Beveiligingsplan Suwinet gemeente Overbetuwe

Versie	Wijzigingen	Datum
1.0	Vernieuwd plan	December 2019
1.1	- Verwijzing nieuw IB beleid - Autorisatiematrix up-to-date gemaakt, bij diverse rollen pagina's toegevoegd/verwijderd - Domeinmanager Sociaal vervangt directeur Ontwikkeling - Whitelist query bijgewerkt en up-to-date gemaakt - TUS in plaats van TUSD - TED ipv Publiekszaken	December 2020
1.2	- Autorisatiematrix up-to-date - Rol Consulent bijzondere bijstand verwijderd - Rol Statushouders adm. Ondersteuning verwijderd - Uitleg gebruik wachtwoord bij toegang Suwinet - SO rapporteert twee maal per jaar aan management over autorisatiebeheerproces - Activiteiten risicovermindering en bewustwording - Strikter maken autorisatiebeheerproces	Januari 2022
1.3	- Wgs aansluiting toevoegen - Rol medewerker SHV toevoegen - Autorisatiematrix up-to-date - Autorisatieformulier, Verklaring en Certificaat door Autorisatiebeheerder gearchiveerd in het Suwinet tabblad van het personeelsdossier (PD) van de gebruiker.	Februari 2023

Gemaakt door M. Spierings (Security Officer Suwinet)
Datum 6 maart 2023
Registratienummer 2023-012228

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.

Per 1 januari 2021 is de Wet gemeentelijke schuldhulpverlening (Wgs) gewijzigd. Ook is per 1 januari het ‘besluit gemeentelijke schuldhulpverlening’ van kracht. In de gewijzigde wet staat dat gemeenten gegevens over inkomen en vermogen mogen raadplegen via Suwinet voor het verlenen van toegang tot schuldhulp en het opstellen van een plan van aanpak.

Binnen de gemeente zijn bepaalde zaken rondom informatieveiligheid geregeld in een voor de gehele organisatie geldend Informatiebeveiligingsbeleid gemeente Overbetuwe. In dit 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.

Maandelijks vinden overleggen plaats in de Suwinet werkgroep. De besproken punten vinden hun weg naar de actualisatie van het voorliggende Beveiligingsplan Suwinet, dat jaarlijks wordt bijgewerkt. Aandachtpunten voor de evaluatie zijn: Wettelijke kaders, Technische ontwikkelingen, Organisatiewijzigingen, Incidenten. Met onderhavige versie wordt het beveiligingsplan Suwinet van gemeente Overbetuwe up-to-date gemaakt, inclusief de Autorisatiematrix.

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 erop 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 typen 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 routering 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 routering 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, WOZ, 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 elk jaar opnieuw.

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.

Er zijn 3 Suwinet aansluitingen actief voor gemeente Overbetuwe:

- Gemeentelijke Sociale Dienst (GSD)
- Burgerzaken (BZ)
- Wet gemeentelijke schuldhulpverlening (WGS)

De algehele Suwinet toepassing en daarmee ook de verantwoordelijkheid voor de informatiebeveiliging ervan valt toe aan de teammanager Team Uitvoering Sociaal. 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 TUS (aansluiting GSD en WGS) en Externe dienstverlening (aansluiting Burgerzaken).
De gegevens die voor team Externe dienstverlening (TED) 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. Om op het netwerk te komen is naast gebruikersnaam en wachtwoord, ook een verificatie vereist via een authenticatie app op de smartphone van de medewerker. De Suwinet-Inkijk toepassing heeft een eigen gebruikersnaam en wachtwoord.

Alle medewerkers en contractanten die voor hun taakuitoefening gebruik moeten maken van Suwinet, dienen voordat zij toegang krijgen tot Suwinet-Inkijk eerst een certificaat te overleggen van de VNG e-learning “Veilig gebruik Suwinet”.

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. 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 TUS. 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 TUS.

