Informatiebeveiligingsplan Suwinet Inkijk GSD

Versie: 2.0
Datum: 15 januari 2020
Vastgesteld dd: 14 januari 2020

Gemeente Borger-Odoorn

Versiebeheer

Versie	Datum	Wijziging
1.0	12-02-2019	Definitieve versie vastgesteld d.d. 22 januari 2019 door college van B&W van gemeente Borger-Odoorn. Op 8 maart 2019 is deze versie gepubliceerd.
2.0	15-01-2020	Naar aanleiding van de jaarlijkse evaluatie van het Informatiebeveiligingsplan Suwinet Inkijk GSD heeft het college van B&W op 14 januari 2020 besloten om versie 1.0 in te trekken en versie 2.0 vast te stellen.

Inhoud

1. Inleiding

1.1.Wat is Suwinet?

Suwinet (Gezamenlijke elektronische Voorziening Suwinet –GeVS/ Suwi staat voor Structuur Uitvoering Werk en Inkomen) is een digitale infrastructuur voor overheidsorganisaties om persoonsgegevens te raadplegen, die zijn opgeslagen bij verschillende partijen of basisregistraties. Op het moment dat een gebruiker van Suwinet een verzoek doet, leveren overheidsadministraties (bronhouders) de gegevens rechtstreeks uit de systemen. Het gaat hier dus om zeer privacygevoelige informatie van de inwoners van Nederland. Er worden alleen gegevens uitgewisseld voor zover daar een wettelijke grondslag voor is. Het BKWI (Bureau Keteninformatisering Werk & Inkomen) is beheerder van het Suwinet.

De gemeente Borger-Odoorn maakt gebruik van Suwinet inkijk GSD om de Participatiewet uit te kunnen voeren. Dit is een raadpleegfunctie voor gemeentelijke sociale diensten en gemeentelijke samenwerkingsverbanden; het is één van de Suwinet-producten. Voor de Participatiewet is het gebruik van Suwinet belangrijk om de rechtmatigheid van een aanvraag te kunnen toetsen en fraude te bestrijden.

1.2.Waarom een informatiebeveiligingsplan?

Het gebruik van Suwinet brengt een grote verantwoordelijkheid mee op het gebied van informatieveiligheid. De partners in de Suwinetketen moeten erop kunnen vertrouwen dat de gegevens op een zorgvuldige en controleerbare wijze worden behandeld. **Dit informatiebeveiligingsplan beantwoordt de vraag hoe de gemeente Borger-Odoorn zorgdraagt voor het gewenste niveau van informatieveiligheid ten aanzien van Suwinet.** Dit gewenste niveau wordt beschreven in de toepasselijke normenkaders: de Baseline Informatiebeveiliging Gemeenten (BIG) en het specifiek Suwinet normenkader. Vanaf 2020 is dit de BIO (Baseline Informatiebeveiliging Overheid)
Jaarlijks vindt er verantwoording plaats (ENSIA). Het beleid wordt ook jaarlijks geëvalueerd. De uitvoering op de werkvloer en het plan moeten daadwerkelijk aansluiten. Dit informatiebeveiligingsplan en het verstevigen van de werkafspraken leiden tot een juist niveau van informatieveiligheid en daarmee zijn veiligheid en privacy ten aanzien van Suwinet goed geborgd.

1.3.Leeswijzer

In hoofdstuk twee zullen allereerst de toepasselijke kaders benoemd worden. Hierna wordt in hoofdstuk drie uiteengezet waarvoor en door wie het Suwinet in de gemeente Borger-Odoorn gebruikt wordt en via welke verbinding. In de hoofdstukken hierna zullen de diverse beheersmaatregelen aan de orde komen:

- Er is duidelijke scheiding van verantwoordelijkheden en rollen. (Hoofdstuk 4)
- Het autorisatieproces staat nauwkeurig omschreven. Er is hierbij aandacht voor in- en uitdiensttreding. Ook worden de gehanteerde toegangsrechten omschreven. (Hoofdstuk 5).
- Bewustwordingsacties rondom veiligheid en privacy worden georganiseerd. Een voorbeeld hiervan is het informeren van nieuwe medewerkers over de informatieveiligheid. (Hoofdstuk 6)
- Daarnaast bestaan er ook werkafspraken rondom onderwerpen als thuiswerken, cleandesk- en cleanscreenpolicy.(Hoofdstuk 7)
- De werkwijze bij een beveiligingsincident is bekend (Hoofdstuk 8)

- Toezicht is een belangrijk aspect van informatieveiligheid. Hieronder vallen diverse thema's, zoals het periodiek opvragen van gebruikersrapportages. (Hoofdstuk 9).
- Jaarlijks vinden er verschillende soorten evaluaties plaats (Hoofdstuk 10).

Als laatste wordt er ingegaan op het recht om de eigen gegevens in te zien. (Hoofdstuk 11)

In de eerste bijlage wordt het tijdspad voor Suwinet geschetst voor de komende drie jaren. In de tweede bijlage is het format voor de actiepuntenlijst opgenomen en als laatste is een verklarende lijst met afkortingen opgenomen.

2.Kaders voor het gebruik van Suwinet

Achtereenvolgens zullen in dit hoofdstuk de relevante wettelijke kaders, normenkaders en het gemeentelijk kader omschreven worden.

2.1.Toepasselijke wet- en regelgeving

De toepasselijke wet- en regelgeving:

- Wet SUWI (Wet Structuurorganisatie Uitvoering Werk en Inkomen)
- Regeling SUWI
- AVG (Algemene Verordening Gegevensbescherming)

Verder wordt het verwerken van persoonsgegevens geregeld in specifieke wetten zoals de Participatiewet.

Het informatiebeveiligingsplan Suwinet Inkijk GSD moet gelezen worden in samenhang met andere beleidsstukken aangaande de privacy.

