Beveiligingsplan Suwinet

2022

Brunssum, 31 augustus 2022
Versie: 1.0

Inhoudsopgave

Algemeen 4
Verantwoordelijken beveiligingsplan 5
Evaluatie en aanpassing op actualiteit 5
Functionaliteiten en beveiligingsmaatregelen 6
Functionaliteiten Suwinet 6
Suwinet Inkijk 6
Samenloopapplicatie 7
Digitaal Klant Dossier (DKD) 7
Suwinet-mail 8
Vast personeel 8
Tijdelijke medewerkers 9
Bewustwording medewerkers 9
Oneigenlijk gebruik en incidenten 10
Maatregelen 10
Toegangsrechten en autorisatiebeheer 11
Beleid ten aanzien van autorisaties 11
Autorisatieplan medewerkers 11
Verzoek inzage dossier en correctie door cliënt en/of gemachtigde 12
Bijlagen 13
Bijlage 1: Autorisaties Suwinet (op 1-1-2022) 14
Applicatiebeheer 14
Deze functionarissen zijn belast met: 14
Medewerker administratieve ondersteuning BBI 14
Deze functionarissen zijn belast met: 14
De Suwinet Security Officer 15
De Inkomensconsulent met rol diagnose. 15
De Inkomensconsulenten rechtmatigheid. 16
Coach dienstverlening, zorg en bijzondere situaties. 16
Werkcoach. 16
De medewerker uitkeringsadministratie 17
De medewerker uitkeringsadministratie met rol debiteuren. 17
De medewerker Inlichtingen Bureau. 17
De medewerker bezwaar en beroep 17
De medewerker Verhaal & Terugvordering. 18

Brunssum, 31 augustus 2022

Versie: 1.0

De medewerker Sociale Recherche 18
Geoorloofd/ongeoorloofd gebruik 18
Bijlage 2: Procedure controle gebruik Suwinet 20
Algemeen 20
Controle gebruik Suwinet en DKD 21
Bijlage 3: Procedure autorisaties 22
Inleiding 22
Verantwoordelijkheid 22
Uitvoering 22
Periodieke controle autorisaties 23
Bijlage 4: Procedure opvragen en inzage gegevens 24
Telefonisch opvragen van gegevens door derden 24
Bijlage 5: Procedure communicatie over beveiliging 25
Inleiding 25
Verantwoordelijkheid 25
Uitvoering 25
Beveiliging bij individuele of functioneringsgesprekken 26
Bijlage 6: Taakbeschrijving Suwinet Security Officer 27
Inleiding 27
Taken Suwinet SO 27

Brunssum, 31 augustus 2022
Versie: 1.0

Algemeen

Het Bureau Keteninformatisering Werk en Inkomen (BKWI), de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, de Informatie Beheer Groep (IBG), de RDW (Rijksdienst voor het Wegverkeer), gemeenten en andere gelieerde organisaties wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur.
Met de faciliteit Suwinet-Inkijk worden gegevens op basis van een zoeksleutel zoals het Burger Service Nummers (BSN) toegankelijk gemaakt voor geautoriseerde medewerkers. Het gaat veelal om privacygevoelige gegevens over onder andere het arbeidsverleden, het inkomen, vermogen en opleiding van inwoners van Nederland. De genoemde organisaties hebben die gegevens nodig om het recht op een uitkering vast te kunnen stellen en of om de juiste dienstverlening te kunnen leveren.
Met de faciliteit Suwinet DKD-inlezen worden gegevens van diverse bronnen direct in de eigen bedrijfsapplicatie ingelezen en/of worden voor-ingevuld op elektronische aanvraagformulieren. Het gaat dan vanzelfsprekend alleen om die gegevens die zij nodig hebben voor de uitvoering van hun wettelijke taken.

De gemeenten Brunssum en Landgraaf hebben de uitvoering van taken op het vlak van de Participatiewet uitbesteed aan ISD BOL. Suwinet bevat privacygevoelige gegevens. Cliënten mogen erop kunnen vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. ISD BOL is in eerste aanleg verantwoordelijk voor de beveiliging van persoonsgegevens van haar cliënten. Ook is ISD BOL verantwoordelijk voor een goede gegevensuitwisseling in het kader van de Wet Suwi.
Als opdracht gevende gemeenten dienen de gemeenten Brunssum en Landgraaf er wel op toe te zien dat de uitvoering van deze taken adequaat en conform de regels gebeurt.

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. Net als in de BIG dient binnen de BIO eveneens door gemeenten een informatiebeveiligingsbeleid te worden vastgesteld. Hierin zijn voor de gemeenteregels vastgesteld voor de beveiliging van gegevens. Het informatiebeveiligingsbeleid vormt het vertrekpunt voor het specifieke beveiligingsplan zoals bedoeld in de bijlage XIV van de regeling SUWI.

Brunssum, 31 augustus 2022
Versie: 1.0

Verantwoordelijken beveiligingsplan

De afdelingshoofden zijn verantwoordelijk voor het gebruik en de beveiliging van Suwinet. De Suwinet security officer (hierna te noemen Suwinet SO) bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet maatregelen worden nageleefd. De Suwinet SO heeft hierin een onafhankelijke positie en rapporteert rechtstreeks aan het MT. En zo nodig aan het Dagelijks Bestuur. Uitvoering van beveiliging van systemen en applicaties ligt bij de systeembeheerders conform opgestelde procedures.

Evaluatie en aanpassing op actualiteit

Het beveiligingsplan Suwinet is geen statisch document. Het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten.
De organisatie en de omgeving van ISD BOL zijn voortdurend in ontwikkeling, onder andere door wijzigende of vernieuwende inzichten en wetgeving of aanpassingen in de informatiesystemen.
Dit betekent dat dit plan periodiek moet worden beoordeeld op actualiteit en dus mogelijk constante aanpassing behoeft inclusief de hieruit voortvloeiende procedures en maatregelen.

