

# **Beveiligingsplan Suwinet 2020 gemeente Overbetuwe**

**Gemaakt door** M. Spierings (Security Officer Suwinet)  
**Datum** 11 december 2019  
**Registratienummer** 19int05215

<b>1</b>	<b>Inleiding .....</b>	<b>4</b>
<b>2</b>	<b>Kader voor het Suwinet beveiligingsplan .....</b>	<b>6</b>
2.1	Aansluiting Suwinet.....	6
<b>3</b>	<b>Toegang Suwinet-Inkijk.....</b>	<b>8</b>
3.1	Persoonsgegevens .....	8
3.2	Gebruikersrollen.....	9
3.3	Functiescheiding .....	10
3.4	Uitgangspunten autorisaties.....	10
3.5	Security Officer Suwinet.....	11
3.6	Autorisatiebeheerder.....	11
3.7	Proces autorisatiebeheer Suwinet-Inkijk .....	12
3.8	College/Management .....	12
3.9	Misbruik.....	12
<b>4</b>	<b>Procedure logging rapportages .....</b>	<b>14</b>
4.1	Whitelist en Escapefunctie .....	14
<b>5</b>	<b>Procedures Suwinet-Inkijk.....</b>	<b>16</b>
5.1	Beheren van wachtwoorden.....	16
5.2	Melden van beveiligingsincidenten .....	16
5.3	Rechtmatig gebruik .....	16
5.4	Kennisname van het beveiligingsplan Suwinet .....	16
5.5	Gegevensverstrekking aan derden via de telefoon.....	16
5.6	Suwinet-Mail.....	17
5.7	Clear desk en clear screen policy .....	17
5.8	Vernietiging van vertrouwelijke gegevens.....	17
5.9	Aanspreken van onbekende personen .....	17
5.10	Dagelijkse werkzaamheden en informatiebeveiliging .....	17
5.11	Sancties .....	18
	Bijlage 1: Verklaring rechtmatig gebruik Suwinet .....	19
	Bijlage 2: Autorisatieformulier Suwinet .....	21
	Bijlage 3: Protocol inzage in Suwinet-Inkijk door cliënt en/of gemachtigde .....	23
	Bijlage 4: Autorisatiematrix .....	24

# 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). Binnenkort 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.

Jaarlijks dient het beveiligingsplan Suwinet geëvalueerd te worden. Met onderhavig document wordt het vorige beveiligingsplan Suwinet van gemeente Overbetuwe, inclusief de Autorisatiematrix, up-to-date gemaakt. Er was al langer duidelijk dat het praktisch is voor de klantmanager en toezichthouder om voor een aantal extra bronpagina's geautoriseerd te worden. Zij konden immers deze bewuste gegevens al raadplegen via de zogenaamde overzichtspagina's. Het is de bedoeling om bij gebruik van Suwinet uit te gaan van dataminimalisatie. Dus als er rechtstreeks naar een bronpagina gegaan kan worden is het overbodig om veel meer gegevens te zien via de uitgebreidere overzichtspagina. Uit de ENSIA audit over 2018 bleek dat het autorisatiebeheerproces voor verbetering vatbaar was. Ook daar zijn verbeteringen doorgevoerd.

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 re-integratie.

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 de afgelopen jaren 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:

- **BIO:** vanaf 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht als opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG). Gemeenten hebben de opdracht om dit gemeentebreed normenkader voor informatiebeveiliging te implementeren. De Informatiebeveiligingsdienst (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, BRO 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. Daarna ook in 2018. Daarbij zijn voor afgelopen jaar voor een deel dezelfde tekortkomingen geconstateerd als dat jaar ervoor, met name op het gebied van het autorisatiebeheerproces. Deze verbeterpunten zijn geaccordeerd door de teammanager Team Uitvoering Sociaal Domein (TUSD).

### 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 over 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 TUSD (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 thuis werkt moet dat papierarm gebeuren. 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 de rol van Autorisatiebeheerder Suwinet belegd bij Applicatiebeheer binnen TUSD. De Autorisatiebeheerder 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 TUSD.

