Beveiligingsplan Suwinet gemeente Olst-Wijhe 2017

Olst-Wijhe, 9 maart 2017
doc. nr.: 17.000228

Inhoudsopgave

Hoofdstuk 1 Inleiding

Het Bureau Keteninformatisering werk en inkomen (BKWI), het Werkbedrijf, de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, de Informatie Beheer Groep (IBG), de RDW (Rijksdienst voor het wegverkeer) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur. Met de faciliteit Suwinet-Inkijk worden gegevens op basis van Burger Service Nummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers.

Het gaat om privacygevoelige gegevens over arbeidsverleden, loon, uitkeringen en opleiding van burgers. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.
Om de SUWI keten effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat “hun” gegevens door de partners in de Suwiketen op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi.

Onderzoek Inspectie SZW
De inspectie SZW heeft vanaf 2013 geconstateerd dat gemeenten niet zorgvuldig omgaan met persoonsgegevens die zij opvragen via Suwinet. De VNG heeft een verbetertraject opgezet. In de zomer van 2015 heeft de Inspectie SZW aangekondigd een nieuw onderzoek te starten naar het gebruik van Suwinet door alle gemeentelijke sociale diensten.
De gemeente Olst-Wijhe voldeed in 2013 aan drie van de zeven normen. Destijds reden om een verbeterplan Suwinet (vastgesteld op 8 april 2014) op te stellen en een aantal verbeteracties uit te voeren. Het beveiligingsplan Suwinet moet jaarlijks geëvalueerd worden, dit plan is op 25 augustus 2015 voor het laatst opnieuw vastgesteld.

In 2014 heeft de Inspectie SZW bij 78 gemeenten onderzoek gedaan naar de informatiebeveiliging van Suwinet. In het rapport “Veilig omgaan met elkaars gegevens (verschenen in mei 2015) is geconstateerd dat slechts een op de zes gemeenten voldoet aan alle zeven normen. Reden voor de inspectie om in september 2015 een zelfde onderzoek te voeren onder alle Nederlandse gemeenten.

Uit het op 18 januari 2016 ingekomen Definitief verslag van bevindingen onderzoek Veilig gebruik Suwinet 2015 blijkt dat de gemeente Olst-Wijhe voldoet aan de eisen van vertrouwelijkheid die worden gesteld aan de beveiliging van informatie die wordt uitgewisseld binnen Suwinet. Hierbij is getoetst aan een zevental geselecteerde normen uit het Normenkader behorende bij de Verantwoordingsrichtlijn Gezamenlijke elektronische Voorzieningen Suwi (GeVS). De gemeente Olst-Wijhe voldoet aan zeven van de zeven geselecteerde normen.

Eén van de normen is dat het beveiligingsplan jaarlijks moet worden geëvalueerd. In overleg met de drie Security Officers en de CISO (Jacques van der Heide) van de DOWR gemeenten is afgesproken om het beveiligingsplan Suwinet te koppelen aan de jaarlijkse evaluatie en deze te bespreken in het Informatiebeveiligingsoverleg. Na vaststelling door het college wordt deze ter kennisname aan de gemeenteraad gestuurd.

Voor Olst-Wijhe geldt dat het beveiligingsplan eigenlijk in augustus 2016 moest worden vastgesteld. Omdat er vanaf vorig jaar geen wijzigingen zijn, we het veilig gebruik van Suwinet goed onder controle hebben lijkt het logisch dit na afloop van het kalenderjaar te evalueren en aan de hand daarvan het nieuwe beveiligingsplan vast te stellen.

Sinds augustus 2013 hebben de medewerkers van Burgerzaken toegang tot Suwinet. De gegevens die opgevraagd kunnen worden blijven beperkt tot de adresgegevens zoals deze door het UWV worden

aangeleverd. Deze gegevens kan de medewerkers helpen bij ‘adresonderzoeken’, dat zijn die situaties waarin onduidelijkheid bestaat waar de burger woont. Dit loopt via een afzonderlijk contract. Dit beveiligingsplan Suwinet richt zich vooral op het gebruik voor de uitvoering van de Participatiewet.

Dit document is geschreven als verbijzondering van het Informatiebeveiligingsbeleid DOWR (14.407040) zoals dat voor de gemeente Olst-Wijhe op 24 september 2014 door de directie is vastgesteld.
Als basis voor dit beveiligingsplan is het voorbeeld beveiligingsplan Suwinet voor kleine gemeenten, zoals opgesteld door het BKWI, genomen. Deze is aangevuld met de specifieke zaken zoals deze voor gemeente Olst-Wijhe gelden

1.1 Leeswijzer

In hoofdstuk twee is een evaluatie van het gebruik Suwinet opgenomen. Deze evaluatie wordt gedaan aan de hand van de zelftest zoals deze door de VNG is opgesteld. Met deze zelftest kan elke gemeente in kaart brengen of zij inzage in Suwinet op maat aanbiedt aan haar medewerkers, of er goed op gebruik wordt toegezien en hoe de waarborgen daartoe zijn ingebed. In paragraaf 1.3 wordt nog wat verder ingezoomd op het gebruik van Suwinet over de periode 1 juni 2015 tot en met 31 december 2016.
In hoofdstuk drie volgt het Beveiligingsplan Suwinet Gemeente Olst-Wijhe 2017. In dit beveiligingsplan zal eerst het kader voor het beveiligingsplan geschetst worden. Vervolgens wordt ingegaan op de bevoegdheden van gebruikers en aangegeven in welke situaties Suwinet gebruikt mag worden.

Hoofdstuk 2 Evaluatie gebruik Suwinet.