Strategisch Informatieoverleg (SIO)

In 2012 werd het Archiefbesluit 2012 gewijzigd. In de Nota van Toelichting op dat besluit is het begrip Strategisch Informatieoverleg (SIO) geïntroduceerd. SIO is een structureel overleg tussen alle partijen die een rol spelen in de inrichting en ontwikkeling van informatiehuishouding. In dit overleg komen vraagstukken rondom waardering en selectie van digitale informatie op tafel, maar ook onderwerpen als informatiebeveiliging, privacybescherming, vervroegde overbrenging en openbaarheidsbeperking. Deze lijst is niet limitatief: alle vraagstukken rondom informatie kunnen worden besproken. Het is een overlegplatform dat adviseert, uitvoeringsbesluiten neemt over informatiehuishouding en beleidskaders ontwikkelt om deze te laten vaststellen door het bestuur. Daarbij spelen maatschappelijke ontwikkelingen, (wettelijke) kaders en actuele organisatiethema's een belangrijke rol. Het SIO is dus ontstaan vanuit de archiefwetgeving.
Deelnemers SIO:

- Directeur
- De afdelingshoofden
- De CISO
- De FG /IBF
- Functioneel / senior applicatiebeheerder DMS (op afroep)
- SO Suwinet (op afroep)

Brunssum, 31 augustus 2022
Versie: 1.0

Suwinet is een belangrijke informatiebron. De informatie verkregen uit deze bron vormt een essentieel onderdeel van de informatiehuishouding van ISD BOL. In het SIO wordt het beveiligingsplan Suwinet over het afgelopen jaar geëvalueerd en constateert waar noodzakelijk onderdelen dienen te worden geactualiseerd. Daarbij is de input van de SO Suwinet onontbeerlijk. Wanneer het beveiligingsplan geen bijstelling behoeft dient het geldend plan opnieuw te worden vastgesteld, voor de duur van één jaar. Wanneer het beveiligingsplan wel dient te worden geactualiseerd zal de Suwinet SO samen met de functionaris gegevensbescherming een geactualiseerd beveiligingsplan Suwinet opstellen. Het plan (ongewijzigd of geactualiseerd) wordt vervolgens ter vaststelling aangeboden aan het MT en het Dagelijks Bestuur. De SO Suwinet draagt hier zorg voor.

Wanneer dringende ontwikkelingen tussentijdse evaluatie noodzaken wordt de overleggroep bijeengebracht voor tussentijdse bijstelling van het plan en/of acties. Het initiatief hiertoe kan door ieder lid van de beveiligingsgroep worden genomen.

Functionaliteiten en beveiligingsmaatregelen

ISD BOL maakt gebruik van meerdere applicaties (S4W, Corsa, Liaan). Beveiliging rondom gebruik van deze applicaties is vastgelegd in het informatiebeveiligingsplan. Dit beveiligingsplan richt zich alleen op Suwinet.

Functionaliteiten Suwinet

Het Suwinet kent verschillende functionaliteiten, te weten:

- Een raadpleegfunctie (Suwinet Inkijk);
- Het uitwisselen van gegevens, de samenloopapplicatie;
- Het Digitaal Klant Dossier;
- Suwinet mail;
- Suwinet inlezen.

Suwinet Inkijk

Suwinet Inkijk is d.m.v. rollen toegankelijk gemaakt voor het raadplegen van cliëntgegevens/informatie. Dit op basis van die taken waarvoor wettelijke grondslag is en doelbinding van gegevensgebruik is vastgesteld. Als Suwinet om andere redenen wordt gebruikt dan zoals in de bijlage ‘autorisaties Suwinet’ verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

Brunssum, 31 augustus 2022
Versie: 1.0

Beveiliging:
In Suwinet zijn zeer privacygevoelige gegevens verzameld. De toegangsverlening tot Suwinet is geregeld in het hoofdstuk Toegangsrechten en autorisatiebeheer en in de bijlage “Procedure autorisaties”.

Samenloopapplicatie

Maandelijks levert ISD BOL zijn actuele uitkeringsbestand aan bij het Inlichtingenbureau. Via deze instantie worden de gegevens vergeleken met de gegevens van o.a. het UWV, de Belastingdienst, de Dienst Uitvoering Onderwijs (DUO – IB-Groep), Justitie (detentie). Bij samenloopgevallen wordt een signaal naar de gemeente gestuurd, die vervolgens een onderzoek kan instellen naar mogelijke fraude.
Beveiliging:
Het aan te leveren bestand wordt maandelijks samengesteld door de applicatiebeheerder, die het bestand vervolgens naar het Inlichtingenbureau verzendt via de beveiligde site van het Inlichtingenbureau. Terugkoppeling van gegevens gaat eveneens via deze site.

Digitaal Klant Dossier (DKD)

Het DKD is een onderdeel van Suwinet. Het is een elektronisch dossier waarin gegevens zijn opgeslagen van het UWV, SVB, RDW en de gemeenten. Vanuit het Digitaal Klantdossier is een groot aantal gegevenselementen uit S4W via webservice te raadplegen. Deze gegevens zijn in principe 24 uur per dag raadpleegbaar, ook in het weekend. Hiermee wordt voldaan aan de verplichting om 7 dagen per week minimaal 20 uur per dag raadpleegbaar te zijn.