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

3.1 Bewustzijn bevorderende en risicoverlagende activiteiten

- Er wordt voor Suwinet accounts een strikt en nauwgezet autorisatiebeheerproces gevolgd.
- Autorisaties worden verstrekt op basis van rollen conform de autorisatiematrix (bijlage 4).
- Bij aanvraagverzoek voor een Suwinet account geeft de autorisatiebeheerder advies aan de proceseigenaar over mogelijke risico's.
- Toegang tot Suwinet-Inkijk wordt alleen verstrekt na aantoonbare opdracht van de proceseigenaar aan de autorisatiebeheerder.
- Ondertekenen door Suwinet gebruiker van de Verklaring rechtmatig gebruik Suwinet voordat toegang tot Suwinet-Inkijk verleend wordt.
- Bij aanmaak Suwinet account door Autorisatiebeheerder worden gelijktijdig instructies en documentatie verstrekt over veilige omgang Suwinet-Inkijk, waaronder dit beveiligingsplan.
- Alle Suwinet gebruikers dienen voordat zij toegang krijgen tot Suwinet-Inkijk eerst een certificaat te overleggen van de VNG e-learning Veilig gebruik Suwinet.
- Alle raadplegingen worden gelogd en hierop worden maandelijks controles gedaan naar onrechtmatige, onregelmatige of doel overschrijdende verwerking.
- Bij een oneigenlijke of onrechtmatige raadpleging neemt de Adviseur participatie persoonlijk contact op met gebruiker en vraagt opheldering en geeft indien nodig instructies aan gebruiker.
- Constatering van een oneigenlijke of onrechtmatige raadpleging wordt te allen tijde door de Adviseur participatie formeel teruggekoppeld aan: proceseigenaar, security officer, gebruiker in kwestie. In dat geval zijn mogelijke maatregelen aan de proceseigenaar voorbehouden.

3.2 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 kantoortijd op kantoor. Printen van Suwinet-Inkijk gegevens is niet toegestaan. Dit laatste uit het oogpunt van privacybescherming én dat te allen tijde alleen de onlinegegevens 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 onderhoudt.

- 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 ondertekent 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 tabblad van het personeelsdossier (PD) van de gebruiker. De digitale versie van de Verklaring rechtmatig gebruik Suwinet, evenals het Certificaat Suwinet wordt tevens door de autorisatiebeheerder in het tabblad Suwinet van het PD van de gebruiker opgeslagen.

- Onnodige verwerking van persoonsgegevens is niet toegestaan (dataminimalisatie). Zo mag het technisch nummer van een klantdossier, 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.

3.3 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 gedefinieerde rollen binnen Suwinet-Inkijk. Waar dit niet mogelijk is worden pagina’s rechtstreeks aan gebruikers gekoppeld.

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 belastingaangiftes van uitkeringsgerechtigden.

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 alsmede het vaststellen van doelgroepers 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.

Toezichthouder
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.

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.

Security Officer
Is bevoegd om de maandelijkse generieke en specifieke rapportages op te vragen. Rapporteert en geeft gevraagd en ongevraagd advies aan verantwoordelijk management.

Medewerker Externe dienstverlening
Enkele medewerkers van team Externe dienstverlening mogen gebruik maken van Suwinet-Inkijk om adresonderzoeken te behandelen.

Medewerker Schuldhulpverlening (SHV)
Enkele medewerkers van TUS mogen gebruik maken van Suwinet-Inkijk ten behoeve van verzoeken voor schuldhulpverlening. Hiermee kunnen onder andere gegevens geraadpleegd worden betreffende BRP, uitkering, inkomen, vermogen, onderneming en schulden.

3.4 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 en doelmatig 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 TUS toegekend dan wel ingetrokken of gewijzigd. De Autorisatiebeheerder Suwinet is verantwoordelijk voor uitvoering van deze opdrachten en archiveert het autorisatieformulier in het PD van de gebruiker. 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.