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 cliënten die hun gegevens willen inzien is een protocol vastgesteld, zie bijlage 3. Mocht een cliënt een verzoek tot correctie van gegevens wensen, dan wordt hij of zij door de dienstdoende medewerker doorgeleide gedaan naar de juiste collega of ketenpartner die deze gegevens onderhoud.
- Personeel dat in dienst is bij de gemeente valt onder het ambtenarenreglement. Bij het aanvaarden van het dienstverband 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 Suwinet 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 gegevens 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 Suwinet wordt het Suwinet autorisatieformulier digitaal opgeslagen in het Suwinet gebruikers archiefdossier van het documentmanagementsysteem. De digitale versie van de Verklaring rechtmatig gebruik Suwinet wordt door DIV opgenomen in het personeelsdossier.
- 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 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 Gebruikersrollen

Er zijn verschillende taakgebieden 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 overeenkomen met de autorisatiematrix. Zoveel als technisch mogelijk zijn pagina's ondergebracht in zelf voorgedefinieerde rollen binnen Suwinet Inkijk. Waar dit niet mogelijk is worden pagina's rechtstreeks aan gebruikers gekoppeld (zoals bij de SCI pagina's van het inburgeringsportaal).

### *Administratie (medewerker uitkeringsadministratie)*

De medewerker uitkeringsadministratie zorgt voor de administratieve en financiële verwerking van uitkeringsdossiers van de Participatiewet, IOAW, IOAZ en BBZ. Ook dragen zij zorg voor de debiteurendossiers, verwerking van IB-signalen en de controle op belastingaangiften van uitkeringsgerechtigden.

### *Consulent bijzondere bijstand*

Consulenten bijzondere bijstand behandelen aanvragen voor bijzondere bijstand en minimabeleid en voeren rechtmatigheidsonderzoeken voor de Participatiewet uit.

### *Klantmanager*

Klantmanagers 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 (besluit bijstandsverlening zelfstandigen) betreft. Ook voeren zij de ondersteuning bij arbeidsre-integratie voor niet uitkeringsgerechtigden uit, evenals het vaststellen van doelgroepen en loonkostensubsidie.

### *Kwaliteitsmedewerker*

Een kwaliteitsmedewerker mag raadplegen om gedurende het besluitvormingsproces te kunnen toetsen. Hierbij is het noodzakelijk dat de kwaliteitsmedewerker overwegend dezelfde autorisaties heeft als de klantmanager en consulent bijzondere bijstand.

### *Toezietherouder*

Een handhaver (Sociaal Rechercheurs en Preventie) voert onderzoek uit bij aanvragen voor een uitkering, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, IOAW, IOAZ en BBZ (besluit bijstandsverlening zelfstandigen) betreft. Deze onderzoeken zijn specifiek gericht op het opsporen en voorkomen van fraude.

### *Statushouders administratieve ondersteuning*

Werkzaamheden inburgeringsportaal ten behoeve van de participatieverklaringen.

#### *Autorisatiebeheer*

Draagt zorg voor autorisatiebeheerproces, dus het zorgvuldig en veilig aanmaken/wijzigen/intrekken van Suwinet accounts. Voert wekelijks de upload uit van de “whitelist”, de zogenaamde participatiewet klantenlijst. Daarnaast draagt de autorisatiebeheerder zorg voor beheerderstaken van het inburgeringsportaal (de SCI pagina's).

#### *Security Officer*

Is bevoegd om de maandelijkse generieke en specifieke rapportages op te vragen.

#### *Medewerker Publiekszaken*

Enkele medewerkers van team Publiekszaken mogen gebruik maken van Suwinet-Inkijk om adresonderzoeken te behandelen.

### **3.3 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 zorgvuldig gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet);
- Beleid voorstellen, 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 autorisatieformulier in opdracht van de teammanager TUSD toegekend dan wel ingetrokken of gewijzigd. 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 eigen logboek om dit achteraf te kunnen verantwoorden.