De ketenpartners kunnen de gegevens in het DKD raadplegen en (her)gebruiken. Dit betekent dat de cliënten in principe maar eenmaal gegevens aanleveren. De cliënt kan zijn gegevens zelf ook bekijken. Hij ziet niet alle informatie die medewerkers van de ketenpartners te zien krijgen, maar een deel ervan. Deze gegevens vindt hij in het z.g. klantbeeld: de klant logt in met zijn DigiD code en zijn BSN. Ook kan hij gebruik maken van elektronische diensten, zoals correctieservice en digitale aanvragen. Het DKD verkeert in een groeiproces en zal steeds verder uitbreiden. Steeds meer partners zullen erop worden aangesloten, zoals DUO, de Belastingdienst, Zorgverzekeraars, Onderwijs, Justitie en de sector Zorg en Wonen.
Het Inlichtingenbureau biedt de mogelijkheid om DKD-klantgegevens digitaal in te lezen in een eigen, gemeentelijke applicatie. Daarnaast is het mogelijk om elektronische aanvraagformulieren gedeeltelijk, automatisch in te laten vullen, bijvoorbeeld bij het aanvragen van een bijstandsuitkering. Hiermee maakt DKD-Inlezen eenmalige gegevensuitvraag en het hergebruik van gegevens mogelijk. De gegevens mogen alleen gebruikt worden voor de uitvoering van de participatiewet taken.

Brunssum, 31 augustus 2022
Versie: 1.0

Beveiliging:
ISD BOL maakt gebruik van DKD-Inlezen om DKD-klantgegevens digitaal in te lezen in een aantal applicaties:

- Liaan Herberekenen
- Liaan Frauderegistratie
- Liaan e-Dienstverlening
- Liaan Inlichtingenbureau

Het is uiteraard de bedoeling dat alleen die gegevens worden ingelezen die voor het gebruik van deze applicatie noodzakelijk zijn.
De toegangsverlening is geregeld in het hoofdstuk Toegangsrechten en autorisatiebeheer en in de bijlage “Procedure autorisaties”.

Suwinet-mail

Met Suwinet-Mail kunnen partijen die gebruik maken van Suwinet, vertrouwelijke informatie sturen via een besloten netwerk. Suwinet-mail is eenvoudig in gebruik.
Beveiliging:
De risico’s die zijn verbonden aan het mailen van klantgegevens zijn aanzienlijk verkleind doordat mailing via een besloten netwerk plaatsvindt.

Vast personeel

ISD BOL werkt met persoonsgegevens. Op basis van de ~~Ambtenarenwet~~ Wnra (Wet normalisering rechtspositie ambtenaren), de AVG en de wet SUWI zijn medewerkers gebonden aan geheimhoudingsbepalingen.
Nieuwe medewerkers moeten een Verklaring omtrent Gedrag (VOG) overleggen. De VOG mag niet ouder zijn dan 3 maanden. Deze moeten zij overleggen voordat zij hun werkzaamheden starten bij ISD BOL. In een persoonlijk gesprek met de directeur ISD BOL worden nieuwe medewerkers geïnformeerd over het werken met privacygevoelige informatie en daarmee gepaard gaande verantwoordelijkheden. De medewerkers dienen vervolgens een integriteitsverklaring te tekenen. Deze verklaring wordt ondertekend op de eerste werkdag voordat zij toegang krijgen tot de systemen. Medewerkers die uit hoofde van hun functie in aanmerking komen voor het raadplegen van Suwinet-inkijk dienen aanvullend:

- Een zorgvuldigheidsverklaring te ondertekenen en de ingevulde zorgvuldigheidsverklaring in te leveren bij de Suwinet SO.
- Deel te nemen (eenmalig) aan de e-learning module Veilig Gebruik Suwinet van de VNG en het bewijs van deelname in te leveren bij de Suwinet SO.
- Bij de aanstelling wordt aan de nieuwe medewerker een document uitgereikt met betrekking tot het gebruik van privacygevoelige informatie en met name Suwinet.

Eerst na deze drie stappen wordt een account aangevraagd.

Tijdelijke medewerkers

Ook tijdelijk medewerkers (inhuurkrachten, uitzendkrachten, stagiaires, personen die een werkervaringsplek invullen) dienen een VOG te overleggen voordat zij hun werkzaamheden bij ISD BOL starten. De VOG mag niet ouder zijn dan 3 maanden. Ook zij worden in een persoonlijk gesprek met de directeur ISD BOL geïnformeerd over het werken met privacygevoelige informatie en daarmee gepaard gaande verantwoordelijkheden. Wanneer zij voor de uitvoering van hun werkzaamheden in aanmerking komen voor Suwinet-inkijk dienen zij eveneens een geheimhoudingsverklaring te ondertekenen. Deze verklaring wordt ondertekend op de eerste werkdag voordat zij toegang krijgen tot de systemen. Medewerkers die uit hoofde van hun functie in aanmerking komen voor het raadplegen van Suwinet-inkijk dienen:

- Een zorgvuldigheidsverklaring te ondertekenen en de ingevulde zorgvuldigheidsverklaring in te leveren bij de Suwinet SO.
- Deel te nemen (eenmalig) aan de e-learning module Veilig Gebruik Suwinet van de VNG en het bewijs van deelname in te leveren bij de Suwinet SO.
  Bij de aanstelling wordt aan de nieuwe medewerker een document uitgereikt met betrekking tot het gebruik van privacygevoelige informatie en met name Suwinet.

Eerst na deze drie stappen wordt een account aangevraagd.

Voor de medewerker wordt een autorisatie voor Suwinet-inkijk aangevraagd. Het afdelingshoofd geeft in principe toestemming maar laat zich hierin, indien noodzakelijk, adviseren door de Suwinet SO. De Suwinet SO zal, indien aan de orde, uit hoofde van zijn functie en verantwoordelijkheid het afdelingshoofd adviseren om de toegang tot één of meerdere onderdelen van Suwinet-inkijk voor een medewerker niet toe te staan, dit gerelateerd aan de functie of werkzaamheden van de medewerker. Hierin kan door de Suwinet SO het BKWI geconsulteerd worden. De Suwinet SO zorgt vervolgens voor autorisatie in Suwinet-inkijk voor de medewerker. De Suwinet SO kan gemotiveerd besluiten geen autorisatie of een beperkte autorisatie toe te kennen. In voorkomende gevallen wordt het MT daarvan in kennis gesteld. Dit geldt zowel voor vaste als voor tijdelijke medewerkers.

