Gemeente Bunschoten

GEMEENTEBLAD

Officiële uitgave van de gemeente Bunschoten

Nr. 156116

8 september 2017

Beveiligingsplan Suwinet 2017-2018

1. Inleiding beveiligingsbeleid Suwinet

De gemeenten Baarn, Bunschoten en Soest hebben als uitvoerder van diverse wetten en regelingen te maken met veel registraties. Om de efficiency en de effectiviteit te verbeteren worden de laatste jaren steeds meer van die registraties gekoppeld en is samenwerking binnen verschillende ketens noodzakelijk. Op basis van de wet Structuur uitvoering werk en inkomen (Suwi) is de uitvoeringsorganisatie BBS één van die ketens. Ketenpartners zijn het Bureau Keteninformatisering werk en inkomen (BKWI), het Uitvoeringsinstituut Werknemersverzekeringen (UWV en het UWV WERKbedrijf), de stichting Inlichtingenbureau Gemeenten (IB) en gemeenten. Zij wisselen via een elektronische infrastructuur persoonsgegevens met elkaar uit. Dit is het Suwinet.

Suwinet is tevens het netwerk waarover we de klantgegevens uitwisselen voor het Digitaal Klant Dossier. Belangrijk aspect hierbij is de Wet eenmalige gegevens uitvraag (WEU), in werking getreden op 1 januari 2008. Bij de start van de WEU is vastgelegd dat gegevens niet meerdere malen mogen worden opgevraagd. De klantgegevens die beschikbaar zijn via Suwinet moeten dus optimaal hergebruikt worden.

Suwinet-inkijk is de applicatie die op Suwinet draait. Binnen deze applicatie worden gegevens op basis van het Burgerservicenummer (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens zoals; inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, uitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. Ook is een Verificatie Informatie Systeem (VIS module) opgenomen waarmee op basis van legitimatiebewijzen en vreemdelingendocumenten gegevens kunnen worden opgevraagd. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Suwinet bevat privacygevoelige gegevens. Klanten mogen er op vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi.

1.1 Kader voor het Suwinet beveiligingsbeleid

De Inspectie SZW ging tot en met 2016 uit van zeven essentiële normen voor het waarborgen van de vertrouwelijkheid, opgenomen in het Normenkader Gezamenlijke elektronische Voorzieningen Suwi (GeVS). In het nieuwe “Specifiek Suwinet-normenkader Afnemers 2017” zijn de bestaande normen geactualiseerd. De normen worden vanaf 1-4-2017 gebruikt voor de periodieke zelfevaluatie. De zelfevaluatie en controles van het Suwinet-gebruik vinden tweemaal per jaar plaats. Hierbij worden behalve de naleving van de nieuwe normen ook de normen uit de Baseline Informatiebeveiliging Gemeenten (BIG) getoetst.

Vanwege de grote bijlage zal het “Overzicht Suwinet Normenkader 2017” afzonderlijk worden toegevoegd.

Het “Beveiligingsbeleid Suwinet” wordt éénmaal per jaar geëvalueerd. De punten die uit de evaluatie komen worden dan meegenomen in het nieuwe beveiligingsplan. Omdat dit jaar per 1-7-2017 een aantal belangrijke wijzigingen zijn ingegaan is voor 2016 besloten in het MT dat het beveilgingsplan 2016 tot 1-7-2017 zou lopen, zodat de wijzigingen meteen werden meegenomen. Dit plan loopt tot 31-12-2018 en heeft dus een duur van 1 ½ jaar.

De aanleiding voor de huidige aanpassing zijn:

1. Evaluatie beveiligingsplan 2016
2. Als gevolg van invoering van de BIG (Baseline informatiebeveiliging Nederlandse Gemeenten) is het Beveiligingsbeleid Suwinet nu specifiek gericht op het gebruik van Suwinet. Het algemeen geldende informatie-beveiligingsbeleid is van toepassing voor meer onderwerpen.

2 Kaders beveiligingsbeleid Suwinet

2.1 Rollen en gebruikers van Suwinet-Inkijk
Onderstaande functies zijn betrokken bij het gebruikmaken van Suwinet-Inkijk:

2.1.1 Management
- Directeur BBS: verantwoordelijk manager en eigenaarschap Suwinet; Formeel verantwoordelijk, ontvangt de rapportages.
- MT: beslist over bevoegdheden en autorisatie van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet.

2.1.2 Beheer van autorisaties
- Applicatiebeheer, tevens Functioneel beheer/Autorisatiebeheer/Operationeel beheer: verzorgt de autorisatie voor Suwinet binnen het pakket.

