

**Beveiligingsplan Suwinet 2018
Gemeente Oegstgeest**



December 2018

Inhoudsopgave

1.	Inleiding.....	2
1.1	Kader regionaal Informatiebeveiligingsbeleid	2
1.2	Kader beveiligingsplan Suwinet 2018 gemeente Oegstgeest	3
1.3.	Compliance-check (audit).....	3
1.4	Vaststelling	3
2.	Gebruikers van Suwinet	5
2.1	Rollen en taken.....	5
2.2	Autorisatie	6
2.3	Beveiligingseisen gebruikers.....	6
2.4	Bewustwording medewerkers	7
3.	Communicatie	8
3.1	Periodiek werkoverleg.....	8
3.2	Individuele gesprekken	8
3.1	Toegang Suwinet documenten.....	8
4.	Controle	9
4.1	Generieke gebruikersrapportage	9
4.2	Specifieke rapportage	9
4.3	Bij twijfel over zorgvuldigheid: vervolgstappen.	9
4.4	Autorisaties.....	10
5.	Evaluatie en actualisatie	11
Bijlage 1	Medebewoners en Suwinet	12
Bijlage 2	Autorisatiestructuur	14
Bijlage 3	Procedure autorisaties Suwinet	15
Bijlage 4	Formulier Aanvraag autorisaties Suwinet	17
Bijlage 5	Formulier Intrekken of wijzigen autorisaties Suwinet	18
Bijlage 6	Zorgvuldigheidsverklaring Suwinet Gemeente Oegstgeest	19
Bijlage 7	Indicatoren analyse gebruikersrapportages Suwinet	21
Bijlage 8	Rapportage aan gemeentesecretaris.....	26

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 Algemene Verordening Gegevensbescherming (AVG) 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 regionaal Informatiebeveiligingsbeleid

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 december 2016 is het regionale Informatiebeveiligingsbeleid 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 compliancy-checks vanuit het Rijk.

De doelstelling van het beleid 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.

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

1.2 Kader beveiligingsplan Suwinet 2018 gemeente Oegstgeest

Het opstellen van een beveiligingsplan Suwinet is onderdeel van de totale informatiebeveiliging rondom Suwinet. In het beveiligingsplan is opgenomen de rollen en taken van de gebruikers, communicatie rondom Suwinet, de periodieke controles en evaluatie en actualisatie.

1.3. Compliancy-check (audit)

Jaarlijks vindt een compliancy-check plaats met betrekking tot Suwinet. Ten behoeve van deze compliancy-check zijn op dit moment 13 normen van kracht. Te weten:

1. Beleidsdocument voor informatiebeveiliging
2. Beoordeling van het informatiebeleid
3. Betrokkenheid van het college van B&W bij informatiebeveiliging
4. Coördineren van informatiebeveiliging
5. Toewijzing van verantwoordelijkheden voor informatiebeveiliging
6. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
7. Functiescheiding
8. Aanmaken auditlogbestanden
9. Controle van het systeemgebruik
10. Registratie van gebruikers
11. Beoordeling van gebruikersrechten van gebruikers
12. Gebruikersidentificatie en -authenticatie
13. Beleid voor het gebruik van crypto grafische beheersmaatregelen

1.4 Vaststelling

Het regionale Informatiebeveiligingsbeleid is op 14 december 2016 door het College van Burgemeester en Wethouders van de gemeente Oegstgeest vastgesteld.

Dit Beveiligingsplan Suwinet is op 18 december 2018 door het College van Burgemeester en Wethouders van de gemeente Oegstgeest vastgesteld. Vervolgens is het in januari 2019 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 Gemeentesecretaris
Functioneel beheerder	Verstrekken autorisaties
Gemeentesecretaris	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, loaw, loaz, Bbz of een andere door de afdeling uitgevoerde regeling betreft. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen.

Het opzoeken van informatie over medebewoners van een klant (in het kader van kostendeling) aan de hand van het BSN van de medebewoner is nodig om de hoogte van de uitkering te kunnen vaststellen en is daarmee geoorloofd. In bijlage 1 is uitgebreide informatie hierover te vinden.

