

Beveiligingsplan Suwinet 2018

gemeente Overbetuwe

Gemaakt door	M. Spierings (Security Officer Suwinet)
Datum	18 juli 2018
Registratienummer	18int02797

1	Inleiding	3
2	Kader voor het Suwinet beveiligingsplan.....	5
2.1	Aansluiting Suwinet	6
3	Toegang Suwinet-Inkijk	7
3.1	Persoonsgegevens	7
3.2	Rollen.....	8
3.3	College/Management	8
3.4	Security Officer Suwinet	9
3.5	Uitgangspunten toekennen autorisaties	9
3.6	Functiescheiding	9
3.7	Proces toekennen autorisaties Suwinet-Inkijk	10
3.8	Beheer van autorisaties.....	11
3.9	Misbruik.....	11
4	Logging rapportages.....	12
4.1	Whitelist en Escapefunctie	12
5	Procedures Suwinet-Inkijk	14
5.1	Beheren van wachtwoorden	14
5.2	Melden van beveiligingsincidenten	14
5.3	Rechtmatig gebruik	14
5.4	Kennisname van het beveiligingsplan Suwinet.....	14
5.5	Gegevensverstrekking aan derden via de telefoon.....	14
5.6	Suwinet-Mail	15
5.7	Clear desk en clear screen policy.....	15
5.8	Vernietiging van vertrouwelijke gegevens.....	15
5.9	Aanspreken van onbekende personen	15
5.10	Dagelijkse werkzaamheden en informatiebeveiliging	15
5.11	Sancties	16
	Bijlage 1: Verklaring rechtmatig gebruik Suwinet	17
	Bijlage 2: Protocol inzage in Suwinet-Inkijk door cliënt en/of gemachtigde	19
	Bijlage 3: Protocol correctieverzoek Suwinet-Inkijk door cliënt en/of gemachtigde.....	20
	Bijlage 4: Autorisatiematrix	21
	Bijlage 5: Verbeterplan Suwinet 2018.....	22

1 Inleiding

Het beveiligingsplan Suwinet beschrijft de maatregelen ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van het gebruik van persoonsgegevens en informatiesystemen met betrekking tot het behandelen van aanvragen aangaande de Participatiewet (PW), IOAW (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers) en IOAZ (Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen). Daarnaast wordt aangegeven welke mensen en middelen hiervoor beschikbaar worden gesteld en hoe de naleving is geregeld. Het beveiligingsplan is geen statisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en de omgeving zijn voortdurend in ontwikkeling, onder andere door gewijzigde of vernieuwde inzichten en wetgeving of aanpassingen in de informatiesystemen. Dat betekent dat dit plan periodiek moet worden beoordeeld op actualiteit.

Binnen de gemeente zijn bepaalde zaken rondom informatieveiligheid geregeld in een voor de gehele organisatie geldend Informatiebeveiligingsbeleid gemeente Overbetuwe (2015). In 2019 wordt dit algemene informatiebeveiligingsbeleid geactualiseerd. In het algemene Informatiebeveiligingsbeleid zijn uitgangspunten geformuleerd die voor alle organisatieonderdelen en processen gelden ongeacht de betreffende systemen die daarbij gebruikt worden. Deze regels zijn dus ook integraal van toepassing op het onderhavige beveiligingsplan Suwinet voor het gebruik van Suwinet-Inkijk.

Diverse ontwikkelingen als de samenvoeging van de teams Werk en Inkomen / Zorg en Inkomen tot [team Uitvoering Sociaal Domein](#), het wijzigen van de te raadplegen bron- en overzichtspagina's binnen Suwinet-Inkijk en het invoeren van de Whitelist en Escapefunctie, leiden ertoe dat actualisering van het [bestaande](#) Beveiligingsplan Suwinet nodig is. Met onderhavig document wordt het vorige beveiligingsplan Suwinet van gemeente Overbetuwe, inclusief de Autorisatiematrix, up-to-date gemaakt. Ook het nieuwe aangescherpte "Specifiek Suwinet-normenkader Afnemers 2017", dat per 1 april 2017 van kracht is geworden voor gemeenten, maakt herziening van het huidige Beveiligingsplan Suwinet noodzakelijk. Dit [specifieke normenkader](#) vervangt het "[Normenkader GeVS 2011](#)".

Suwinet is het systeem van informatie-uitwisseling in de keten van werk en inkomen. Als basis geldt onder andere de wet Structuur uitvoering werk en inkomen (afgekort met Suwi). De Regeling Suwi verplicht elke gemeente te beschikken over een actueel informatieveiligheidsplan voor Suwinet. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle ketenpartners is dit met beveiligingsvoorschriften uitgewerkt in artikel 6.4 en bijlage 1 van de Regeling Suwi.

Suwinet-Inkijk is de webapplicatie die draait op de beveiligde Suwinet-infrastructuur. Binnen deze applicatie worden gegevens, die bij diverse andere overheidsorganisaties of basisregistraties zijn opgeslagen, op basis van het burgerservicenummer (BSN) veilig toegankelijk gemaakt voor bevoegde medewerkers. De organisaties hebben de informatie over werk en inkomen nodig om de gegevensuitvraag aan de klant te beperken. Suwinet wordt gebruikt om informatie over werk en inkomen van een klant te verzamelen in het kader van onder meer uitkeringen, werk en reïntegratie.

Om de Suwi-keten (afspraken om samenwerking tussen ketenpartijen te stroomlijnen) effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat de door hun instantie aangeleverde gegevens door de partners in de Suwi-keten op een zorgvuldige en controleerbare wijze worden behandeld en de privacy van die gegevens bij alle partners afdoende is gewaarborgd.

De Gezamenlijke elektronische Voorzieningen Suwi (GeVS) zijn voorzieningen waarin drie type partijen participeren: Bronhouders, Beheerders van de centrale (BKWI) en decentrale (Inlichtingenbureau) omgeving en Afnemers.

- **Bronhouders** – Bronhouders zijn de partijen die - ten behoeve van Afnemers - authentieke gegevens beschikbaar stellen aan de Beheerders via de centrale omgeving. De bronhouders vormen de zogeheten leveranciers van gegevens, zoals UWV, SVB en de

Gemeenten, BRP, RDW, Kadaster, Handelregister (KvK).

- **Beheerders** - Beheerder van de centrale omgeving (BKWI) is de partij die - conform de ketenafspraken en –standaarden zorg draagt voor het beschikbaar stellen van de centrale omgeving Suwi en voor de transformatie, autorisatie, transport en verdere routing van gegevens/berichten.