2.1.3 Controle op rechtmatigheid
De security-officer ziet toe op een correcte beveiliging van Suwinet. Zij is in haar rol onafhankelijk, maar laat zich in de uitvoering uiteraard adviseren vanuit verschillende rollen en lagen in de organisatie. Naar aanleiding van periodieke controles en (eventueel tussentijdse) evaluatie worden eventueel aanvullende maatregelen genomen om de rechtmatigheid te borgen. Indien noodzakelijk stelt zij voor het beleid daarop aan te passen en ziet toe op juiste implementatie van de wijzigingen.

Taken security officer:

- Periodiek, per kwartaal, controle logging gegevens.
  Doel: controleren of het gebruik van de gegevens binnen Suwinet-inkijk plaatsvindt binnen de wettelijke kaders en in overeenstemming met de doelen die de organisatie hiertoe heeft geformuleerd
- Periodieke, per half jaar, rapportage over controle login en gebruik Suwinet
- Jaarlijkse controle op actualiteit. Het beveiligingsplan controleren op actualiteit en volledigheid.
- Bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.

2.1.4 Uitvoering van taken
Het raadplegen van Suwinet is voorbehouden aan:

- Medewerkers uitkeringsadministratie
- Klantmanager inkomen
- Klantmanager werk
- Klantregisseur
- Medewerker terugvordering en verhaal
- Fraudecontroleur
- Juridisch medewerker

2.2 Gebruik van Suwinet-Inkijk
Hierboven is beschreven wie Suwinet-Inkijk mogen raadplegen. Deze paragraaf geeft aan wanneer dat mag. Er is sprake van ongeoorloofd gebruik wanneer Suwinet om andere dan de omschreven redenen wordt gebruikt. Over het algemeen geldt dat slechts mag worden geraadpleegd indien de stap binnen het werkproces van het klantvolgsysteem expliciet is beschreven.

De Security Officer controleert de handhaving van dit beveiligingsbeleid door rapportages bij het Bureau Keteninformatisering Werk & Inkomen (BKWI) op te vragen en te analyseren. In uitzonderlijke gevallen krijgt de Security Officer toegang tot Suwinet Inkijk. Dit kan alleen incidenteel op verzoek van de teamleider of manager.

In het kader van de functiescheiding is het beheer voor het gebruik van Suwinet neergelegd bij het applicatiebeheer. Deze is uitvoerend verantwoordelijk voor het beheren van alle accounts. Juridische medewerkers mogen raadplegen om besluiten te kunnen toetsen.

Medewerkers mogen raadplegen bij het behandelen van aanvragen of bij een melding dat belanghebbende een uitkering of aanverwante regeling wil aanvragen, voor rechtmatigheidsonderzoeken en tussentijdse onderzoeken voor zover het de Participatiewet, de Wet Inkomensvoorziening oudere gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet Inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (Ioaz), het Besluit bijstandsverlening zelfstandigen 2004 (Bbz 2004) betreft.

De autorisatiematrix[1] is per 1-7-2017 herzien. Hierin is opgenomen dat de medewerker enkel de voor hem/haar van belang zijnde gegevens kan raadplegen. Zo kan de uitvoerder van terugvordering en verhaal specifiek raadplegen bij onderzoeken die samenhangen met vorderingen of met verhaal op onderhoudsplichtigen. Dit bijvoorbeeld ter vaststelling van de woonplaats, de draagkracht, het inkomen of de werkgever.

Whitelist
Wanneer een medewerker toegang heeft tot Suwinet kan hij van iedere in Nederland woonachtige burger alle gegevens opvragen. 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. Dit is onwenselijk omdat dit kan leiden tot het raadplegen van gegevens van burgers waar geen dienstverlening relatie mee 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/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde 'escapefunctie'. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers.

BBS heeft de volgende selectie gemaakt voor de whitelist:

- Alle actieve uitkeringen Periodiek Levensonderhoud als Periodiek Bijzondere Bijstand;
- Alle debiteurendossiers waarvan het saldo <> € 0,00;
- Alle actieve Werkprocessen van het soort aanvraag voor regeling 0 PWI, 6 IOAWZ, 7 Voorschotten, 8 Crediteuren, 10 Debiteuren, 17 PWW.

Escaperol
In bepaalde situaties is het nodig dat er toch persoonsgegevens worden ingezien van personen waar op 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 ervoor dat de medewerker toch het BSN kan inzien dat niet op de whitelist staat.

Wanneer de medewerker gebruik maakt van de escapefunctie wordt gevraagd waarom de medewerker dit wil. Tevens wordt de reden gevraagd. De redenen worden geregistreerd en gelogd. De security-officer krijgt hier periodiek een rapport van.

Er zijn vijf escapes:

- Nieuwe klant of aanvraag
- Vaststellen onderhoudsbijdrage
- Inkomsten van 16 en 17 jarigen
- Bijzonder onderzoek

1) Zie autoristiebesluit 2017

- Overig (wanneer deze gekozen wordt moet de medewerker zelf bijhouden in een logboek waarom voor deze escape is gekozen)

Wanneer een medewerker niet is geautoriseerd voor de escapefunctie en hij/zij vraagt gegevens op van een BSN dat niet op de whitelist staat, zullen de gegevens niet worden getoond.