### **3.4 Uitgangspunten 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 in het kader van de Participatiewet krijgen toegang tot Suwinet-Inkijk.
- Bij de gemeente Overbetuwe zijn dat geen andere personen dan medewerkers van het team TUSD, met aandachtsgebied Werk en Inkomen, behalve een enkele medewerker voor adresonderzoek 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.
- Autorisaties worden toegekend aan de hand van de voorgedefinieerde rollen uit de autorisatiematrix.
- 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 de rol Toezichthouder.
- Bij vertrek van een medewerker of verandering van taakstelling worden de toegekende autorisaties in opdracht van de teammanager TUSD ingetrokken, dan wel aangepast aan de nieuwe rol.
- Alleen de teammanager TUSD is bevoegd om autorisatieformulieren te ondertekenen. Bij afwezigheid is de plaatsvervangend teammanager tekenbevoegd.

### 3.5 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 TUSD gepositioneerd. De SO beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet in overeenstemming met 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 TUSD en de directeur Ontwikkeling.

Jaarlijks controleert de SO of actualisering van het beveiligingsplan noodzakelijk is. Een geactualiseerd beveiligingsplan wordt ter vaststelling aan het college van B&W en ter informatie aan de gemeenteraad voorgelegd. De SO 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 SO 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

### 3.6 Autorisatiebeheerder

De rol van Autorisatiebeheer Suwinet-Inkijk is belegd bij Applicatiebeheer binnen TUSD. Het uitvoeren van het aanmaken, verwijderen en rolwijzigingen van Suwinet accounts wordt hieronder verstaan. Tevens valt Functioneel beheer en Operationeel beheer van de Suwinet-Inkijk online applicatie hieronder.

De autorisatiebeheerder is verantwoordelijk voor de uitvoer van het toekennen/wijzigen/intrekken van autorisaties binnen de Suwinet-inkijk applicatie. Hierbij zijn de volgende taken te onderkennen:

- Het instrueren en doen toekomen van relevante documenten aan de potentiële nieuwe gebruiker.
- Het doorvoeren van het autorisatieverzoek op basis van een standaard formulier dat geformaliseerd wordt door ondertekening van de teammanager TUSD.
- Het na verwerking zorgdragen voor archivering van het autorisatieformulier en de Verklaring rechtmatig gebruik Suwinet.
- Het daarna zorgdragen voor vernietiging van de papieren versie van het autorisatieformulier en de Verklaring rechtmatig gebruik Suwinet.
- Maakt na iedere gebruikersmutatie hiervan melding in het logboek.

- Na de gebruikersmutatie wordt de gebruikersmatrix bijgewerkt.

De autorisatiebeheerder maakt samen met de kwaliteitsmedewerker en onder leiding van de Security Officer deel uit van de werkgroep Suwinet. Daarbij heeft de autorisatiebeheerder evenals de kwaliteitsmedewerker een controlerende rol bij het beoordelen van de rechtmatigheid en doelmatigheid van zoekopdrachten (zie hoofdstuk 4).

### 3.7 Proces autorisatiebeheer Suwinet-Inkijk

Het proces van autorisatiebeheer Suwinet-Inkijk wordt gekenmerkt door de volgende stappen.

- Een gebruiker kan alleen toegang tot Suwinet krijgen als de teammanager TUSD hier toestemming voor geeft. De teammanager TUSD is verantwoordelijk voor het tijdig toekennen/wijzigen/intrekken van accounts.
- Een verzoek aan de autorisatiebeheerder tot toekenning, wijziging van rol of beëindiging van autorisaties gebeurt aan de hand van een standaardformulier (zie bijlage 2).
- Bij intrekking van een account wordt de autorisatiebeheerder per omgaande geïnformeerd.
- De teammanager TUSD ondertekent het autorisatieformulier. De autorisatiebeheerder kent vervolgens de rol(len) met bijbehorende rechten toe aan de gebruiker.
- De autorisatiebeheerder verstuurt per mail aan gebruiker het Beveiligingsplan Suwinet, de actuele versie van de Factsheet Wie-mag-Suwinet-gebruiken van de VNG en ter ondertekening de Verklaring rechtmatig gebruik Suwinet. De mail wordt ter archivering opgeslagen.
- De autorisatiebeheerder digitaliseert het originele autorisatieformulier in kleur en archiveert het, evenals de door de medewerker ondertekende Verklaring rechtmatig gebruik Suwinet. De medewerker DIV draagt er zorg voor dat ook de Verklaring rechtmatig gebruik Suwinet aan het personeelsdossier wordt toegevoegd. De autorisatiebeheerder draagt hierna zorg voor de vernietiging van beide papieren exemplaren.
- 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. Tevens wordt de gebruikersmatrix bijgewerkt.
- De teammanager TUSD is verantwoordelijk voor het tijdig melden van accountmutaties aan de autorisatiebeheerder Suwinet.