2.2. Normenkaders

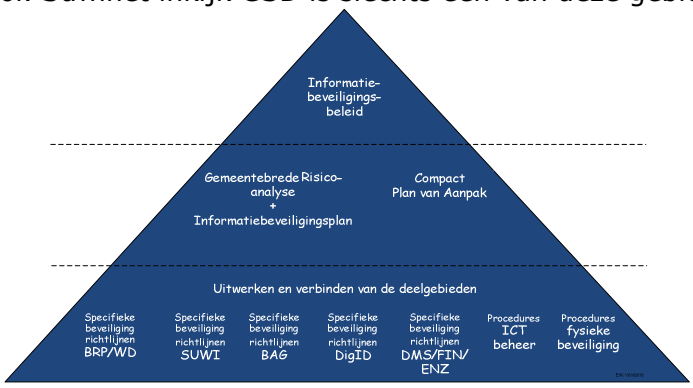
De verschillende stakeholders (bronhouders, beheerder en afnemers) van Suwinet dienen allen vanuit de eigen verantwoordelijkheid de juiste beveiligingsmaatregelen te treffen, zodat de beveiliging van het Suwinet tot een volle omvang kan komen. Als afnemer dient de gemeente Borger-Odoorn daarom te voldoen aan het specifiek Suwinet-normenkader. [1]

De gemeente dient verantwoording af te leggen over de informatieveiligheid. Dit heet ENSIA (Eenduidige Normatiek Single Information Audit). Dit is een verantwoordingsstelsel voor de informatieveiligheid en was tot eind 2019 gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Hierin is de verantwoordingsytematiek voor Suwinet in ondergebracht. Voor Suwinet houdt dit in een jaarlijkse zelfevaluatie en audit in.

In 2020 gaat de verantwoordingsrichtlijn wijzigen, omdat de Baseline Informatiebeveiliging Overheid (BIO) van kracht wordt.

2.3. Gemeentelijke kader

Gemeente Borger-Odoorn heeft een gemeentebreed informatiebeveiligingsbeleid. De gemeente is een informatie-intensieve organisatie met een primaire focus op dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening
De veiligheid van informatie speelt binnen een groot aantal gebieden van de gemeente een rol. Suwinet inkijk GSD is slechts één van deze gebieden.



1 https://www.bkwi.nl/_Resources/Persistent/452839ba4df373fc47b945af6c04514759f015f5/Specifiek%20Suwinet-normenkader%20Afnemers.1.01.2017.pdf

In het gemeentebreed informatiebeveiligingsbeleid worden organisatiebrede, overkoepelende onderwerpen geïntegreerd in algemeen beleid en worden algemene procedures vastgelegd. Het gemeentebreed informatiebeveiligingsbeleid zorgt samen met informatiebeveiligingsmaatregelen en procedures voor een adequaat en gewenst betrouwbaarheidsniveau. Bij dit niveau zijn de volgende kwaliteitskenmerken gewaarborgd:

- Beschikbaarheid.
- Integriteit.
- Vertrouwelijkheid.
- Controleerbaarheid.

De borging van het gemeentebreed informatiebeveiligingsbeleid geschiedt door een PDCA cyclus (Plan, Do, Check, Act)

3.De aansluiting van Suwinet in Borger-Odoorn

Dit informatiebeveiligingsplan betreft de aansluiting op Suwinet Inkijk GSD van de gemeente Borger-Odoorn. Waarvoor is deze aansluiting nodig en voor wie? Via wat voor een verbinding worden de gegevens uitgewisseld? De volgende paragrafen zullen deze vragen beantwoorden.

3.1. Uitvoering van Participatiewet

Suwinet Inkijk kan gebruikt worden voor een aantal wettelijke taken. Voor iedere taak moet een aparte aansluiting gerealiseerd worden. Dit informatiebeveiligingsplan betreft enkel de aansluiting van Borger-Odoorn voor Suwinet inkijk GSD en is bestemd voor de uitvoering van de Participatiewet. Dat betekent dat de aansluiting ook uitdrukkelijk niet voor andere taken gebruikt mag worden.

3.2.Administratie Sociaal Domein (ASD)

De aansluiting Suwinet Inkijk GSD in Borger-Odoorn wordt gebruikt door cluster ASD. Dit informatiebeveiligingsplan betreft enkel deze aansluiting.

Cluster ASD voert diverse taken uit. Suwinet wordt enkel gebruikt voor de aanvragen bijzondere bijstand voor niet-bijstandsgerechtigden. Voor de andere werkzaamheden van ASD mag en wordt Suwinet niet gebruikt. Dit is/wordt bereikt via:

1. Activiteiten gericht op bewustwording (Hoofdstuk 6)
2. Controle via het opvragen van generieke en specifieke rapportages. (Hoofdstuk 9)

De aansluiting op Suwinet wordt daarnaast ook gebruikt door een medewerker van de gemeente Borger-Odoorn om het inburgeringsportaal van DUO (Dienst Uitvoering Onderwijs) te kunnen gebruiken voor participatieverklaringen.

De uitvoering van de Participatiewet is op te splitsen in 'Werk' en 'Inkomen'. De uitvoering van de Participatiewet ten aanzien van 'Inkomen' geschiedt voor het grootste deel bij het Werkplein in Emmen. Ook hier wordt gebruik gemaakt van Suwinet inkijk GSD. Het beveiligingsplan voor Suwinet van Emmen maakt deel uit van de deelovereenkomst sociale zaken en werkgelegenheid. Dat beleid is ook van toepassing op de aansluiting bij Menso. Emmen laat hier de Bbz 2004 (bijstand voor zelfstandigen) uitvoeren.

De eindverantwoordelijkheid voor Suwinet inkijk GSD in Emmen voor de inwoners van Borger-Odoorn is echter niet overgedragen via de deelovereenkomst. Dat is ook niet mogelijk. De gemeente Borger-Odoorn moet zich zowel over de aansluiting in Emmen als de aansluiting voor cluster Administratie Sociaal Domein (ASD) verantwoorden.

Team Werk verricht de Participatiewettaken ten aanzien van 'Werk'. Team Werk heeft geen aansluiting op Suwinet.

3.2.Beveiligde verbinding

De netwerkverbinding waarover Suwinet gegevens worden uitgewisseld, is beveiligd voor ongeautoriseerde toegang. Het Suwinet heeft een besloten karakter. De Suwinet verbinding is tweezijdig versleuteld.

Suwinet Inkijk wordt benaderd via een reguliere browser, maar wel in de veilige gemeentelijke omgeving (Citrix). Suwinet kan enkel benaderd worden via een Gemnet verbinding. Dit is een dubbele veiligheid.

Gemnet
Het Gemnet-netwerk is een besloten digitaal netwerk met het allerhoogste veiligheidsniveau om problemen met data-uitwisseling te voorkomen. Het biedt daarnaast de toegang tot het besloten Diginetwerk. Het Gemnet-netwerk werkt onafhankelijk van het openbare internet.[2]

[2] https://www.kpn.com/zakelijk/branches/overheid/gemnet.htm

4.Verdeling van verantwoordelijkheden en taken

Taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, processen en infrastructuur moeten zijn beschreven en duidelijk en gescheiden zijn belegd. Onduidelijkheid hierover kan namelijk leiden tot misbruik van bevoegdheden, te ruim toegekende bevoegdheden, over het hoofd zien van en/of implementatie van tegenstrijdige beveiligingsmaatregelen.