- 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
 - controle verzamelinkomen in het kader van de Collectieve Zorgverzekering voor Minima (CZM)
- 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.

- Twee medewerkers van gemeente Leiden zijn geautoriseerd voor Suwinet Oegstgeest in het kader van het ophalen van de participatieverklaringen van inwoners woonachtig in Oegstgeest. De medewerkers van gemeente Leiden hebben een zorgvuldigheidsverklaring ondertekend.

2.2 Autorisatie

Het gebruik van Suwinet is voorbehouden aan medewerkers van Team Maatschappij die werkzaam zijn op het gebied van Werk en Inkomen en twee medewerkers van gemeente Leiden voor het kunnen ophalen van de gegevens in het kader van de participatieverklaring. De autorisaties voor Suwinet zijn op basis van functieprofiel toegekend en vastgelegd in een autorisatiematrix (zie bijlage 2). 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 3).

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 Algemene Verordening Gegevensbescherming (AVG). In de wet SUWI zijn geheimhoudingsbepalingen opgenomen, waarin bepaald is 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 4) ondertekenen.

Extern personeel

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

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

2.4 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 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.

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 Gemeentesecretaris 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.

3.1 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.

3.2 Individuele gesprekken

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

3.1 Toegang Suwinet documenten

Ten behoeve van de opslag rapportages en beveiligingsplan en verslagen van werkoverleggen, wijzigingen in autorisaties wordt zaaksysteem JOIN gebruikt. Ter beveiliging van deze documenten hebben slechts de Security Officers en de gebruikersbeheerder Suwinet en de medewerkers van team Documentaire Informatie Voorziening (DIV) toegang tot de informatie.

4. Controle

4.1 Generieke gebruikersrapportage

Het Bureau Keteninformatisering BKWI stelt maandelijks een generieke gebruikersrapportage op over de logging van het gebruik van Suwinet. De Security Officer Suwinet ontvangt deze rapportage per e-mail en bevat 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.

Aan de hand van deze rapportage 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).

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.

Eén exemplaar wordt aan de functioneel beheerder gegeven voor de uitvoering van de accountscontrole.

4.2 Specifieke rapportage

Per kwartaal moet een specifieke gebruikersrapportage opgevraagd bij het BKWI door de gemandateerde (teammanager Maatschappij) met in ieder de 4.2. Whitelist Escape. Uit de whitelist Escape worden de raadplegingen met codering "Anders" geselecteerd. De uitval worden door gebruikersbeheerder Suwinet van team Maatschappij verklaard. Raadplegingen die niet kunnen worden verklaard worden door teammanager Maatschappij bij consultants Werk en Inkomen nagevraagd en verklaard.

4.3 Bij twijfel over zorgvuldigheid: vervolgstappen.

Zijn er op basis van de generieke gebruikersrapportages 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 wordt 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.

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 oneigenlijk gebruik danwel misbruik wordt de zaak overgedragen aan het organisatie onderdeel dat het integriteitsbeleid uitvoert. Mocht dit het geval zijn dan start procedure integriteitsbeleid.

4.4 Autorisaties

De Security Officer Suwinet 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.

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 jaarlijks geëvalueerd en zo nodig geactualiseerd te worden of het beveiligingsplan nog steeds aansluit op de organisatie, de actuele wetgeving en of de juiste maatregelen daarvoor getroffen zijn. Dit valt onder de verantwoordelijkheid van de Security Officer Suwi.

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 Medebewoners en Suwinet

Medebewoners spelen een rol in de gemeentelijke processen bij de bijstandsverlening op grond van de Participatiewet. Het kunnen delen van de kosten voor levensonderhoud met andere inwoners¹ dan kinderen en partner is van invloed op de hoogte van de bijstandsuitkering. Omdat er dus sprake kan zijn van kostendeling, zullen medewerkers van de gemeentelijke sociale dienst het een en ander moeten weten over die medebewoners.