De volgende functies krijgen de escape-rol binnen BBS:

- Klantregisseur (speciale doelgroepen)
- Klantmanager inkomen
- Terugvordering en verhaal
- Fraudecontroleur

2.3 Logging rapportages
Het BKWI heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van onder andere de gemeente kan worden nagegaan. De logging wordt gebruikt voor controles over onrechtmatige, onregelmatige of doel overschrijdende verwerking.

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd. Voorafgaand aan de toegang tot Suwinet krijgen medewerkers uitleg over het gebruik van suwinet en worden zij gevraagd het beveiligingsbeleid door te nemen wat centraal opgeslagen staat. Tevens tekenen zij de "Geheimhoudingsverklaring" (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;
- Ingeval van onrechtmatig of doel overschrijdend gebruik van het Suwinet-Inkijk bespreekt de teamleider dit met de betreffende medewerker(s).

Het BKWI levert verschillende soorten rapportages. Een periodiek rapport gaat automatisch naar de Security Officer. Deze signaleert eventuele onvolkomenheden en overlegt met de teamleider of er mogelijk sprake is van misbruik. De (logging) gegevens over het gebruik van Suwinet-Inkijk worden twee maal per jaar uitgevraagd door de Security Officer. Deze analyseert de logging gegevens en controleert of de gemeente aan de gemaakte afspraken voldoet. Een rapport over het gebruik van de escape-rol.

De resultaten van deze analyse worden gerapporteerd aan het MT.

2.4 Tijdelijke medewerkers
Een tijdelijk ingehuurde medewerker heeft de volgende aanvullende voorwaarden waaraan voldaan moet zijn voordat er toegang gegeven kan worden voor Suwinet inkijk, te weten:

- De medewerker moet een verklaring over gedrag (VOG) overleggen;
- De geheimhoudingsverklaring en gebruikersverklaring die medewerkers ondertekenen bij binnenkomst dient te worden aangepast op medewerkers die tijdelijk worden ingehuurd;
- waarbij aangevuld wordt dat alle logging wordt vastgelegd zodat gecheckt kan worden dat mensen geen onrechtmatig gebruik maken van hun (tijdelijke) bevoegdheid tot het gebruik van Suwinet inkijk.

3. Procedures Suwinet-inkijk

3.1 Beheren van wachtwoorden
De applicatiebeheerder bepaalt hoe lang een wachtwoord geldig is. De gebruiker moet het toegekende wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord. Het account van Suwinet blokkeert automatisch als het langer dan één kwartaal niet is gebruikt.

3.2 Einde dienstverband
Zodra een medewerker niet langer gebruik maakt van Suwinet, wordt het account verwijderd.

3.3 Geheimhoudingsplicht
Gebruikers van Suwinet-Inkijk werken met persoonsgegevens. Voor het werken met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP).

Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de gegevens, inclusief persoonsgegevens, niet verder bekend mogen worden gemaakt dan strikt voor de uitoefening van de functie noodzakelijk is.

3.4 Kennisnemen van het beveiligingsbeleid Suwinet
Dit beveiligingsbeleid Suwinet is van toepassing op alle gebruikers van Suwinet-Inkijk binnen BBS. Het beleid is voor iedereen toegankelijk op de algemene N-schijf en digitale dossier Verseon. De teamleider attendeert de gebruikers minimaal twee keer per jaar tijdens een teamoverleg op de inhoud van het beleid en de noodzaak van het veilig omgaan met Suwinet.

Nieuwe medewerkers worden via de teamleider op het beleid 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 het gedrag kan worden gecontroleerd. Van dat laatste moeten ze zich bewust zijn, ook in relatie tot hun eigen privacy. De organisatie kan de opgeslagen gegevens niet lukraak gebruiken: er moeten redelijke gronden zijn om de privacy van medewerkers te schenden.

3.5 Gegevensverstrekking aan derden via de telefoon
In principe wordt geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. Het uitgangspunt is dat zeer terughoudend wordt omgegaan met verzoeken om telefonische informatie over klanten. Dit vanwege het risico dat de identiteit van de gesprekspartner onvoldoende kan worden vastgesteld of dat persoonsgegevens worden verstrekt aan personen of instanties, die geen recht hebben op 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 wanneer het een vaste contactpersoon betreft.

3.6 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.

3.7 Clear desk policy
Het is noodzakelijk ook ten opzichte van collega's en dienstverleners zorgvuldig om te gaan met de privacy van klanten. Onbevoegden mogen niet de beschikking krijgen over vertrouwelijke informatie. Daarom mogen die 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 is gesloten.

Kortom: geen rondslingerende documenten in de werkruimte.

