

Beveiligingsplan Suwinet gemeente Bunschoten 2016

1. Inleiding

De gemeente Bunschoten heeft 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 BBS Werk en Inkomen één van die ketens. Ketentpartners 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 gegevensuitvraag (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 onder andere 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.

Aanvullend wordt Suwinet gebruikt binnen de gemeente Soest bij de afdeling financiën bij het uitvoeren van de taken in het kader van de WOZ belasting.

Om de Suwi keten effectief te laten functioneren moeten partijen erop kunnen vertrouwen dat 'hun' gegevens door de partners in de Suwi-keten 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 ketentpartners is dit met beveiligingsvoorschriften uitgewerkt in artikel 6.4 en bijlage 1 van de regeling Suwi. Dit betekent dat bevoegde gebruikers van Suwinet over nogal wat privacygevoelige informatie van cliënten kunnen beschikken. Daarnaast neemt het aantal bronnen waarvan Suwinet gebruik kan maken alleen maar toe. Naast de Rijksdienst voor het Wegverkeer (RDW), Sociale Verzekeringsbank (SVB), UWV en de Dienst Uitvoering Onderwijs (DUO) is ook de Belastingdienst aangesloten op Suwinet.

Als gevolg van de Regeling Suwi is elke gemeente verplicht te beschikken over een actueel informatiebeveiligingsplan. In de Wet Bescherming Persoonsgegevens (WBP) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan. Ook staat hierin welke beveiligingsmaatregelen er moeten worden getroffen. Er zijn dus genoeg redenen om met regelmaat het Beveiligingsplan Suwinet voor BBS Werk en Inkomen te actualiseren.

Het Beveiligingsplan is geen statisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisaties en de omgeving BBS Werk en Inkomen zijn voortdurend in ontwikkeling, onder andere door gewijzigde of vernieuwende inzichten en wetgeving of aanpassingen in de informatiesystemen. Dat betekent dat dit plan periodiek moet worden beoordeeld op actualiteit en dus mogelijk constante aanpassing behoeft.

Dit beveiligingsplan heeft veel raakvlakken met het algemene beveiligingsbeleid waarvoor wij als gemeente Bunschoten aanhaken bij het beleid vanuit Soest. Daarom moet dit plan in samenhang met het stuk 'Informatiebeveiligingsbeleid 1.0' van de gemeente Soest gelezen worden. Wat niet specifiek in het beveiligingsplan is geregeld, valt onder het algemene informatiebeveiligingsbeleid.

2. Verdeling verantwoordelijkheden

De directeur BBS Werk en Inkomen is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk. Zij geeft aan de gebruikersbeheerder van Suwinet aan wie en met welke rol krijgt tot Suwinet-inkijk. De gebruikersbeheerder geeft hierna het gebruik voor de medewerker vrij.

2.1 Security-officer

De functie van security-officer is voor BBS Werk en inkomen bij een specifieke medewerker bedrijfsvoering/vakspecialist A neergelegd. Gekozen is voor deze, ten opzichte van het vorige beveiligingsplan

gewijzigde opzet, om te voorkomen dat er bij eventuele geconstateerde onrechtmatigheden een zorgvuldige afweging van de belangen van de betrokken medewerker kan plaatsvinden¹. Daarmee krijgt de monitoring van de beveiliging van Suwinet een stevige permanente basis in het uitvoeringsproces.

De security-officer ziet toe op een correcte beveiliging van Suwinet. Hij is in zijn 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 hij voor het beleid daarop aan te passen en ziet toe op juiste implementatie van de wijzigingen.

Taken voor 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 omtrent 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.

3. Taken en verantwoordelijkheden

3.1 Rechten voor medewerkers algemeen

Er is een aantal functies binnen BBS Werk en Inkomen die geautoriseerd zijn om gebruik te maken van Suwinet-inkijk. Het gaat om de volgende functies:

- Applicatiebeheerder
- Klantregisseur
- Klantmanager inkomen
- Klantmanager werk
- Juridisch medewerker
- Uitkeringsadministratie

Taken van de applicatiebeheerder:

- Gebruikers Suwinet-inkijk (functie raadplegen) autoriseren voor toegang;
- Operationeel houden van de applicatie.

Bij afwezigheid neemt de vervanger van de applicatiebeheerder deze taken over.