In onderstaande tabel wordt de verdeling in gemeente Borger-Odoorn beschreven.

Functie	Verantwoordelijkheden ten aanzien van Suwinet
Medewerkers ASD (gebruikers)	- Gebruik van Suwinet ten behoeve van het behandelen van de aanvragen bijzondere bijstand voor niet-bijstandsgerechtigden. - Innemen actieve rol ten aanzien van bewustwording informatieveiligheid.
Functioneel beheerder	- Bijhouden van een autorisatiematrix. - Autorisaties voor Suwinet verlenen op verzoek van de overall coördinator sociaal domein. Het toekennen van rollen en rechten geschiedt conform de autorisatiematrix. - Autorisaties intrekken (bij einde dienstverband of bij wijziging werkzaamheden van een medewerker). - Verstrekken van wachtwoorden op verzoek van de overall coördinator sociaal domein, bijvoorbeeld bij blokkering van een account door inactiviteit. - Opvoeren van BSN's op de whitelist na realisering van de aansluiting op de whitelist. De functioneel beheerder heeft toegang tot Suwinet, maar kan geen persoonsgegevens inzien.
Overall coördinator sociaal domein / Gemandateerde Suwinet	- Bepalen welke medewerkers toegang tot Suwinet nodig hebben. - Verstrekken van de juiste gegevens aan de functioneel beheerder ten behoeve van een juiste gebruikersadministratie bij in- en uit diensttreding van medewerkers. - Bevorderen en op peil houden van een goede bewustwording van veilig gebruik van Suwinet. - Vastleggen van bewustwordingsacties, belangrijke mutaties, incidenten, rapportages gebruik Suwinet (bijhouden Suwinet administratie). - Maandelijks opvragen van generieke rapportages. - Periodiek opvragen van specifieke rapportages. Dit geschiedt zeker halfjaarlijks. - Controleren of het gebruik van gegevens binnen Suwinet inkijk plaatsvindt binnen de kaders en overeenkomstig de autorisatie per rol met behulp van de opgevraagde rapportages. - Juiste acties uitzetten bij constatering van oneigenlijk gebruik of misbruik en rapporteren aan manager afdeling Bestuurs- en Concernondersteuning (BCO). - Bevindingen uit de rapportages jaarlijks rapporteren aan manager BCO. - Bijdrage leveren aan ENSIA

	De overall coördinator sociaal domein heeft toegang tot het Suwinet voor het opvragen van rapportages, maar heeft geen directe inzage in persoonsgegevens.
Beleidsmedewerker	- Informatiebeveiligingsplan Suwinet inkijk GSD jaarlijks controleren op actualiteit en volledigheid. - Informatiebeveiligingsplan Suwinet inkijk GSD herijken indien dit nodig is. - Leveren van een bijdrage aan de bewustwordingsacties. - Bijdrage leveren aan ENSIA - Eigenaar van jaarlijkse actiepuntenlijst Suwinet De beleidsmedewerker heeft geen toegang tot het Suwinet en is niet werkzaam in het team, waar gebruik gemaakt wordt van Suwinet.
Security Officer (SO)	- Bewaking van de integraliteit van het informatiebeveiligingsplan Suwinet inkijk GSD en het gemeentebrede informatiebeveiligingsbeleid. - Organiseren van –gemeentebrede-bewustwordingsacties. - Adviseren ten aanzien van de informatieveiligheid - Toezicht houden op proces rondom IAA rapportages - Coördinatie ENSIA De SO is niet werkzaam in het team waar gebruik gemaakt wordt van Suwinet. De SO heeft geen direct toegang tot persoonsgegevens.
Manager BCO	- Dragen van de eindverantwoordelijkheid voor het zorgvuldig gebruik van Suwinet. (evaluatie IAA rapportages- Identificatie, Authenticatie en Autorisatie) De manager BCO heeft geen toegang tot het Suwinet.

5.Autorisaties

In de eerste paragraaf wordt het autorisatieproces behandeld. In de tweede paragraaf worden de gebruikte toegangsrechten beschreven en als laatste wordt in paragraaf 3 beschreven hoe er wordt gehandeld ten aanzien van verlopen accounts.

5.1. Autorisatieproces

Het toekennen en intrekken van autorisaties moet een helder en duidelijk proces zijn. De werkafspraken ten aanzien van in- en uitdiensttreding gelden uiteraard ook voor de medewerkers die in dienst zijn en blijven, maar te maken hebben met een veranderend takenpakket waardoor toegang tot Suwinet wel of juist niet meer nodig is.Het autorisatieproces ziet er als volgt uit:

Indiensttreding

Stap	Actie
1	Overall coördinator sociaal domein mailt de functioneel beheerder met het verzoek om autorisatie te verlenen aan een medewerker.
2	De overall coördinator sociaal domein vraagt de nieuwe medewerker om de Elearning veilig gebruik Suwinet te doen en legt de het certificaat van deelname vast in de administratie van Suwinet. Daarnaast wordt het informatiebeveiligingsplan verstrekt en besproken. Er is hierbij ook aandacht voor het loggen van elke handeling in Suwinet.
3	De functioneel beheerder regelt de toegang tot Suwinet en mailt het wachtwoord en de gebruikersnaam aan de gebruiker. Het verstrekken van het wachtwoord en de gebruikersnaam gebeurt afzonderlijk en niet in 1 mail.
4	De functioneel beheerder werkt de autorisatiematrix bij en mailt de bijgewerkte versie aan de overall coördinator sociaal domein.
6	De gewijzigde autorisatiematrix wordt vastgelegd een map op de Qschijf door de overall coördinator sociaal domein. Enkele aangewezen medewerkers hebben autorisatie om betreffende map te bekijken.
7	De mutatie wordt vastgelegd in een jaarlijks mutatieoverzicht door de overall coördinator sociaal domein.

Uitdiensttreding

Stap	Actie
1	De uitdiensttreding van een medewerker met toegang tot het Suwinet wordt onmiddellijk doorgegeven door de overall coördinator sociaal domein aan de functioneel beheerder per mail.
2	De functioneel beheerder trekt de autorisatie in en bevestigt deze intrekking per mail aan de overall coördinator sociaal domein.
3	De functioneel beheerder werkt de autorisatiematrix bij en mailt dit aan de overall coördinator sociaal domein.
4	De gewijzigde autorisatiematrix wordt vastgelegd op de Qschijf door de overall coördinator sociaal domein.
5	De mutatie wordt vastgelegd in een jaarlijks mutatieoverzicht door de overall coördinator sociaal domein .