2.1 Inleiding

De gemeente Olst-Wijhe werkt voor wat betreft bedrijfsvoering samen met Deventer en Raalte. Onderdeel van deze samenwerking is de I-werkorganisatie. Het informatiebeveiligingsbeleid DOWR (Deventer Olst-Wijhe en Raalte) is door de I-werkorganisatie opgesteld en is door de directie van gemeente Olst-Wijhe op 24 september 2014 vastgesteld.
In het Informatiebeveiligingsbeleid DOWR zijn algemene beleidsuitgangspunten over informatiebeveiliging opgenomen. Het document is opgesteld aan de hand van de in opdracht van de VNG ontwikkelde Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Er is een aanzienlijk aantal beleidsuitgangspunten nader uitgewerkt en er zijn beveiligingseisen en -maatregelen opgenomen. Het biedt het basisbeveiligingsniveau dat geldt voor de gehele gemeentelijke organisatie, voor alle processen en systemen. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Bijvoorbeeld SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties. Dit beveiligingsplan Suwinet gemeente Olst-Wijhe 2017 is een aanvulling/verdieping op het algemene informatiebeveiligingsbeleid DOWR.
Voor de evaluatie is (nu nog) gebruik gemaakt van de zelftest zoals aangeboden door de Vereniging van Nederlandse Gemeenten. In deze zelftest zijn de zeven meest elementaire normen opgenomen. Deze normen komen een op een terug in de Baseline Informatiebeveiliging (BIG).

Inmiddels heeft de werkgroep Herijking Normenkader Suwinet de bestaande normen tegen het licht gehouden, aangescherpt en vergeleken met de generieke bestaande baselines of normenkaders (BIR en BIG). Dit heeft geresulteerd in een (nieuw) normenkader van 26 normen die aansluiten bij de BIG.
Op dit moment wordt er in DOWR verband gewerkt aan het opstellen van nieuw (algemeen)beveiligingsbeleid en het doorlopen van de Gap Analyse. Het doel van de GAP-analyse is om te controleren of en in welke mate de maatregelen uit de Baseline Informatiebeveiliging zijn geïmplementeerd. Omdat een aantal normen overeenkomen met de Suwi-normen wordt voorgesteld om de komende periode te gebruiken de analyse ook voor wat betreft Suwinet uit te voeren en waar nodig verbeteracties uit te voeren.

2.2 Zelftest

Hieronder volgt een opsomming (vetgedrukt) van de vragen en de toelichting bij de beantwoording. De zelftest is nagelopen op basis van de Handreiking Veilig Gebruik Suwinet.

1.3. Het informatiebeveiligingsbeleid en beveiligingsplan zijn goedgekeurd door het management en / of de directie en / of het college van B&W.
Er is een algemeen informatiebeveiligingsbeleid voor de gemeente Olst-Wijhe. Daarnaast is er specifiek beleid gericht op Suwinet. Het Beveiligingsplan 2015 is op 25 augustus 2015 door het College van B&W vastgesteld.

Aan norm 1.3 is voldaan

1.4 Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage worden uitgedragen.
Het informatiebeveiligingsbeleid en het beveiligingsplan Suwinet 2015 zijn beschikbaar via Corsa en daar voor alle medewerkers te raadplegen.
Na het opstellen van het beveiligingsplan zijn alle medewerkers uitgebreid geïnformeerde over het (veilig) gebruik van Suwinet. Ook heeft Suwinet diverse malen op de agenda van het teamoverleg gestaan. Suwinet staat in het teamoverleg Werk en Inkomen als vast punt op de agenda.

Op 23 november 2015 en 19 september 2016 heeft de Security Officer de BKWI bijeenkomsten over veilig gebruik Suwinet bezocht.

Aan norm 1.4 is voldaan

1.5 Het informatiebeveiligingsbeleid, het beveiligingsplan of de beveiligingspassage worden jaarlijks geëvalueerd
De laatste evaluatie is vastgesteld op 25 augustus 2015. In overleg met de CISO DOWR gemeenten is besloten om jaarlijks te evalueren en het beveiligingsplan te actualiseren.
Het beveiligingsplan is besproken met de consulenten, de teamleider, de security officers DOWR en de werkgroep Informatiebeveiliging.

Aan norm 1.5 is voldaan

2.2 Functiescheiding
In de procedure autorisatie tot Suwinet (17.000243) en de procedure Controleren gebruik Suwinet (17.000244) is de functiescheiding vastgelegd. Voor wat betreft de functiescheiding is in het verbeterplan geconstateerd dat een aantal rollen tegelijkertijd aan één medewerker zijn toegekend. Dit is bij ons het geval omdat de medewerkers verschillende taken combineren. In het overzicht autorisaties is hierop een toelichting gegeven. Dit overzicht is als bijlage bij het plan gevoegd.

Aan norm 2.2 is voldaan

2.3 Security officer
Henrike Reinders is benoemd tot security officer. Er wordt periodiek een rapportage uitgebracht aan de teamleider over de uitgevoerde controles. Deze rapportage wordt door de teamleider ondertekend.
Deze taak is niet vastgelegd in haar functieomschrijving of takenoverzicht.
Met de overgang naar HR21 heeft de organisatie bewust gekozen voor een generieke functieomschrijving die niet op de persoon is toegespitst. Aanvullende afspraken kunnen worden vastgelegd in individuele afspraken, bijvoorbeeld via het HRM gesprek of team-plan. Er is voor gekozen om in de bijlagen een taakomschrijving Security Officer Suwinet op te nemen.

Aan norm 2.3 is voldaan.

13.1 Autorisatieprocedure
Er is een formeel vastgestelde procedure autorisatie tot Suwinet (17.000243).
Daarnaast is er een autorisatiematrix vastgesteld (17.000258), deze wordt telkens aangepast bij vertrek of komst nieuwe medewerkers. De laatste versie dateert van 10-1-2017.
Het accountbestand is gecontroleerd13-7-2015, 29-9-2016,13-10-2016 en 10-1-2017.
Bij vertrek van medewerkers wordt het account gelijk geblokkeerd, dit is opgenomen in de procedure autorisatie Suwinet. Aan de laatste voorwaarde is voldaan, er hebben geen andere medewerkers, dan uitvoerenden Participatiewet, toegang tot Suwinet. Voor de medewerkers van team Burgerzaken is een apart contract afgesloten.

