Beveiligingsplan
Suwinet
Gemeente Oegstgeest

Maart 2016

Inhoudsopgave

1. Inleiding

Het Bureau Keteninformatisering Werk en Inkomen (BKWI), de stichting Inlichtingenbureau Gemeenten(IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur. Met de faciliteit Suwinet zijn gegevens op basis van Burgerservicenummers toegankelijk gemaakt voor bevoegde medewerkers. Het gaat om privacygevoelige gegevens, zoals arbeidsverleden, loon, uitkeringen, kentekenregistraties en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. De organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Om de Suwi-keten effectief te laten functioneren, moeten partijen er op kunnen vertrouwen dat “hun” gegevens door de partners in de 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 Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi. Ook in de Wet Bescherming Persoonsgegevens (WBP) is uitgebreid geregeld hoe met persoonsgegevens moet worden omgegaan, voor welke doeleinden ze mogen worden verzameld, op welke wijze ze mogen worden verwerkt en welke beveiligingsmaatregelen moeten worden getroffen.

1.1 Kader

Oegstgeest maakt sinds 1 januari 2012 deel uit van de Gemeenschappelijke Regeling Servicepunt71 (SP71), samen met de gemeenten Leiden, Leiderdorp en Zoeterwoude. In deze regeling zijn ICT, HRM, Financiën, Juridische Zaken en Inkoop ondergebracht. Oegstgeest maakt hier gebruik van.
In maart 2013 is het Statuut Informatiebeveiliging voor de gemeenten Oegstgeest, Leiden, Leiderdorp, Zoeterwoude en Servicepunt71 vastgesteld. Hierin worden uitgangspunten benoemd met betrekking tot de organisatie van informatieveiligheid en enkele beleidsuitgangspunten met betrekking tot informatieveiligheid.

Het normenkader NEN-ISO/IEC 27002 wordt als uitgangspunt gehanteerd, deze 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO-IEC 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid. Ook wordt gesteld dat de organisatie en de beveiligingsmaatregelen behoren te voldoen aan de wettelijke eisen en audits vanuit het Rijk.

De doelstelling van het Statuut luidt als volgt:
"Het bieden van een gezamenlijk raamwerk van beleidsuitgangspunten met betrekking tot de exclusiviteit, integriteit en beschikbaarheid van de (geautomatiseerde) informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt op basis van NEN-ISO/IEC 27002, teneinde de (geautomatiseerde) informatievoorziening te beschermen tegen interne en externe bedreigingen."

In mei 2013 is de Baseline informatiebeveiliging Nederlandse gemeenten (BIG) ontwikkeld door VNG en KING. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de

veiligheid van informatie binnen gemeentelijke organisaties. Bij het buitengewone VNG ledencongres (29 november 2013) is door de leden een resolutie aangenomen die van de gemeenten vraagt informatieveiligheid bestuurlijk en organisatorisch te borgen, de Baseline Informatiebeveiliging voor Nederlandse Gemeenten als standaard te hanteren en informatieveiligheid transparant te maken voor burgers, bedrijven en ketenpartners. Deze Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor de gemeenten.

De gemeente Oegstgeest hanteert deze nieuwe gemeente standaard (BIG) als uitgangspunt bij de inrichting van de gemeentebrede informatieveiligheid. De ambitie is om in 2016 één gezamenlijk gemeentebreed informatieveiligheidsbeleid vast te stellen voor de gemeenten Oegstgeest, Leiden, Oegstgeest, Zoeterwoude en Servicepunt71, op basis van deze Baseline.

Dit Beveiligingsplan Suwinet Gemeente Oegstgeest dient in samenhang met bovengenoemde te worden gelezen. Wat niet specifiek in dit plan is geregeld, valt onder het Statuut Informatiebeveiliging.

1.2 Vaststelling

Het Statuut Informatiebeveiliging is op 2 juli 2013 door het College van Burgemeester en Wethouders van de gemeente Oegstgeest vastgesteld.

Dit Beveiligingsplan Suwinet is op 1 maart 2016 door het College van Burgemeester en Wethouders van de gemeente Oegstgeest vastgesteld. Vervolgens is het op 8 maart 2016 goedgekeurd door de ondernemingsraad.

2. Gebruikers van Suwinet

2.1 Rollen en taken

In onderstaande tabel is weergegeven welke functies binnen de gemeente Oegstgeest geautoriseerd zijn om Suwinet te raadplegen of anderszins een taak hebben rond (de beveiliging van) Suwinet.

Functie	**Taak**
Consulent Werk en Inkomen	Raadplegen klantgegevens Suwinet
Medewerker uitkeringsadministratie	Raadplegen klantgegevens Suwinet
Medewerker verhaal en terugvordering	Raadplegen klantgegevens Suwinet
Teammanager Maatschappij	Verantwoordelijk voor gebruik en beveiliging Suwinet + aanvragen autorisaties
Security Officer Suwi	Controle en kwaliteitsborging + beheer en onderhoud beveiligingsplan → rapporteren aan Directeur Dienstverlening
Functioneel beheerder	Verstrekken autorisaties
Directeur Dienstverlening	Eindverantwoordelijk voor gebruik en beveiliging Suwinet

Voor de functies die geautoriseerd zijn om Suwinet te raadplegen, wordt hieronder per functie aangegeven wanneer zij dit mogen (= geoorloofd gebruik). Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is in principe sprake van ongeoorloofd gebruik.