De autorisatie rollen voor gebruikers zijn vormgegeven in zogenaamde stapelbare autorisaties waarbij aan een gebruiker meerdere autorisaties kunnen worden toegewezen. Met deze stapelbare autorisaties is BBS Werk en Inkomen zelf in staat per functionaris te bepalen welke informatie te raadplegen is voor welke taken (zie bijlage).

Het doel is te borgen dat het gebruik van de gegevens binnen Suwinet-inkijk plaatsvindt binnen de wettelijke kaders en overeenkomstig de doelen die de organisatie hiertoe heeft geformuleerd

Functie	Taken/verantwoordelijkheden
BBS Werk en Inkomen	
Klantregisseur	• Raadplegen Suwinet-inkijk, conform de rol klantregisseur
Klantmanager inkomen	• Raadplegen Suwinet-inkijk, conform de rol inkomensconsulent
Klantmanager werk	• Raadplegen Suwinet-inkijk, conform de rol werkconsulent
Juridisch medewerker	• Raadplegen Suwinet-inkijk conform de rol juridisch medewerker
Uitkeringsadministratie	• Raadplegen Suwinet-inkijk conform de rol uitkeringsadministratie
Applicatiebeheer	• Beheer van Suwinet / gebruikersondersteuning
Inburgering	• Raadplegen Suwinet-inkijk conform de taken m.b.t. inburgering
Security Officer	• Periodieke (per kwartaal) controle login gegevens. • Periodieke (per half jaar) rapportage omtrent controle login en gebruik Suwinet • Jaarlijkse controle beveiligingsplan op actualiteit en volledigheid. • Verantwoording afleggen over beveiliging

1) In de vorige beveiligingsnota was deze rol toebedeeld aan de directeur van BBS. De directeur is uiteindelijk ook eindverantwoordelijk voor het HR proces, waarbij het wenselijk is dat dit gescheiden is. E.e.a. gekoppeld dat een uitvoerende rol in de organisatie belegd moet worden.

4. Gebruik Suwinet-inkijk

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie. In het onderstaand overzicht volgt per functie in welke gevallen Suwinet-inkijk gebruikt mag worden. We spreken in die gevallen van geoorloofd gebruik. Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

Functie	Afspraken over gebruik Suwinet-Inkijk
BBS Werk en Inkomen Medewerker uitkeringsadministratie	<ul style="list-style-type: none"> • Afhandeling van de maandelijkse signalen Inlichtingen Bureau (IB) • controle van opgave van inkomsten bij uitkeringsverwerking • Controle van de ingevulde gegevens op het wijzigingsformulier. • Beheer van het debiteurenbestand • Overige beoordelingen om het werk goed uit te kunnen voeren. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in een rapportage
Inburgering	<ul style="list-style-type: none"> • Via de inburgeringsportal raadplegen Informatiesysteem Inburgering (ISI) en bestand potentiële inburgeringsplichtigen (BPI)
Klantregisseur, Inkomensconsulent, werkconsulent, uitkeringsadministratie en Juridisch medewerker	<ul style="list-style-type: none"> • Aanvragen PW, IOAW, IOAZ, Bijzondere Bijstand en Bbz-uitkering • Heronderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken) • Debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen en/of werkgever • Overige beoordelingen die via een mutatieformulier binnenkomen. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage
Applicatiebeheerder	<ul style="list-style-type: none"> • 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 • Melden beveiligingsincidenten • Verzorgt de maandelijkse upload van data aan het systeem (gemeente als dataleverancier) • Ondersteuning bij gebruikersvragen.
Security-officer	<ul style="list-style-type: none"> • 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.

Logging rapportages en controle op gebruik

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld over de logging van het gebruik van Suwinet-inkijk. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-inkijk per medewerker van o.a. de gemeente kan worden nagegaan. De volgende gegevens worden gelogd:

- Het tijdstip van iedere log-in en log-out en andere actie;
- De gebruikersnaam van degene die inlogt/uitlogt;
- Elk burgerservicenummer (BSN) of een andere zoek sleutel, waarvan gegevens worden opgevraagd wordt als actie geregistreerd;
- elke actie, zoals de bekeken kolom- of overzichtspagina's.