Bij uitdiensttreding van een medewerker van de gemeente wordt ook de toegang tot Citrix beëindigd. Thuis inloggen op de gemeentelijke omgeving is dan niet meer mogelijk. Dit heeft ook tot gevolg dat het Suwinet niet meer benaderbaar is. Het intoetsen van de URL, het internetadres, vanaf een reguliere verbinding zal alleen een wit scherm opleveren.

5.2. Toegangsrechten Suwinet

De medewerkers van cluster ASD hebben allemaal het functieprofiel 'financieel administratief medewerker uitvoering sociaal domein'. Tot de taken behoort het behandelen van de aanvragen bijzondere bijstand voor niet-bijstandsgerechtigden. Hierbij horen toegangsrechten Suwinet. In dit geval gaat het voor alle medewerkers om toegang tot de overzichtspagina Rechtmatigheid+. Daarnaast is er een medewerker met de rol (SC108) ten aanzien van het inburgeringsportaal DUO. Uiteraard hebben de gemandateerde en de functioneel beheerder ook een autorisatie passend bij de functie.

De administratie van het gebruikersbeheer wordt bijgehouden in een autorisatiematrix door de functioneel beheerder. De overall coördinator sociaal domein controleert deze matrix op actualiteit na elke mutatie. Mutaties worden vastgelegd in een jaaroverzicht. Dit is weer onderdeel van de jaarlijkse evaluatie van IAA-rapportages.

5.3.Verlopen accounts

Bij het opvragen van generieke rapportages door de overall coördinator sociaal domein komen ook verlopen accounts in beeld. De overall coördinator sociaal domein controleert wat de reden hiervan is en of het account nog noodzakelijk is voor de betreffende medewerker. Indien het account weer geactiveerd moet worden, dan geeft de overall coördinator sociaal domein hiertoe opdracht aan de functioneel beheerder. Mocht het blijken dat dit account opgeheven kan worden, dan onderneemt de overall coördinator sociaal domein onmiddellijk hiertoe de nodige stappen. Hiervoor kan hier verwezen worden naar het autorisatieproces in- en uitdiensttreding van paragraaf 5.1.

De wachtwoordeisen voor Suwinet: Het wachtwoord moet bestaan uit minimaal 8 tekens, waarvan in ieder geval één teken voorkomt uit elk van de onderstaande series:

- 0123456789
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Abcdefghijklmnopqrstuvwxyz
- ~!@#$%^&*()-_=+[ ]{ }|;:,.<>/?

Het wachtwoord mag niet gelijk zijn aan voornaam, achternaam of gebruikersnaam. Het wachtwoord mag niet gelijk zijn aan één van de laatste 10 eerder gekozen wachtwoorden. Het wachtwoord moet minimaal 3 tekens verschillen van een eerder gebruikt wachtwoord. Het wachtwoord is 56 dagen geldig. Na deze periode verplicht Suwinet-Inkijk de gebruiker het wachtwoord te wijzigen. Suwinet-Inkijk geeft een aantal dagen voor het verlopen van het wachtwoord op het inlogscherm aan hoeveel dagen het wachtwoord nog geldig is. Als het wachtwoord na 56 dagen niet gewijzigd is wordt het account automatisch geblokkeerd. Indien een gebruiker van Suwinet-Inkijk langer dan 45 dagen niet inlogt op Suwinet-Inkijk wordt het account automatisch geblokkeerd. Zowel het wachtwoord wijzigen na 56 dagen als eenmaal in de 45 dagen inloggen op Suwinet-Inkijk geldt voor alle gebruikers, dus ook voor gebruikersbeheerders.

6.Bewustwording van veilig gebruik

Dit hoofdstuk gaat over bewustwording van het veilig gebruik van Suwinet. Allereerst wordt ingegaan op het uitdragen van beveiligingsbeleid bij indiensttreding. Hierna komen andere bewustwordingsacties aan de orde.

6.1. Uitdragen beveiligingsbeleid bij indiensttreding

De volgende acties worden opgevolgd bij indiensttreding van een nieuwe medewerker en zijn van belang voor het gebruik van Suwinet:

1. Het informatiebeveiligingsplan wordt uitgereikt en besproken.
2. Bij de uitleg omtrent informatieveiligheid is er specifiek aandacht voor logging en de rapportages.
3. De Elearning Veilig Gebruik Suwinet van de VNG wordt afgelegd door de nieuwe medewerker. Het certificaat van deze Elearning wordt vastgelegd
4. De nieuwe medewerker dient de eed of de belofte af te leggen.

Hieronder zullen deze acties nader uitgelegd worden.

1.Het informatiebeveiligingsplan wordt uitgereikt en besproken

Bij de indiensttreding van nieuwe medewerkers, die toegang tot het Suwinet moeten krijgen, wordt het informatiebeveiligingsplan Suwinet uitgereikt en besproken.
Deze actie is opgenomen in het autorisatieproces. De verantwoordelijkheid hiervoor ligt bij de overall coördinator sociaal domein.

2.Aandacht voor logging en rapportages

Elke klik in Suwinet wordt gelogd. Hiervan worden rapportages opgevraagd door de overall coördinator sociaal domein, waardoor er toezicht ontstaat op het juiste gebruik van Suwinet. Het is belangrijk dat medewerkers op de hoogte zijn van dit toezicht op de werkzaamheden. Het volgende moet bekend zijn bij de medewerkers die (gaan) werken met Suwinet:

- het bestaan van logging.
- het doel van logging.
- de aard van de gegevens die worden gelogd.
- het feit dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd.
- het feit dat onrechtmatig of doel overschrijdend gebruik van het Suwinet-Inkijk kan worden gecontroleerd.
- dat bij bovenstaande constatering de verantwoordelijke afdelingsmanager BCO de betreffende medewerker(s) daarop aanspreekt en dat hieraan gevolgen kunnen zitten.

3.Elearning veilig gebruik Suwinet

Er wordt aan nieuwe medewerkers verzocht om de Elearning veilig gebruik Suwinet van de VNG af te leggen. Het certificaat van de Elearning wordt vastgelegd in de administratie van Suwinet door de overall coördinator sociaal domein.