3.5 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 het hoofdzakelijk medewerkers van het team TUS, met aandachtsgebied Werk en Inkomen of Schuldhulpverlening, die met Suwinet moeten werken. Ook een enkele medewerker van team Externe dienstverlening werkt voor adresonderzoek met Suwinet Burgerzaken.
- 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 zoeksleutels 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 TUS ingetrokken, dan wel aangepast aan de nieuwe rol.
- Alleen de teammanager TUS is bevoegd om autorisatieformulieren te ondertekenen. Bij afwezigheid is de plaatsvervangend teammanager tekenbevoegd.

3.6 Proces autorisatiebeheer Suwinet-Inkijk

De rol van Autorisatiebeheer Suwinet-Inkijk is belegd bij Applicatiebeheer binnen TUS. Alle taken behorende bij het aanmaken, verwijderen en wijzigen van Suwinet accounts worden hieronder verstaan. Tevens vallen Functioneel beheer en Operationeel beheer van de Suwinet-Inkijk onlineapplicatie hieronder.

Voordat een medewerker door de autorisatiebeheerder Suwinet toegang verleend wordt tot Suwinet-Inkijk moet eerst aan de volgende drie voorwaarden voldaan zijn:

1. Er moet aantoonbaar en raadpleegbaar akkoord zijn van de proceseigenaar voor de toe te kennen autorisaties. Het autorisatieformulier wordt door de Autorisatiebeheerder gearchiveerd in het PD van de gebruiker.

2. De Verklaring rechtmatig gebruik Suwinet moet door de medewerker worden ondertekend en door de Autorisatiebeheerder worden gearchiveerd in het PD van de gebruiker.
3. De e-learning Veilig gebruik Suwinet moet door de medewerker succesvol doorlopen zijn met het behalen van een het certificaat. Het certificaat moet door de Autorisatiebeheerder worden gearchiveerd in het PD van de gebruiker.

Alleen als aan bovenstaande drie voorwaarden voldaan is en deze documenten door de Autorisatiebeheerder zijn gearchiveerd in het Suwinet tabblad van het PD van de gebruiker en deze ook controleerbaar zijn voor de Security Officer Suwinet, mag het Suwinet-Inkijk account worden aangemaakt en de autorisaties worden toegekend.

Voorts gelden voor autorisatiebeheer de volgende procedurestappen.

- Een gebruiker kan alleen toegang tot Suwinet krijgen als de teammanager TUS hier aantoonbaar toestemming voor geeft. De teammanager TUS 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 TUS ondertekent het autorisatieformulier. De Autorisatiebeheerder kent vervolgens de rol(len) met bijbehorende rechten toe aan de gebruiker.
- De Autorisatiebeheerder verstuurt per mail aan een nieuwe gebruiker het actuele 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 autorisatieformulier en archiveert het, evenals de door de medewerker ondertekende Verklaring rechtmatig gebruik Suwinet. Het autorisatieformulier evenals de Verklaring rechtmatig gebruik Suwinet worden aan het PD van de medewerker toegevoegd. De autorisatiebeheerder draagt hierna zorg voor de vernietiging van papieren exemplaren.
- Bij de aanvraag van elk nieuw account meldt de Autorisatiebeheerder Suwinet de gebruiker aan voor een VNG-leeromgeving account en instrueert de gebruiker om eerst de Suwinet e-learning Veilig gebruik Suwinet succesvol te doorlopen.
- Er vindt een controle plaats op het succesvol doorlopen hebben van de e-learning Veilig gebruik Suwinet.
- 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 TUS is verantwoordelijk voor het tijdig melden van accountmutaties aan de Autorisatiebeheerder Suwinet.
- In het Suwinet werkgroep overleg vindt maandelijks analyse plaats van de account mutaties.
- Tweemaal per jaar rapporteert de Security Officer aan de proceseigenaar Suwinet over het verloop van het autorisatiebeheerproces en de uitstaande actuele autorisaties.