Wordt een medewerker gedetacheerd bij een andere werkgever wordt de suwinet-account/ autorisatie ingetrokken.

Bewustwording medewerkers

Alle medewerkers van ISD BOL (die gebruik maken van de Suwinet applicatie) worden geïnformeerd over logging die vastgelegd wordt m.b.t. hun gebruik van Suwinet. Met het oog hierop is de navolgende informatie verstrekt aan de medewerkers die (gaan) werken met Suwinet:

- Het bestaan van de logging-applicatie en het doel hiervan;

- De (aard van de) gegevens die worden verzameld;
- Het gebruik van de gelogde gegevens; deze worden niet voor andere doeleinden gebruikt dan waarvoor ze zijn vastgelegd;
- Wanneer er sprake is van onrechtmatig of doel overschrijdend gebruik en de acties die hieruit kunnen leiden;

In de bijlage “Procedure controle gebruik Suwinet” wordt nader ingegaan op de gelogde gegevens en de interne controle op rechtmatig gebruik van Suwinet.

Oneigenlijk gebruik en incidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de SO Suwinet (en/of het afdelingshoofd). Door de SO wordt een onderzoek wordt ingesteld naar eventuele gevolgen van het geconstateerde incident. Incidenten en het resultaat van het verrichte onderzoek kunnen onderwerp zijn in de Overleggroep. Incidenten en het resultaat worden te allen tijde gemeld bij het Management.

Maatregelen

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) stelt maandrapportages op over onder andere de logging van het gebruik van Suwinet. Deze rapportages worden digitaal beschikbaar gesteld aan de betreffende Ketenpartners. Aan de hand hiervan wordt maandelijks (z.s.m. na beschikbaarstelling van de rapportage) gecontroleerd op het gebruik van Suwinet en wordt geprobeerd een goed beeld te krijgen van de wijze waarop Suwinet door de medewerkers wordt geraadpleegd. Bij een vermoeden van onjuist gebruik kan specifieke informatie per onderdeel of per medewerker worden opgevraagd/gegenereerd. De medewerkers die gebruik maken van Suwinet worden in kennis gesteld van het feit dat gegevens van hun raadpleegactiviteiten worden vastgelegd en dat deze gegevens worden gebruikt voor de controle op een rechtmatig gebruik van Suwinet. Deze controle is nader uitgewerkt in de bijlage “Procedure controle gebruik Suwinet”.
Fysieke beveiliging van publieke en werkruimtes vindt plaats conform het informatiebeveiligingsplan. Dit betreft onder andere omgang met bezoekers, gebruik van spreekkamers, omgang met vertrouwelijk papier, archivering en printers.
Bij ISD BOL is een beleid rond clean desk en clear screen. Op deze manier wordt geborgd dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven of digitaal toegankelijk zijn. Deze moeten te allen tijde veilig worden opgeborgen/geborgd.

Brunssum, 31 augustus 2022
Versie: 1.0

Toegangsrechten en autorisatiebeheer

Beleid ten aanzien van autorisaties

Het gebruik van Suwinet is voorbehouden aan de medewerkers van ISD BOL die werkzaam zijn op het gebied van Werk en Inkomen. De autorisaties voor Suwinet worden per functie (functierol) toegekend. De Suwinet SO geeft aan welke autorisaties voor een functie nodig zijn voor het uitvoeren van de aan de functie gelieerde taken.
De wijze waarop de individuele autorisaties –op medewerker niveau– worden toegekend, gewijzigd of ingetrokken is vastgelegd in procesbeschrijving toekennen/wijzigen/intrekken suwinet-account.

Autorisatieplan medewerkers

In de bijlage "Suwinet autorisatiematrix" zijn de rollen en het daarbij behorende toegestane gebruik van dit medium uitgebreid beschreven. Er vindt ieder kwartaal controle plaats of de individuele suwinet accounthouders over de juiste toegang tot informatiebronnen in suwinet beschikt. In de bijlage "Procedure controle gebruik Suwinet" is de controleprocedure vastgelegd. Alle autorisaties zijn vastgelegd in het Overzicht autorisaties.
De Suwinet SO:

- Bewaart alle verzoeken om verstrekking, wijziging of intrekking van autorisaties;
- Bewaakt tijdige intrekking accounts bij detachering/einde dienstbetrekking/einde inhuur/langdurige ziekte;
- Stelt een rapport op van de bevindingen van de autorisatiecontrole en bespreekt dit rapport in de overleggroep Informatiebeveiliging;
- Past autorisaties aan bij gewijzigde functies;
- Past autorisaties aan bij gewijzigde functionaliteiten Suwinet;
- Past autorisaties aan bij gewijzigd inzicht over gebruik;
- Onderzoekt reden(en) blokkering accounts en/of bij langdurig geen gebruik account;
- Onderzoekt mate van gebruik van Suwinet tussen medewerkers met gelijke functies (en gelijke autorisaties).

De afdeling P&O informeert de Suwinet SO tijdig over de indiensttreding van medewerkers, de uitdiensttreding van medewerkers, wijziging in functies van medewerkers en wanneer er sprake is van langdurig ziekteverzuim van medewerkers.

Brunssum, 31 augustus 2022
Versie: 1.0

Verzoek inzage dossier en correctie door cliënt en/of gemachtigde

Behalve de Ketenpartners kunnen ook cliënten hun gegevens raadplegen in het DKD (onderdeel van Suwinet). Om toegang tot hun gegevens te krijgen moeten zij inloggen met hun DigiD-code.