Hiertoe stelt de Beheerder van de centrale omgeving instrumenten, zoals applicaties beschikbaar. De Beheerder van de centrale omgeving is BKWI. De Beheerder van de decentrale omgeving is de partij die voor de routing van 'berichten-op-maat' tussen de centrale omgeving en de gemeenten zorg draagt, gegevens van de gemeenten verzamelt en als Bron voor de uitwisseling van gegevens met de ketenpartijen fungeert. Hiertoe stelt de Beheerder van de decentrale omgeving instrumenten (voorzieningen en applicaties) beschikbaar. De Beheerder van de decentrale omgeving is Inlichtingenbureau.

- **Afnemers** - Afnemers zijn de partijen die via de GeVS - voor hun bedrijfsvoering en uitvoering van hun wettelijke taken - gegevens betrekken uit gegevensbronnen van bronhouder.

2 Kader voor het Suwinet beveiligingsplan

De VNG zet in op een generieke en proactieve gemeentelijke aanpak met betrekking tot informatiebeleid in het algemeen en informatiebeveiliging in het bijzonder. Samen met VNG realisatie heeft VNG in 2016 diverse handreikingen en ander ondersteuningsmateriaal ontworpen. Dit om gemeenten beter te helpen met de beveiliging van de informatievoorziening en Suwinet in het bijzonder. In dit kader kunnen worden genoemd:

- *De BIG en de IBD*: de Baseline Informatiebeveiliging Gemeenten (BIG) en de totstandkoming en doorontwikkeling van de Informatiebeveiligingsdienst (IBD) zijn in het leven geroepen in de bijzondere ledenvergadering van najaar 2013. Toen nam de ALV van de VNG met een overgrote meerderheid een resolutie aan waarin gemeenten verklaren de BIG als gemeentebreed normenkader voor informatiebeveiliging te zullen implementeren. De IBD ondersteunt en adviseert gemeenten daarbij.
- *ENSIA*: ENSIA staat voor Eenduidige Normatiek Single Information Audit. ENSIA is ontwikkeld om gemeenten in staat te stellen op transparante wijze aan de gemeenteraad verantwoording af te leggen over het gerealiseerde niveau van informatieveiligheid. Daarmee wordt de bestaande verantwoordingslast rond SUWI, DigiD, BRP, PNIK, BAG en BGT eenvoudiger gemaakt. ENSIA is een interbestuurlijk traject waarbij departementen én gemeenten samenwerken om de verantwoordingslast (op termijn) te beperken. Gemeenten worden in de toekomst aan één IT-Audit onderworpen. ENSIA is voor de audit van 2017 voor het eerst toegepast. Daaruit is eerder dit jaar een collegeverklaring voortgekomen met een aantal verbeterpunten. Deze verbeterpunten zijn verwerkt in een Verbeterplan Suwinet 2018, met als doel om deze dit jaar te realiseren (zie bijlage 5).
- *Digitale Agenda 2020*: in 2016 heeft de ALV ingestemd met een brede beweging van activiteiten gericht op de doorontwikkeling van gemeenten in de informatiesamenleving. Eén van de activiteiten onder deze noemer was de Bestuurlijke Visitatiecommissie Informatiebeveiliging. Deze commissie heeft meer dan 100 colleges van B&W bezocht en gesproken over de lokale status van de informatiebeveiliging en hoe deze op niveau te brengen of houden. De resultaten zijn gepubliceerd in het eindverslag "[Durven leren](#)".
- *Algemene Verordening Gegevensbescherming (AVG)*: deze verordening heeft de privacyregelgeving in Europa geharmoniseerd en verbetert de privacybescherming van burgers. De AVG is in 2016 in werking getreden. Uit de AVG volgt dat gemeenten tot 25 mei 2018 de tijd hadden om te voldoen aan de AVG, daarna wordt gehandhaafd. Ook gemeente Overbetuwe heeft hier werk van gemaakt.

Normenkader

De Gezamenlijke elektronische Voorziening Suwinet wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. De GeVS en de informatie die via GeVS wordt uitgewisseld dienen te voldoen aan specifieke beveiligingseisen en aan de Europese privacy verordening AVG. De beveiliging van GeVS kan in volle omvang alleen worden gerealiseerd wanneer de ketenpartijen gezamenlijk, ieder vanuit hun eigen verantwoordelijkheid, de juiste beveiligingsmaatregelen treffen.

Voor een adequate werking en bescherming van GeVS zijn ketenafspraken noodzakelijk op het gebied van uitgangspunten en randvoorwaarden, wijze van implementatie, beheersen en het geven van wederzijds inzicht omtrent deze afspraken. De ketenafspraken staan dan ook in het teken van de beveiligingsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Het doel van deze afspraken is een passend beveiligingsniveau van de keten te garanderen.

Vanaf 1 april 2017 is het oude normenkader GeVS 2011 vervangen door het nieuwe specifieke normenkader Suwinet Afnemers. In de basis dekt dit dezelfde risico's af, het is alleen opgesplitst naar doelgroep (afnemers, beheerder en bronhouders), waardoor niet op de doelgroep van toepassing zijnde normen konden worden weggelaten.

2.1 Aansluiting Suwinet

Gemeente Overbetuwe maakt gebruik van het besloten, veilig en volledig beheerd netwerk voor Nederlandse gemeenten, KPN Lokale Overheid genaamd. Om de Suwinet-inkijk applicatie te kunnen gebruiken wordt eerst verbinding gemaakt met KPN Lokale Overheid waarna verbinding wordt gemaakt met Suwinet-inkijk. KPN Lokale Overheid zorgt ervoor dat er geen onbevoegden kunnen binnenkomen op het netwerk van Suwinet.

De infrastructuur en internetapplicaties vallen technisch, qua gebruik en beveiligingsaspecten onder verantwoordelijkheid van team Informatie van gemeente Overbetuwe. Het gebruik van internet en het beveiligingsbeleid is organisatiebreed geregeld. De Suwi wetgeving eist een beveiligingsplan en stelt specifieke eisen aan (controle op) het gebruik door de functionele teams Uitvoering Sociaal Domein (aansluiting GSD) en Publiekszaken (aansluiting Burgerzaken).

De gegevens die voor Publiekszaken via Suwinet-Inkijk beschikbaar zijn, betreffen de adresgegevens van iedereen die werkt of een uitkering ontvangt. Deze komen uit de loonaangifte die werkgevers en uitkeringsinstanties periodiek doen naar de Belastingdienst.

De adresgegevens vanuit UWV mogen alleen gebruikt worden voor het bijhouden van adresgegevens in de Basisregistratie Personen BRP.