4.Eed of belofte

Alle nieuwe aangestelde medewerkers van de gemeente Borger-Odoorn moeten een belofte of een eed afleggen. Deze eed of belofte is een integriteitsverklaring; medewerkers beloven om zich als een goed ambtenaar te gedragen (artikel 6 ambtenarenwet 2017). Zonder integere ambtenaren is er immers geen betrouwbare overheid. Onderdeel van de eed of belofte is het zorgvuldig omgaan met vertrouwelijke informatie. Juist gebruik van Suwinet is een voorbeeld hiervan.
De eed of belofte wordt afgelegd bij de burgemeester tijdens een sessie. Tijdens deze sessie is integriteit een onderwerp.

Alle medewerkers die bij de gemeente werken ondertekenen een integriteitsverklaring. Dit geldt voor stagiares, ingehuurde en gedetacheerde medewerkers en medewerkers in vaste en tijdelijke dienst. De verklaring wordt opgenomen in het personeelsdossier van de medewerker.

6.2. Bewustwordingsacties informatieveiligheid

Bewustwording van informatieveiligheid is een terugkerend thema in de overleggen van de cluster ASD. De notulen, waaruit dit blijkt, worden vastgelegd in de administratie van Suwinet op de Qschijf. Hierbij kan worden aangemoedigd om lastige situaties ten aanzien van het gebruik van Suwinet juist te bespreken: van specifieke cases is veel te leren.
De generieke gebruikersrapportages bevatten geen BSN's van inwoners of gegevens van de individuele medewerkers. Hierdoor zijn deze rapportages ook goed te bespreken tijdens clusteroverleggen. Dit bevordert de bewustwording ten aanzien van de informatieveiligheid. Tevens kan het bijdragen aan het voorkomen van een terughoudendheid om Suwinet te gebruiken

Gemeente breed vinden er ook bewustwordingsactiviteiten ten aanzien van informatieveiligheid plaats. Voorbeelden hiervan zijn;

- berichten op het intranet over informatieveiligheid
- posters in de koffiecorners
- presentaties tijdens afdelings- en clusteroverleggen
- externe sprekers, workshops en crisis games
- resultaten mystery guest
- test phishing mail

7. Werkafspraken veilig gebruik

De volgende afspraken gelden op de werkvloer:

- Enkel inwoners van Borger-Odoorn worden geraadpleegd in Suwinet. Dit wordt geborgd door gebruik van de whitelist.

- Gegevens uit Suwinet worden niet lokaal opgeslagen (bijvoorbeeld op USB stick of harde schijf)

- Informatie uit Suwinet wordt niet uitgeprint.

- Bij het verlaten van de werkplek wordt de computer vergrendeld door de medewerkers door gebruik te maken van het slotje op de taakbalk (clear screen policy) Indien dit vergeten wordt door een medewerker, dan vergrendelt het systeem alsnog na 15 minuten.

- Thuiswerken is mogelijk. Suwinet is immers enkel te benaderen via de veilige gemeentelijke Citrix omgeving. Het spreekt voor zich dat de medewerkers hiermee op verantwoordelijke wijze omgaan. De generieke rapportages geven inzicht in het gebruik van Suwinet thuis.

- Suwinet raadplegen via een open onbeveiligde Wifi verbinding is niet toegestaan.

8. Beveiligingsincidenten

Bij beveiligingsincidenten wordt het gemeentelijk protocol gevolgd aangaande het melden van beveiligingsincidenten. Voor de melding en de rapportage van beveiligingsgebeurtenissen, zoals zwakke plekken in de beveiliging, (beveiligings)incidenten en datalekken, is een incidentmanagementprocedure ingericht. Daarin is voorzien in:

- de rapportage van beveiligingsgebeurtenissen
- een reactie- escalatieprocedure
- communicatie met de Informatiebeveiligingsdienst voor gemeenten (IBD)
- een contactpersoon voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
- vastlegging van alle beveiligingsincidenten in een systeem en escalatie aan de IBD.
- aanmerking van vermissing of diefstal van apparatuur of media, die gegevens van de gemeente kunnen vatten, als een beveiligingsincident.
- snelle en eenvoudige melding van beveiligingsincidenten en zwakke plekken in de beveiliging.
- evaluatie van informatie uit het beoordelen van beveiligingsmeldingen met als doel het verbeteren van beheersmaatregelen (PDCA-cyclus).
- het verzamelen, bewaren en presenteren van bewijsmateriaal conform de voorschriften voor bewijs vanuit strafrechtelijke wetgeving.
- analyse en beoordeling van de logging-resultaten en naar aanleiding daarvan het initiëren van nader onderzoek en/of verbeteracties.

Medewerkers worden geïnformeerd over hoe zij meldingen kunnen doen en wanneer dat van hen wordt verwacht.

Daarnaast worden beveiligingsincidenten aangaande Suwinet ook gemeld bij de Security Officer van het BKWI, de beheerder van het Suwinet.

9. Toezicht

Toezicht is een belangrijk thema in het kader van informatieveiligheid. In dit hoofdstuk wordt ingegaan op logging, de gebruikersrapportages, handelswijze bij oneigenlijk gebruik of misbruik, whitelist en ENSIA.

9.1. Logging en gebruikersrapportages

Elke klik in Suwinet wordt gelogd en wordt vastgelegd in rapportages. Deze informatie wordt beschikbaar gesteld door het BKWI (beheerder van Suwinet) aan de aangesloten organisaties. Aangesloten organisaties moeten toezicht houden op het juiste gebruik van het Suwinet via deze gebruikersrapportages. Uiteraard gaat het hier om enkel het eigen gebruik.
Er bestaan twee soorten gebruikersrapportages; generieke en specifieke gebruikersrapportages.

De gemeente Borger-Odoorn slaat deze gebruikersrapportages op in de Suwinetadministratie op de Qschijf. Deze locatie is slechte voor aangewezen medewerkers te benaderen. Specifieke rapportages kunnen persoonsgegevens bevatten

Generieke gebruikersrapportages

De generieke gebruikersrapportage wordt maandelijks opgevraagd door de overall coördinator sociaal domein. Deze rapportage geeft inzicht in het gebruik van Suwinet. Hierdoor is het mogelijk om toezicht te houden op het gebruik van klantgegevens en hierop te sturen. Mochten bijzonderheden worden geconstateerd, dan kan dit aanleiding zijn om een specifieke rapportage op te vragen. Voorbeelden van bijzonderheden zijn:

- Het veelvuldig raadplegen van een specifiek BSN.
- Een plotseling bijzonder hoog aantal raadplegingen van een medewerker.
- Een account dat kortdurend bestaan heeft.
- Afwijkende trends.

In generieke gebruikersrapportages zijn geen BSN's of gegevens van individuele medewerkers te vinden.