- Consulenten Werk en Inkomen mogen raadplegen bij het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen en bij rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Pw, Ioaw, Ioaz, Bbz of een andere door de afdeling uitgevoerde regeling betreft.
- Medewerkers van de uitkeringsadministratie mogen Suwinet raadplegen bij:
  - afhandeling van de maandelijkse signalen Inlichtingen Bureau (IB)
  - controle van opgave van inkomsten bij uitkeringsverwerking
  - het beheer van het debiteurenbestand.
- De medewerker die verantwoordelijk is voor terugvordering en verhaal mag raadplegen bij onderzoeken die samenhangen met verhaal op onderhoudsplichtigen of vorderingen. Dit bijvoorbeeld ter vaststelling van woonplaats, draagkracht, inkomen of werkgever.

Raadplegen van Suwinet in andere situaties wordt gemotiveerd vastgelegd; een afschrift van de Suwinet-raadpleging met daarop aangegeven wanneer en waarom is geraadpleegd, wordt toegevoegd aan het dossier van de klant. Hierdoor kunnen raadplegingen achteraf indien nodig verantwoord worden aan de Security Officer Suwi en/of de Teammanager Maatschappij. Dit geldt ook voor het opzoeken van een BSN dat onbekend is in Civision SamenlevingsZaken in verband met een rechtmatigheids- en/of fraudeonderzoek. Het

afschrift wordt dan bewaard in het dossier van de klant in relatie tot wie de raadpleging heeft plaatsgevonden.

2.2 Autorisatie

Het gebruik van Suwinet is voorbehouden aan medewerkers van Team Maatschappij die werkzaam zijn op het gebied van Werk en Inkomen. De autorisaties voor Suwinet zijn op basis van functieprofiel toegekend en vastgelegd in een autorisatiematrix (zie bijlage 1). De autorisatiematrix is ook beschikbaar op persoonsniveau.

De wijze waarop de autorisaties worden toegekend, gewijzigd of ingetrokken is nader geregeld in de "Procedure autorisaties" (zie bijlage 2).

2.3 Beveiligingseisen gebruikers

Vast personeel
Binnen Team Maatschappij wordt met persoonsgegevens gewerkt. Voor het werken en de omgang met persoonsgegevens heeft de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). In de wet SUWI zijn geheimhoudingsbepalingen opgenomen, waarin bepaald is dat dat de persoonsgegevens niet verder bekend gemaakt mogen worden dan voor de uitoefening van de functie noodzakelijk is. Bovendien wordt in artikel 125a van de Ambtenarenwet geheimhouding opgelegd aan ambtenaren.

Nieuwe medewerkers moeten een Verklaring Omtrent Gedrag (VOG) overleggen voordat ze definitief worden benoemd. Daarnaast wordt na benoeming de *ambtseed* afgelegd.

Zowel in de ambtseed als in de *Gedragscode bestuurlijke integriteit ambtenaren* is de geheimhoudingsplicht en het zorgvuldig omgaan met informatie gemeentebreed geregeld. Deze regelingen zijn van toepassing op het personeel dat in dienst is van de gemeente Oegstgeest.

De medewerkers met een autorisatie voor Suwinet moeten daarnaast ook een Zorgvuldigheidsverklaring Suwinet (zie bijlage 3) ondertekenen.

Extern personeel
Het gaat hier om mensen die bijvoorbeeld via een uitzend- of detacheringsbureau voor een bepaalde periode worden ingehuurd. Deze ingehuurde mensen werken onder gezag en toezicht van de gemeente Oegstgeest.

Extern personeel moet een *Geheimhoudingsverklaring* ondertekenen. Deze verklaring wordt ondertekend op de eerste werkdag. Verder moet extern personeel dat een autorisatie krijgt voor Suwinet ook de zorgvuldigheidsverklaring ondertekenen.

Bewustwording medewerkers
Aan alle medewerkers van Team Maatschappij alsook de externe medewerkers die gebruik maken van Suwinet is het Beveiligingsplan Suwinet Oegstgeest digitaal beschikbaar gemaakt en mondeling toegelicht. Gebruikers van Suwinet moeten weten dat over hen gegevens worden vastgelegd en verzameld (**logging**). Van deze loggegevens worden geanonimiseerde rapporten opgesteld door het BKWI. Deze rapportages worden beschikbaar gesteld aan de betreffende ketenpartners. Aan de hand hiervan wordt gecontroleerd op het gebruik van Suwinet (zie hoofdstuk 4) en wordt geprobeerd een goed beeld te krijgen van de wijze waarop Suwinet door de medewerkers wordt geraadpleegd.