3.8 Clear screen policy
De toegang tot werkplekken (inlog van computers) is beveiligd met een gebruikersnaam gecombineerd met een wachtwoord. De Suwinet-inkijk applicatie kent een eigen wachtwoord. Tijdens 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 bureaublad vergrendeld.

3.9 Telewerken
BBS voert een pilot uit met telewerken. Het breder en intensiever inzetten van e-dienstverlening, mobiele apparaten en telewerken stelt Suwi-ketenpartijen in staat aan te sluiten bij de hedendaagse eisen van klanten en medewerkers. Daarnaast werken medewerkers van ketenpartijen steeds meer samen

met andere overheidsmedewerkers. Mobiele apparaten en netwerken die dit ondersteunen zijn extra gevoelig. Tegelijkertijd zijn de bedreigingen vanuit de buitenwereld toegenomen. Het gevolg van deze twee ontwikkelingen is dat de beveiligingsrisico's voor ketenpartijen groter zijn geworden. Daardoor bestaat meer kans op schade voor de omgeving van de Afnemers. Daarom worden specifieke eisen gesteld aan telewerk voorzieningen.

3.10 Vernietiging van vertrouwelijke gegevens
Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Ook het vernietigen van deze gegevens moet op een veilige manier gebeuren. Daarom zijn in het gebouw speciale containers geplaatst, waarin het te vernietigen materiaal is verzameld. Het vernietigingsbedrijf voert dit periodiek af.

3.11 Aanspreken van onbekende personen
Als een medewerker een voor hem/haar onbekende persoon in het gebouw tegenkomt waar officieel geen publiek zonder begeleiding mag komen, moet de medewerker deze persoon aanspreken, zichzelf voorstellen en de persoon in kwestie vragen wat hij/zij hier doet. Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hen beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naartoe te begeleiden.

3.12 De dagelijkse werkzaamheden versus Informatiebeveiliging
Informatiebeveiliging is belangrijk voor het werk binnen een afdeling waar de medewerkers veelvuldig met privacygevoelige informatie werken en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Klanten mogen vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom in het werkoverleg regelmatig aandacht voor dit onderwerp moet zijn.

3.13 Sancties
Als een medewerker de regels overtreedt, dan spreekt zijn teamleider hem daarop aan. Er zijn rechtspositionele maatregelen mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen. Dit geldt voor alle werkzaamheden binnen BBS, niet alleen voor het gebruik van Suwinet.

3.14 Beleid bij misbruik
Bij geconstateerd misbruik van Suwinet geldt het gemeente brede beleid bij misbruik. Voor de betrokken medewerker kan dit rechtspositionele gevolgen hebben.

20-6-2017

A. Pruijssers
Adviseur bedrijfsvoering

Bijlage 1: Geheimhoudingsverklaring

Geheimhoudingsverklaring

Naam: geb. datum:

Functie: Datum in dienst:

1) Ondergetekende, geautoriseerd tot het opvragen van gegevens uit de al dan niet geautomatiseerd toegankelijke gemeentelijke gegevensbestanden, GBA en Suwinet, verklaart zijn/haar werkzaamheden te zullen verrichten onder de volgende voorwaarden:
   a) Geen andere informatie door middel van een werkstation uit de gemeentelijke gegevensbestanden 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 hetgeen ten aanzien van de geheimhouding in de wet is bepaald (art. 272 Wetboek van Strafrecht) en met het feit dat schending van de geheimhoudingsplicht een zogenaamde dringende reden kan betekenen die ontslag op staande voet rechtvaardigt (art. 7:678 BW);
   d) Geen andere personen gebruik te zullen laten maken van zijn/haar unieke gebruikersprofiel en/of -wachtwoord;
   e) Zonder toestemming van zijn direct leidinggevende zal ondergetekende geen andere personen dan de in dienstverband werkende personeelsleden toelaten bij het werkstation dat toegang geeft tot de gegevensbestanden;
   f) Bij het verlaten van de werkplek, zullen alle sessies van applicaties die toegang geven tot de gegevensbestanden vanuit het werkstation door ondergetekende worden afgesloten;
   g) Wanneer ondergetekende de laatste is die aan het einde van de werkdag de ruimte verlaat waarin het werkstation is opgesteld dat toegang geeft tot de gegevensbestanden, zal hij/zij er voor zorg dragen dat ramen en deuren worden gesloten en dat alle werkstations zijn afgemeld en zonodig zijn uitgezet.
   h) Bekend te zijn met het feit dat inloggegevens van telefoon en software-applicaties gelogd worden.
   i) Het telewerkbeleid te volgen van BBS indien op een andere locatie gewerkt wordt.

2) Deze verklaring blijft voor lid 1b en 1c van kracht, ook na beëindiging van bovengenoemde werkzaamheden, of beëindiging van het dienstverband.