Uitzonderingen

Niet iedere inwoner wordt als kostendeler aangemerkt. Er zijn uitzonderingen. Gemeenten moeten vaststellen of een medebewoner als uitzondering moet worden aangemerkt of dat deze meetelt als kostendeler en dus van invloed is op de hoogte van de bijstand aan de klant. De uitzonderingen op de kostendelersnorm zijn (artikel 22a en artikel 19a van de Participatiewet) zijn:

Als het gaat om de klant zelf:

- De belanghebbende die gehuwd is en die niet met een of meer andere meerderjarige personen dan de echtgenoot in dezelfde woning zijn hoofdverblijf heeft, tenzij die echtgenoot geen recht op algemene bijstand heeft;
- De belanghebbende die de leeftijd van 21 jaar nog niet heeft bereikt.

Als het gaat om inwonende personen:

- Inwonende personen die de leeftijd van 21 jaar nog niet hebben bereikt;
- Inwonende personen, niet zijnde een bloed- of aanverwant in de eerste (kinderen, ouders) of tweede graad van belanghebbende (broer, zus, grootouders) die op basis van een schriftelijke overeenkomst met de belanghebbende, waarbij een commerciële prijs is overeengekomen, als verhuurder, huurder, onderverhuurder, onderhuurder, kostgever of kostganger in dezelfde woning als de belanghebbende zijn hoofdverblijf heeft;
- Inwonende personen die op basis van een schriftelijke overeenkomst met een derde, waarbij een commerciële prijs is overeengekomen, als huurder, onderhuurder of kostganger in dezelfde woning als de belanghebbende zijn hoofdverblijf heeft, mits hij de overeenkomst heeft met dezelfde persoon als met wie de belanghebbende een schriftelijke overeenkomst heeft, waarbij een commerciële prijs is overeengekomen, als huurder, onderhuurder of kostganger;
- Inwonende personen die onderwijs volgen waarvoor aanspraak op studiefinanciering kan bestaan op grond van de Wet studiefinanciering 2000 en op enig moment tijdens dat onderwijs gelet op zijn leeftijd in aanmerking kan komen voor die studiefinanciering, de persoon die onderwijs volgt waarvoor aanspraak kan bestaan op een tegemoetkoming op grond van hoofdstuk 4 van de Wet tegemoetkoming onderwijsbijdrage en schoolkosten, en de persoon die een beroepsopleiding als bedoeld in artikel 7.2.2, eerste lid, onderdelen a tot en met e, van de Wet educatie en beroepsopleiding in de beroepsbegeleidende leerweg volgt.

¹ 1 meerderjarige perso(o)n(en) die in dezelfde woning zijn/hun hoofdverblijf heeft/hebben

Als een medebewoner niet tot een van deze uitzonderingen behoort, telt hij mee als kostendeler in de norm van de belanghebbende, tenzij de belanghebbende (en zijn eventuele partner) dus zelf jonger is (zijn) dan 21 jaar.

Benodigde informatie

De gemeente heeft informatie nodig om vast te kunnen stellen of de medebewoner moet meetellen voor de kostendelersnorm. Op basis van de wet en de uitzonderingen die gemaakt worden voor kostendeling dan is er over medebewoners slechts de volgende informatie nodig:

- Het aantal medebewoners op het adres;
- De leeftijd van de medebewoner;
- De relatie van de medebewoner ten opzichte van de belanghebbende ;
- De datum waarop de medebewoner zich op het adres vestigt (BRP)
- De datum waarop de medebewoner vertrekt van het adres (BRP)
- Of er sprake is van commerciële overeenkomsten zoals beschreven bij de uitzonderingen;
- Of er sprake is van het volgen van onderwijs zoals beschreven bij de uitzonderingen.

Het is dus niet nodig en eveneens niet toegestaan om voor het vaststellen van kostendeling van een medebewoner, te achterhalen wat zijn/haar inkomsten zijn, of er daadwerkelijk studiefinanciering wordt ontvangen, in welke auto hij/zij rijdt, of hij toevallig ingeschreven staat voor werk, etc.