3 Toegang Suwinet-Inkijk

De werkstations (thincliënts) zijn binnen de kantoorruimten van de gemeente Overbetuwe beveiligd door een gebruikersnaam en wachtwoord. Van buiten het gemeentehuis kan een medewerker alleen met behulp van een zogenaamde tweeweg authenticatie via een VPN verbinding op het interne netwerk inloggen. Naast gebruikersnaam en wachtwoord, is dan ook een veilig gegenereerde tokencode vereist om op het netwerk te komen. De Suwinet-Inkijk toepassing heeft een eigen gebruikersnaam en wachtwoord.

Bij het gebruik van Suwinet is het niet toegestaan om de werkplek te verlaten. Bij het verlaten van de werkplek moet de applicatie worden afgesloten en het scherm worden vergrendeld.

Indien een medewerker thuiswerkt moet dat papierarm. Het is af te raden om dossiers of documenten daaruit mee naar huis te nemen. Zijn er toch stukken met persoonsgegevens nodig dan dienen die goed te worden opgeborgen en uit het zicht van derden te blijven. Om thuis te kunnen werken is vooraf toestemming van de teammanager vereist.

In het kader van de functiescheiding is het autorisatiebeheer voor het gebruik van Suwinet (voorlopig) neergelegd bij Applicatiebeheer binnen team Uitvoering Sociaal Domein. Deze beheert de Suwinet gebruikersadministratie en is uitvoerend verantwoordelijk voor het beheren van alle Suwinet-Inkijk accounts en het up-to-date houden van de autorisatiematrix (zie bijlage 4). Het up-to-date houden van de autorisatieprocedure is de verantwoordelijkheid van de teammanager Uitvoering Sociaal Domein.

Zodra een medewerker de gemeentelijke organisatie verlaat, wordt het account tegelijkertijd verwijderd of ontoegankelijk gemaakt.

3.1 Persoonsgegevens

Medewerkers gaan op verantwoorde wijze om met de persoonsgegevens die zij raadplegen via Suwinet-inkijk. Er mag alleen geraadpleegd worden als daar een wettelijke grondslag voor is en het nodig is voor de taakuitoefening van de functie. De volgende richtlijnen gelden:

- Gegevens uit Suwinet-Inkijk mogen nooit gemaild worden, niet intern en niet extern. Het gebruik van Suwinet is toegestaan, bij voorkeur binnen kantoor tijd op kantoor. Printen van Suwinet-Inkijk gegevens is niet toegestaan. Dit laatste uit het oogpunt van privacybescherming én dat te allen tijde alleen de online gegevens actueel zijn.
- De persoonsdossiers worden digitaal opgeslagen dan wel bewaard in een archiefkast welke wordt afgesloten wanneer de laatste medewerker de kamer verlaat. Bij het verlaten van de werkplek dient men zich af te melden van Suwinet-Inkijk. Voor uitkeringsgerechtigden die hun gegevens willen inzien en eventueel wensen te corrigeren is een protocol vastgesteld, zie bijlage 3 en 4.
- Personeel dat in dienst is bij de gemeente valt onder het ambtenarenreglement. Bij indiensttreding ondertekent de medewerker een integriteitsverklaring, over het op verantwoorde wijze omgaan met privacygevoelige informatie. De desbetreffende medewerker wordt voordat toegang tot de diverse applicaties wordt verleend, door de Autorisatiebeheerder gewezen op de gebruikersafspraken en de regels over de vertrouwelijkheid en ondertekend de "Verklaring rechtmatig gebruik Suwinet" (zie bijlage 1). Pas daarna wordt toegang tot Suwinet verleend. Hierbij wordt uiteraard gewezen op doelbinding (wettelijke basis) en proportionaliteit (niet meer dan noodzakelijk) voor het legitiem raadplegen van persoonsgegevens.
- Voor extern of ingehuurd personeel dat dient te beschikken over de Suwinet-Inkijk applicatie behoort via de inleenovereenkomst van het uitzendbureau of de daaraan gekoppelde algemene voorwaarden de geheimhouding van vertrouwelijke gegevens door het bureau en de medewerker gewaarborgd te zijn.

- Door de Autorisatiebeheerder wordt het Suwinet autorisatieformulier samen met de Verklaring rechtmatig gebruik Suwinet digitaal opgeslagen in het Suwinet gebruikers archiefdossier in het documentmanagementsysteem. Daarnaast wordt de digitale versie van de Verklaring rechtmatig gebruik Suwinet opgenomen in het personeelsdossier bij personeelszaken.
- Onnodige verwerking van persoonsgegevens is niet toegestaan (dataminimalisatie). Zo mag het technisch nummer van een klant dossier, waarmee veelvuldig met derden wordt gecommuniceerd, niet gelijk zijn aan het BSN (beginselen van proportionaliteit en subsidiariteit).

Informatieveiligheid is uitermate belangrijk voor het werk binnen een team waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Inwoners vertrouwen op een zorgvuldige omgang en verwerking van hun gegevens. Reden waarom in het werk- en of teamoverleg informatiebeveiliging altijd een terugkerend agendapunt moet zijn.

3.2 Rollen

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van klantgegevens. Binnen Suwinet wordt voor de gemeente een aantal gegevens afgeschermd omdat deze voor de gemeente niet functioneel zijn.

Autorisaties voor Suwinet-Inkijk worden per gebruikersrol toegekend. Deze gebruikersrollen moeten in de autorisatiematrix zijn gespecificeerd en omschreven.

- Klantmanagers mogen raadplegen bij het behandelen van aanvragen dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken, voor zover het de Participatiewet, IOAW, IOAZ en BBZ (besluit bijstandsverlening zelfstandigen) betreft. 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.
- Handhaving (Sociaal Rechercheur en Preventie) mag raadplegen bij het behandelen van aanvragen dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, IOAW, IOAZ en BBZ betreft.
- Een kwaliteitsmedewerker mag raadplegen om gedurende het besluitvormingsproces te kunnen toetsen.
- 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 administratief medewerker mag raadplegen om standaard uitdraaien voor het onderzoek van de klantmanager Werk en Inkomen te maken.
- De medewerker uitkeringsadministratie mag gegevens uit Suwinet-Inkijk raadplegen. Dit ten behoeve van de berekening en uitbetaling van de uitkering.
- Enkele medewerkers van team Publiekszaken mogen gebruik maken van Suwinet-Inkijk om adresonderzoeken te behandelen.

3.3 College/Management

De verantwoordelijkheid voor het gebruik van Suwinet ligt te allen tijde bij het College van B&W en namens het college bij de teammanager Uitvoering Sociaal Domein. Het college is bestuurlijk eindverantwoordelijk voor een adequaat stelsel van procedures, afspraken en werkwijzen rondom het gebruik en beheer en de interne verantwoording daarover.

De teammanager Uitvoering Sociaal Domein is verantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk.