Als een cliënt een correctie van een bepaald gegeven wil kan hij hiertoe een verzoek indienen bij de Suwinet SO. In het DKD, waarin de gegevens worden geraadpleegd, is bij een aantal gegevens een digitale correctieservice opgenomen. Dat wil zeggen dat een cliënt rechtstreeks van uit het DKD een elektronisch correctieverzoek kan indienen. Desgewenst kan hij dit ook schriftelijk of mondeling doen. Bij de overige gegevens staat vermeld hoe een eventuele correctie kan worden aangevraagd.

Daarnaast kan een cliënt ook inzage vragen in zijn digitale bijstandsdossier. Ook in dit geval kan hij om correctie van een bepaald gegevens verzoeken. In de bijlage “Procedure correctie gegevens” zijn protocollen opgenomen voor inzage en correctie. Medewerkers kunnen hiermee te maken krijgen en zijn hiervan op de hoogte.

Brunssum, 31 augustus 2022
Versie: 1.0

Bijlagen

Brunssum, 31 augustus 2022
Versie: 1.0

Bijlage 1: Autorisaties Suwinet (op 1-1-2022)

Er zijn 13 verschillende functies bij ISD BOL die geautoriseerd zijn om gebruik te maken van Suwinet, te weten:

- Applicatiebeheer (gebruikersbeheer);
- Medewerker administratieve ondersteuning BBI (gebruikersbeheer);
- Suwinet SO (gebruikersbeheer);
- Inkomensconsulent met rol diagnose (raadplegen);
- Inkomensconsulent rechtmatigheid (raadplegen);
- Coach dienstverlening, zorg en bijzondere situaties (raadplegen);
- Werkcoach (raadplegen);
- De medewerker uitkeringsadministratie (raadplegen);
- De medewerker uitkeringsadministratie met rol debiteuren (raadplegen);
- De medewerker inlichtingenbureau (raadplegen);
- Medewerker bezwaar en beroep (raadplegen);
- Medewerker Verhaal & Terugvordering (raadplegen);
- Medewerker Sociale Recherche (raadplegen);

Eindverantwoordelijke voor het gebruik en de beveiliging is de directeur.

Applicatiebeheer

Deze functionarissen zijn belast met:

- Het actueel houden van de applicatie waardoor een goed gebruik van Suwinet en het DKD mogelijk is;
- Het verlenen van toegang tot en het autoriseren voor het gebruik van Suwinet;
- Storingen die aan derden, zoals het Inlichtingenbureau of de softwareleverancier moeten worden gemeld, direct doorgeven.

Medewerker administratieve ondersteuning BBI

Deze functionarissen zijn belast met:

- Het actueel houden van de applicatie waardoor een goed gebruik van Suwinet en het DKD mogelijk is;
- Het verlenen van toegang tot en het autoriseren voor het gebruik van Suwinet;
- Storingen die aan derden, zoals het Inlichtingenbureau of de softwareleverancier moeten worden gemeld, direct doorgeven.

Brunssum, 31 augustus 2022
Versie: 1.0

De Suwinet Security Officer

Deze functionaris is belast met de volgende taken:

- Moet de beveiligingsprocedures en -maatregelen in het kader van Suwinet zo beheren en beheersen dat de beveiliging van Suwinet overeenkomt met de wettelijke eisen;
- Rapporteert en adviseert periodiek rechtstreeks aan het MT en het Dagelijks Bestuur;
- De Suwinet SO 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;
- Toestemming geven voor het verlenen van toegang tot en het autoriseren voor het gebruik van Suwinet;
- Het maandelijks genereren en analyseren van loggingsrapportages van het BKWI;
- Het maandelijks genereren en analyseren van loggingsrapportages DKD door LIAAN;
- Het genereren van specifieke rapportages als hier aanleiding toe is;
- Het signaleren van gewenste aanpassingen van het beveiligingsplan op actualiteit en volledigheid hiervan;
- Zorgt mede voor het actueel houden van de applicatie, waardoor een goed gebruik van Suwinet en het DKD mogelijk is;
- Storingen die aan derden, zoals het Inlichtingenbureau of de softwareleverancier moeten worden gemeld, direct doorgeven (via applicatiebeheer);
- Zorgt voor de jaarlijkse evaluatie van het suwinet beveiligingsplan;
- Geeft (periodiek) voorlichting aan (nieuwe) medewerkers;
- Zorgt voor publicaties op intranet m.b.t. Suwinet;
- Houdt registraties bij met betrekking tot de uitvoering van zijn taken.

De Inkomensconsulent met rol diagnose.

Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op:

- Aanvragen PW en IOAW en
- Rechtmatigheidsonderzoeken en
- Diagnose werkfitheid aan de poort en
- Aanvragen minimabeleid en kinderopvang (m.u.v. lokale regelingen).

Wanneer de consulent raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de inkomensconsulent.

Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit.

Brunssum, 31 augustus 2022

Versie: 1.0

De Inkomensconsulenten rechtmatigheid.

Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op:

- Aanvragen PW en IOAW en
- Rechtmatigheidsonderzoeken en
- Aanvragen minimabeleid en kinderopvang (m.u.v. lokale regelingen).

Wanneer de consulent raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de inkomensconsulent.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist.

Coach dienstverlening, zorg en bijzondere situaties.

Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op:

- Aanvragen PW en IOAW en
- Rechtmatigheidsonderzoeken en
- Aanvragen minimabeleid en kinderopvang (m.u.v. lokale regelingen).

Wanneer de consulent raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de inkomensconsulent.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit.

Werkcoach.

Deze groep gebruikers is geautoriseerd voor het raadplegen van gegevens die betrekking hebben op:

- Doelmatigheidsonderzoeken en
- Re-integratiewerkzaamheden.

En wel in die gevallen waarin de werk-/participatieconsulent dit nodig oordeelt. Wanneer de consulent raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de werk/participatieconsulent.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit.