Aan norm 13.1 is voldaan

13.5 Controle op toegang en gebruik
Vanaf 2014 zijn door de security officer alle gebruiksrapportages opgevraagd. Deze worden door de Security officer beoordeeld aan de hand van de vastgelegde Procedure controleren gebruik Suwinet.
De uitkomst wordt gerapporteerd op het Format gebruikrapportage Suwinet. Deze wordt ter accordering voorgelegd aan de teamleider. Deze gebruiksrapportages en het format worden opgeborgen in het dossier Suwinet. Er is in een aantal gevallen een specifieke rapportage van het BKWI opgevraagd. Deze specifieke rapportages zijn gecheckt. Nagenoeg alle geraadpleegde BSN nummers komen voor in het uitkeringen systeem (GWS). Daar waar dit niet het geval was is er een goede verklaring gegeven waarom het BSN nummer moest worden geraadpleegd.

De uitkomsten en opvallende zaken zijn in het Teamoverleg Werk en Inkomen met de consulenten gedeeld. Dit resulteert uiteindelijk in minder (dubbele) opvragingen. Zo bleek uit navraag bij het BKWI dat dubbelklikken met de muis telt als twee raadplegingen. Er is geen oneigenlijk gebruik c.q. misbruik geconstateerd. De te nemen stappen, als het zich onverhoopt wel voordoet, zijn opgenomen in de procedure controleren gebruik Suwinet.

Aan norm 13.5 is voldaan

De conclusie is dat Olst-Wijhe voldoet aan 7 van de 7 normen.

2.3 Evaluatie gebruik Suwinet.

In deze paragraaf wordt verder ingezoomd op het gebruik van Suwinet, de autorisaties en de beoordeling van de rapportages gebruik Suwinet. In de bijlage is de laatste gebruiksrapportage bijgevoegd, de uitkomsten zijn telkens aan de teamleider Werk, Inkomen en Zorg gerapporteerd en worden in het dossier Suwinet opgeborgen.

Rapportages gebruik Suwinet
Vanaf januari 2013 worden de gebruiksrapportages structureel opgevraagd uit Suwinet. Deze worden door de beleidsmedewerker Werk en Inkomen en de medewerker gebruikersbeheerder Suwinet beoordeeld. Dit mede aan de hand van de toelichting die is opgenomen bij de rapportages.
Als daar aanleiding toe is, bijvoorbeeld bij een onverklaarbaar hoog aantal opvragingen, door een medewerker of raadplegingen buiten kantoortijden, dan wordt een specifieke rapportage opgevraagd bij het BKWI. Deze specifieke rapportage geeft details over wie, wanneer welke persoon heeft geraadpleegd. Ook is na te gaan welke zoeksleutel is gebruikt, bijvoorbeeld BSN nummer of kenteken.

Hieronder wordt verder ingegaan op de controles over de periode juni 2015 tot en met november 2016.
Alle gebruiksrapportages zijn opgevraagd en er is een controle overzicht van gemaakt, ondertekent door de teamleider Werk, Inkomen en Zorg.
In een aantal gevallen zijn er specifieke rapportages opgevraagd en is er een steekproef genomen.
Hier gaat het om het aantal raadplegingen in Suwinet, raadplegingen buiten kantoortijd, hoogst aantal gebruikers dat hetzelfde BSN heeft geraadpleegd en het hoogst aantal raadplegingen per actieve gebruiker.
Over de maanden oktober en november 2016 is van alle geraadpleegde BSN nummers gecontroleerd of deze voorkomen in ons uitkeringssysteem. Dit bleek op een paar raadplegingen na het geval te zijn. Daar waar dit niet het geval was betrof het burgers die zich wel hebben gemeld voor een uitkeringsintake maar die verder geen aanvraag hebben ingediend en dus niet als zodanig geregistreerd zijn of het ging om mogelijke partners waar een bijzonder onderzoek naar is ingesteld. De medewerkers van het Team Werk en Inkomen houden voor zich zelf bij wanneer en waarom ze een BSN nummer die niet in het systeem voorkomt raadplegen. Er is niet gebleken van ongeoorloofde raadplegingen.

In een aantal maanden is het aantal opvragingen hoger geweest dan gebruikelijk, dit had bijvoorbeeld te maken met de extra aanvragen voor de Bijzondere bijstand.
Wat opvalt, is dat een aantal BSN-nummers door meerdere collega's geraadpleegd wordt. Dit komt omdat we werken met een scheiding van taken op het gebied van inkomen, doelmatigheid en minimabeleid (waaronder de bijzondere bijstand valt). Het kan dus voorkomen dat een BSN nummer in een maand door drie klantmanagers geraadpleegd wordt.

De uitkomsten van de rapportages en de, zoals hierboven genoemde, bijzonderheden zijn telkens gedeeld met de klantmanagers. Al deze acties hebben inmiddels geleid tot een aanzienlijke vermindering van het aantal raadplegingen, en het belangrijkste de bewustwording dat we zorgvuldig moeten omgaan met de privacy van onze burgers.

Autorisaties
Het BKWI heeft eind 2016 (opnieuw) een handleiding uitgeven: "Toegangsrechten voor Suwinet-inkijk". Dit document geeft een overzicht van de pagina's op Suwinet-inkijk. Naast een korte uitleg van de inhoud van

de pagina's wordt ook aangegeven voor welke functie of taken de rol bedoeld is. Deze handleiding vormde aanleiding om een nieuwe autorisatie-matrix op te stellen. De autorisaties zijn daarop op 10 januari 2017 en voor het laatst op 8 maart 2017 aangepast volgens deze lijst. Deze zijn beide opgeborgen in het dossier. In de bijlage wordt een actuele autorisatie-matrix bijgevoegd.

Accounts
In de gebruiksrapportage is ook informatie opgenomen over accountbeheer. Een account wordt geblokkeerd als er een aantal keren een foutief wachtwoord wordt ingegeven of als er langere tijd niet wordt ingelogd. Dit laatste kan wijzen op een langdurig zieke collega of de gebruiker is niet meer in dienst. Er is een procedure Autorisatie tot Suwinet vastgesteld. Zoals uit de rapportage gebruikbeheer blijkt hebben we een geblokkeerd account. Dit heeft te maken met langdurige ziekte van één collega. Bovenstaande wijst er op dat de procedure autorisatie bij vertrek van medewerkers goed werkt. Daarnaast is er nog een account niet actief. Dit klopt dit is het account voor de vervanger van de gebruikersbeheerder. Deze hoeft dus niet vaak in actie te komen.