Ook geeft de generieke rapportage aanleiding om stil te staan bij het aantal ongebruikte of verlopen en geblokkeerde accounts. Hierin kan overigens aanleiding te vinden zijn om een specifieke rapportage op te vragen.

Specifieke gebruikersrapportages

In ieder geval tweemaal per jaar wordt een specifieke gebruikersrapportage opgevraagd door de overall coördinator sociaal domein. Bij bijzonderheden in de generieke rapportage wordt er ook een specifieke rapportage opgevraagd. Een verslag van bevindingen uit deze gebruikersrapportage worden vastgelegd op de Qschijf en ook teruggekoppeld aan de Security Officer. De bevindingen worden jaarlijks gerapporteerd aan de manager BCO in een jaarevaluatie.
De rapportages worden enkel gebruikt voor de controle op rechtmatig gebruik.

Borging proces

De gemandateerde (overall coördinator sociaal domein) vraagt de gebruikersrapportages op. De Security Officer houdt toezicht op het proces. Dit vindt in ieder geval plaats bij de halfjaarlijkse beoordeling van de specifieke rapportages. Er wordt daarnaast gezamenlijk gerapporteerd in de jaarevaluatie van de IAA-rapportages door gemandateerde en Security Officer. Tussentijds wordt enkel verslag gemaakt bij afwijkingen.

9.2. Oneigenlijk gebruik of misbruik

Het is mogelijk dat er oneigenlijk gebruik of misbruik wordt geconstateerd, bijvoorbeeld na het opvragen van een specifieke gebruikersrapportage. In dat geval zijn de volgende protocollen en beleidsstukken van belang:

- Gemeentebreed informatiebeveiligingsbeleid
- Gedragscode ambtenaren gemeente Borger-Odoorn
- Regeling melden integriteitsschending

Elke medewerker heeft de integriteitsverklaring ondertekend. Elke medewerker, die langer dan 6 maanden bij de gemeente werkt, legt daarbij de eed of de belofte af (artikel 5 Ambtenarenwet 2017). Overtreding van de Gedragscode kan leiden tot sancties, zoals een mondelinge of schriftelijke waarschuwing, schorsing als ordemaatregel of ontslag op staande voet. Deze sancties zijn terug te vinden in het Burgerlijk Wetboek. De Gedragscode ambtenaren gemeente Borger-Odoorn is terug te vinden in het Personeelshandboek op het intranet (ibo).

9.3. Gebruik van de whitelist

In 2017 is de whitelist landelijk geïntroduceerd. In Borger-Odoorn gaan we gebruik maken van de whitelist ingaande Q4 2019/Q1 2020. Er was niet direct in 2017 hiervoor gekozen gezien de beperkte omvang van het gebruik van Suwinet in Borger-Odoorn.

Wat is de whitelist?

Het is een filter dat ervoor zorgt dat enkel inwoners in de werkvoorraad geraadpleegd kunnen worden in Suwinet. De whitelist is een borging dat er enkel personen worden opgevraagd voor wie dat nodig is voor het uitoefenen van een wettelijke taak.

Bij sommige taken is het uiteraard nodig om wel ‘onbekende’ personen te raadplegen in Suwinet. Hierbij valt te denken aan inwoners met een nieuwe aanvraag voor een bijstandsuitkering.. Medewerkers, die belast zijn met dergelijke taken, hebben een escapemogelijkheid.

Waarom gaan we de whitelist gebruiken?

De whitelist geeft meer inzicht in het juiste gebruik van Suwinet in de organisatie en daarmee de mogelijkheid om hierop te sturen. De whitelist is een extra borg. Hiermee geven we ook het signaal dat wij de privacy en de informatieveiligheid serieus nemen. Op grond van de AVG zijn wij verplicht om het gebruik van persoonsgegevens tot een minimum te beperken. De techniek geeft ons een extra beveiligingsmogelijkheid

Welke BSN’s staan er op de whitelist?

BSN’s worden opgevoerd op de whitelist bij een aanvraag bijzondere bijstand. Na 1 jaar op de whitelist (vanaf datum invoer) wordt een BSN automatisch afgevoerd. Alle aanvragers van bijzondere bijstand van het afgelopen jaar zijn daarom te vinden op de whitelist.

9.4. ENSIA

Gemeenten moeten jaarlijks verantwoording afleggen over de gehele informatiebeveiliging middels ENSIA (Eenduidige Normatiek Single Information Audit). Suwinet is een onderdeel van de zelfevaluatie. Ook vindt er een Suwinet audit plaats. Na de zelfevaluatie en de audit wordt er een collegeverklaring opgesteld en conclusies worden opgenomen in het jaarverslag voor de gemeenteraad. Op deze wijze vindt er een horizontale verantwoording plaats. Verticale verantwoording vindt vervolgens ook plaats doordat de getoetste collegeverklaring wordt verzonden naar het ministerie van Sociale Zaken en Werkgelegenheid.

10. Evaluatie

Op diverse momenten in een jaar vindt er een evaluatie plaats. In dit hoofdstuk worden deze evaluaties op een rij gezet.

10.1. Evaluatie van informatiebeveiligingsplan

Dit informatiebeveiligingsplan wordt jaarlijks gecontroleerd op actualiteit en volledigheid. De organisatie en wet- en regelgeving zijn voortdurend in beweging. Ketenafspraken en inzichten kunnen wijzigen. Daarnaast kunnen er uit ENSIA ook relevante punten vloeien voor het informatiebeveiligingsplan. Om die reden is een jaarlijkse evaluatie van het plan noodzakelijk om deze actueel en juist te houden.

10.2. Evaluatie IAA rapportages

Jaarlijks wordt een evaluatie gehouden door de overall coördinator sociaal domein met de manager BCO (eindverantwoordelijke). Het doel is het borgen van de beveiliging van IAA-mechanismen (Identificatie, Authenticatie, Autorisatie) door te rapporteren over de beveiliging en rechtmatig gebruik van het Suwinet en de controle op de toegangsrechten.

Bij deze evaluatie worden de volgende stukken betrokken:
- Jaaroverzicht mutaties
- Autorisatiematrix
- Bevindingen uit generieke rapportages
- Bevindingen uit specifieke rapportages
- Jaarcyclus Suwinet (bijlage 1)

10.3. Zelfevaluatie ENSIA

In het kader van ENSIA vindt elk jaar een zelfevaluatie plaats op Suwinet. De resultaten hiervan moeten elk jaar op 31 december ingediend zijn.