3.4 Security Officer Suwinet

Het gebruik van Suwinet vindt plaats onder toezicht van de Security Officer (SO) Suwinet. Hij is in zijn rol onafhankelijk en bewust buiten het team Uitvoering Sociaal Domein gepositioneerd. De SO beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De SO adviseert over en bevordert de beveiliging van Suwinet, verzorgt rapportages over de status met betrekking tot de beveiliging van Suwinet, evalueert de uitkomsten en adviseert en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De SO rapporteert en adviseert aan de teammanager Uitvoering Sociaal Domein en de directeur Bedrijfsvoering.

Jaarlijks controleert de Security Officer of actualisering van het beveiligingsplan noodzakelijk is. Een hernieuwd beveiligingsplan wordt ter vaststelling aan het college van B&W voorgelegd. De Security Officer onderzoekt met regelmaat of de toegangsverlening en toegangsintrekking tot Suwinet-Inkijk correct verloopt. Daartoe kan hij spreken met de betrokkenen, zoals deze in dit plan zijn vermeld. Tevens kan de Security Officer de volgende bronnen raadplegen:

- Het logboek van de accounts van de autorisatiebeheerder
- De gearchiveerde autorisatie aanvragen/intrekkingen
- De getekende verklaringen rechtmatig gebruik Suwinet
- De bijgewerkte autorisatiematrix

3.5 Uitgangspunten toekennen autorisaties

Medewerkers mogen Suwinet-Inkijk raadplegen bij het behandelen van aanvragen met betrekking tot de Participatiewet, IOAW, IOAZ en BBZ. Het doel van de Participatiewet is om zoveel mogelijk mensen aan het werk te helpen en bijstand te verlenen aan mensen die niet in hun eigen levensonderhoud kunnen voorzien.

Bij toekennen van autorisaties gelden vanuit het oogpunt van taakstelling en privacybescherming de volgende uitgangspunten:

- Alleen medewerkers die Suwinet-gegevens nodig hebben voor het uitvoeren van een wettelijke taak krijgen toegang tot Suwinet-Inkijk.
- Bij de gemeente Overbetuwe zijn dat geen andere personen dan medewerkers van het team Uitvoering Sociaal Domein, met aandachtsgebied Werk en Inkomen, en een enkele medewerker voor adresonderzoeken van team Publiekszaken.
- Autorisaties worden toegekend op basis van 'need-to-know': alleen de informatie die nodig is voor de opgedragen taakuitoefening mag opgevraagd worden.
- Gemeenten zijn verplicht het Burgerservicenummer (BSN) in de administratie vast te leggen. Dit betekent dat van ieder persoon van wie informatie in Suwinet-Inkijk moet worden opgezocht, dat aan de hand van het BSN moet gebeuren. Informatie via Suwinet-inkijk is daarom in beginsel alleen via het BSN te benaderen.
- Autorisaties waarbij op andere of meer zoek sleutels dan alleen het BSN naar informatie gezocht kan worden, worden alleen toegekend aan preventie en Sociale Recherche.
- Bij vertrek van een medewerker of verandering van taakstelling worden de toegekende autorisaties in opdracht van de teammanager Uitvoering Sociaal Domein ingetrokken, dan wel aangepast aan de nieuwe rol.

3.6 Functiescheiding

Er zijn verschillende functies in relatie tot het gebruik van Suwinet-inkijk. De taken en verantwoordelijkheidsgebieden zijn gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Hiervoor zijn onderstaande taken bij verschillende personen belegd:

- Uitvoering van taken (het gebruik van Suwinet);
- Het beheer van autorisaties (toegang verlenen tot Suwinet, onderhouden autorisatiematrix);
- Kwaliteitszorg en borging van rechtmatig gebruik;

- Management (beslissen over bevoegdheden van rollen, en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet);
- Beleid formuleren, opvragen rapportages en doen van controles op gebruik van Suwinet.

In het toekennen van autorisaties is de functiescheiding als volgt verwerkt:

- 1 Verlenen en ontnemen toegang is gescheiden van het gebruik van Suwinet-Inkijk.
- 2 Beveiligingsmaatregelen alsook advisering over gebruik en beveiliging Suwinet zijn belegd bij de Security Officer Suwinet.
- 3 De autorisaties worden met inachtneming van punt 1 en 2 aan de hand van een ondertekend autorisatie formulier in opdracht van de teammanager Uitvoering Sociaal Domein toegekend dan wel ingetrokken. De Autorisatiebeheerder Suwinet is verantwoordelijk voor uitvoering van deze opdrachten en archiveert autorisatieformulier in het digitaal archief. In de opdracht wordt gemotiveerd aangegeven waarom aan een (groep) gebruiker(s) een bepaalde autorisatie moet worden toegekend of ontnomen.
- 4 Raadplegen van Suwinet-Inkijk in andere situaties wordt gemotiveerd in de rapportage. Een BSN raadplegen van een klant die onbekend is in het klantvolgsysteem wordt door de medewerker zelf geregistreerd in een logboek om dit achteraf te kunnen verantwoorden.

3.7 Proces toekennen autorisaties Suwinet-Inkijk

Eén van de mogelijke risico's is dat autorisaties voor toegang tot gegevens te wijd open zijn gezet waardoor medewerkers meer informatie onder ogen kunnen krijgen dan voor hun taak noodzakelijk is. Bij het toekennen van autorisaties gelden vanuit het oogpunt van doelbinding en privacy bescherming daarom de volgende uitgangspunten:

1. De medewerker die in dienst komt (of tijdelijk wordt ingehuurd) en voor de uitoefening van zijn of haar taak het gebruik van Suwinet nodig heeft, wordt in opdracht van de teammanager Uitvoering Sociaal Domein geautoriseerd. De Autorisatiebeheerder kent vervolgens de rol(len) met bijbehorende rechten toe aan de gebruiker. Dit verzoek wordt neergelegd in een apart autorisatieformulier voor Suwinet.
2. Wanneer Suwinet om andere redenen wordt gebruikt, 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.
3. Klantmanagers/consulenten mogen raadplegen bij het behandelen van aanvragen dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, IOAW, IOAZ of BBZ betreft.
4. 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.
5. De administratief medewerker mag raadplegen om standaard uitdraaien voor het onderzoek van de consulent Werk en Inkomen te maken.
6. De medewerker uitkeringsadministratie mag gegevens uit Suwinet-Inkijk raadplegen. Dit ten behoeve van de berekening en uitbetaling van de uitkering.
7. De kwaliteitsmedewerker mag raadplegen om gedurende de besluitvorming te kunnen toetsen.
8. De medewerker van team Burgerzaken mag Suwinet-Inkijk raadplegen om adresonderzoeken te behandelen.
9. Handhaving (Sociaal Rechercheur en Preventie) mag raadplegen bij het behandelen van aanvragen dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, IOAW, IOAZ of BBZ betreft.
10. 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. Bij de onderzoeken wordt telkens de afweging gemaakt over noodzaak, subsidiariteit en proportionaliteit van het instrument wat wordt ingezet. Aan deze medewerkers zijn de zogenaamde 'zware rollen' toegekend.