Informatie via Suwinet

Welke van bovengenoemde benodigde informatie is te verkrijgen op Suwinet, waar staat deze en in welke vorm?

Op de 'Kostendelerstoets-pagina', wordt onder de persoonsgegevens van de klant een tabel weergegeven van de medebewoners op het adres van de klant². In die tabel staat:

- BSN
- naam + voornamen
- geboortedatum
- 'datum vestiging op het adres' (BRP)
- 'de relatie van de medebewoner tot de klant' (ouder, kind, partner of 'onbekend')

Met de geboortedatum kan vastgesteld worden of de medebewoner 21 jaar of ouder is en de datum vestiging laat zien sinds wanneer de medebewoner eventueel moet meetellen als kostendeler. Als achterhaald moet worden wanneer een medebewoner vertrokken is van het adres, dan is dat te vinden in de bron BRP van de klant zelf (dus onder het BSN van de klant) bij de historische adresgegevens.

Informatie over commerciële overeenkomsten is niet aanwezig op Suwinet. Dat zal door de gemeente zelf moeten worden uitgevraagd bij of via de klant.

² De toegang tot gegevens van medebewoners uit de BRP is afhankelijk van het autorisatiebesluit die de gemeente heeft ontvangen van de RvIG.

Bijlage 2 Autorisatiestructuur

Verwijzing naar autorisatiematrix

<G:\OEGODI\ODIMA\SZ\sz\Kelly\4. Projecten\Suwi\Autorisatiematrix nieuw.xls>

De autorisatiematrix is ook beschikbaar op persoonsniveau.

Bijlage 3 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 in JOIN.

- **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.

Bijlage 4 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:

Bijlage 5 Formulier Intrekken of wijzigen autorisaties Suwinet

Naam medewerker	
Team	
Functie	
Wijzigen of intrekken?	<input type="radio"/> wijzigen <input type="radio"/> intrekken
Reden intrekking/wijziging	
Wijzigingen in autorisatie aangevraagd door Teammanager Maatschappij	Handtekening: Datum:
Gewenste wijzigingen in autorisatie verwerkt door functioneel beheerder.	Handtekening: Datum:

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 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:

Tabel	Signaal	Mogelijke vervolgactie
Hoofdstuk 1. Algemeen beeld gebruik Suwinet Inkijk.		
<p>1.1: Totaal gebruik Deze tabel bevat het absoluut aantal raadplegingen (geraadpleegde pagina's) over de afgelopen zes maanden.</p>	<p>De trend is hier belangrijk.</p> <p>Een plotselinge stijging kan wijzen op:</p> <ul style="list-style-type: none"> • extra uitgevoerde controles, • wetswijzigingen en herbeoordelingen, • plotselinge sterke stijging van aanvragen. <p>Een plotselinge daling kan wijzen op:</p> <ul style="list-style-type: none"> • vakantieperiode, • ziekte onder medewerkers, • wijziging in processen, bijvoorbeeld door invoering geautomatiseerde controles of afschaffen toetsing. 	<p>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.</p>
Hoofdstuk 2 Zorgvuldig gebruik.		
<p>2.1 Percentage raadplegingen op zoekleutel anders dan BSN. Wordt niet gebruikt, autorisaties staan niet aan.</p>	Geen.	Geen.
<p>2.2 Percentage raadplegingen buiten kantoortijd, dat wil zeggen tussen 19.00 uur en 07.00 uur.</p>	<p>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.</p>	<p>De Teammanager Maatschappij kan uitsluitel geven over overwerk in de avonden. Indien de verklaring niet afdoende is, wordt bij BKWI een specifieke rapportage opgevraagd.</p>
<p>2.3 Meest geraadpleegde BSN's. De tabel bevat de top-5 meest geraadpleegde BSN's en het aantal raadplegingen</p>	<p>Wanneer het aantal raadplegingen op de top 5 per maand sterk verschilt en/of sterk verschilt in %, dan moet worden</p>	<p>Wanneer er niet een verklaring te vinden is, wordt bij BKWI een specifiek rapportage opgevraagd over het BSN en de medewerkers</p>