De geldende regels voor het autorisatiebeheerproces dienen te allen tijde nauwgezet nagevolgd te worden. Afwijking van het autorisatiebeheerproces kan alleen na uitdrukkelijke afstemming en aantoonbare goedkeuring van de Security Officer Suwinet.

3.7 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 TUS 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 TUS en de domeinmanager Sociaal.

Jaarlijks controleert de SO of actualisering van het beveiligingsplan noodzakelijk is. Een hernieuwd beveiligingsplan wordt ter vaststelling aan het college van B&W 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 gearchiveerde Verklaringen rechtmatig gebruik Suwinet
- De gearchiveerde Certificaten Veilig gebruik Suiwinet
- De bijgewerkte autorisatiematrix en gebruikersmatrix

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 TUS. 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 TUS 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. Het is niet toegestaan Suwinet te gebruiken voor taken rondom uitvoering van de WMO of Jeugdzorg. Voor schuldhulpverlening is een aparte Suwinet aansluiting in het leven geroepen. Aansluiting hierop is pas mogelijk nadat hiervoor een aanvraag wordt ingediend. 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 vermoedt of constateert wordt een onderzoek ingesteld en betrekt hij hierbij altijd de teammanager TUS. 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. Rechtspositionele maatregelen zijn 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 raadplegingen en account mutaties opgevraagd. Maandelijks worden de algemene rapportage en de Escapelijst besproken met de Autorisatiebeheerder Suwinet en de Adviseur participatie. De Security Officer Suwinet stelt zijn bevindingen daarna vast en rapporteert deze samen met een eventueel advies aan de teammanager TUS. De teammanager TUS geeft aan welke eventuele actie hij onderneemt en ondertekent daarna het controlerapport.

De Adviseur participatie en de Autorisatiebeheerder Suwinet doen inhoudelijk controles op afzonderlijke raadplegingen die afwijkend zijn of vragen oproepen. Indien nodig doet de Adviseur participatie navraag bij de betreffende medewerker en koppelt de bevindingen terug aan de teammanager TUS 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 betrekt daarbij altijd de volgende personen:

- Autorisatiebeheerder Suwinet en Adviseur participatie
- Teammanager TUS

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 TUS 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:

- In geval van GSD, 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 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

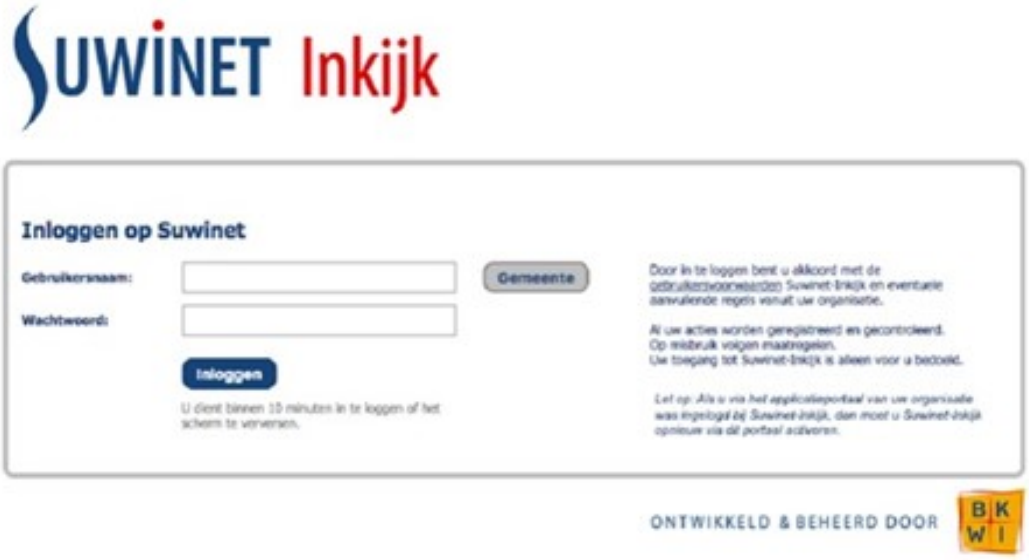
Voor het werken met persoonsgegevens is vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Daaruit zijn gedragsregels afgeleid die gelden voor medewerkers van de gemeente Overbetuwe in relatie tot al hun werkzaamheden en bij het gebruik van Suwinet-Inkijk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