Handtekening: Datum:

Bijlage 2: Inwerkprogramma

Inwerkprogramma Uitvoeringsorganisatie BBS

Naam nieuwe medewerker/stagiair* Functie: Afdeling:			
1e werkdag op:			
Activiteiten	***Wie/paraaf***	***Wanneer***	***Uitgevoerd dd.***
** Voor stagiairs wordt dit programma doorlopen voor zover van toepassing*			
Voorbereiding vooraf aan de 1e werkdag			
Arbeidsvoorwaardelijk gesprek / het invullen van AG-formulier	HR-adviseur		
Versturen naar de nieuwe medewerker:	Personeels-administratie (PA)		
o Akte van benoeming			
o Benoemingsbrief + indiensttredingformulieren			
Nieuwe medewerker informeren over tijdstip 1e werkdag	Direct leidinggevende (LG)		
Aanvragen kantoormeubilair/-benodigdheden via de bodekamer	LG		
naamkaartje (op/naast de deur) via de bodekamer			
Adresgegevens en behaalde opleidingen opnemen voor schema's adressenbestand en opleidingsplan	Managementassistent		
Autorisatie computer en aanvragen email account via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht	Bedrijfsvoering (BV)		
Regelen toegangsbadge via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht	BV		
Aanmelden tijdregistratie via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht	BV		
Aanmelden telefoonlijst via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht	BV		
Mentor aanstellen	LG		
Introductie- en inwerkprogramma samenstellen, gericht op functie • Inwerken binnen het team, incl. PC-programma's en toepassing • Roostert meelopen in verschillende werkeenheden	LG/mentor		
Bestellen welkomstboeket en aanbieden op de eerste werkdag	Managementassistente		
Autorisatie applicaties: Rol binnen de applicaties: Klantregisseur / Klantmanager inkomen/werk/ Juridisch kwaliteit / WMO consulent / administratie WMO / uitkeringsadministratie GWS4all / Suite voor inkomen ja / nee GWS4all / Suite voor Werk ja / nee GWS4all / Suite voor WMO ja / nee GWS4all / Suite voor Jeugd ja / nee Suwinet inkijk ja / nee Matchcare ja / nee Stekker 4 / erow ja / nee CAK ja / nee	Via indiensttredingsbericht		

SVB ja / nee			

Tijdens de eerste werkdagen	***Wie?****/paraaf*	***Wanneer***	***Uitgevoerd dd.***
Ontvangst (met bloemetje op bureau) nieuwe medewerker en voorstellen aan collega's afdeling (bijv. koffiedrinken met alle collega's)	LG / kamergenoot		
Voorstellen aan de mentor	LG		
Informatie geven over de afdeling, de producten, de werkverdeling, de functie, de organisatie en de burgers	LG		
Geheimhoudingsverklaring (o.a. Suwi en GBA) laten tekenen; opslaan in Verseon	Management assistent		
E-learning veilig gebruik internet volgen van de VNG	BV		
Dienst- en afdelingsinformatie (gedoseerd):	LG		
o Overlegstructuur			
o Taakverdeling afdeling			
o Functie-/taakbeschrijving nieuwe medewerker			
o Overdracht taken			
o Belangrijke nota's die relevant zijn voor de functie			
o Werkplan van de dienst			
o Waar info verkrijgbaar			
o Begin maken met eigen werkzaamheden			
o Afspraken maken met belanghebbende collega's m.b.t. werkzaamheden			
o Informatie geven over procedures:	LG		
o Rechtmatigheden en (begroting)cyclussen	LG		
Nieuwe medewerker informeren over performance cyclus (fuge, beo, pop en competentiescan)	LG		
Ziekmeldingen	LG		
Wat te doen bij agressie/beveiliging afdeling/integriteit	Algemeen manager		
Informatie geven over intranet	LG/Mentor		
Rondleiding door het gemeentehuis (bedrijfsrestaurant/fitness/raadzaal/rookruimte	LG/Mentor		
Uitleg over de huisregels en de gang van zaken:	LG/Mentor kamergenoot		
o Werkplek laten zien, huisregels	LG		
o Uitleg werktijden/klokken	LG		
o Evt. werkkleding, gebruik fietsenstalling, dienstfietsen en parkeermogelijkheden	LG		
o Roken, pauzes (wanneer, hoelang)	LG		
o Pantry's, toilet.	Mentor kamergenoot		
o Hoe kantoorartikelen te bestellen;	Mentor kamergenoot		
o Uitleg printer/kopieerapparaat/pc/telefoon/fax	Mentor kamergenoot		
o Uitleg post	Mentor		