Brunssum, 31 augustus 2022
Versie: 1.0

De medewerker uitkeringsadministratie

De medewerkers Uitkeringsadministratie zijn geautoriseerd voor het raadplegen van Suwinet in verband met werkzaamheden betreffende de uitkeringsverwerking, de afhandeling van bijzondere bijstandsaanvragen en aanvragen minimabeleid (m.u.v. lokale regelingen).
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist.

De medewerker uitkeringsadministratie met rol debiteuren.

De medewerkers Uitkeringsadministratie zijn geautoriseerd voor het raadplegen van Suwinet in verband met werkzaamheden betreffende de uitkeringsverwerking, de afhandeling van bijzondere bijstandsaanvragen en aanvragen minimabeleid (m.u.v. lokale regelingen).
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist. Verder kan de medewerker gebruik maken van de LIAAN-module 'herberekenen'.

De medewerker Inlichtingen Bureau.

De medewerker Inlichtingen Bureau is geautoriseerd voor Suwinet in verband met werkzaamheden betreffende het analyseren en verwerken van signalen ontvangen van het Inlichtingen Bureau.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit. Verder kan de medewerker gebruik maken van de LIAAN-module 'inlichtingenbureau'.

De medewerker bezwaar en beroep

De medewerker bezwaar en beroep zijn geautoriseerd voor het raadplegen van Suwinet in verband met de afhandeling van bezwaar- en beroepszaken.
En wel in die gevallen waarin de medewerker dit nodig oordeelt. Wanneer de medewerker raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist.

Brunssum, 31 augustus 2022
Versie: 1.0

De medewerker Verhaal & Terugvordering.

De medewerkers verhaal & terugvordering zijn geautoriseerd voor het raadplegen van Suwinet in verband met:

- Debiteurenheronderzoeken ter vaststelling van de actuele woonplaats, de draagkracht, de hoogte van het inkomen en
- Debiteurenonderzoeken in verband met het terugvorderen van vorderingen en het beslag leggen op inkomen.

En wel in die gevallen waarin de medewerker verhaal & terugvordering dit nodig oordeelt. Wanneer de medewerker raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de medewerker.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit.

De medewerker Sociale Recherche

De medewerker Sociale Recherche/ lid team bijzonder onderzoek zijn geautoriseerd voor het raadplegen van Suwinet in verband met:

- Fraudeonderzoeken.

En wel in die gevallen waarin de medewerker team bijzonder onderzoek dit nodig oordeelt. Wanneer de medewerker raadpleging van Suwinet nodig acht wordt het raadplegen van Suwinet nader gemotiveerd in de rapportage van de medewerker.
Het raadplegen van gegevens is uitsluitend mogelijk met de zoeksleutel BSN. Er is toegang tot personen op de whitelist én er kan gebruik worden gemaakt van de whitelist escape functionaliteit. Verder kan de medewerker gebruik maken van de LIAAN-module 'fraude registratie'.

Geoorloofd/ongeoorloofd gebruik

Als de geautoriseerde medewerkers Suwinet gebruiken voor de hiervoor gemelde gevallen dan is er sprake van geoorloofd gebruik. Wordt Suwinet om andere redenen gebruikt dan is er in principe sprake van ongeoorloofd gebruik. Dit ongeoorloofd gebruik wordt onderzocht door de Suwinet SO. Wanneer uit het onderzoek van de Suwinet SO blijkt dat er sprake kan zijn van ongeoorloofd gebruik van Suwinet door een medewerker meldt de Suwinet SO dit bij het verantwoordelijk afdelingshoofd. Het afdelingshoofd zal vervolgens een gesprek aangaan met de betreffende medewerker om de mogelijke redenen van het geconstateerde gebruik van Suwinet door de medewerker te achterhalen. Wanneer blijkt dat de medewerker bewust ongeoorloofd gebruik heeft gemaakt van Suwinet zal hierop een passende maatregel worden genomen. Dit kan variëren van het geven van een waarschuwing tot het afsluiten van het gebruik van Suwinet voor de medewerker. In geval van zeer ernstig misbruik van Suwinet-

inkijk (te denken valt aan ‘eigen gewin’) kan dit leiden tot schorsing van het uitoefenen van de functie.

Brunssum, 31 augustus 2022
Versie: 1.0

Bijlage 2: Procedure controle gebruik Suwinet

Algemeen

Door het Bureau Keteninformatisering Werk & Inkomen (BKWI) worden rapportages samengesteld over de logging van het gebruik van Suwinet. Het doel van deze logging is naast wetenschappelijke en statistische doeleinden het tegengaan en controleren van onrechtmatig, onregelmatig of doel overschrijdend gebruik van Suwinet.
De volgende gegevens worden gelogd:

- Het tijdstip van iedere log-in, log-out en andere actie;
- De gebruikersnaam van degene die inlogt of uitlogt;
- Burger Service Nummers (BSN) of andere zoeksleutels waarvan gegevens worden opgevraagd worden als actie geregistreerd;
- Elke actie, zoals de bekeken kolom- of overzichtspagina"s.

Indien gewenst genereren wij informatie onder andere aangaande:

- Inkijkacties;
- Opvragingen unieke BSN;
- Inlog pogingen;
- Administrator account;
- Aantal accounts per rol;
- Gebruikte zoeksleutels;
- Aantal geregistreerde accounts ten opzichte van de actieve accounts;
- Aantal opvragingen binnen/buiten kantoortijd.
- Geblokkeerde account / verlopen accounts

Door Wolters-Kluwer (Liaan) worden rapportages samengesteld over de logging van het gebruik van het DKD. Het doel van deze logging is naast wetenschappelijke en statistische doeleinden het tegengaan en controleren van onrechtmatig, onregelmatig of doel overschrijdend gebruik van Suwinet.
De volgende gegevens worden gelogd:

- Het tijdstip van iedere log-in, log-out en andere actie;
- De gebruikersnaam van degene die inlogt of uitlogt;
- Burger Service Nummers (BSN) of andere zoeksleutels waarvan gegevens worden opgevraagd worden als actie geregistreerd;

Indien gewenst genereren we informatie onder andere aangaande het gebruik van de Liaan modules: herberekenen, frauderegistratie, inlichtingenbureau en e-dienstverlening.