Gebruik van wachtwoord bij inloggen op Suwinet-Inkijk.



Afbeelding 1. Inlogscherm Suwinet-Inkijk

Suwinet-Inkijk vraagt u wanneer u voor het eerst inlogt het wachtwoord te wijzigen in een nieuw wachtwoord.

De eisen waaraan dit nieuwe wachtwoord moet voldoen zijn als volgt:

1.Het wachtwoord moet bestaan uit minimaal 8 tekens, waarvan in ieder geval één teken voorkomt uit elk van de onderstaande series:

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

2.Het wachtwoord mag niet gelijk zijn aan uw voornaam, uw achternaam of uw gebruikersnaam

3. Het wachtwoord mag niet gelijk zijn aan één van de laatste 10 eerder gekozen wachtwoorden

4. Het wachtwoord moet minimaal 3 tekens verschillen van een eerder gebruikt wachtwoord

Het wachtwoord is **56** dagen geldig. Na deze periode verplicht Suwinet-Inkijk de gebruiker het wachtwoord te wijzigen. Suwinet-Inkijk geeft een aantal dagen voor het verlopen van het wachtwoord op het inlogscherm aan hoeveel dagen het wachtwoord nog geldig is.

Als het wachtwoord na 56 dagen niet gewijzigd is wordt het account automatisch geblokkeerd.

Indien een gebruiker van Suwinet-Inkijk langer dan **45** dagen niet inlogt op Suwinet-Inkijk wordt het account automatisch geblokkeerd.

Zowel het wachtwoord wijzigen na 56 dagen als eenmaal in de 45 dagen inloggen op Suwinet- Inkijk geldt voor alle gebruikers, dus ook voor gebruikersbeheerders.

Wanneer u als gebruikersbeheerder een wachtwoord verstrekt aan een Suwinet-Inkijk gebruiker, moet deze gebruiker het door u verstrekte wachtwoord binnen **14** dagen wijzigen anders wordt het account geblokkeerd.

5.2 Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de teammanager TUS 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 tweemaal per jaar in een periodiek teamoverleg op geattendeerd dat ze kennis moeten nemen van het plan.

Nieuwe medewerkers worden via de teammanager TUS 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 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 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 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. Rechtspositionele maatregelen zijn 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, buren, 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

De proceseigenaar Suwinet geeft opdracht om met ingang van

[datum invullen]

- de medewerker volgens onderstaand profiel toegang te verlenen tot Suwinet.
- de rechten in Suwinet voor de medewerker te wijzigen in onderstaand profiel
- de toegang tot Suwinet voor deze medewerker in te trekken

Autorisatieprofiel

- Administratie
- Klantmanager
- Kwaliteit
- Toezichthouder
- Medewerker SHV
- Medewerker Externe Dienstverlening
- Autorisatiebeheer
- Security Officer

Ondertekening	
Voor akkoord, Teammanager	Datum: Naam: Handtekening:
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 inkijksessie.

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 inkijksessie.

Een derde verzoekt om inzage in cliëntgegevens
Dit is niet mogelijk.