	kamergenoot		
o Declaratie overuren, dienstritten en avondvergaderingen;	LG		
o Verjaardagen en lief & leedpot	Beheerder Lief&Leedpot		
o Bedrijfsrestaurant	Mentor kamergenoot		
Afspraak maken met een HR-adviseur/medewerker personeelsadministratie voor een introductiegesprek	PA		
Afspraak maken met de KAM-coördinator	PA/Arbo coördinator		
Bespreken Arbo, milieu, EHBO, brandalarm, ontruiming en hygiënevoorschriften	Arbo coördinator		
Identiteitskaart BBS (bij cliëntcontactfuncties) en visitekaartje maken	managementassistent		
Bevindingen eerste werkdag Opmerkingen en aandachtspunten	LG		
Na twee maanden	***Wie?****/paraaf*	***Wanneer***	***Uitgevoerd dd***
Evalueert het inwerkproces samen met nieuwe medewerker. Regelt zonodig vervolg.	LG		
Indien gewenst korte snuffelstage op andere afdelingen binnen de dienst.	LG		

Bijlage 3: Indiensttredingsbericht BBS

Indiensttredingsbericht

Bestemd voor : RID, Interne Dienst, Dienstverlening (balie/TIP), Andy Romijn, Regina van Overeem, Karolina de Munck Mortier, Bert van der Weerd, Jenny van der Zouw, Jeroen de Keijzer, Evert de Kruijff, J. Wildenburg-van Bedum, Marco van Merkerk, Angelique Pruijssers

Van : Afdeling Bedrijfsvoering cluster HR voor Uitvoeringsorganisatie BBS

Roepnaam	:
Voorletters	:
Tussenvoegsel (getrouwd)	:
Achternaam (getrouwd)	:
Tussenvoegsel (geslachtsnaam)	:
Achternaam (geslachtsnaam)	:
Voorkeursnaamgebruik *(let op: te gebruiken voor telefonie en mail)*	:
Geboortedatum	:
Titel	:
Status (vast, uitzendkracht etc.)	:
Ingangsdatum	:
Einddatum (indien van toepassing)	:
Functiebenaming	:
FAB-er rol ja/nee *(is deze medewerker ook applicatiebeheerder?)*	:
Organisatie	:
Afdeling	:
Team	:
Locatie (gemeentehuis of buitenverblijf)	:
Toegang tot groepsschijven	:
Welke rechten per groepsschijf *(lezen; schrijven; modificeren; deleten, etc.)*	:
Telefoonnummer bestaande werkplek	:
Aanpassen naam in telefooncentrale	:
Telefoon beschikbaar ja/nee	:
Mobiel telefoonnummer i.v.m. thuiswerken *(alleen nodig voor thuiswerkers)*	:
Mailgroep waartoe toegang	:
PC nummer	:
PC nodig ja/nee	:
PC beschikbaar ja/nee	:
Badgenummer	:
Kamernummer	:
Aantal uren	:
In plaats van	:
Aangestuurd door	:
Overige opmerkingen(bijv. speciale hardware)	:

	Benodigd	**Bestemd voor**
X	Account, telefoon, autorisatie	RID
X	Xential	Applicatiebeheerder div, financiën en informatievoorziening
X	Suite4sociaaldomein	Applicatiebeheerder BBS
X	Suwinet	Applicatiebeheerder BBS
X	Verseon	Applicatiebeheerder div, financiën en informatievoorziening
X	Badge	Bodekamer
X	TIM	Applicatiebeheer financiën Soest
X	PIV/GBA	Teamleider dienstverlening
X	WBS/Sonar	Medewerker bedrijfsvoering BBS
X	Decade	Applicatiebeheerder financiën Soest

Afgesproken Rooster

Maandag	Dinsdag	Woensdag	Donderdag	Vrijdag

Bijlage 4: Autorisatiebesluit

Autorisatiebesluit

Inleiding
Het via Suwinet uitwisselen van gegevens tussen gemeenten, SVB, UWV en andere bronnen is om meerdere reden noodzakelijk. Allereerst om burgers beter te kunnen helpen en ten tweede om fraude of misbruik te voorkomen.
De persoonsgegevens die via Suwinet worden uitgewisseld zijn zeer privacygevoelig. Daarom is het van belang dat gebruikers zorgvuldig met de gegevens die via het systeem worden uitgewisseld omgaan. In de praktijk gaat dat niet altijd goed. In het programmaplan 'Borging veilige gegevensuitwisseling via Suwinet' staan maatregelen om oneigenlijk gebruik van Suwinet tegen te gaan. Eén van die maatregelen is het verbeteren van de autorisatiestructuur. Een fijnmaziger structuur betekent dat de afstemming tussen de gegevenslevering en de informatiebehoefte van de professional wordt verbeterd (verfijnd). Daarmee wordt voorkomen dat ambtenaren gegevens onnodig raadplegen of meer gegevens onder ogen krijgen dan echt nodig is.
Alle gemeenten moeten vóór 1 juli 2017 hun Suwinet-autorisaties opnieuw inrichten.