Conclusie
Er is over de periode juni 2015 tot en met 31 december 2016 (voor zover na te gaan) geen onrechtmatig gebruik gemaakt van Suwinet inkijk.
Er is een toename van de bewustwording dat we omgaan met privacy gevoelige gegevens en dat we hier zorgvuldig mee om moeten gaan. Dit komt mede door de toegenomen aandacht en het delen van de uitkomst van controles met de klantmanagers. We zien dan ook een afname van het aantal raadplegingen.

Hoofdstuk 3 Beveiligingsplan Suwinet

Zoals uit de evaluatie in hoofdstuk 2 is gebleken kan worden geconstateerd dat we zorgvuldig omgaan met Suwinet. Jaarlijks wordt het Beveiligingsplan Suwinet geactualiseerd. Als basis voor dit plan is het voorbeeld Beveiligingsplan Suwinet (voor kleine gemeenten) genomen zoals in augustus 2013 gepubliceerd op de website van het BKWI. Als eerste wordt ingegaan op het kader voor het Suwinet beveiligingsplan.

3.1 Kader voor het Suwinet beveiligingsplan

Zowel het Bureau Keteninformatisering Werk en Inkomen als het Coördinatiepunt ICT ondersteunt de invoering bij gemeenten en stellen diverse voorbeelden via hun website beschikbaar. De gehanteerde plannen zijn veelal informatiebeveiligingsplannen die van toepassing zijn op de gehele organisatie. Onderwerpen zijn bijvoorbeeld:
- fysieke toegangsbeveiliging gebouwen
- fysieke toegangsbeveiliging dossiers
- fysieke toegangsbeveiliging tot computerapparatuur
- beveiliging van digitaal opgeslagen gegevens
- beveiliging van (digitale) communicatiekanalen
- back-ups van gegevens
- integriteitbeleid gemeente
- calamiteitenplan
- waarborgen continuïteit (noodstroom e.d.)
- periodieke testen en evaluatie van bovengenoemde zaken.

De gemeente Olst-Wijhe heeft gemeentebreed regels vastgesteld voor de beveiliging van gegevens. Deze standaardbeveiliging vormt het vertrekpunt voor het specifieke beveiligingsplan van de afdeling zoals bedoeld in de bijlage XIV van de regeling SUWI.
De gemeente Olst-Wijhe gaat ervan uit dat het voldoende is om voor de medewerkers van het team Werk en Inkomen gebruikersnormen voor het gebruik van Suwinet op te stellen.
NB de medewerkers die gebruik maken van Suwinet maken deel uit van het team Werk, Inkomen en Zorg. De medewerkers van het onderdeel Zorg hebben geen toegang tot Suwinet, vandaar dat hier wordt gekozen voor de benaming Team Werk en Inkomen.

3.2 Gebruikers van Suwinet-Inkijk

De volgende functies zijn geautoriseerd om gebruik te maken van Suwinet-Inkijk:
- Medewerker Uitkeringsadministratie verzorgt autorisatie voor Suwinet
- Beleidsmedewerker Werk en Inkomen (Security officer) vraagt logging gegevens op
- Consulenten Werk en Inkomen, Minimabeleid, Terugvordering en Verhaal en de medewerker uitkeringsadministratie mogen raadplegen
- Medewerkers Sociale Recherche
- Medewerkers Burgerzaken belast met adresonderzoeken, mogen raadplegen.

De teamleider Werk, Inkomen en Zorg is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet Inkijk.

3.3 Functie raadplegen

Hierboven is benoemd wie Suwinet-Inkijk mogen raadplegen. Hier wordt aangegeven wanneer dat mag. Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik. Over het algemeen geldt dat slechts mag worden geraadpleegd, indien die stap binnen het werkproces expliciet is beschreven.
Consulenten Werk en Inkomen mogen raadplegen bij het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, Ioaw, Ioaz, Bbz, bijzondere bijstand of een andere door de afdeling uitgevoerde regeling op grond van de Participatiewet betreft. Het raadplegen van Suwinet Inkijk wordt met een afschrift in het dossier vastgelegd. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen.
Medewerkers die verantwoordelijk zijn voor terugvordering en verhaal mogen raadplegen bij onderzoeken die samenhangen met verhaal op onderhoudsplichtigen of vorderingen. Dit bijvoorbeeld ter vaststelling van woonplaats, draagkracht, inkomen of werkgever.
De medewerkers van het team Burgerzaken mogen de gegevens uit Suwinet-Inkijk raadplegen om adresonderzoeken te behandelen.

Een BSN raadplegen van een cliënt die onbekend is in GWS in verband met een rechtmatigheids- en/of fraudeonderzoek wordt door de medewerker zelf geregistreerd om dit indien nodig achteraf te kunnen verantwoorden aan de security officer en de teamleider Werk, Inkomen en Zorg. Hierbij kan men denken aan “mogelijke huisgenoot”, “mogelijk kind”, “mogelijke partner”. Dit overzicht moet op verzoek aan de security officer of teamleider getoond worden.

3.4 Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van o.a. de gemeente kan worden nagegaan.

Het doel van deze logging is tweeledig:
1. Tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking:
2. Wetenschappelijke en/of statistische doeleinden.

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd.
Bij indiensttreding krijgen zij het protocol ‘Suwinet-Inkijk’ (bijlage 1) uitgereikt. Dit is opgenomen in de procedure Autorisatie tot Suwinet. De gemeente Olst-Wijhe kent voor alle medewerkers de integriteitsbelofte. Desondanks wordt er voor gekozen om de medewerkers die Suwinet raadplegen ook een verklaring, zoals in bijlage 4, te laten ondertekenen. Alle huidige medewerkers hebben een dergelijke verklaring ondertekend.
Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. De medewerkers zijn op de hoogte van de volgende informatie:

- Het bestaan van de logging-gegevens;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd;

Doelen van de logging;

- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doel overschrijdend gebruik van het Suwinet-Inkijk wordt geconstateerd.
- Dat bij bovenstaande constatering dit door de teamleider wordt gecommuniceerd met de betreffende medewerker(s).