3.8 Beheer van autorisaties

Autorisatiebeheer van Suwinet-Inkijk is (voorlopig) belegd bij Applicatiebeheer binnen team Uitvoering Sociaal Domein. Het uitvoeren van het aanmaken, verwijderen en wijzigen van Suwinet accounts wordt hieronder verstaan. Tevens valt Functioneel beheer en Operationeel beheer van de Suwinet-Inkijk online applicatie hieronder.

- Een verzoek aan de Autorisatiebeheerder tot toekenning, wijziging of beëindiging van autorisaties gebeurt aan de hand van een standaardformulier (zie Formulier aanvraag autorisaties en Formulier intrekken of wijzigen autorisaties).
- De Autorisatiebeheerder kent het autorisatieniveau toe op basis van de rol van de nieuwe medewerker;
- De werkzaamheden van medewerkers kunnen veranderen. Dit kan een uitbreiding of beperking betekenen. Wijzigingen als gevolg van veranderende taken doorlopen dezelfde stappen als bij een autorisatie toekenning.
- De autorisatiebeheerder werkt bij iedere accountmutatie (toekennen/wijzigen/intrekken) het logboek bij met vermelding van de handeling.
- De teammanager Uitvoering Sociaal Domein is verantwoordelijk voor het tijdig melden van accountmutaties aan de Autorisatiebeheerder.
- Het door de teammanager ondertekende autorisatieformulier wordt door de Autorisatiebeheerder digitaal gearhiveerd.
- De Security Officer Suwinet besteedt in deze gevallen in het bijzonder aandacht aan het voorkomen van een onbedoelde stapeling van bevoegdheden. Hiermee wordt bedoeld dat niet (meer) benodigde autorisatie rollen ook daadwerkelijk worden ingetrokken bij toekennen van rollen die vanwege het nieuwe takenpakket rechtmatig noodzakelijk zijn en dat de verleende autorisatie afgestemd doelmatig blijft.

3.9 Misbruik

Geautoriseerde medewerkers bij de (I)GSD van gemeenten die belast zijn met de uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW en IOAZ, mogen gebruik maken van Suwinet. Suwinet wordt onder andere gebruikt in processen om de grondslag voor het toekennen of afwijzen van een uitkering te bepalen of voor reïntegratie. In de onderlinge wet- en regelgeving wordt ook nadrukkelijk uitgesloten waar Suwinet niet voor mag worden gebruikt. Dit betreft raadpleging voor uitvoering van wetten anders dan de drie voornoemde wetten. Zo is het niet toegestaan Suwinet te gebruiken voor taken rondom schuldhelpverlening en de uitvoering van de [WMO](#) of Jeugdzorg. Ook voor bijvoorbeeld de wet [Taaleis](#) is raadpleging van Suwinet niet toegestaan. De handreiking van de VNG geeft een goede beschrijving van wat wel en niet mag (zie [factsheet](#)).

Als de Security Officer op basis van nadere inspectie van specifieke rapportages misbruik vermoed of constateert wordt een onderzoek ingesteld en betreft hierbij altijd de teammanager Uitvoering Sociaal Domein. Onderzocht wordt of er sprake was van doelmatig en rechtmatig gebruik van de Suwinet-Inkijk voorziening. Het kan nodig zijn met de betrokken medewerker te spreken om dit uiteindelijk vast te stellen.

Bij geconstateerd misbruik van Suwinet geldt het algemeen geldende misbruik beleid van de organisatie. Conform de Ambtenarenwet en de CAR/UWO zijn rechtspositionele maatregelen mogelijk.

4 Logging rapportages

Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker kan worden nagegaan. De logging wordt gebruikt voor controles over onrechtmatige, onregelmatige of doel overschrijdende verwerking.

Bij controle van het gebruik kunnen er naast algemene ook specifieke rapportages worden opgevraagd. Indien controle daar aanleiding toe geeft stelt de Security Officer Suwinet een onderzoek in naar rechtmatig en doelmatig gebruik en betreft daarbij altijd de volgende personen;

- Autorisatiebeheerder Suwinet en Kwaliteitsmedewerker
- Teammanager Uitvoering Sociaal Domein

Onderzocht wordt of er sprake was van doelmatig en rechtmatig gebruik van de Suwinet inkijk voorziening. Het kan nodig zijn met betrokken medewerker te spreken om dit uiteindelijk vast te stellen. Indien er geen misbruik is geconstateerd is hiermee het onderzoek ten einde. De gegevens kunnen geanonimiseerd in de rapportage verwerkt worden.

De gebruikers van Suwinet weten dat gegevens over hun gebruik van Suwinet worden verzameld en vastgelegd. Voorafgaand aan toegang tot Suwinet krijgen zij door de Autorisatiebeheerder uitleg over het gebruik van Suwinet en worden zij gevraagd het centraal opgeslagen beveiligingsbeleid door te nemen. Tevens tekenen zij een "Verklaring rechtmatig gebruik Suwinet" (bijlage 1). Dit is een belangrijk onderdeel van de privacybescherming. 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;
- In geval van onrechtmatig of doel overschrijdend gebruik van Suwinet-Inkijk bespreekt de teammanager Uitvoering Sociaal Domein dit met de betreffende medewerker, met mogelijke sancties tot gevolg (zie paragraaf 3.9).

4.1 Whitelist en Escapefunctie

Per 5 december 2017 wordt er bij gemeente Overbetuwe gewerkt met de zogenaamde Whitelist en Escapefunctie.

Wanneer een medewerker toegang heeft tot Suwinet kan in beginsel iedere in Nederland woonachtige burger geraadpleegd worden. Dat betreft dan ook burgers waar geen dienstverleningsrelatie mee is op basis van de gemeentelijke wettelijke taken. De gegevensraadpleging is dus niet begrensd tot de 'eigen' burgers, hetgeen onwenselijk is. Om dit tegen te gaan en om het raadplegen van gegevens te begrenzen tot die 'eigen' burgers, is het mogelijk om binnen Suwinet-Inkijk gebruik te maken van een filtermechanisme. Dit filtermechanisme is vormgegeven als een zogenaamde 'whitelist'. 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 in verband met de uitvoering van wettelijke taken, dan kan de medewerker, mits hiervoor geautoriseerd, 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 burgers.