Doel
Een fijnmaziger autorisatiestructuur bevordert 'proportionaliteit van gegevenslevering' en gaat daarmee overmatig gegevensgebruik tegen. De toegang tot gegevens wordt beter afgestemd op wat voor de uitoefening van een taak noodzakelijk is. Niet meer en niet minder. Naast een fijnmaziger autorisatiestructuur vergt dit uiteraard ook een juist gebruik van zoeksleutels

De huidige situatie
1. Gebruikers kunnen via de webapplicatie Suwinet-Inkijk gegevens uit verschillende bronnen opvragen.
   De bronhouder bepaalt per wettelijke taak welke gegevensset aan welke organisatie mag worden geleverd. Die gegevens worden getoond op de inkijkpagina's van Suwinet-inkijk. Deze inkijkpagina's bestaan uit bronpagina's en overzichtspagina's:
2. Bronpagina: toont de gegevens van één bron

Overzichtspagina: combineert gegevens van verschillende bronnen

Probleem: meer gegevens dan nodig In sommige situaties vragen medewerkers meer gegevens op dan voor de uitvoering van hun taak nodig is. Daarmee is er sprake van disproportionaliteit. Dit gebeurt niet altijd bewust. De huidige opbouw en samenstelling van de inkijkpagina's is hier debet aan.

Wijzigingen per 1-7-2017

1. Nieuwe pagina's en nieuwe indeling.
Om disproportionele gegevenslevering op korte termijn te beperken veranderen er drie dingen:
1. De huidige overzichtspagina's (Klant Algemeen(+)) worden opgedeeld in twee afzonderlijke overzichtspagina's:
   - overzichtspagina Rechtmatigheid GSD
   - verzichtspagina Re-integratie GSD

2. Overzichtspagina's worden verwijderd per 1 juli 2017
   - overzichtspagina's Klant Algemeen (+)
   - overzichtspagina Klantbeeld

3. Bronpagina's worden toegevoegd.

Zo komen voor meer bronnen aparte pagina's beschikbaar. Het betreft:
- bronpagina SVB voor GSD
- bronpagina UWV Uitkeringen voor GSD
- bronpagina DUO gegevens voor GSD
- bronpagina UWV Inkomensverhoudingen voor GSD

De nieuwe pagina's bevatten dezelfde en daarmee evenveel gegevens als in de huidige situatie. Er is geen sprake van gegevensverlies. De bronhouders hebben immers al eerder toestemming gegeven voor het verwerken van deze gegevens en deze gegevens zijn nodig om de klant optimaal te kunnen bedienen. De meest in het oog springende wijziging is dat de overzichtspagina Klant Algemeen(+) wordt opgeknipt. Deze pagina's worden vervangen voor rechtmatigheid en re-integratie.

2. Whitelist
Wanneer een medewerker toegang heeft tot Suwinet kan hij van iedere in Nederland woonachtige burger alle gegevens opvragen. 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. Dit is onwenselijk omdat dit kan leiden tot het raadplegen van gegevens van burgers waar geen dienstverleningsrelatie mee 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/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde 'escapefunctie'. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers.
BBS heeft de volgende selectie gemaakt voor de whitelist:

- Alle actieve uitkeringen Periodiek Levensonderhoud als Periodiek Bijzondere Bijstand;
- Alle debiteurendossiers waarvan het saldo <> € 0,00;
- Alle actieve Werkprocessen van het soort aanvraag voor regeling 0 PWI, 6 IOAWZ, 7 Voorschotten, 8 Crediteuren, 10 Debiteuren, 17 PWW.

3. Escape-rol
In bepaalde situaties is het nodig dat er toch persoonsgegevens worden ingezien van personen waar op 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 ervoor dat de medewerker toch het BSN kan inzien dat niet op de whitelist staat.

Wanneer de medewerker gebruik maakt van de escapefunctie wordt gevraagd waarom de medewerker dit wil. Tevens wordt de reden gevraagd. De redenen worden geregistreerd en gelogd. De security-officer krijgt hier periodiek een rapport van.

Er zijn vijf escapes:

- Nieuwe klant of aanvraag
- Vaststellen onderhoudsbijdrage
- Inkomsten van 16 en 17 jarigen
- Bijzonder onderzoek
- Overig (wanneer deze gekozen wordt moet de medewerker zelf bijhouden in een logboek waarom voor deze escape is gekozen)

Wanneer een medewerker niet is geautoriseerd voor de escapefunctie en hij/zij vraagt gegevens op van een BSN dat niet op de whitelist staat, zullen de gegevens niet worden getoond.

De volgende functies krijgen de escape-rol binnen BBS:

- Klantregisseur (speciale doelgroepen)
- Klantmanager inkomen
- Terugvordering en verhaal
- Fraudecontroleur

Autorisatiematrix
Door deze wijzigingen volstaat de oude autorisatiematrix niet meer. Onderstaand is de nieuwe autorisatiematrix opgenomen. Hierin staan de functies met de daarbij horende autorisaties vermeld.
Nadat het MT deze heeft vastgesteld zullen de medewerkers op de hoogte worden gesteld en zal deze werkwijze worden ingevoerd.