In het kader van de beveiliging wordt het beheer voor het gebruik van Suwinet neergelegd bij de medewerker Functioneel Beheer. De medewerker uitkeringsadministratie is werkzaam voor de Olst-Wijhe maar heeft zijn werkplek in Deventer. Zij zijn verantwoordelijk voor het beheren van accounts. De (logging)-gegevens over het gebruik van Suwinet-Inkijk worden regelmatig uitgevraagd door de beleidsmedewerker Werk en Inkomen. De medewerker houdt per kwartaal een steekproef of bevragingen Suwinet aan de gemaakte afspraken voldoen. De resultaten van deze steekproef worden gerapporteerd aan de teamleider Werk, Inkomen en Zorg.

3.5 Whitelist en escapefunctie op Suwinet-Inkijk

Sinds eind 2016 kan binnen Suwinet-Inkijk gebruik worden gemaakt van de zogenoemde Whitelist. Dit is een filtermechanisme, het raadplegen van gegevens wordt begrensd tot de “eigen ”burgers”.
Een whitelist is een lijst die de BSN’s bevat van alleen die burgers waar de gemeente een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde “escapefunctie”. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van de burgers.
Voorgesteld wordt om in 2017 over te gaan tot implementatie van deze whitelist en escapefunctie op Suwinet-Inkijk. Hiervoor is extra inzet nodig van Functioneel Beheer DOWR. Voor zover nu na te gaan betreft het hier alleen (geringe) personele capaciteit voor het aanleveren van de gegevens.

3.6 Autorisaties voor meer gemeenten functionaliteit

Medewerkers van gemeenten met uitvoerende taken binnen een samenwerkingsverband hebben momenteel per afzonderlijke gemeente waar zij taken voor uitvoeren één account waarmee zij inloggen op Suwinet-Inkijk. Een voorbeeld zijn de medewerkers Functioneel Beheer die in DOWR verband werken maar ook de Sociale Recherche die voor zowel gemeente Deventer, Olst-Wijhe als ook Raalte werkzaamheden uitvoert.

Vanaf eind 2016 is het voor deze gemeenten mogelijk om binnen 1 account aan te geven voor welke (verantwoordelijke) gemeente de medewerker een bevraging uitvoert.

Medewerkers hoeven dus niet meer steeds uit te loggen uit Suwinet-Inkijk om naar een gemeente account te gaan, maar blijven binnen hun eigen account werken en kunnen daar dan aangeven voor welke gemeente zij werken.
Zowel de uitvoerende als de verantwoordelijke gemeente worden per bevraging vastgelegd in de logging van Suwinet-Inkijk.

Voorgesteld wordt om in samenwerking met DOWR voor wat betreft de Sociale Recherche deze functionaliteit aan te vragen.

Bijlage 1 Tien gouden tips bij beveiliging van persoonsgegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving.
Als handvat hierbij 10 gedragsregels voor medewerkers van het team Werk en Inkomen.

1. Beheren van wachtwoorden
De gebruiker moet het door de medewerker uitkeringsadministratie uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord uiterlijk na een jaar.
De gebruiker heeft dus het eigen beheer over het wachtwoord.
Zodra een medewerker de gemeente verlaat, wordt het account verwijderd.
Wanneer het account niet wordt gebruikt, vervalt het account automatisch.

2. Melden van beveiligingsincidenten
Het is belangrijk dat beveiligingsincidenten worden gemeld bij de functioneel beheerder. De functioneel beheerder kan vervolgens een andere functionaris die daartoe is bevoegd is, inschakelen om dat incident te onderzoeken.
Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht
Binnen de afdeling wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

4. Gedragscode internet- en e-mailgebruik
De gemeente hanteert een protocol voor gebruik van e-mail en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe e-mail en internet wordt geobserveerd.

5. Kennisnemen van het informatiebeveiligingsbeleid
Het binnen de gemeente geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is op iedereen binnen het team van toepassing die gebruik maakt van Suwinet-Inkijk. Bestaande gebruikers zijn op de hoogte; nieuwe gebruikers worden op de hoogte gesteld.
Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Jaarlijks wordt dit onderwerp geagendeerd voor het teamoverleg.

6. Gegevensverstrekking aan derden via de telefoon
Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen.
Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben.
In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging.
Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien afkomstig van een vaste contactpersoon.

7. Clean desk en clear screen policy
De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is

ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven.
Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers.
Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord), zodra de medewerker de werkplek verlaat.

8. Geen vertrouwelijke gegevens in de prullenbak
De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de afdeling. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Binnen de gemeente is geregeld hoe vertrouwelijke stukken worden verzameld en vernietigd en iedereen is daarvan op de hoogte. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een prullenbak of een bak die bestemd is voor oud papier.

9. Aanspreken van onbekende personen
In het geval dat een medewerker van de afdeling een voor hem/haar onbekende persoon in de gang van de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet.
Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hun beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naar toe te begeleiden.

10. De dagelijkse werkzaamheden vs. Informatiebeveiliging
Informatiebeveiliging is uitermate belangrijk voor het werk binnen een afdeling waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom in het werkoverleg geregeld aandacht voor dit onderwerp dient te zijn.

Bijlage 2 Procedure Autorisatie tot Suwinet (17.000243)

Inleiding
De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn.

Doel
Deze procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet. Hiermee wordt de logische toegangsbeveiliging afgedicht voor de Suwinet gegevens en de vertrouwelijkheid hiervan gewaarborgd.

Definitie
Met een autorisatie wordt een door het bevoegd gezag gelegitimeerde toegang tot één of meerdere informatiesystemen van de gemeente bedoeld.
De procedure bestaat uit drie afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:
Autorisatie tot het netwerk;
Autorisatie tot Suwinet;
Periodieke controle autorisaties.

Beheer
Om toegang te kunnen krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie(s) tevens een bevoegdheid nodig op netwerk- en/of het systeemniveau. Deze bevoegdheden worden beheerd door de systeembeheerder. De bevoegdheden binnen Suwinet worden beheerd door Gebruiksbeheerder Suwinet .

Proceseigenaar
De proceseigenaar is de Teamleider Werk, Inkomen en Zorg.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het college van B&W en namens deze bij de Teamleider Werk, Inkomen en Zorg.