Bijlage 4: Autorisatiematrix

Autorisatiematrix Werk en Inkomen							
Onderdeel Suwinet	**Code**	**Administratie**	**Klantmanager**	**Kwaliteit**	**Toezichthouder**	**Autorisatiebeheer**	**Security Officer**
Overzichtspagina's							
Handhaving	R4967				✓		
Kostendelerstoets	R2786	✓	✓	✓	✓		
Landelijk doelgroepenregister	R4549		✓	✓			
Rechtmatigheid +	R3728	✓	✓	✓	✓		
Re-integratie	R3725		✓	✓			
Terugvordering en Verhaal	R4968						
Bronpagina's							
Bedrijvenregister	G024	✓	✓	✓	✓		
Belastingdienst	R1043	✓	✓	✓	✓		
Bijstandsregelingen	G019	✓	✓	✓	✓		
DUO gegevens	R3724		✓	✓	✓		
Fraude vorderingen	R1272						
BRP	G005	✓	✓	✓	✓		
Inkomstenverhoudingen	R3726	✓	✓	✓	✓		
Kadaster	via creatie eigen rol		✓	✓	✓		
RDW	G020	✓	✓	✓	✓		
RDW+	R1919				✓		
RDW Peildata	R454	✓	✓	✓	✓		
SVB gegevens	R3722	✓	✓	✓	✓		
UWV uitkeringen	R3723	✓	✓	✓	✓		
UWVWb	G003	✓	✓	✓	✓		
correctieservice	G031						
Onderhouden status wijzigingsverzoeken	G040						
Zoekpagina's							
Zoek in BRP	G018						
Zoek+ in BRP	G030				✓		
Zoek in Kadaster	via creatie eigen rol						
Zoek in PIVA	apart aanvragen via BKWI						
Zoek in RDW	R2355						
Zoek in RDW+	R1920				✓		
Overige (beheer)pagina's							
Beheer: ww & blokkeren	R3130						
Gebruikersbeheerder	GSDADM					✓	
Onderhouden correctieservice	G032						
Onderhouden werkvoorraad	R3846					✓	
Opvragen generieke gebruiksrapportage	R347						✓
Opvragen specifieke gebruiksrapportage	Rapport Specifiek GSD						✓
SBR query	via creatie eigen rol						
Whitelist escape	WE GSD		✓		✓		
toegangsrechten tot andere applicaties							
R1525 EROW beheer	R1525						

Autorisatiematrix Publiekszaken

Onderdeel Suwinet	code	Medewerker Externe dienstverlening	Security Officer	Autorisatiebeheer*
Bronpagina				
Actuele adresgegevens	R1265	✓		
Overige (beheer)pagina's				
Burgerzaken adm	DelAdmins			
Opvragen generieke gebruiksrapportage	R1417		✓	
Opvragen specifieke gebruiksrapportage	R5087		✓	

**het gebruikersbeheer voor Publiekszaken geschiedt via de beheerpagina GSDADM onder GSD en valt onder de rol van autorisatiebeheer*

Autorisatiematrix Wgs

Onderdeel Suwinet	code	Medewerker SHV	Security Officer	Autorisatiebeheer*
Bronpagina				
EXT4010089 Suwi bedrijvenregister 401-0089	FR4010089			
EXT4110089 WGS Toegang 411-0089	FR4110089			
EXT4120089 WGS Toegang (escape-optie) 412-0089	FR4120089	✓		
EXT4130089 WGS Toegang vorderingen 413-0089	FR4130089			
EXT4140089 WGS Toegang vorderingen (escape-optie) 414-0089	FR4140089			
EXT4150089 WGS Plan van aanpak 415-0089	FR4150089	✓		
Overige (beheer)pagina's				
Gebruikersadministratie	R5777			
Onderhouden werkvoorraad	R5920			✓
Opvragen generieke gebruiksrapportage	R5891		✓	
Opvragen specifieke gebruiksrapportages	R5971		✓	

**het gebruikersbeheer voor Wgs geschiedt via de beheerpagina GSDADM onder GSD en valt onder de rol van autorisatiebeheer*