De volgende gegevens worden gelogd:

- datum en tijdstip van iedere log-in en log-out en andere actie;
- de gebruikersnaam van degene die inlogt/uitlogt;
- elk bsn-nummer (of andere zoeksleutel) 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.

Zoals gezegd is het belangrijk dat gebruikers van Suwinet 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 wordt in de Zorgvuldigheidsverklaring Suwinet onder andere de volgende informatie verstrekt aan de medewerkers die (gaan) werken met Suwinet:

- Het bestaan van de logging;
- De (aard van de) gegevens die worden verzameld;
- Doelen van de logging;
- Het gebruik van de gelogde gegevens; deze worden niet voor andere doeleinden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze, het moment waarop en door wie een onrechtmatig of doeloverschrijdend gebruik van Suwinet geconstateerd kan worden;
- Dat bij bovenstaande constatering de Teammanager Maatschappij hierover ingelicht wordt en contact opneemt met de betreffende medewerker(s);
- Op basis van de zwaarte van de overtreding bepaalt de Teammanager Maatschappij in overleg met de Directeur Dienstverlening wat de consequenties zijn. Dit kan variëren van een schriftelijke waarschuwing tot ontslag.

3. Communicatie

Communicatie over informatieveiligheid en het gebruik van Suwinet in het bijzonder kan plaatsvinden in drie situaties:

- Als onderwerp op het periodieke werkoverleg;
- Bij individuele gesprekken;
- Bij informatieverstrekking om het bewustzijn (ten aanzien van informatieveiligheid en het gebruik van Suwinet) van het eigen personeel te verhogen.

De verantwoordelijkheid voor de communicatie ligt bij de Teammanager Maatschappij.
De Security Officer Suwi zorgt ervoor dat nieuwe ontwikkelingen bij de Teammanager Maatschappij bekend worden gemaakt; zij stemmen samen af hoe deze informatie aan de medewerkers doorgegeven wordt.

Periodiek werkoverleg
Het onderwerp wordt op initiatief van de leidinggevende, eventueel op verzoek van een van de medewerkers of de Security Officer Suwi, op de agenda geplaatst. Dit gebeurt tenminste twee maal per jaar. De verslaglegging van de onderwerpen welke zijn besproken tijdens het werkoverleg wordt toegezonden aan en bewaard door de Security Officer Suwi.

Individuele gesprekken
Wanneer daar aanleiding toe is kan de Teammanager Maatschappij het onderwerp in een individueel gesprek met een medewerker bespreken.

4. Controle

4.1 Periodieke controle

Het Bureau Keteninformatisering BKWI stelt (anonieme) rapportages op over de logging van het gebruik van Suwinet. Deze rapportages worden beschikbaar gesteld aan de betreffende ketenpartners en bevatten de volgende gegevens:

- Inkijkacties;
- Opvragingen unieke bsn-nummers;
- Geldige ten opzichte van ongeldige rollen;
- Inlogpogingen;
- Administrator accounts;
- Accounts per status;
- Opvragingen per pagina;
- Geregistreerde ten opzichte van actieve accounts.

De rapportages worden door de Security Officer Suwi opgevraagd en beoordeeld. Aan de hand hiervan wordt gecontroleerd op het gebruik van Suwinet en wordt geprobeerd een goed beeld te krijgen van de wijze waarop Suwinet door de medewerkers wordt geraadpleegd. Dit gebeurt aan de hand van een aantal indicatoren en bijbehorende criteria (zie bijlage 4).

De stappen op hoofdlijnen zijn als volgt;

1. Opvragen van de gebruikersrapportage.
   De Security Officer Suwi haalt 1 keer per kwartaal de gebruikersrapportage op uit Suwinet. Eén exemplaar wordt aan de functioneel beheerder gegeven voor de uitvoering van de accountscontrole.
2. Uitvoeren vergelijk geraadpleegde BSN nummers versus cliëntenbestand Oegstgeest.
   De Security Officer Suwi vraagt 1 keer per kwartaal een overzicht aan van alle geraadpleegde BSN nummers bij BWKI. Deze worden vergeleken met het actieve cliëntenbestand van Oegstgeest.
3. Opvragen van de specifieke rapportage.
   De Security Officer Suwi vraagt in het kader van een steekproef twee keer per jaar een specifieke rapportage op bij BKWI.
4. Analyse van de gebruikersrapportage en trekken van conclusies.
   De analyse van tabellen door de Security Officer Suwi leidt tot conclusies over het algemeen gebruik van Suwinet, de zorgvuldigheid, de efficiënte inzet van Suwinet en de actualiteit en proportionaliteit van het accountbeheer. De bevindingen worden kort door de Security Officer Suwi gerapporteerd aan de Directeur Dienstverlening. Deze is eindverantwoordelijke hiervoor.
5. Bij twijfel over zorgvuldigheid: vervolgstappen.
   Zijn er op basis van de rapportages twijfels over het zorgvuldig gebruik dan zijn er verschillende vervolgstappen mogelijk. Allereerst kan de rapportage worden besproken met de Teammanager Maatschappij om meer inzicht te krijgen in de achtergrond van bijvoorbeeld een afwijkend patroon. Zijn er geen voldoende verklaringen, dan kan een specifieke rapportage worden opgevraagd bij BKWI, waarin het raadpleeggedrag op persoonsniveau wordt getoond. Het opvragen van een specifieke rapportage kan alleen door een daartoe gemandateerde functionaris (Teammanager Maatschappij en Security Officer Suwi). Zij kunnen BKWI daarbij om hun interpretatie vragen.
6. Analyse specifieke rapportage: vervolgstappen.
   De specifieke rapportages worden geanalyseerd. Blijkt er een afwijkend patroon bij een medewerker, dan gaat de Teammanager Maatschappij of de Security Officer Suwi