10.4. Actiepuntenlijst

Het tijdspad (bijlage 1), met daarin onder meer de evaluatie van beleid, ENSIA en de bevindingen uit de rapportages, leidt tot actiepunten. Dat kunnen vaste acties zijn, maar ook verbeterpunten. Deze punten worden opgenomen in een actiepuntenlijst. Deze lijst is ook een doorlopend onderdeel van het tijdspad zelf. De beleidsmedewerker is eigenaar van de actiepuntenlijst. Een leeg format van deze actiepuntenlijst is opgenomen als bijlage 2.

11. Inzage in de gegevens

Inwoners hebben het recht om de eigen gegevens in te zien. Gegevensinzage Suwinet voor inwoners is mogelijk. In dit hoofdstuk worden de voorwaarden hiervoor omschreven. Allereerst zal in worden gegaan op inzage in de eigen gegevens. In de tweede paragraaf wordt omschreven hoe moet worden omgegaan met inzage van gegevens door een gemachtigde. De derde paragraaf betreft inzage in gegevens door een derde.

De gegevens via Suwinet zijn in elektronisch vorm te raadplegen. De gegevens mogen niet lokaal worden opgeslagen (bijvoorbeeld op harde schijf of USB stick)

11.1. Inzage in eigen gegevens

Een verzoek van een inwoner om de eigen gegevens in te zien dient schriftelijk te worden gedaan. Mocht een inwoner inzage willen in alle gegevens die bij een ketenpartner geregistreerd zijn, dan dient deze inwoner verwezen te worden naar de betreffende ketenpartner.

Behandeling schriftelijk verzoek inzage in eigen gegevens

1. Maak een afspraak met de inwoner. Verzoek hierbij om een geldig legitimatiebewijs mee te nemen.
2. Stel tijdens de afspraak allereerst de identiteit vast van de inwoner aan de hand van het legitimatiebewijs.
3. De inwoner kan vervolgens tijdens de afspraak meekijken op het scherm van de computer in de eigen gegevens. Uiteraard zorgt de medewerker ervoor dat het onmogelijk is dat per abuis gegevens van een derde worden gezien. (Gegevens van een minderjarig kind onder gezag van de inwoner zijn hier weer een uitzondering op)
4. Indien de inwoner hierom verzoekt, dan is het mogelijk dat er een uitdraai van de gegevens meegegeven wordt.

Inwoner is niet in staat om naar het gemeentehuis te komen

Om inzage in de eigen gegevens te verkrijgen kan de inwoner een gemachtigde aanwijzen. Paragraaf 11.2. zal hierop ingaan.

11.2. Inzage in gegevens door gemachtigde

Een schriftelijk verzoek tot inzage in gegevens door een gemachtigde kan alleen ingewilligd worden na overlegging van een machtiging. De identiteit van de gemachtigde en de identiteit van de betreffende inwoner moeten worden vastgesteld aan de hand van geldige legitimatiebewijzen. Het proces om de gegevens in te zien is verder gelijk aan hetgeen omschreven is in paragraaf 11.1.

11.3. Inzage in gegevens door een derde

Dit is niet mogelijk.

Bijlage 1: Tijdspad 2019 – 2022

2019	Q1 Jan	Q1 Feb	Q1 Mrt	Q2 Apr	Q2 Mei	Q2 Jun	Q3 Jul.	Q3 Aug	Q3 Sep	Q4 Okt	Q4 Nov	Q4 Dec
Opvragen Generieke Rapportage	X	X	X	X	X	X	X	X	X	X	X	X
Opvragen Specifieke Rapportage				X						X		
Rapportages beoordelen				X						X		
Zelfevaluatie ENSIA							X	X	X	X	X	X
Audit 2018 ENSIA	X											
Inleveren collegeverklaring (ENSIA)					X							
Toezending gemeentelijk jaarverslag aan Ministerie							X					
Uitvoering Actiepuntenlijst	X	X	X	X	X	X	X	X	X	X	X	X
Evaluatie IAA rapportages												X
Overleg ASD gebruik Suwinet				X						X		
Beleid,						X						

procedures en werkafspraken evalueren												
Aansluiten op de Whitelist						X						
2020	**Q1 Jan**	**Q1 Feb**	**Q1 Mrt**	**Q2 Apr**	**Q2 Mei**	**Q2 Jun**	**Q3 Jul.**	**Q3 Aug**	**Q3 Sep.**	**Q4 Okt.**	**Q4 Nov**	**Q4 Dec**
Opvragen Generieke Rapportage	X	X	X	X	X	X	X	X	X	X	X	X
Opvragen Specifieke Rapportage				X						X		
Rapportages beoordelen/ Tussentijdse evaluatie				X						X		
Zelfevaluatie ENSIA							X	X	X	X	X	X
Audit 2019 ENSIA	X											
Inleveren college verklaring (ENSIA)					X							
Toezending gemeentelijk jaarverslag aan Ministe							X					

rie												
Uitvoering Actiepuntenlijst	X	X	X	X	X	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Evaluatie IAA rapportages												**X**
Overleg ASD gebruik Suwinet				**X**						**X**		
Beleid, procedures en werkafspraken evalueren									**X**			
2021	**Q1 Jan**	**Q1 Feb**	**Q1 Mrt**	**Q2 Apr**	**Q2 Mei**	**Q2 Jun**	**Q3 Jul.**	**Q3 Aug**	**Q3 Sep.**	**Q4 Okt.**	**Q4 Nov**	**Q4 Dec**
Opvragen Generieke Rapportage	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
Opvragen Specifieke Rapportage				**X**						**X**		
Rapportages beoordelen/Tussentijdse evaluatie				**X**						**X**		
Zelfevaluatie ENSIA							**X**	**X**	**X**	**X**	**X**	**X**
Audit 2020 ENSIA	**X**											
Inleveren college verklari					**X**							

ng (ENSIA)												
Toezending gemeentelijk jaarverslag aan Ministerie							X					
Uitvoering Actiepuntenlijst	X	X	X	X	X	X	X	X	X	X	X	X
Evaluatie IAA rapportages												X
Overleg ASD gebruik Suwinet				X						X		
Beleid, procedures en werkafspraken evalueren									X			
Herijken informatiebeveiligingsplan Suwinet inkijk										X	X	X