Wie staan er op de whitelist:

- Alle klanten en hun eventuele partners die een uitkering levensonderhoud of bijzondere bijstand ontvangen of in de afgelopen maanden hebben ontvangen, een openstaande schuld aan de organisatie hebben of onderhoudsplichtig zijn.
- Deze klanten blijven op de whitelist staan tot een 180 dagen na het beëindigen van de regeling.

Escapefunctie

In bepaalde situaties is het nodig dat er toch persoonsgegevens worden ingezien van personen waarop dat moment (nog) geen dienstverleningsrelatie mee is en die daarom ook niet op de actieve whitelist staan. Hier kunnen verschillende redenen voor zijn, zoals:

- er is nog geen dienstverlening, maar deze wordt wel gevraagd (nieuwe aanvraag);
- er wordt een verhaalsonderzoek uitgevoerd waarbij de verhaalsplichtige nog onbekend is;
- er moet (bijzonder) onderzoek worden verricht waarbij ook gegevens van derden moeten worden geraadpleegd.

De escapefunctie is een specifieke autorisatie voor medewerkers met specifieke taken. Het gaat daarbij om een autorisatie die aan de rol of het account van de gebruiker wordt gekoppeld. De escapefunctie zorgt er voor dat de medewerker toch het BSN kan raadplegen ondanks dat het niet op de whitelist staat.

Wanneer de medewerker gebruik maakt van de escapefunctie wordt gevraagd om een algemene voorgedefiniëerde rede aan te geven. Tevens houdt de medewerker zelf een logboek bij over de gebruikte escapes om zich daarvoor desgevraagd te kunnen verantwoorden.

5 Procedures Suwinet-Inkijk

Voor het werken met persoonsgegevens is vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Daaruit zijn gedragsregels afgeleid die gelden voor medewerkers van de gemeente Overbetuwe in relatie tot al hun werkzaamheden en bij het gebruik van Suwinet-Inkijk voor medewerkers van het Uitvoering Sociaal Domein in het bijzonder.

Concreet kunnen deze regels als volgt worden vertaald:

5.1 Beheren van wachtwoorden

Autorisatiebeheer Suwinet stelt in hoe lang een wachtwoord geldig is. De gebruiker moet het toegekende wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Suwinet dwingt in alle gevallen een sterk woord af. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord. Een wachtwoord is strikt persoonlijk en mag niet gedeeld worden met anderen. Het account blokkeert automatisch wanneer het 90 dagen niet is gebruikt.

5.2 Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de teammanager Uitvoering Sociaal Domein en de Security Officer Suwinet. Voorbeelden van incidenten zijn: autorisatiemisbruik (bijvoorbeeld doorgeven van wachtwoorden aan anderen en mee laten kijken op het scherm door onbevoegden), doorgeven van gegevens aan onbevoegden (bijvoorbeeld doorspelen aan vrienden of bekenden), oneigenlijk gebruik (bijvoorbeeld informatie opvragen van personen die niet werk gerelateerd is).

5.3 Rechtmatig gebruik

Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de persoonsgegevens waarmee gewerkt wordt, niet verder bekend mogen worden gemaakt dan voor het uitvoeren van de taak noodzakelijk is. Ten behoeve van de borging van de vertrouwelijke omgang met persoonsgegevens, laat Gemeente Overbetuwe de gebruikers en autorisatiebeheerders van Suwinet een "Verklaring rechtmatig gebruik Suwinet" ondertekenen (zie bijlage 1).

5.4 Kennisname van het beveiligingsplan Suwinet

Het onderhavige beveiligingsplan Suwinet is van toepassing op iedereen die gebruik maakt van Suwinet of beheer voert op de gebruikersaccounts van Suwinet binnen de gemeente Overbetuwe. Het beveiligingsplan wordt na vaststelling gepubliceerd op intranet. Alle gebruikers worden er minimaal twee maal per jaar in een periodiek teamoverleg op geattendeerd dat ze kennis moeten nemen van het plan.

Nieuwe medewerkers worden via de teammanager Uitvoering Sociaal Domein uitdrukkelijk op het plan gewezen met de opdracht er kennis van te nemen.

Hierdoor weten medewerkers welk gedrag de organisatie van hen verwacht én weten ze dat er gegevens worden bewaard waarmee hun gedrag kan worden gecontroleerd. Van dat laatste moeten ze zich bewust zijn in relatie tot hun eigen privacy en dat van de klant.

5.5 Gegevensverstrekking aan derden via de telefoon

In principe wordt geen telefonische informatie over cliënten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. Het uitgangspunt is namelijk dat zeer terughoudend wordt omgegaan met verzoeken van telefonische informatie over cliënten. Dit vanwege het risico dat de identiteit van de gesprekspartner verkeerd kan worden vastgesteld of dat persoonsgegevens worden

verstrekt aan personen of instanties, die geen recht hebben op deze informatie. In voorkomende 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 als zeker is dat het een vaste contactpersoon betreft.

5.6 Suwinet-Mail

Suwinet-Mail is een communicatiefaciliteit in de vorm van een besloten netwerk, dat bestaat uit een centraal deel en meerdere decentrale delen. Dit biedt gebruikers en aangesloten organisaties de mogelijkheid om vertrouwelijke informatie met elkaar uit te wisselen. Hiermee worden de risico's die zijn verbonden aan het mailen van klantgegevens aanzienlijk verkleind. Op Suwinet-Mail zijn diverse overheidsorganisaties aangesloten.

5.7 Clear desk en clear screen policy

Het is noodzakelijk ook ten opzichte van collega's en dienstverleners zorgvuldig om te gaan met de privacy van klanten. Onbevoegden, zowel binnen als buiten de organisatie, mogen niet de beschikking krijgen over vertrouwelijke informatie. Daarom mogen gegevens niet onbeheerd op het bureau of het beeldscherm achterblijven. Voor zover stukken nog niet zijn gedigitaliseerd, worden deze in een kast bewaard die na werktijd wordt afgesloten.

Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging en met een wachtwoord weer ontgrendeld kan worden. De systemen zijn door systeembeheer zodanig ingesteld dat na een vaste periode de schermbeveiliging intreedt. Daarnaast kan de gebruiker zelf het scherm vergrendelen door de toetscombinatie "Windowsvlaggetje-L" gelijktijdig aan te slaan (L staat voor "lock"). Lock de pc als je wegloopt van jouw werkplek.

5.8 Vernietiging van vertrouwelijke gegevens

Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Daarom zijn er bij de gemeente Overbetuwe speciale blauwe containers geplaatst, waarin het te vernietigen materiaal verzameld wordt. De verzamelde papieren worden regelmatig aangeleverd bij het vernietigingsbedrijf.