### 3.8 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 TUSD. 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 TUSD is verantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk.

### 3.9 Misbruik

Geautoriseerde medewerkers bij de 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 re-integratie. 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 Suwinet op basis van nadere inspectie van specifieke rapportages misbruik vermoed of constateert wordt een onderzoek ingesteld en betreft hierbij altijd de teammanager TUSD. 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 Procedure 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.

Door de Security Officer Suwinet worden er maandelijks voor controledoeleinden zowel een algemene alsook specifieke rapportages van zoekopdrachten en account mutaties opgevraagd. De specifieke rapportages zijn alleen opvraagbaar voor de Security Officer Suwinet en zijn niet openbaar. Maandelijks wordt met de autorisatiebeheerder en de kwaliteitsmedewerker de algemene rapportage besproken. Indien wenselijk worden voor controledoeleinden zoekopdrachten met hen gedeeld. Daarnaast wordt door de kwaliteitsmedewerker en de autorisatiebeheerder een check gedaan op de raadplegingen van “niet-klanten” (de zogenaamde escape lijst) en worden andere afwijkingen besproken. De Security Officer Suwinet stelt zijn bevindingen daarna vast en rapporteert deze samen met een eventueel advies aan de teammanager TUSD. De teammanager TUSD geeft aan welke eventuele actie hij onderneemt en ondertekend daarna het controle rapport. Deze controle rapporten worden gearchiveerd.

De kwaliteitsmedewerker en de Autorisatiebeheerder Suwinet doen inhoudelijk controles op afzonderlijke zoekopdrachten die afwijkend zijn of welke vragen oproepen. Indien nodig doet de kwaliteitsmedewerker navraag bij de betreffende medewerker en koppelt de bevindingen terug aan de teammanager TUSD en de Security Officer Suwinet.

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 TUSD

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 en beheerders 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 beveiligingsplan 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 TUSD 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.

Het whitelist bestand wordt door de Autorisatiebeheerder Suwinet wekelijks op de BKWI site ge-upload.

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 reden 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 team TUSD in het bijzonder.

Concreet kunnen deze regels als volgt worden vertaald:

### **5.1 Beheren van wachtwoorden**

Bij het aanmaken van een gebruikersaccount wordt een tijdelijk wachtwoord gegenereerd. Dit tijdelijke wachtwoord wordt naar de gebruiker gemaild in de voorbeeldmail voor het verstrekken van gebruikersgegevens. 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 TUSD 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 TUSD 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 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, maar minder dan 15 minuten, 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 het werkstation 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 afgesloten 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 belangrijk voor het werk binnen een team waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwaame 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

# Verklaring rechtmatig gebruik Suwinet

### Gegevens medewerker

Naam	
Team	
Datum in dienst	

### Verklaring

- 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

Overbetuwe, \_\_\_\_\_ (datum)