Het doel van deze logging is tweeledig:

1. Tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking;
2. Wetenschappelijke en/of statistische doeleinden.

De gebruikers van Suwinet-inkijk moeten weten dat over hen gegevens worden verzameld en vastgelegd. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Met het oog hierop moet de navolgende informatie worden verstrekt aan de medewerkers die (gaan) werken met Suwinet-inkijk:

- Het bestaan van de logging-applicatie;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd;
- Doelen van de logging;
- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doeloverschrijdend gebruik van het Suwinet-inkijk wordt geconstateerd.
- Dat bij bovenstaande constatering de directeur van Werk en Inkomen de betreffende medewerker(s) daarop aanspreekt.

- Dat ten aanzien van privacyaspecten in het algemeen, de zorgvuldigheid in de omgang met gegevens en vertrouwelijkheid van gegevens, regels bestaan die dienen te worden nageleefd (bijlage 1).
- Dat ten aanzien van inzageverzoeken van uitkeringsgerechtigden van de in Suwinet geregistreerde gegevens een protocol bestaat dat gevolgd moet worden (bijlage 2).

Controle van het beveiligingsplan Suwinet kan uitgevraagd worden t.b.v. de managementrapportages en het jaarlijkse accountantsverslag. Het betreft de volgende gegevens: inijkacties; opvragingen unieke burgerservicenummer; geldige ten opzichte van ongeldige rollen; inlogpogingen; administrator accounts; accounts per status; opvragingen per pagina; geregistreerde ten opzichte van actieve accounts.

De logginggegevens worden door de security-officer beoordeeld en gerapporteerd aan de directeur, die de desbetreffende medewerker(s) bij ongeoorloofd gebruik daarop aanspreekt en gepaste maatregelen neemt.

5. Tien gouden regels bij beveiliging van persoonsgegevens

Regels bij beveiliging van persoonsgegevens in relatie tot verkregen Suwi gegevens Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Concreet kunnen deze regels in relatie tot de SUWI wetgeving als volgt worden vertaald:

1. Beheren van wachtwoorden

De gebruiker moet het door de administrator uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord iedere keer na 32 dagen (is standaard ingesteld vanuit de applicatie).

De gebruiker heeft dus het eigen beheer over het wachtwoord.

Zodra een medewerker de gemeente verlaat, wordt het aanmeldaccount voor Suwinet voor deze persoon verwijderd door de applicatiebeheerder.

2. Melden van beveiligingsincidenten

Het is belangrijk dat eventuele beveiligingsincidenten binnen Suwinet worden gemeld bij de applicatiebeheerder. Algemene beveiligingsincidenten worden gemeld bij de functionaris genoemd in het informatiebeveiligingsplan van de gemeente Soest.

Voorbeelden van dergelijke incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

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

4. Gedragscode internetgebruik

Onze dienst heeft een protocol voor gebruik van internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van internet wordt geobserveerd. Het protocol is voor medewerkers te raadplegen op het gemeentelijke Intranet.

5. Kennisnemen van het informatiebeveiligingsbeleid van BBS zowel als van het centrale informatiebeveiligingsbeleid

Het binnen BBS Werk en Inkomen geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is op iedereen binnen de afdelingen van toepassing die gebruik maakt van Suwinet-Inkijk. Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. In het beveiligingsplan is hier uitgebreid aandacht aan besteed.

Jaarlijks, bij de evaluatie van dit beveiligingsplan, wordt dit onderwerp ook geagendeerd voor de teamoverleggen van BBS.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen.

Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben.

In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging.

7. Clear desk en clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven.

Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat het workstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat na een paar minuten de schermbeveiliging intreedt. Dit is voor iedere medewerker standaard ingesteld.

8. Geen vertrouwelijke gegevens in de prullenbak

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen BBS Werk en Inkomen en de gemeente Bunschoten. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. De vertrouwelijke gegevens die moeten worden vernietigd worden regelmatig aangeleverd bij het vernietigingsbedrijf.

9. Aanspreken van onbekende personen

In het geval dat een medewerker een voor hem/haar onbekende persoon op de afdeling tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet.

10. De dagelijkse werkzaamheden t.a.v. informatiebeveiliging

Informatiebeveiliging is uitermate belangrijk voor het werk binnen BBS Werk en Inkomen en de gemeente Bunschoten waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook klanten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom middels de interne overleggen geregeld aandacht aan dit onderwerp wordt besteed.