(gemandateerd door de Teammanager Maatschappij) een gesprek aan om naar de achtergronden daarvan te vragen. Hier wordt een verslag van gemaakt. Bij aanwijzingen voor norm overschrijdend gedrag wordt de zaak overgedragen aan het organisatie onderdeel dat het integriteitsbeleid uitvoert.

7. Overdracht: start procedure integriteitsbeleid.

Autorisaties

De Security Officer Suwi controleert twee keer per jaar de actualiteit en rechtmatigheid van de ingevoerde autorisaties. De wijze van controleren is opgenomen in de Procedure Autorisaties (zie bijlage 2). Eén keer per jaar doet de Security Officer Suwi dit samen met de Senior adviseur Administratieve Organisatie/Interne Controle.

4.2 Specifieke rapportages n.a.v. incidentele of lokale gebeurtenissen

Het is bekend dat personen die landelijk de publiciteit halen aanleiding zijn voor medewerkers om gegevens op te zoeken in Suwinet. Denk aan voetballers (rond EK's en WK's), Bekende Nederlanders (BN-ers), personen die vanwege misdrijven in de pers komen. Maar ook personen die lokaal in de belangstelling staan zijn wel eens aanleiding voor medewerkers om persoonsgegevens op te zoeken. Denk aan politieke figuren in verkiezingstijd, nieuwe collegeleden of iemand anders die de lokale pers heeft gehaald. Er kan bij het BKWI worden gevraagd om voor Oegstgeest een rapportage op te stellen om te achterhalen of specifieke personen (- niet-cliënten) worden geraadpleegd. BKWI kan worden gevraagd om een interpretatie van de uitkomsten van deze specifieke rapportage. Dit kan helpen bij de analyse binnen Oegstgeest, er kunnen echter geen rechten aan ontleend worden.

5. Evaluatie en actualisatie

Het maken en vaststellen van een beveiligingsplan is nog geen garantie voor een goede werking in de praktijk. Daarom dient het beveiligingsplan regulier geëvalueerd en zo nodig geactualiseerd te worden. Dit valt onder de verantwoordelijkheid van de Security Officer Suwi. Evaluatie vindt jaarlijks plaats door na te gaan of het beveiligingsplan nog steeds aansluit op de organisatie, de actuele wetgeving en of de juiste maatregelen daarvoor getroffen zijn.

De Security Officer Suwi maakt van de jaarlijkse evaluatie een verslag, waarin is opgenomen welke punten worden aangepast. Ook als geen aanpassingen nodig bleken, wordt dit in het verslag aangegeven. De bevindingen van de periodieke/incidentele controles die het betreffende jaar hebben plaatsgevonden en eventuele andere bijzonderheden worden ook in het evaluatieverslag opgenomen.

Het evaluatieverslag wordt besproken en vastgesteld in het DT. De Teammanager Maatschappij bespreekt het evaluatieverslag ook in het periodiek werkoverleg.

Bijlage 1 Autorisatiestructuur

		Consulent Werk en inkomen	Uitkeringsadministratie	Terugvordering en verhaal	Teammanager Maatschappij	Security Officer	Functioneel beheerder
R1043	Belastingdienst	x	x	x			x
R1377	DPS Matrix : Case beheer						
R1379	DPS Matrix : Toevoegen						
R1272	Fraude vorderingen	x	x	x			x
G002	G002 B&O						
G003	G003 CWI	x	x	x			x
G004	G004 FSK	x	x	x			x
G005	G005 LRD op BSN						
G018	G018 LRD zoeken						
G019	G019 GSD						
G020	G020 RDW intake	x	x	x			x
G021	G021 RDW fraude			x			
G024	G024 SBR	x	x	x			x
G025	G025 VIS	x	x	x			x
G026	G026 werk.nl						
G029	G029 klantbeeld	x	x	x			x
G030	G030 LRD zoeken uitgebreid						
G031	G031 Correctieservice						
G032	G032 Configureren correctieservice						
G034	G034 Langdurigheidstoeslag						
G040	G040 Status Correctie						
G042	G042 Klant algemeen	x	x	x			x
Rxxxx	Rxxx Terugvordering						
Rxxxx	Rxxxx Handhaving						
G043	G043 Klant algemeen+	x	x	x			x
GSDADM	Gebruikersbeheerder						x
R678	Kadaster	x	x	x			x
R347	Opvragen gebruiksrapportages *				x	x	
R454	RDW peildata						
SC101	SCI01 Raadplegen BPI						
SC102	SCI02 Raadplegen ISI op BSN						
SC103	SCI03 Raadplegen ISI op BSN of selectie						
SC104	SCI04 Muteren BPI en ISI						
SC105	SCI05 Muteren ISI						
SC106	SCI06 Alle bevoegdheden incl signalen						
SC107	SCI07 Raadplegen BPI en ISI						