De verantwoordelijkheid om de toegang tot het netwerk te verlenen berust bij de Teamleider Werk, Inkomen en Zorg. De uitvoering hiervan ligt bij de systeembeheerder.
De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet berust bij de Teamleider Werk, Inkomen en Zorg**.** De uitvoering hiervan ligt bij de Gebruiksbeheerder Suwinet.

Actualiteit
De Beleidsmedewerker Werk en Inkomen is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, leidt dit tot de goedkeuringsprocedure opgenomen in het Informatiebeveiligingsplan.

Uitvoering
<u>Autorisatie tot het netwerk</u>
De autorisatie voor gebruik van het standaard gemeentelijk netwerk wordt bij aanstelling geregeld:

- Bij aanstelling van een nieuwe medewerker vraagt de Teamleider Werk, Inkomen en Zorg schriftelijk een netwerk account aan bij de i-Werkorganisatie DOWR;
- De i-Werkorganisatie DOWR beoordeelt het autorisatieverzoek;
- Na honorering van het verzoek maakt de systeembeheerder een standaard netwerk account aan;
- Het informatiesysteem is voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes (passwords). Deze wachtwoorden zijn maximaal 60 dagen geldig. De toegangscode bestaat uit minimaal 8 posities. Na maximaal 3 foutieve aanmeldpogingen vervalt

het wachtwoord automatisch. Wachtwoorden van anderen zijn niet door (eind)gebruikers op te vragen;
- De gebruiker krijgt van de systeembeheerder een korte instructie hoe zich aan te melden en hoe om te gaan met wachtwoorden;
- Bij vertrek van een medewerker geeft de Teamleider Werk, Inkomen en Zorg dit door aan de i-Werkorganisatie DOWR waarna de systeembeheerder de autorisatie intrekt.

Autorisatie tot Suwinet
- De om autorisatie verzoekende medewerker dient een verzoek in voor een nieuwe of gewijzigde autorisatie voor Suwinet bij de Teamleider Werk, Inkomen en Zorg.
- De Teamleider Werk, Inkomen en Zorg beoordeelt het autorisatieverzoek. Hierbij worden de raadpleegbare gegevens afgestemd op de taakinhoud van de aanvrager;
- De medewerker ontvangt van de Teamleider Werk, Inkomen en Zorg het Protocol Suwinet-Inkijk.
- De Gebruiksbeheerder Suwinet die het bericht van de Teamleider Werk, Inkomen en Zorg ontvangt regelt vervolgens de autorisatie in Suwinet;
- De systemen zijn voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes. Deze wachtwoorden zijn maximaal 56 dagen geldig en bestaan uit minimaal 6 posities. Na maximaal 3 foutieve aanmeldpogingen vervalt het wachtwoord automatisch. Wachtwoorden van anderen zijn niet door (eind)gebruikers op te vragen;
- De gebruiker krijgt van de Gebruiksbeheerder Suwinet die het autorisatieniveau heeft verwerkt een terugmelding over het autorisatieverzoek. Tevens krijgt de gebruiker een korte instructie hoe hij zich aan kan melden en hoe om te gaan met Suwinet.
- Bij vertrek of wijziging van de functie van een medewerker geeft de Teamleider Werk, Inkomen en Zorg dit door aan de Gebruiksbeheerder Suwinet, waarna de Gebruiksbeheerder de autorisatie intrekt of wijzigt;

Periodieke controle autorisaties
De Gebruiksbeheerder Suwinet zorgt eenmaal per jaar voor een overzicht (geprint verslag van de in het systeem toegekende autorisaties).
Mede op basis van dit overzicht brengen de Gebruiksbeheerder en de beleidsmedewerker Werk en Inkomen een rapportage uit aan de Teamleider Werk, Inkomen en Zorg. Deze rapportage wordt opgenomen in de Evaluatie gebruik Suwinet.

In deze rapportage wordt aangegeven:
- of de geïmplementeerde autorisaties overeenkomen met de toegekende autorisaties;
- of de geregistreerde gebruikers en de aan hen toegekende autorisaties correct zijn. Hierbij wordt het controleverslag vergeleken met de autorisatieformulieren en tevens vergeleken met wat is vastgelegd in het beveiligingsplan Suwinet van de gemeente;
- of bij tussentijdse wijzigingen in taak/functie de Teamleider Werk, Inkomen en Zorg de Gebruiksbeheerder Suwinet hierover informeert en of bij ontslag of vertrek de autorisatie direct wordt geblokkeerd.

Indien de uitgevoerde controle hiertoe aanleiding geeft, geeft Teamleider Werk, Inkomen en Zorg opdracht aan de Gebruiksbeheerder Suwinet, om de nodige correcties aan te brengen. De Gebruiksbeheerder Suwinet past zo nodig de autorisatie(s) aan stelt de betreffende gebruiker op de hoogte van een wijziging in zijn bevoegdheidsprofiel.

Bijlage 3 Procedure controleren gebruik Suwinet (17.000244)

Inleiding
De gemeente moet in een procesbeschrijving vastleggen hoe dit proces verloopt, de periodiciteit en wie daarbij betrokken zijn, aan wie gerapporteerd wordt. De resultaten van de controles zijn input voor bijscholing /bewustwording van de medewerkers.

Doel
Deze procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het controleren van het gebruik van Suwinet.

Procedure
De procedure bestaat uit vijf afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:
Het opvragen van Gebruiks-rapportages;
Het uitvoeren van controles op de Gebruiksrapportages;
Het rapporteren over de uitgevoerde controle;
Het informeren over de rapportages en adviseren over vervolgstappen;
Periodieke rapportage over controles, resultaten en maatregelen aan bestuur.

Proceseigenaar
De proceseigenaar is de Teamleider Werk, Inkomen en Zorg.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het college van B&W en namens deze bij de Teamleider Werk, Inkomen en Zorg.

De verantwoordelijkheid voor de controle op het gebruik Suwinet berust bij Teamleider Werk, Inkomen en Zorg. De uitvoering hiervan ligt bij de Gebruiksbeheerder Suwinet en de Security Officer Suwinet. Beide zijn geautoriseerd voor het opvragen van de Gebruiks-rapportage. Bij constatering van mogelijk onrechtmatig gebruik wordt opgeschaald naar de Teamleider Werk, Inkomen en Zorg.