De ambtenaar/medewerker (handtekening),

\_\_\_\_\_

## Bijlage 2: Autorisatieformulier Suwinet

# Formulier autorisatieverzoek Suwinet-Inkijk

Gegevens medewerker	
Naam:	
Team:	
Autorisatie	
<p>Teammanager geeft opdracht om met ingang van</p> <p><input type="checkbox"/> de medewerker volgens onderstaand profiel <u>toegang te verlenen</u> tot Suwinet.</p> <p><input type="checkbox"/> de rechten in Suwinet voor de medewerker <u>te wijzigen</u> volgens onderstaand profiel</p> <p><input type="checkbox"/> de toegang tot Suwinet voor deze medewerker <u>in te trekken</u></p>	
Autorisatieprofiel	
<p><input type="checkbox"/> Administratie</p> <p><input type="checkbox"/> Consulent Bijzondere Bijstand</p> <p><input type="checkbox"/> Klantmanager</p> <p><input type="checkbox"/> Kwaliteit</p> <p><input type="checkbox"/> Toezichthouder</p> <p><input type="checkbox"/> Statushouders Administratieve Ondersteuning</p> <p><input type="checkbox"/> Medewerker Publiekszaken</p> <p><input type="checkbox"/> Autorisatiebeheer</p> <p><input type="checkbox"/> Security Officer</p>	
Ondertekening	
Voor akkoord, Teammanager	<p>Datum:</p> <p>Naam:</p> <p>Handtekening:</p>

Verwerking Autorisatieverzoek,  
Applicatiebeheerder

Datum:

Naam:

Handtekening:

### **Bijlage 3: 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 4: Autorisatiematrix

	RoI	Administratie	Consulent bijzondere bijstand	Klantmanager	Kwaliteit	Toezichthouder	Statushouders admin ondersteuning	Autorisatiebeheer	Security Officer
<b>Overzichtspagina's</b>									
Handhaving						✓			
Kostendelerstoets	✓	✓	✓	✓	✓	✓			
Landelijk doelgroepenregister				✓	✓				
Rechtmatigheid +	✓	✓	✓	✓	✓	✓			
Re-integratie				✓	✓				
Terugvordering en Verhaal									
<b>Bronpagina's</b>									
Bedrijvenregister			✓	✓	✓	✓			
Belastingdienst	✓	✓	✓	✓	✓	✓			
Bijstandsregelingen	✓	✓	✓	✓	✓	✓			
DUO gegevens			✓	✓	✓	✓			
Fraude vorderingen									
BRP	✓	✓	✓	✓	✓	✓			
Inkomstenverhoudingen	✓			✓	✓	✓			
Kadaster			✓	✓	✓				
RDW	✓	✓	✓	✓	✓	✓			
RDW+						✓			
RDW Peildata	✓	✓	✓	✓	✓	✓			
SVB gegevens	✓	✓	✓	✓	✓	✓			
UWV uitkeringen	✓	✓	✓	✓	✓	✓			
UWVWb	✓	✓	✓	✓	✓	✓			
correctieservice									
Onderhouden status wijzigingsverzoeken									
<b>Zoekpagina's</b>									
Zoek in BRP									
Zoek+ in BRP						✓			
Zoek in Kadaster									
Zoek in PIVA									
Zoek in RDW									
Zoek in RDW+						✓			
<b>Overige (beheer)pagina's</b>									
Beheer: ww & blokkeren									
Fraude scorekaart			✓	✓	✓	✓			
Gebruikersbeheerder								✓	
Onderhouden correctieservice									
Onderhouden werkvoorraad								✓	
Opvragen generieke gebruiksrapportage									✓
Opvragen specifieke gebruiksrapportage									✓
SBR query									
Whitelist escape			✓	✓		✓			
<b>toegangsrechten tot andere applicaties</b>									
R1525 EROW beheer									
SCI02 Raadplegen ISI op BSN									
SCI03 Raadplegen ISI op BSN of selectie									
SCI05 Muterer ISI									
SCI06 Alle bevoegdheden incl signalen								✓	
SCI07 Raadplegen PV gegevens							✓		
SCI08 Muterer PV gegevens							✓		



Rol	Medewerker publiekszaken	Security Officer
<b>Bronpagina</b>		
Actuele adresgegevens	✓	
<b>Overige (beheer)pagina's</b>		
Burgerzaken adm		
Opvragen generieke gebruiksrapportage		✓
Opvragen specifieke gebruiksrapportage		✓