<p>dat daarop is gedaan (ook in %).</p>	<p>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.</p>	<p>die op dat BSN raadplegingen hebben gedaan.</p>
<p>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.</p>	<p>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.</p>	<p>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.</p>
<p>2.5 Hoogst aantal raadplegingen per gebruiker. Dit is de top 5 van Suwinet gebruikers.</p>	<p>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).</p>	<p>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.</p>
<p>Hoofdstuk 3: Accountbeheer.</p>		
<p>3.1 Percentage geblokkeerde</p>	<p>Alle afwijkingen van 0 zijn aanleiding voor nader</p>	<p>Vervolgacties kunnen zijn:</p> <ul style="list-style-type: none"> • account afsluiten,

<p>accounts. Accounts worden automatisch geblokkeerd bij BKWI na 3 mislukte pogingen om in te loggen. Gemeenten kunnen zelf instellen wanneer een account (automatisch) geblokkeerd moet worden, bijvoorbeeld na 90 dagen niet-gebruik.</p>	<p>onderzoek. De functioneel beheerder kan daarvoor zijn gebruikersadministratie raadplegen. Hij / zij kan onderzoeken:</p> <ul style="list-style-type: none"> • is de medewerker nog wel in dienst (bij uit dienst had zijn account direct afgesloten moeten worden), • heeft de betreffende medewerker Suwinet wel nodig voor zijn werk • waarom gebruikt de medewerker Suwinet niet. 	<ul style="list-style-type: none"> • wijzen op afspraken over het gebruik van Suwinet in de processen. • procedures met betrekking aan- en afsluiten van accounts aanscherpen of beter naleven
<p>3.2 Aantal ongebruikte accounts. Deze tabel geeft aan hoeveel accounts de afgelopen 90 dagen niet gebruikt zijn.</p>	<p>De functioneel beheerder kan in zijn gebruikersadministratie per account achterhalen wat de laatste datum van gebruik was. Hij kan deze verifiëren bij BKWI.</p> <p>In alle gevallen zijn niet-gebruikte accounts reden voor nadere actie door de functioneel beheerder.</p>	<p>Vervolgstap kan zijn:</p> <ul style="list-style-type: none"> • 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
<p>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.</p>	<p>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</p>	<p>Deze toets voert de Security Officer Suwi 2 keer per jaar uit in het kader van het proces autorisaties (bijlage 2)</p>

	<p>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.</p>	
<p>Hoofdstuk 4. Doelmatig gebruik.</p>		
<p>4.1 Gemiddeld aantal gebruikers dat een BSN heeft geraadpleegd.</p>	<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>Afwijkingen in het patroon kunnen mogelijk worden verklaard door specifieke controles, een nieuwe pagina of een vervallen pagina.</p> <p>Speciale aandacht moet worden besteed naar de pagina's met de speciale zoekleutels:</p> <ul style="list-style-type: none"> • GBA Zoek in GBA, • GSD Zoek in de GBA uitgebreid, • GSD Zoek in de RDW. <p>Steeds moet de vraag worden gesteld of het aantal raadplegingen op deze zoekleutels rechtmatig (en proportioneel) is. Pieken in het gebruik van deze pagina's moeten worden onderzocht op misbruik.</p>	<p>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.</p>
<p>4.3 en 4.4 Mail verkeer via Suwi-mail. Suwi-mail is beveiligde mail.</p>	<p>Een dalend gebruik, vermoedelijk laag gebruik of niet-gebruik kan erop wijzen</p>	<p>Breng Suwi-mail onder de aandacht van de medewerkers.</p>

Ketenpartijen worden geacht deze beveiligde Suwi-mail te gebruiken.	dat de onbeveiligde mail wordt gebruikt. Mogelijk is de gemeente niet aangesloten op Suwi-mail.	
--	---	--

Bijlage 8 Rapportage aan gemeentesecretaris

Security Officer 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