Brunssum, 31 augustus 2022
Versie: 1.0

Deze lograpporten worden iedere maand door de Suwinet SO gedownload en gecontroleerd. Als uit deze controle onregelmatigheden blijken, dan genereert de Suwinet SO een specifieke rapportage op. Ook kan de Suwinet SO op verzoek van leden van de beveiligingsgroep specifieke rapportages genereren en/of opvragen. Hiervoor moet het betreffende lid wel een gegronde reden hebben. Dit is ter beoordeling aan de SO.

Controle gebruik Suwinet en DKD

- De Suwinet SO downloadt maandelijks de via het Inlichtingenbureau beschikbaar gestelde BKWI-rapportages én de LIAAN-rapportages;
- De Suwinet SO bepaalt of en van welke medewerker(s) specifieke raadpleeggegevens worden opgevraagd;
- De Suwinet SO controleert de rapportages op onregelmatigheden. Bij geconstateerde onregelmatigheden wordt een specifieke rapportage gegenereerd;
- Ook kunnen van medewerker(s) raadpleeggegevens worden opgevraagd;
- De Suwinet SO gaat na of er geregistreerde accounts zijn die volgens de BKW-rapportages niet actief zijn geweest in de controleperiode en achterhaalt welke medewerkers geen of (te) weinig gebruik maken van Suwinet en wat daarvan de reden is;
- De Suwinet SO bespreekt met het verantwoordelijk afdelingshoofd mogelijke geconstateerde verschillen. Het is aan het afdelingshoofd om hierin actie te ondernemen;
- De Suwinet SO beoordeelt de geanonimiseerde en op naam gestelde rapportages en doet periodiek -zo spoedig mogelijk na afloop van ieder kwartaal- verslag van de bevindingen aan het MT;
- De controleverslagen worden (digitaal) bewaard en de resultaten worden opgenomen in het verslag van de jaarlijkse evaluatie van het vastgestelde beveiligingsplan Suwinet.

Ook kan de Suwinet SO n.a.v. signalen van derden of externen BKWI-rapportages opvragen. Wanneer de Suwinet SO vervolgens mogelijk ongeoorloofd gebruik constateert, bespreekt hij dit met de directeur. De directeur onderneemt zo nodig actie.

Brunssum, 31 augustus 2022
Versie: 1.0

Bijlage 3: Procedure autorisaties

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 drie afzonderlijke deelprocedures die apart kunnen worden uitgevoerd:

- Autorisaties tot Suwinet;
- Periodieke controle autorisaties;
- Toekennen van een tijdelijk wachtwoord.

Met een autorisatie wordt bedoeld het door het bevoegd gezag verstrekken van een gelegitimeerde toegang tot een of meerdere informatiesystemen van ISD BOL.

Om toegang te krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie tevens een bevoegdheid nodig op het netwerk en/of het systeemniveau. Deze laatstgenoemde bevoegdheden worden beheerd door systeembeheer. De bevoegdheden binnen de applicatie Suwinet worden beheerd door de Security Officer.

Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het Dagelijks Bestuur en namens dit Dagelijks Bestuur bij het MT ISD BOL.
De verantwoordelijkheid om toegang te verlenen, de toegang te wijziging of de toegang in te trekken tot de gegevens behorend bij Suwinet berust bij de SO. Het besluit wordt in nauw overleg met het verantwoordelijke afdelingshoofd -van de betreffende medewerker- genomen. Het verantwoordelijke afdelingshoofd voorziet de SO tijdig van de benodigde informatie. De uitvoering hiervan en het up- to-date houden van de procedure ligt bij de Suwinet SO.

Uitvoering

Autorisatie tot Suwinet

- Autorisaties voor Suwinet worden per medewerker/per functie - rol toegekend;
- Het afdelingshoofd verzoekt de Suwinet SO de nieuwe medewerker toegang te verlenen tot Suwinet. Tevens adviseert het afdelingshoofd het autorisatieniveau;
- Bij tussentijdse wijzigingen in taak/functie verzoekt het afdelingshoofd de Suwinet SO, 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;
- Een verzoek aan de Suwinet SO tot toekenning, wijziging of beëindiging gebeurt via het formulier ‘inlichtingenformulier personeel ISD BOL’;

Brunssum, 31 augustus 2022
Versie: 1.0

- Bij akkoord: de Suwinet SO geeft het formulier door aan applicatiebeheer. Deze zorgen vervolgens voor de juiste autorisaties in Suwinet voor de betreffende medewerker;
- De gebruiker krijgt van applicatiebeheer en 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;
- Het wachtwoord voor Suwinet is maximaal 14 dagen geldig indien dit is toegekend door de gebruikersbeheerder (BKWI). Binnen deze termijn moet het wachtwoord worden gewijzigd. Een wachtwoord dat niet is toegekend door de gebruikersbeheerder is 56 dagen geldig.
- Als een gebruiker gedurende 45 dagen achtereen niet heeft ingelogd wordt het wachtwoord automatisch geblokkeerd;
- Na driemaal foutief inloggen wordt het account automatisch geblokkeerd. Alleen de applicatiebeheer kan het account weer vrijgeven.