Indien er een onverhoopt toch een print is gemaakt van Suwinet-Inkijk gegevens, moet deze na afhandeling van het werkproces worden vernietigd.

5.9 Aanspreken van onbekende personen

Op de werkplekken mag geen publiek komen. In het geval dat een medewerker een voor hem/haar onbekende persoon in het gebouw tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken. 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 hen beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naartoe te begeleiden.

5.10 Dagelijkse werkzaamheden en informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen een team waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Klanten vertrouwen op een zorgvuldige wijze van omgang met en verwerken van hun gegevens. Reden waarom in het werk- en of teamoverleg informatiebeveiliging altijd een

terugkerend agendapunt moet zijn. Tevens maakt de aandacht voor informatiebeveiliging onderdeel uit van de jaarlijkse W&O cyclus van iedere medewerker.

5.11 Sancties

Een medewerker die de beveiligingsregels onvoldoende naleeft wordt daar door de teammanager op aangesproken. Conform de Ambtenarenwet en de CAR/UWO zijn daarop rechtspositionele maatregelen mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen.

Bijlage 1: Verklaring rechtmatig gebruik Suwinet

Naam	
Team	☐ Uitvoering Sociaal Domein ☐ Publiekszaken
Functie/rol	☐ Klantmanager ☐ Consulent bijzondere bijstand ☐ Kwaliteitsmedewerker ☐ Medewerker uitkeringsadministratie ☐ Administratief medewerker Uitvoering Sociaal Domein ☐ Medewerker team Publiekszaken ☐ Anders, nl.:
Datum in dienst	

- 1 Bij besluit van het college van burgemeester en wethouders van de gemeente Overbetuwe, geautoriseerd tot het opvragen van gegevens uit de gemeentelijke en andere gegevensbestanden, verklaart ondergetekende zijn/haar werkzaamheden te zullen verrichten onder de volgende voorwaarden:
 - a Geen andere informatie uit Suwinet te zullen opvragen dan die welke voor de hem/haar opgedragen werkzaamheden nodig zijn;
 - b Zich te verplichten tot geheimhouding van al datgene wat hem/haar in zijn/haar dienstverband ter kennis komt, tenzij enig wettelijk voorschrift mededeling vordert;
 - c Bekend te zijn met wat ten aanzien van geheimhouding in de wet is bepaald (zie artikel 272 van het Wetboek van Strafrecht) en met het feit dat schending van de geheimhoudingsplicht als uiterste consequentie tot strafontslag kan leiden;
 - d Bekend te zijn met de controles die door de Beveiligingsfunctionaris Suwinet op het gebruik van Suwinet worden gehouden en bekend te zijn met de mogelijke consequenties van onrechtmatig gebruik.
 - e Geen andere personen gebruik te zullen laten maken van zijn/haar unieke gebruikersnaam en/of wachtwoord voor Suwinet of die op enige andere wijze aan hen te doen toekomen;
 - f Ondergetekende zal geen andere personen, ook niet de in dienstverband werkende teamleden, toelaten tot de persoonsgebonden toegang tot Suwinet;
 - g Ondergetekende zal geen informatie opzoeken van en over personen die niets met zijn/haar werkzaamheden te maken hebben, zoals bekende Nederlanders, burens, familie, vrienden, kennissen of collega's;
 - h Bij het tijdelijk verlaten van de werkplek (op kantoor of elders) zal het beeldscherm op de werkplek, door ondergetekende worden afgesloten m.b.v. de schermbeveiliging;
 - i Bij het verlaten van de werkplek (op kantoor of elders) voor lange duur, zullen alle sessies van applicaties die toegang geven tot de gegevensbestanden en van portalen, dus ook van Suwinet, op de werkplek door ondergetekende worden afgesloten;

- j Uitdraaien van Suwinet ten behoeve van het klantdossier worden bij het werken buiten kantoorlocaties van gemeente Overbetuwe buiten bereik en zicht van huisgenoten en bezoekers gehouden.
- 2 Deze verklaring blijft voor lid 1b van kracht, ook na beëindiging van bovengenoemde werkzaamheden.
- 3 Ondergetekende heeft voorafgaand aan de ondertekening van deze verklaring een exemplaar ontvangen van het Beveiligingsplan Suwinet gemeente Overbetuwe en voldoende tijd gehad om kennis te nemen van de inhoud ervan.
- 4 Ondergetekende verklaart akkoord te zijn met de inhoud van het Beveiligingsplan Suwinet gemeente Overbetuwe en in overeenstemming met de hierin genoemde bepalingen en gedragsregels te handelen.
- 5 Ondergetekende verklaart een Verklaring omtrent het Gedrag te hebben overhandigd aan een medewerker van Personeelszaken & Organisatie van gemeente Overbetuwe.

Ondertekening

Naam

Plaats

Datum

Handtekening

Bijlage 2: Protocol inzage in Suwinet-Inkijk door cliënt en/of gemachtigde

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, hieronder beschreven gevallen, is gegevensinzage door derden mogelijk. De via Suwinet opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op diskette). Er mag wel een afdruk worden gemaakt voor de cliënt of zijn gemachtigde. Een cliënt kan zijn gegevens op 2 manieren inzien:

- Online via <http://www.bkwi.nl/over-bkwi/wat-doet-bkwi-met-mijn-gegevens/> bevindt zich daar een link "mijn gegevens inzien"
- Schriftelijk verzoek aan de gemeentelijke sociale dienst

Hieronder volgt een instructie voor enkele situaties waar de gebruiker van Suwinet-Inkijk mee te maken kan krijgen.

De cliënt verzoekt om inzage in zijn gegevens, schriftelijk of mondeling

Het is mogelijk dat een cliënt telefonisch vraagt om een uitdraai van zijn/haar gegevens. In dat geval dient de cliënt verwezen te worden naar team Zorg en Inkomen van de gemeente Overbetuwe. Is dit niet mogelijk, dan moet hij/zij een schriftelijk verzoek indienen dat binnen de wettelijk verplichte termijn dient te worden beantwoord.

Handel het verzoek als volgt af:

- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs;
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
- Vernietig het uitgedraaide exemplaar als de cliënt het niet meeneemt;
- Beëindig inkijsessie.

Als de cliënt inzage wil in gegevens die bij een ketenpartner zijn geregistreerd (maar die niet op Suwinet staan), dient de cliënt te worden verwezen naar de betreffende ketenpartner.

Gemachtigde verzoekt schriftelijk om inzage in cliëntgegevens

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs;
- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs;
- Maak een uitdraai van de geraadpleegde gegevens of laat gemachtigde meekijken op het scherm;
- Vernietig het uitgedraaide exemplaar als de gemachtigde het niet meeneemt;
- Beëindig inkijsessie.