Bijlage 2: Format actiepuntenlijst

Actiepuntenlijst Suwinet

Suwinet <jaartal>			
Wat willen we bereiken?		**Het gewenste niveau van informatieveiligheid bereiken en handhaven zoals omschreven in de BIG en het specifiek Suwinet normenkader.**	
Wat gaan we daarvoor doen?		**Eigenaar**	**Voortgang Voortgang wordt weergegeven volgens de kleuren in de legenda**
1. Toezicht houden op juist gebruik van Suwinet	1.1. Opvragen generieke rapportages (inclusief monitoren verlopen accounts)	1.1.	
	1.2. Opvragen en beoordelen specifieke rapportages	1.2.	
	1.3 Jaarlijkse evaluatie IAA Rapportages	1.3.	De jaarlijkse evaluatie vindt plaats aan het einde van een kalenderjaar
2. Horizontale en verticale verantwoording afleggen (ENSIA)	2.1. Uitvoeren audit	2.1.	
	2.2. College legt verantwoording af aan de gemeenteraad	2.2.	
	2.3. College stelt jaarverslag vast	2.3	
	2.4. Gemeenteraad keurt jaarverslag goed	2.4.	
	2.5. Toezending jaarverslag aan ministerie van BZK	2.5.	
	2.6. Zelfevaluatie	2.6.	
3. Beleid, procedures en werkafspraken up-to-date houden	3.1. Het nemen en uitvoeren van verbetermaatregelen n.a.v. Ensia	3.1.	
	3.2. het jaarlijks evalueren van het beleidsplan en bijstellen indien nodig	3.2.	
4. Bewustwordings-activiteiten ondernemen	4.1. Overleg ASD betreffende gebruik Suwinet	4.1.	
	4.2. Bewustwordings-activiteiten ontplooien	4.2.	
	4.3. Doorlopen van 4 stappen van bewustwording bij indiensttreding van een medewerker	4.3.	

5. Nadere actiepunten	5.1.	5.1.	
6. Nadere actiepunten	6.1	6.1	

	Afgewerkt
	Volgens planning
	Niet volgens planning
	Nog niet gestart

Bijlage 3: gebruikte afkortingen

AVG	Algemene Verordening Gegevensbescherming Europese verordening met rechtstreekse werking, die de verwerking van persoonsgegevens door particuliere bedrijven en overheidsorganisaties in de hele Europese Unie regelt.
Bbz 2004	Besluit bijstandsverlening zelfstandigen 2004
BIG	Baseline Informatiebeveiliging Gemeenten De BIG bestaat uit drie delen: de strategische baseline, de tactische baseline en de operationele baseline. De BIG is bedoeld om de beveiliging van de gemeentelijke informatiehuishouding op orde te brengen en te houden en bestaat uit diverse beveiligingsmaatregelen die geïmplementeerd en beheerd moeten worden.
BIO	Baseline Informatiebeveiliging Overheid De BIG wordt per 1 januari 2020 vervangen door de BIO. De BIO vervangt ook de bestaande baselines informatieveiligheid voor Rijk, Waterschappen en Provincies. Hierdoor is er vanaf 1 januari 2020 één normenkader voor informatiebeveiliging binnen de gehele overheid.
BKWI	Bureau Keteninformatisering Werk en Inkomen Het BKWI is opgericht ten behoeve van de uitvoering van wet SUWI (Structuur Uitvoering Werk en Inkomen) en is een organisatieonderdeel van het UWV. Het BKWI is beheerder van Suwinet. Het BKWI bewerkstelligt het delen van informatie over personen en bedrijven tussen overheidsorganisaties op een veilige en snelle wijze. [3]
DUO	Dienst Uitvoering Onderwijs DUO voert onderwijswetten en –regelingen uit en de wet Inburgering. Zo bekostigt DUO onderwijsinstellingen, verstrekt studiefinanciering, int lesgelden en beheert het diplomaregister.
ENSIA	Eenduidige Normatiek Single Information Audit Ensia stelt gemeenten in staat om in 1 keer slim verantwoording af te leggen over informatieveiligheid gebaseerd op de BIG (Baseline Informatiebeveiliging Gemeenten). De verantwoordingssystematiek over de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) is samengevoegd en gestroomlijnd. Het gaat hierbij om zowel horizontale verantwoording als de verticale verantwoording. Alle noodzakelijke informatie voor de verticale verantwoording is onderdeel van de horizontale verantwoording.[4]

[3] https://www.bkwi.nl/over-bkwi
[4] https://www.ensia.nl/#!/

GeVS	Gezamenlijke elektronische Voorzieningen SUWI Digitale infrastructuur voor uitwisselen van gegevens: art. 62 wet SUWI.
IAA rapportages	Identificatie, authenticatie en autorisatie rapportages Het doel van deze rapportages is het borgen van de beveiliging van IAA-mechanismen (Identificatie, Authenticatie, Autorisatie). Dit gaat over de beveiliging en rechtmatig gebruik van het Suwinet en de controle op de toegangsrechten.
IBD	Informatiebeveiligingsdienst De IBD ondersteunt gemeenten met informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Center. De IBD beheer de BIG en geeft regelmatig kennisproducten uit. De IBD faciliteert kennisdeling onderling. [5]
PDCA cyclus	Plan Do Check Act cyclus Cyclus om kwaliteitsverbetering te borgen in een organisatie.
Pw	Participatiewet De Participatiewet is de actuele bijstandswetgeving sinds 1 januari 2015. De Participatiewet heeft als doel om mensen naar werk toe te leiden en bijstand te verlenen aan mensen die niet op andere wijze in staat zijn om te voorzien in het inkomen.
SO	Security Officer De Security Officer adviseert over de informatieveiligheid en houdt toezicht op processen. Ook heeft de Security Officer een belangrijke rol in het organiseren van bewustwordingsacties. Tevens bewaakt de Security Officer de integraliteit van dit informatiebeveiligingsplan en het gemeentebrede informatiebeveiligingsbeleid. Ook is de Security Officer de coördinator van ENSIA.
Suwinet	De digitale infrastructuur die voortvloeit uit wet SUWI: Structuur Uitvoering Werk en Inkomen
Suwinet inkijk GSD	Het BKWI heeft diverse 'Suwinet-producten'. Suwinet inkijk GSD is het product waarmee een raadpleeg-aansluiting gerealiseerd wordt voor sociale diensten (GSD = Gemeentelijke Sociale Dienst. Dit kunnen ook gemeentelijke samenwerkingsverbanden zijn) op het Suwinet. Hierdoor zijn verschillende registraties te raadplegen voor sociale diensten in 1 webtoepassing. De informatie wordt uitgewisseld op basis van wet SUWI.
URL	Uniform Resource Locator Het adres van een bestand op internet, zoals een webpagina.

[5] https://www.informatiebeveiligingsdienst.nl/over-de-ibd/