Het nieuwe werken, flexibel werken

Binnen BBS Werk en Inkomen is het van essentieel belang om op een correcte wijze om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Tevens is dit een belangrijk aandachtspunt voor het thuiswerken. Specifiek voor het thuiswerken zijn er interne richtlijnen. Hierin staat onder andere dat we in het oog van de privacy gevoelige informatie goed moeten blijven beveiligen. Dit betekent geen dossiers mee naar huis en geen Suwinet raadplegen thuis.

BIJLAGEN

Bijlage 1 Inwerkprogrammamedewerkers

Inwerkprogramma Werk en Inkomen Baarn Bunschoten Soest

Naam nieuwe medewerker/stagiair/inhuur*

Functie:

Afdeling:

1e werkdag op:

Activiteiten

Wie/paraaf

Wanneer

Uitgevoerd dd.

* Voor stagiairs wordt dit programma doorlopen voor zover van toepassing

Vorbereiding vooraf aan de 1^e 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

Management-assistent

Autorisatie computer en aanvragen email account via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht

LG

Regelen toegangsbadge via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht

LG

Aanmelden tijdregistratie via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht

LG

Aanmelden telefoonlijst via afdeling Bedrijfsvoering d.m.v. indiensttredingbericht

LG

Mentor aanstellen

LG

Introductie- en inwerkprogramma samenstellen, gericht op functie

LG/mentor

• Inwerken binnen het team, incl. PC-programma's en toepassing

• Roostert meelopen in verschillende werkeenheden

Bestellen welkomstboek en aanbieden op de eerste werkdag

LG

Autorisatie applicaties:

Rol binnen de applicaties:

Inkomensconsulent / Juridisch kwaliteit / uitkeringsadministratie / werkconsulent / WMO consulent / administratie WMO

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

Competensys ja / nee

Stekker 4 / erow ja / nee

CAK ja / nee

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

Informatie geven over de afdeling, de producten, de werkverdeling, de functie, de organisatie en de burgers

LG

Geheimhoudingsverklaring (o.a. Suwi en BRP) laten tekenen; doorzenden aan afd. Bedrijfsvoering HRM gem. Bunschoten. Kopie eigen dossier

Management assistent

Dienst- en afdelingsinformatie (gedoseerd):

LG

o Overlegstructuur

o Taakverdeling afdeling

o Rechten / plichten in het kader van gegevensgebruik en gegevenshuishouding (Suwi, BRP, Stekker4)

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 en het bedrijfsblad 'Signalen'	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, dienstdiensen 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 en chippen	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		
Foto maken voor het personeelsinformatiesysteem	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 2 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, BRP 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 WvSr) 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.
- 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 3 Autorisaties in Suwinet, algemeen overzicht

		Klantregis- seur	Inkomens consulent	Werk consu- lent	Juridisch medewer- ker	Uitkerings administratie	Applicatie beheer	Inburge- ring
1	Alle bevoegdheden incl signa- len						✓	✓
2	Bedrijvenregister	✓	✓		✓	✓	✓	
3	Beheer WW & Blokkeren							
4	Belastingdienst	✓	✓		✓	✓	✓	
5	Bijstandsregelingen	✓	✓	✓	✓	✓	✓	
6	Correctieservice						✓	
7	Downloaden Rapportages							
8	Fraude scorekaart						✓	
9	Fraude vorderingen	✓	✓		✓	✓	✓	
10	BRP	✓	✓		✓	✓	✓	
11	BRP volledig							
12	Gebruikersadministratie						✓	
13	GSD voor IB groep			✓				
14	Kadaster	✓	✓		✓	✓	✓	
15	Klant algemeen							
16	Klant algemeen +	✓	✓	✓	✓	✓	✓	
17	Klantbeeld	✓	✓	✓	✓	✓	✓	
18	Kostendelerstoets	✓	✓		✓	✓	✓	
19	Onderhouden correctieservice						✓	
20	Onderhouden status wijzigings- verzoeken						✓	
21	Opvragen gebruiksrapportages						✓	
22	Raadplegen ISI op BSN						✓	✓
23	Raadplegen ISI op BSN of selec- tie						✓	✓
24	RDW						✓	
25	RDW+						✓	
26	RDW peildata	✓	✓		✓	✓	✓	
27	SBR Query							
28	SCI			✓				
29	UWVWB	✓	✓	✓	✓	✓	✓	
30	VIS	✓	✓		✓	✓	✓	
31	WIS-Proxy			✓				
32	www.werk.nl	✓	✓	✓	✓	✓	✓	