Een derde verzoekt om inzage in cliëntgegevens

Dit is niet mogelijk.

Bijlage 3: Protocol correctieverzoek Suwinet-Inkijk door cliënt en/of gemachtigde

De cliënt verzoekt om correctie

- Informeer de cliënt dat hij/zij een officieel verzoek voor correctie moet indienen;
- Dit recht is geregeld in artikel 36 van de Wet bescherming persoonsgegevens;
- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs;
- Maak een verzoekschrift en laat het ondertekenen;
- Maak een kopie van het verzoek;
- Verstrek een kopie aan de cliënt;
- Gebruik het origineel om het verzoek af te handelen en archiveer het in het cliëntdossier;
- Informeer de klant over de doorgevoerde wijziging.

Gemachtigde verzoekt om correctie

- Informeer zo nodig de gemachtigde dat hij/zij een officieel schriftelijk verzoek moet indienen;
- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs;
- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs;
- Handel het verzoek af en archiveer het in het cliëntdossier;
- Informeer de gemachtigde over de doorgevoerde wijziging.

Een derde verzoekt om correctie

Dit is niet mogelijk.

Bijlage 4: Autorisatiematrix

	Administratie	Autorisatiebeheer	Consulent bijzondere bijstand	Klantmanager	Kwaliteit	Security Officer	Klantmanager Statushouders	Statushouders admin ondersteuning	Toezichthouder	Medewerker Publiekszaken
Rol in Suwi										
<i>Vaste gebruikersrollen voor 1 pagina</i>										
R1043 Belastingdienst	x		x	x	x					
G019 Bijstandsregelingen	x		x	x	x					
R3724 DUO gegevens										
R1272 Fraude vorderingen										
G003 UWVWb	x		x	x	x				x	
G004 Fraude scorekaart			x	x	x				x	
G005 GBA	x		x	x	x				x	
G018 Zoek in GBA										
G024 Bedrijvenregister	x		x	x	x				x	
G030 Zoek+ in GBA									x	
G031 Correctieservice	x									
G040 Onderhouden status wijzigingsverzoeken									x	
R3726 Inkomstenverhoudingen										
R2786 Kostendelerstoets	x		x	x	x				x	
R4549 Landelijk doelgroepregister									x	
G020 RDW	x		x	x	x					
R1919 RDW+										
R454 RDW peildata	x		x	x	x				x	
R3728 Rechtmatigheid+	x		x	x	x				x	
R3725 Re-integratie										
R3722 SVB gegevens									x	
R3723 UWV Uitkeringen										
R2355 Zoek in RDW										
R1920 Zoek in RDW+									x	
<i>Vaste rollen buiten Suwinet-Inkijk</i>										
R1525 EROW beheer										
SCI02 Raadplegen ISI op BSN										
SCI03 Raadplegen ISI op BSN of selectie										
SCI05 Muteren ISI										
SCI06 Alle bevoegdheden incl signalen										
R3841 Raadplegen PV gegevens							x			
R4692 Muteren PV gegevens								x		
<i>Vaste beheerrollen</i>										
R3130 Beheer ww&blokkeren										
G032 Onderhouden correctieservice										
GSDADM Gebruikersbeheerder		x								
R3846 Onderhouden werkvoorraad		x								
R347 Opvragen generieke gebruiksrapportage						x				
RAPPORT_SPECIFIEK_GSD Opvragen specifieke gebruiksrapportage						x				
WE_GSD ESCAPE Whitelist escape			x	x					x	
<i>Eigen rollen</i>										
R699 Pilot kadastergegevens					x				x	
R1694 Terugvordering										
<i>Vaste beheerrollen</i>										
BURGERZAKENADMIN DelAdmins										
R1417 Opvragen generieke gebruiksrapportage burgerzaken						x				
<i>Vaste gebruikersrollen 1 pagina</i>										
R1265 Actuele adresgegevens										x

Bijlage 5: Verbeterplan Suwinet 2018

Nr	Actiepunt	Eigenaar	Datum gereed	Status
1.	Logboek Suwinet accounts kloppend maken (voor zover nog mogelijk) en vanaf heden ook kloppend houden	Rob	Q1	
2.	Controles van GSD maandrapportages kort na verschijnen uitvoeren (daaropvolgende maand)	Rob/Heleen/Mark	Q1	
3.	Per email verantwoording geven aan teammanager Sociaal domein over (instruerend) bespreken Suwinet raadplegingen van gebruikers buiten Whitelist om of anderszins waar vermoeden is geconstateerd van oneigenlijk gebruik (vanaf heden), met cc aan Security Officer Suwinet	Heleen	Q1	
4.	Vernieuwen Autorisatiematrix, met daarin opgenomen profielen en rollen in relatie tot taakomschrijving, als onderdeel van het Beveiligingsplan Suwinet	Rob	Q2	
5.	Profiel, rol en taakomschrijving van Handhaving i.h.k.v. gebruik Suwinet opnemen in Autorisatiematrix	Rob	Q2	
6.	Borgen van alle getekende formulieren (vanaf 29 september 2015) Autorisaties Suwinet en Verklaringen rechtmatig gebruik Suwinet in Corsa archiefdossier en personeelsdossier	Rob	Q2	
7.	Van alle huidige Suwinet beheerders en gebruikers getekende Suwinet Autorisatie aanvraag en Verklaringen rechtmatig gebruik op orde	Rob	Q2	
8.	Verslag doen van account controles	Mark	Q2	
9.	Actualiseren en door college van B&W laten vaststellen hernieuwd Beveiligingsplan Suwinet (met inbegrip van benoemen van Suwinet levering Burgerzaken)	Mark	Q2	
10.	Procesbeschrijving van borging autorisatieformulieren en Verklaring rechtmatig gebruik Suwinet opnemen in Beveiligingsplan Suwinet	Mark	Q2	
11.	Procesbeschrijving bij raadplegen Suwinet tijdens zogenaamde meldingsfase in Beveiligingsplan Suwinet opnemen	Mark	Q2	
12.	Procesbeschrijving bij vermoeden oneigenlijk gebruik of misbruik Suwinet in Beveiligingsplan Suwinet opnemen	Mark	Q2	
13.	Passage opnemen over thuiswerken in Beveiligingsplan Suwinet	Mark	Q2	
14.	Controle- en verantwoordingssysteem voor reeds bestaande en in gebruik zijnde Suwinet levering Burgerzaken (aan team Publiekszaken) opzetten	Mark	Q3	
15.	Bewustwordingssessie Suwinet	Heleen/Rob/Mark	Q3	