Functies	Uitkerings adm.	Klantmanager inkomen	Klantmanager werk	Klantregisseur	Klantregisseur plus (speciale doelgroepen)	Terugvordering en verhaal	Fraudecontroleur	Juridisch medewerker	Gebruikersbeheer	Security officer
Overzichtpagina's										
Rechtmatigheid +	X	X		X	X	X		X		
Reintegratie			X	X	X			X		
Handhaving							X	X		
Terugvordering en verhaal						X		X		
Kostendelerstoets	X	X		X	X	X		X		
Bronpagina's										
GBA	X	X		X	X	X	X	X		
Kadaster	X	X	X	X	X	X	X	X		
Belastingdienst	X	X		X	X	X	X	X		
RDW	X	X		X	X	X	X	X		
RDW peildata	X	X		X	X	X		X		
RDW+							X			
Bijstandsregelingen	X	X		X	X	X	X	X		
Fraudevorderingen						X	X	X		
UWV Werkbedrijf		X	X	X	X		X	X		
UWV uitkeringen	X	X		X	X	X	X	X		
UWV inkomstenverhoudingen	X	X	X	X	X	X	X	X		
SVB	X	X		X	X	X	X	X		
DUO	X	X		X	X	X	X	X		
Bedrijvenregister		X	X	X	X			X		
Zoekpagina's										
Zoek in GBA							X			
Zoek in GBA+							X			
Zoek in RDW							X			
Zoek in RDW+							X			
Zoek in kadaster							X			
Overige										
Escape Whitelist		X			X	X	X			
SBR Qeury			X	X						
Fraudescorekaart		X		X			X	X		
Wachtwoorden blokkeren									X	
Gebruikersadministratie									X	
Opvragen rapportages									X	X
Onderhouden correctieservice										
Correctieservice										
Statuswijziging										
Inburgeringsportaal		X								
EROW										
Onderhoud werkvoorraad									X	
Opvragen specifieke rapportages										X

Functie	**Afspraken over gebruik Suwinet-Inkijk**
Uivoeringsorganisatie BBS	**Hoofdtaken**
Medewerker uitkeringsadministratie	• Afhandeling van de maandelijkse signalen Inlichtingen Bureau (IB) • controle van opgave van inkomsten bij uitkeringsverwerking • Verwerken van uitkeringen, bijzondere bijstand en mutaties • Controle van de ingevulde gegevens op het wijzigingsformulier. • Beheer van het debiteurenbestand • Overige beoordelingen om het werk goed uit te kunnen voeren.
Klantregisseur	• Voert intakegesprekken • Aanvragen PW, IOAW, IOAZ, Bijzondere Bijstand en Bbz-uitkering • Voert regie op de klant en de producten die zijn ingezet • Overige beoordelingen die via een mutatieformulier binnenkomen.
Klantregisseur plus (speciale doelgroepen)	• Beoordelen doelgroepenregister, loonkostensubsidie en loonwaardebepaling voor uitkeringsgerechtigden en niet uitkeringsgerechtigden
Klantmanager inkomen	• Aanvragen PW, IOAW, IOAZ, Bijzondere bijstand en BBZ-uitkering • Heronderzoeken rechtmatigheid • Inburgeringportal raadplegen • Overige beoordelingen die via een mutatieformulier binnenkomen. • Overige beoordelingen om het werk goed uit te kunnen voeren.
Klantmanager werk	• Activeren en re-integreren van klanten
Medewerker terugvordering en verhaal	• Debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen en/of werkgever • Terugvorderingen en verhaal

Fraudecontroleur	• Onderzoek rechtmatigheid • Onderzoekt signalen en tips • Handhaving
Applicatiebeheerder	• Beheren van het toepassingsbereik (tot welk niveau kan de autorisatie verleend worden) van de Suwinet webapplicatie • Verlenen van aanmeldaccounts volgens de richtlijnen en verwijderd de accounts bij vervallen van de functie • (de)blokkeren accounts • Melden beveiligingsincidenten • Verzorgt de maandelijkse upload van data aan het systeem (gemeente als dataleverancier) • Ondersteuning bij gebruikersvragen. • Uploaden gegevens t.b.v. de whitelist
Security-officer	• Rapporteert aan het managementteam over de logins • Rapporteert aan het managementteam over het gebruik. • Attendeert de medewerkers op zorgvuldig gebruik Suwinet. • Vraagt detail rapportages op, indien er vermoeden bestaat van onrechtmatig gebruik. • Maakt het beveiligingsplan, evalueert en rapporteert aan het managementteam hierover.