingsbeleid, hoofdstuk 6 organiseren van informatiebeveiliging en hoofdstuk 18 naleving)* | 31 | 7 | Voldoet niet |
| Categorie 2: Personeel en toegang<br><br>*(hoofdstuk 7 veilig personeel, hoofdstuk 9 toegangsbeveiliging en hoofdstuk 11 fysieke beveiliging en beveiliging van de omgeving)* | 59 | 8 | Voldoet niet |
| Categorie 3: Continuïteit en incidenten<br><br>*(hoofdstuk 16 beheer van informatie-beveiligingsincidenten en hoofdstuk 17 informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer)* | 20 | 6 | Voldoet niet |
| Categorie 4: Informatiesystemen<br><br>*(hoofdstuk 12 beveiliging bedrijfsvoering, hoofdstuk 14 acquisitie, ontwikkeling en onderhoud van informatiesystemen en hoofdstuk 15 leveranciersrelaties)* | 57 | 21 | Voldoet niet |
| Categorie 5: Databescherming<br><br>*(hoofdstuk 8 beheer van bedrijfsmiddelen, hoofdstuk 10 cryptografie en hoofdstuk 13 communicatiebeveiliging)* | 32 | 5 | 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 2022 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 alle geselecteerde normen voldaan.

## 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 2022 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 door de gemeente Waterland aan alle geselecteerde normen inzake Suwinet 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 afgegeven. Naar oordeel van de IT auditor is de Collegeverklaring ENSIA 2022 inzake informatiebeveiliging van DigiD en Suwinet in alle van materieel belang zijnde aspecten juist. De Collegeverklaring informatiebeveiliging DigiD en Suwinet is vastgesteld op 18 april 2023, 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 2022 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 eind januari 2022 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 1.821 punten van de maximaal 2.000 punten. Dat geeft een percentage van 91%.

## 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 1.775 punten van de maximaal 2.000 punten. Dat geeft een percentage van 88,7%.

## 4.4. Verbeterpunten BRP en Reisdocumenten

Verbeterpunten voor zowel de BRP als de Reisdocumenten zijn het actualiseren en opnieuw vaststellen van een autorisatiematrix en op basis daarvan een frequentere beoordeling van toegangsrechten, het implementeren en inrichten van een ondersteunend securitymanagement systeem en het vaststellen van een geactualiseerd back-up en restorebeleid. Deze punten worden in 2023 opgepakt.

# 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 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.

## 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

Processen zijn grotendeels vastgelegd. In 2023 worden rondom deze processen de risico's, controls, maatregelen en verantwoordelijkheden vastgelegd.

## 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

- Rollen en verantwoordelijkheden zijn vastgelegd, maar voor enkele systemen ontbreekt een actueel vastgestelde autorisatiematrix.
- De ondersteunende maatregelen voor het beheren van risico's ten aanzien van het gebruik van mobiele apparatuur zijn onvoldoende.
- De organisatie beschikt nog niet over goed ingericht Information Security Management System (ISMS).

### Verbetermaatregelen

- In 2023 worden de ontbrekende autorisatiematrixen opgesteld en vastgesteld.
- In 2023 wordt een Mobile Device Management (MDM) systeem geïmplementeerd.
- In 2023 wordt een ISMS tool, waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt, ingericht.

## 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 de 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

- Met het MDM wordt deze tekortkoming opgepakt.
- Aan de hand van de nieuw vastgestelde autorisatiematrixen wordt ook de frequentie van controles opgevoerd.
- Geen verbetermaatregel. Er zijn voldoende maatregelen genomen ten aanzien van bedreigingen van buitenaf.

## 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.
- Een continuïteitsplan is aanwezig, maar wordt niet jaarlijks getest.
- Procesonderdelen zijn niet geïdentificeerd op basis van een specifieke risicoafweging.

### Verbetermaatregelen

- Niet van toepassing. Dit heeft betrekking “eigen” software, bijvoorbeeld van onze leveranciers. De gemeente ontwikkelt zelf geen software.
- In 2023 wordt het continuïteitsplan herzien. Het jaarlijks testen wordt daarin meegenomen.
- Dit onderdeel is buiten de scope voor 2023.

## 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.

### Verbetermaatregelen

- De procedure voor wijzigingenbeheer wordt in 2023 opgesteld.
- Het back-up beleid wordt in 2023 herzien en vastgesteld.
- Een procedure voor het installeren/downloaden van software wordt in 2023 opgesteld.
- Buiten de scope voor 2023.
- Bij afspraken met nieuwe leveranciers worden de beveiligingseisen en prestatie-indicatoren op basis van expliciete risicoafwegingen opgenomen.

## 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 gebruik gemaakt van PKI Overheidscertificaten. Er zijn geen afspraken met andere leveranciers over reserve certificaten.
- Er is nog geen Cryptografiebeleid vastgesteld.
- Er is geen beleid of procedure voor informatietransport.

### Verbetermaatregelen

- Dit wordt zo mogelijk opgepakt in 2023 met ‘Het Nieuwe Werken’.
- Er wordt een cryptografiebeleid opgesteld en toegepast in de organisatie, inclusief eventuele afspraken over certificaten.
- Zie bovenstaande maatregel.
- Een procedure voor informatietransport wordt opgesteld en gedeeld.

# 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 2022

In 2022 zijn meerdere meldingen geweest waarvan er 11 meldingen zijn geclassificeerd als mogelijke beveiligingsincident/datalek en opgenomen in het meldingenregister:

- Er zijn meerdere meldingen van phishing/ CEO-fraude (phishing voor financieel gewin) geweest. Er zijn er 3 gemeld als gevaarlijk en daar is adequaat op gehandeld zonder nadelige gevolgen. Eén van deze fraudepoging is ter informatie gemeld aan de IBD;
- 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 2 technische kwetsbaarheden die snel en adequaat opgelost moesten worden. Er zijn (voor zover bekend) geen nadelige gevolgen van ondervonden;
- 6 mogelijke incidenten waarbij persoonsgegevens waren betrokken. 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.

# Bijlage 1: Tekst Collegeverklaring ENSIA 2022

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 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 2022.

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

- Bijlage 1 DigiD met kenmerk 25444-2022:822875.
- Bijlage 2 Suwinet met kenmerk 25444-2022:693823.

## Verklaring college

Het college verklaart dat bij gemeente Waterland op 31 december 2022 de beheersingsmaatregelen (in opzet en bestaan) voldoen aan de geselecteerde normen inzake DigiD en Suwinet.

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), de Gezamenlijke Elektronische Voorzieningen Structuur uitvoeringsorganisatie Werk en Inkomen (GeVS/Suwinet) en de Wet Onroerende Zaken (WOZ).

## Samenvattend beeld

| Onderwerp | Wordt aan alle normen voldaan? | Zijn de uitzonderingen in [een] verbeterplan[nen] opgenomen en zijn de verbetermaatregelen belegd en worden deze gemonitord? |
|---|---|---|
| DigiD 999913 | Ja | Niet van toepassing |
| Suwinet voor SUWI-taken | Ja | Niet van toepassing |
| Suwinet voor niet-SUWI-taken | Ja | Niet van toepassing |

Monnickendam, 18 april 2023

College van burgemeester en wethouders gemeente Waterland