Periodiciteit
De Gebruiksrapportage wordt een keer per kwartaal over de afgelopen periode opgevraagd door de Security Officer Suwinet en samen met de gebruiksbeheerder geanalyseerd. Hiervan wordt per kwartaal een rapportage opgemaakt volgens een vastgesteld format. Deze rapportages worden ter kennisname aangeboden aan de Teamleider Werk, Inkomen en Zorg en de medewerkers van het Team Werk en Inkomen. Jaarlijks wordt hierover gerapporteerd in de Evaluatie gebruik Suwinet.

Actualiteit
De Teamleider Werk, Inkomen en Zorg is verantwoordelijk voor het actueel houden van deze procedure. Indien de procedure inhoudelijk wijzigt, leidt dit tot de goedkeuringsprocedure opgenomen in het Informatiebeveiligingsplan.

Uitvoering
<u>Het opvragen van de Gebruiks-rapportages</u>
De gebruiks-rapportages worden een keer per kwartaal opgevraagd door de Security Officer

<u>Het controleren van de Gebruiks-rapportages</u>
De Security Officer en de gebruiksbeheerder voeren een controle uit op de gebruiks-rapportage Suwinet. Dit doen zij aan de hand van de leeswijzer die het BKWI met de rapportage meestuurt.

<u>Het opvragen van individuele gebruiksrapportages</u>
Indien daartoe aanleiding is kan de Security Officer individuele gebruiksrapportages opvragen bij het BKWI. Deze worden in ieder geval twee keer per jaar voor alle gebruikers opgevraagd.

Indien hiertoe aanleiding bestaat (bijvoorbeeld door een bijzondere gebeurtenis) kan er ook een steekproef op het gebruik worden opgevraagd. Dit alleen in opdracht van de Teamleider Werk, Inkomen en Zorg. Deze opdracht wordt schriftelijk gegeven en bij de rapportage gevoegd.

Het rapporteren over de uitgevoerde controle;
De controle en conclusies daaruit worden vastgelegd in de rapportage format en ondertekent door de Teamleider Werk, Inkomen en Zorg.

De rapportage wordt door de Security Officer gearchiveerd.

Het informeren over de rapportages en adviseren over vervolgstappen;
Zijn er signalen over oneigenlijk gebruik dan wordt opgeschaald naar de Teamleider Werk, Inkomen en Zorg. De Individuele medewerker wordt gevraagd zijn/haar zoekgedrag te verantwoorden.

Indien blijkt dat de medewerker het zoekgedrag niet kan verantwoorden en er zijn aanwijzingen voor norm overschrijdend gedrag dan wordt gehandeld volgens het vastgestelde integriteitsbeleid. De vakgroep P&O wordt in dat geval ingeschakeld Er wordt dan gehandeld conform artikel 16 van de CAR/UWO. . In het Privacyreglement e-mail en internetgebruik gemeente Olst-Wijhe is vastgelegd wat wel en niet mag.

Periodieke rapportage over controles, resultaten en maatregelen aan bestuur.
In het Beveiligingsplan Suwinet, dat jaarlijks moet worden vastgesteld, is een hoofdstuk Evaluatie gebruik Suwinet opgenomen. In dit hoofdstuk worden de resultaten van de uitgevoerde controles vermeld.

Bijlage 4 Verklaring medewerkers

Door aansluiting op Suwinet is het mogelijk om gegevens uit te wisselen met o.a. de Belastingdienst, de Informatiebeheergroep, het Uitvoeringsorgaan Werknemersverzekeringen, het CWI, de RDW en gemeenten (zijnde de bronnen).
Als gevolg daarvan zijn genoemde instanties te beschouwen als “verantwoordelijke” in de zin van de wet Bescherming Persoonsgegevens (WBP) en daarom allemaal gebonden aan de bepalingen in deze wet.
In de toekomst zal het aantal bronnen uitgebreid worden. Deze verklaring geldt ook voor bronnen die in de toekomst aangesloten gaan worden.

De gemeente is op grond van voornoemde bepalingen gehouden om interne maatregelen te nemen ter voorkoming van een (mogelijk) onrechtmatig, onregelmatig of doel overschrijdend gebruik van de beschikbare (persoons-)gegevens.
Dit betekent dat de teamleider Werk, Inkomen en Zorg de verplichting heeft om regelmatig (met behulp van zogeheten audit-logging gegevens) te laten controleren of het gebruik van de gegevens uit Suwinet niet onwettig geschiedt of verder gaat dan is toegestaan.

Ondergetekende,……

verklaart:

- het raadplegen van de gegevens in Suwinet te beperken tot de gegevens van cliënten die blijkens de in gemeentelijke applicatie opgenomen werkprocessen bij haar of hem in behandeling zijn;
- deze gegevens enkel aan te wenden voor het behandelen van de desbetreffende bijstandsaangelegenheid;
- het raadplegen van de gegevens uit Suwinet te beperken tot de gegevens die noodzakelijk zijn om de adresonderzoeken te behandelen.
- op de hoogte te zijn van de controle die de security-officer regelmatig dient in te stellen.
- bekend te zijn met de sancties die volgen bij onrechtmatig gebruik van Suwinet zoals opgenomen in de CAR-UWO, met als uiterste gevolg ontslag.

Datum:……..……

Handtekening:……...