* Opvragen van specifieke rapportages is gemandateerd aan de personen die de functie van Teammanager Maatschappij en Security Officer vervullen.

Bijlage 2 Procedure autorisaties Suwinet

Inleiding
De procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet en de controle hierop.

De procedure bestaat uit twee afzonderlijke deelprocedures die apart worden uitgevoerd:
- Autorisaties tot Suwinet;
- Periodieke controle autorisaties.

Met een autorisatie wordt bedoeld het verstrekken van een gelegitimeerde toegang tot Suwinet. Wat betreft het verstrekken van autorisaties voor Suwinet is de functioneel beheerder het 'bevoegd gezag' hiervoor.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure, geborgd in dit beveiligingsplan, ligt te allen tijde bij het College van B&W. Het up-to-date houden van de procedure ligt bij de Security Officer Suwi.

De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet berust bij de Teammanager Maatschappij. De uitvoering hiervan ligt bij de functioneel beheerder.

Uitvoering autorisaties
Autorisatie tot Suwinet
- Autorisaties voor Suwinet worden per functie/taak toegekend;
- De Teammanager Maatschappij verzoekt de functioneel beheerder om de nieuwe medewerker toegang te verlenen tot Suwinet (inclusief gewenste autorisatieniveau) middels het formulier "Aanvraag autorisaties Suwinet";
- Bij tussentijdse wijzigingen in functie/taak verzoekt de Teammanager Maatschappij de functioneel beheerder het autorisatieniveau -voor zover van toepassing- te wijzigen of de toegekende autorisaties in te trekken. Bij vertrek van de medewerker worden de hem/haar toegekende autorisaties direct beëindigd. Hiervoor wordt het formulier "Intrekken of wijzigen autorisaties Suwinet" gebruikt;
- Na daadwerkelijke toekenning, wijziging of beëindiging tekent de functioneel beheerder het door de Teammanager Maatschappij aangeleverde formulier;
- De gebruiker krijgt van de functioneel beheerder een melding als de autorisaties zijn geregeld. Ook krijgt de nieuwe gebruiker een korte instructie over de wijze van aanmelden en het direct aanpassen van het wachtwoord;
- Suwinet is voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes;
- De wachtwoorden voor Suwinet zijn maximaal 90 dagen geldig.
- Als een gebruiker gedurende 90 dagen achtereen niet heeft ingelogd wordt het wachtwoord automatisch geblokkeerd;
- Na drie maal foutief inloggen wordt het account automatisch geblokkeerd. Alleen de functioneel beheerder kan het account weer vrijgeven;
- Het originele autorisatieformulier wordt door de functioneel beheerder gearchiveerd.

Periodieke controle autorisaties
De Security Officer Suwi controleert twee keer per jaar de actualiteit en rechtmatigheid van de ingevoerde autorisaties. De wijze van controleren is als volgt:

- De functioneel beheerder draait een lijst van gebruikers, gebruikersgroepen en ingevoerde autorisaties voor Suwinet uit;
- De Security Officer Suwi maakt een inventarisatie van de gebruikers, gebruikersgroepen en de toegekende autorisaties;
- Vervolgens controleert de Security Officer Suwi of het overzicht van de actieve gebruikers en de samenstelling van de gebruikersgroepen nog actueel zijn en of de bij die gebruikersgroepen behorende autorisaties (nog) juist zijn (conform bijlage 4, punten 3.1 t/m 3.3);
- Wanneer nodig doet de Security Officer Suwi een verzoek aan de Teammanager Maatschappij om de autorisatie(s), middels het formulier, te wijzigen ofwel in te trekken.

Formulier Aanvraag autorisaties Suwinet

Naam medewerker	
Team	
Functie	
Eventueel aanvullende autorisaties (anders dan bij de functie behorend)	
Autorisatie aangevraagd door Teammanager Maatschappij	Handtekening: Datum:
Gewenste autorisatie verstrekt door functioneel beheerder.	Handtekening: Datum:

Formulier Intrekken of wijzigen autorisaties Suwinet

Naam medewerker	
Team	
Functie	
Wijzigen of intrekken?	O wijzigen O intrekken
Reden intrekking/wijziging	
Wijzigingen in autorisatie aangevraagd door Teammanager Maatschappij	Handtekening: Datum:
Gewenste wijzigingen in autorisatie verwerkt door functioneel beheerder.	Handtekening: Datum:

Bijlage 3 Zorgvuldigheidsverklaring Suwinet Gemeente Oegstgeest

Zorgvuldigheidsverklaring Suwinet

Ondergetekende,

Naam: ----------

Functie: ----------

Team: ----------

Belooft/verklaart dat hij/zij:

- Er van op de hoogte is dat privacy wet- en regelgeving een zorgvuldige omgang met persoonsgegevens beoogt en dat deze wet- en regelgeving het gebruik van persoonsgegevens – in de ruimste zin van het woord – verbindt aan regels.
- Kennis heeft genomen van het Beveiligingsplan Suwinet Oegstgeest.
- Zorgvuldig zal omgaan met de (persoons)gegevens en de inhoud van de documenten die hij/zij bij de uitvoering van de werkzaamheden in Suwinet-verband mag inzien.
  Concreet betekent dit onder meer dat hij/zij:
  - niet meer of vaker (persoons)gegevens raadpleegt dan strikt noodzakelijk is;
  - enkel die (persoons)gegevens gebruikt, die van belang zijn voor het nastreven van het doel van Suwinet.
  - het raadplegen van Suwinet in andere dan bij de functie horende situaties gemotiveerd vastlegt; een afschrift van de Suwinet-raadpleging met daarop aangegeven wanneer en waarom is geraadpleegd, wordt toegevoegd aan het dossier van de klant.
  - bovenstaande ook doet voor het opzoeken van een BSN dat onbekend is in Civision Samenlevings Zaken in verband met een rechtmatigheids- en/of fraudeonderzoek (het afschrift wordt dan bewaard in het dossier van de klant in welk kader de raadpleging heeft plaatsgevonden).
  - (persoons)gegevens niet aan onbevoegden verstrekt;
  - het Suwinet-account (en wachtwoord) zorgvuldig hanteert en niet aan anderen ter beschikking stelt.
- Alle medewerking zal geven aan het naleven van de privacywet- en regelgeving.
- Gedurende de duur van zijn/haar inzet voor de werkzaamheden in Suwinet-verband en ook na beëindiging van deze werkzaamheden (tegenover derden) geheimhouding zal betrachten met betrekking tot alle (persoons)gegevens waarvan hij/zij bij de uitvoering van deze werkzaamheden kennis neemt.
- Bekend is met het feit dat er over hem/haar gegevens worden vastgelegd en verzameld (**logging**).

  Het gaat om de volgende gegevens:
  - datum en tijdstip van iedere log-in en log-out en andere actie;
  - de gebruikersnaam van degene die inlogt/uitlogt;
  - elk BSN (of andere zoeksleutel) 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.

Van deze loggegevens worden geanonimiseerde rapporten opgesteld door het BKWI, die door de Security Officer Suwi van de gemeente Oegstgeest opgevraagd en geanalyseerd worden.
Bij geconstateerde onregelmatigheden kan een specifieke rapportage (op gebruikersniveau) opgevraagd worden.

Door de Security Officer Suwi wordt verslag gedaan van de bevindingen bij de Teammanager Maatschappij. Bij onrechtmatig of doeloverschrijdend gebruik kan deze contact met de betreffende medewerker(s) opnemen. Afhankelijk van de zwaarte van de overtreding bepaalt de Teammanager Maatschappij in overleg met de Directeur Dienstverlening wat de consequenties zijn. Dit kan variëren van een schriftelijke waarschuwing tot ontslag.

Datum:

Handtekening medewerker:

Bijlage 4 Indicatoren analyse gebruikersrapportages Suwinet

Tabel	Signaal	Mogelijke vervolgactie
Hoofdstuk 1. Algemeen beeld gebruik Suwinet Inkijk.		
1.1: Totaal gebruik Deze tabel bevat het absoluut aantal raadplegingen (geraadpleegde pagina's) over de afgelopen zes maanden.	De trend is hier belangrijk. Een plotselinge stijging kan wijzen op: • extra uitgevoerde controles, • wetswijzigingen en herbeoordelingen, • plotselinge sterke stijging van aanvragen. Een plotselinge daling kan wijzen op: • vakantieperiode, • ziekte onder medewerkers, • wijziging in processen, bijvoorbeeld door invoering geautomatiseerde controles of afschaffen toetsing.	Indien er niet onmiddellijk een verklaring voor een afwijking in het patroon is, dan raadpleegt de Security Officer Suwi de Teammanager Maatschappij. Als ook afwijkende patronen in andere overige tabellen worden gevonden, dan kan een specifieke rapportage op medewerkersniveau worden opgevraagd bij het BKWI. Dat kan van alle accounts of van specifieke rollen.
Hoofdstuk 2 Zorgvuldig gebruik.		
2.1 Percentage raad-plegingen op zoeksleutel anders dan BSN. De norm is om op te vragen via de BSN. Specifieke functionarissen zijn geautoriseerd met een zogenaamde "zware rol". Zij kunnen ook buiten het BSN persoonsgegevens raadplegen, zoals op naam en geboortedatum, op kenteken.	Bij een plotselinge stijging is de vraag: • zijn er meer medewerkers geautoriseerd met deze zware rol? • zijn er specifieke handhavingscontroles uitgevoerd waarbij het BSN niet gebruikt kon worden? Bij een hoger percentage in vergelijking met andere gemeenten is de vraag: • zijn er niet teveel medewerkers geautoriseerd voor deze zware rol?	De vraag naar bijzondere handhavingsacties kan beantwoord worden door de Teammanager Maatschappij. De vraag over de juiste toewijzing van deze zware rollen kan aan de functioneel beheerder worden gesteld. Uit de autorisatiematrix kan worden geconcludeerd of de rollen juist zijn toegewezen. Indien daar geen verklaring uit valt af te leiden, wordt bij BKWI een specifieke rapportage opgevraagd voor de medewerkers die geautoriseerd zijn voor deze rollen.
2.2 Percentage raad-plegingen buiten kantoortijd, dat wil zeggen tussen 19.00 uur en 07.00 uur.	Een afwijkende trend kan wijzen op overwerk- en inhaalacties of een tijdelijke avondopenstelling. Voor raadplegingen buiten kantoortijden moet in alle gevallen naar een verklaring worden gezocht.	De Teammanager Maatschappij kan uitsluitsel geven over overwerk in de avonduren. Indien de verklaring niet afdoende is, wordt bij BKWI een specifieke rapportage opgevraagd.
2.3 Meest geraadpleegde	Wanneer het aantal	Wanneer er niet een verklaring

BSN's. **De tabel bevat de top-5 meest geraadpleegde BSN's en het aantal raad-plegingen dat daarop is gedaan (ook in %).**	raadplegingen op de top 5 per maand sterk verschilt en/of sterk verschilt in %, dan moet worden gezocht naar een verklaring. Allereerst moeten worden onderzocht of het een klant betreft. Volgens kan worden nagegaan of de klant bewerkelijk is: bijvoorbeeld er moet nader onderzoek worden gedaan, veel mensen zijn met de klant bezig. Aan de andere kant kan dit een sterke aanwijzing zijn dat een persoon die om de een of andere reden in de belangstelling staat, niet op rechtmatige gronden wordt geraadpleegd.	te vinden is, wordt bij BKWI een specifiek rapportage opgevraagd over het BSN en de medewerkers die op dat BSN raadplegingen hebben gedaan.
2.4 Hoogst aantal gebruikers dat hetzelfde BSN heeft geraadpleegd. De vorige tabel bevatte het aantal meest geraad-pleegde BSN's, ongeacht of dat door een of meerdere personen is geraadpleegd. In deze tabel gaat het om het BSN dat door de meeste gebruikers is geraadpleegd.	Wanneer het aantal personen dat eenzelfde BSN raadpleegt per maand sterk verschilt en/of sterk verschilt van het gemiddelde, dan moet worden gezocht naar een verklaring. Een afwijkend patroon kan een indicatie zijn voor misbruik. Verschillen tussen gemeenten kunnen (ook) wijzen op verschillende werkprocessen.	Er wordt een specifieke rapportage op medewerkersniveau opgevraagd bij BKWI. Vervolgens wordt door koppeling van het BSN met het cliëntenbestand vastgesteld of deze BSN's wel tot het cliëntenbestand horen.
2.5 Hoogst aantal raadplegingen per gebruiker. Dit is de top 5 van Suwinet gebruikers.	Grote afwijkingen van het gemiddelde of afwijkingen in de tijd kunnen worden verklaard door bv. opdracht aan een medewerker om specifiek bepaalde controles uit te voeren (in bulkwerk).	Wanneer geen verklaring kan worden gevonden in de taaktoedeling/procesgang of het gebruik van bijvoorbeeld een groepsaccount wordt een specifieke rapportage aangevraagd bij BKWI om deze top-gebruikers te identificeren.
Hoofdstuk 3: Accountbeheer.		
3.1 Percentage geblokkeerde accounts. **Accounts worden automatisch geblokkeerd bij BKWI na 3 mislukte pogingen om in te loggen.** **Gemeenten kunnen zelf instellen wanneer een**	Alle afwijkingen van 0 zijn aanleiding voor nader onderzoek. De functioneel beheerder kan daarvoor zijn gebruikersadministratie raadplegen. Hij / zij kan onderzoeken: • is de medewerker nog wel in dienst (bij uit dienst had zijn account direct afgesloten	Vervolgacties kunnen zijn: • account afsluiten, • wijzen op afspraken over het gebruik van Suwinet in de processen. • procedures met betrekking aan- en afsluiten van accounts aanscherpen of beter naleven

account (automatisch) geblokkeerd moet worden, bijvoorbeeld na 90 dagen niet-gebruik.	moeten worden), • heeft de betreffende medewerker Suwinet wel nodig voor zijn werk • waarom gebruikt de medewerker Suwinet niet.	
3.2 Aantal ongebruikte accounts. Deze tabel geeft aan hoeveel accounts de afgelopen 90 dagen niet gebruikt zijn.	De functioneel beheerder kan in zijn gebruikersadministratie per account achterhalen wat de laatste datum van gebruik was. Hij kan deze verifiëren bij BKWI. In alle gevallen zijn niet-gebruikte accounts reden voor nadere actie door de functioneel beheerder.	Vervolgstap kan zijn: • navraag doen bij de betreffende medewerker naar de reden niet-gebruik, • afsluiten van accounts van mensen die uit dienst zijn, • afsluiten accounts van mensen die Suwinet niet nodig hebben voor hun werk. • autorisatie aanpassen • autorisatiebeleid aanpassen of beter naleven
3.3 Verdeling van de rollen en het aantal autorisaties. De tabel geeft een overzicht van de beschikbare rollen (die gekoppeld zijn aan specifieke pagina's in Suwinet Inkijk) en het aantal medewerkers dat een autorisatie voor die rol heeft. Het kan zijn dat een medewerker voor meerdere rollen is geautoriseerd. Dat is af te lezen uit de autorisatietabel van de gebruikers-beheerder.	Speciale aandacht moet besteed worden aan het aantal 'zware' rollen: zijn daar logisch te verklaren wijzigingen in, zijn ze nog proportioneel in verhouding tot het aantal medewerkers dat met die controle- en opsporingstaken is belast. Meer in het algemeen biedt deze tabel de mogelijkheid om de toedeling van rollen te toetsen aan de functie van medewerkers: zijn rollen te ruim, te krap en wel juist toebedeeld. De functioneel beheerder kan in zijn administratie achterhalen wie welke autorisatie heeft. Afwijkingen in de aantallen moeten logisch verklaard kunnen worden, bijvoorbeeld door een wijziging in de inrichting van een proces.	Deze toets voert de Security Officer Suwi 2 keer per jaar uit in het kader van het proces autorisaties (bijlage 2)
Hoofdstuk 4. Doelmatig gebruik.		
4.1 Gemiddeld aantal gebruikers dat een BSN heeft geraadpleegd.	Afwijkingen in de tijd, en afwijkingen van de regio en vergelijkbare gemeenten kan een reden zijn om te kijken naar de inrichting van het proces.	Kennis van het proces is belangrijk om de tabel te interpreteren. De tabel kan gebruikt worden als aanleiding om de procesinrichting en het gebruik van Suwinet door te lichten.

4.2 Aantal raadplegingen per pagina. **In de tabel staan alle beschikbare pagina's van Suwinet Inkijk en het aantal keren dat die pagina is geraadpleegd. In de autorisatietabel van de functioneel beheerder is aangegeven welke medewerker voor welke rollen is geautoriseerd.**	Afwijkingen in het patroon kunnen mogelijk worden verklaard door specifieke controles, een nieuwe pagina of een vervallen pagina. Speciale aandacht moet worden besteed naar de pagina's met de speciale zoeksleutels: • GBA Zoek in GBA, • GSD Zoek in de GBA uitgebreid, • GSD Zoek in de RDW. Steeds moet de vraag worden gesteld of het aantal raadplegingen op deze zoeksleutels rechtmatig (en proportioneel) is. Pieken in het gebruik van deze pagina's moeten worden onderzocht op misbruik.	Een vervolgactie kan zijn een nader onderzoek naar de roltoedeling op basis van de autorisatietabel van de functioneel beheerder. Indien er mogelijk misbruik wordt vermoed, wordt een specifieke rapportage opgevraagd bij BKWI.
4.3 en 4.4 Mail verkeer via Suwi-mail. **Suwi-mail is beveiligde mail. Ketenpartijen worden geacht deze beveiligde Suwi-mail te gebruiken.**	Een dalend gebruik, vermoedelijk laag gebruik of niet-gebruik kan erop wijzen dat de onbeveiligde mail wordt gebruikt. Mogelijk is de gemeente niet aangesloten op Suwi-mail.	Breng Suwi-mail onder de aandacht van de medewerkers.

Rapportage aan Directeur Dienstverlening n.a.v. controle gebruikersrapportage en eventuele specifieke rapportage(s) door Security Officer Suwi

Security Officier Suwi .....

Functioneel beheerder .....

Registratienummer .....

Tijdvak gebruikersrapportage .....

Tijdvak bestandsvergelijking .....

Bevindingen Security Officer Suwi
Bevindingen gebruikersrapportage
Bevindingen vergelijking geraadpleegde BSN's versus actief cliëntenbestand
Bevindingen controle autorisaties
Overleg geweest met Teammanager Maatschappij Ja/Nee
Bevindingen overleg Teammanager Maatschappij
Aanleiding tot opvragen specifieke rapportage(s) Ja/Nee
Bevindingen specifieke rapportage(s)

Bevindingen functioneel beheerder
Overleg geweest met Teammanager Maatschappij Ja/Nee
Overleg geweest met Security Officer Suwi Ja/Nee

Datum & Ondertekening:

H.A. Leegstra
Directeur Dienstverlening