Bijlage 5 Autorisaties Suwinet

Autorisaties Suwinet	Functie groepen								
Overzichtspagina's	**Beheer**	**Klantmanager Inkomen**	**Klantmanager Werk**	**Minimabeleid**	**Terugvordering en Ver**	**Toetsing***	**Sociale recherche**	**DUO**	**Security Officer**
Rechtmatigheid		X		X	X	X	X		
Rechtmatigheid+		X		X	X	X			
Re-integratie		X	X			X			
Handhaving							X		
Terugvordering en Verhaal					X				
Kostendelerstoets		x		x		x	x		
Bronpagina's									
Bedrijvenregister		x	x	x	x	x	x		
GBA, GBA2, GBA3, GBA-volledig		x	x	x	x	x	x		
Bijstandsregelingen		x	x	x	x	x	x		
Fraude-vorderingen					x	x	x		
Belastingdienst		x		x		x			
Kadaster		x		x	x	x	x		
RDW		x		x		x	x		
RDW peildata		x		x		x	x		
RDW+							x		
UWVWb		x	x	x	x	x	x		
SVB gegevens		x		x	x	x	x		
UWV uitkeringen		x		x	x	x	x		
Inkomstenverhoudingen		x		x	x	x	x		
DUO gegevens		x	x	x	x	x	x		
Zoek in GBA							x		
Zoek+ in GBA							x		
Zoek in Kadaster							x		
Zoek in RDW							x		
Zoek in RDW+							x		
Fraudescorekaart		x		x		x	x		
SBR Query			x						
Beheer: ww & blokkeren	x								
Gebruikersadminsitratie	x								
Onderhoud en correctieservice	x								
Onderhouden status wijzigingsverzoeken	x								
Correctieservice	x								
Opvragen gebruiksrapportages	x								x
WIS/professional module,									
WIS/professional module EROW beheer									
SCI02 Raadplegen ISI op BSN								x	
SCI03 Raadplegen ISI op BSN of selectie								x	
SCI05 Muteren ISI								x	
SCI06 Alle bevoegdheden incl signalen								x	
Whitelist escape		x	x	x	x		x		

Bijlage 6 Taakomschrijving Security officer Suwinet (17.000246)

Naam Functionaris	Security officer Suwinet
Functie medewerker:	Beleidsmedewerker team Werk, Inkomen en Zorg
Datum beschrijving:	10 januari 2017
Taakbenaming:	Security officer Suwinet
Plaats in de organisatie:	I werkorganisatie of Sociaal Domein

Algemene beschrijving
De security officer Suwinet is verantwoordelijk voor:

- het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen rond het gebruik van Suwinet.
- het toetsen op de uitvoering van regelgeving en procedures ten aanzien van Suwinet.
- het houden en evalueren van controles, toetsen en steekproeven en het verzorgen van een managementrapportage aan het MT Sociaal Domein.

Organisatie van de beveiliging binnen Suwinet
De werkzaamheden als security officer Suwinet omvatten ten minste de volgende onderdelen:

- het (laten) verzorgen van voorlichting en stimuleren van risicobewust gedrag bij medewerkers die gebruik maken van Suwinet (minimaal 1x per jaar).
- het (laten) verzorgen van een introductie over het veilig gebruik van Suwinet voor nieuwe medewerkers.
- het (laten) verzorgen van rapportage over de verleende autorisaties aan de betreffende leidinggevenden (minimaal 1x per half jaar).
- het steekproefsgewijs uitvoeren van controles op de uitvoering en naleving van beveiligingsprocedures binnen Suwinet (minimaal 1x per half jaar).
- het periodiek opvragen van logging-gegevens over het gebruik van Suwinet bij het BKWI en het analyseren van deze gegevens om mogelijk misbruik of oneigenlijk gebruik te signaleren (minimaal 1x per kwartaal).
- het direct signaleren van misbruik en/of oneigenlijk gebruik van Suwinet aan de eigen leidinggevende en aan de informatiebeveiligingscoördinator zodat deze maatregelen kunnen nemen.
- het actueel houden van het overzicht waarbij de door het BKWI gedefinieerde Suwinet-rollen worden gekoppeld aan functies/personen die werkzaam zijn voor de gemeente Olst-Wijhe.
- het controleren van verleende autorisaties - toets of de juiste rol is toegekend aan een persoon – in overleg met de betreffende leidinggevenden (minimaal 1x per half jaar).
- het toetsen op onverenigbare rollen – combinatie van niet te verenigen rollen die aan een persoon zijn toegekend – (minimaal 1x per jaar).
- het toetsen of de beveiligingsprocedures rond Suwinet aangepast dienen te worden op basis van gewijzigde wet- en regelgeving en/of organisatiewijzigingen (minimaal 1x per jaar).
- het zo nodig (laten) ontwikkelen en/of actualiseren van beveiligingsprocedures.
- het regelmatig toetsen van gemelde incidenten die binnen Suwinet voorkomen en zo nodig ondernemen van acties.
- het bespreken van beveiligingsonderwerpen met betrokken organisaties en/of derden met betrekking tot het gebruik van Suwinet.
- het controleren of de medewerkers binnen Suwinet beschikken over voldoende kennis en vaardigheden en waar nodig te vereiste kennis bijbrengen.
- het gevraagd en ongevraagd adviseren van de eigen organisatie ten aanzien van technische, organisatorische of fysieke verbeteringen m.b.t. het gebruik van Suwinet.
- het periodiek (één keer per kwartaal) bespreken van beveiligingsonderwerpen met de informatiebeveiligingscoördinator.

- het rapporteren over de beveiliging en het gebruik van Suwinet aan de directie en de informatiebeveiligingscoördinator (minimaal 1x per jaar).

Rapportage en verantwoording
Tenminste 1x per jaar wordt over de beveiligingsstatus van Suwinet gerapporteerd aan de directie. Deze rapportage bevat minimaal informatie over:

- de uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken en toetsingen;
- aanwezigheid van onverenigbare rollen.
- frauduleus gedrag van medewerkers of niet volgen van procedures.
- geconstateerde tekortkomingen in de beveiligingsvoorzieningen.
- wijziging van procedures / afspraken / opvolgingspatroon.
- het handelen in afwijking met de vastgelegde functiescheiding.
- afwijkingen of wijzigingen op volgens de toegestane rol toegekende autorisaties.

Functietypering

Functietypering:	- Kennis van de werkprocessen waarbij gebruik wordt gemaakt van Suwinet; - Bekendheid met beveiligingseisen & procedures; - Redactionele en communicatieve vaardigheden; - Organisatorisch inzicht; - Probleemoplossend vermogen.
Contacten:	Gebruikers van Suwinet binnen de gemeente Olst-Wijhe, informatiebeveiligingscoördinator, vertrouwenspersoon, leveranciers, BKWI en Inspectie SZW.