Periodieke controle autorisaties

- De Suwinet SO controleert (bij voorkeur) ieder kwartaal de actualiteit en rechtmatigheid van de ingevoerde autorisaties. De wijze van controleren is als volgt:
    - De Suwinet SO draait een lijst van gebruikers, gebruikersgroepen en ingevoerde autorisaties voor Suwinet uit;
    - De Suwinet SO maakt een inventarisatie van de gebruikers, gebruikersgroepen en de toegekende autorisaties;
    - Vervolgens controleert de Suwinet SO 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;
    - Voor zover nodig actualiseert de Suwinet SO het gebruikersoverzicht en de gebruikersgroepen.
    - Voor zover nodig informeert de SO het MT.

Bijlage 4: Procedure opvragen en inzage gegevens

Telefonisch opvragen van gegevens door derden

Het uitgangspunt is dat geen telefonische informatie over personen wordt verstrekt. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner heeft het de voorkeur om via Suwinet-mail de gevraagde informatie te verstrekken. Wanneer dit niet lukt dient als volgt te worden gehandeld:
De verzoeker wordt teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien afkomstig van een vast contactpersoon. Het UWV heeft een speciaal telefoonnummer geopend voor medewerkers van Sociale Diensten.

Brunssum, 31 augustus 2022
Versie: 1.0

Bijlage 5: Procedure communicatie over beveiliging

Inleiding

De procedure voorziet in het vastleggen van de communicatie rond het beveiligingsproces. Communicatie over het onderwerp informatiebeveiliging kan plaatsvinden in drie situaties:

- Beveiliging als onderwerp bij de periodieke briefings;
- Beveiligingsonderwerpen bij individuele en functioneringsgesprekken;
- Beveiliging als onderwerp bij informatieverstrekking om het beveiligingsbewustzijn van het eigen personeel te verhogen.

Verantwoordelijkheid

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij de verantwoordelijke, in deze het Dagelijks Bestuur en namens het Dagelijks Bestuur bij de directeur van ISD BOL. De Suwinet SO zorgt er enerzijds voor dat nieuwe ontwikkelingen op het gebied van Suwinet binnen de organisatie bekend worden gemaakt en anderzijds dat de kennis met betrekking tot het gebruik en beveiliging rondom Suwinet bij de medewerkers regelmatig onder de aandacht wordt gebracht. Zodat de medewerkers zich er altijd bewust van zijn dat zij zorgvuldig om dienen te gaan met Suwinet-gegevens.

Ook worden de betrokken medewerkers onder verantwoordelijkheid van de Suwinet SO jaarlijks (via werkoverleg) geïnstrueerd over de mogelijke risico's en (verplichtende) richtlijnen en procedures om schade en incidenten te voorkomen.
De Suwinet SO is verantwoordelijk voor het up to date houden van deze procedure.

Uitvoering

Periodiek werkoverleg
De afdelingshoofden dragen er zorg voor dat op het periodieke werkoverleg het onderwerp beveiliging/ suwinet wordt besproken. Het onderwerp is een vast agendapunt bij elk werkoverleg.

Onderwerpen die aan de orde kunnen komen zijn (niet limitatief):

- De functionaliteit van de beveiligingsprocedures;
- Tekortkomingen, aanpassingen en adviezen op het gebied van regelgeving;
- Attenderen op ongewenste situaties;
- Beveiligingstekortkomingen in operationele handelingen;
- Gevaarlijk of ongewenst gedrag van medewerkers.
- Beantwoorden van vragen en ophelderen onduidelijkheden m.b.t. het gebruik.

Brunssum, 31 augustus 2022
Versie: 1.0

De verslaglegging van de werkoverleggen worden geregistreerd en gearchiveerd in het DMS, Corsa.

Beveiliging bij individuele of functioneringsgesprekken

Iedere medewerker wordt in de gelegenheid gesteld om beveiligingsonderwerpen te bespreken waarvan de inhoud vertrouwelijk of delicaat is. De aangewezen gesprekspartners daarvoor zouden kunnen zijn:

- Het afdelingshoofd;
- De Suwinet SO;
- Een vertrouwensmedewerker (op uitnodiging van de melder).

Het onderwerp beveiliging kan aan de orde komen in de periodieke functionerings-gesprekken:

- De medewerker kan in eerste instantie terecht bij zijn of haar direct leidinggevende, het afdelingshoofd. Daarnaast kan ook rechtstreeks contact worden opgenomen met de Suwinet SO. Beide zijn gehouden de vertrouwelijk verstrekte informatie ook als zodanig te behandelen;
- Vrijwillig verstrekte informatie mag nimmer leiden tot repercussie op de informatie verstrekkende medewerker;
- De Suwinet SO beoordeelt de verkregen informatie en bespreekt deze informatie met het betreffende afdelingshoofd. De informatie en de verstrekker worden daarbij zo deugdelijk mogelijk anoniem gemaakt;
- Individueel verkregen informatie wordt ook op individuele basis teruggekoppeld met de informatie verstrekkende medewerker;
- De Suwinet SO of andere genoemde medewerkers die vertrouwelijke informatie ontvangen handelen naar de aard en inhoud van die informatie.

Bijlage 6: Taakbeschrijving Suwinet Security Officer

Inleiding

Het MT heeft een Suwinet SO benoemd. Deze functionaris is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het Beveiligingsplan, specifiek het beveiligingsplan Suwinet. Hij bevordert de informatie rondom Suwinet en de communicatie naar de medewerkers betreffende dit onderwerp. Het beveiligingsplan Suwinet kan niet los worden gezien van het informatiebeveiligingsplan. In het informatiebeveiligingsbeleid is vastgesteld dat jaarlijks het plan wordt bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses, conform de PDCA-cyclus. Dit betekent dat het beveiligingsplan Suwinet eveneens jaarlijks moet worden geëvalueerd en waar nodig bijgesteld. Dit kan gelijktijdig opgaan met het actualiseren van het informatiebeveiligingsplan. De Suwinet SO zorgt eens per jaar dat evaluatie en mogelijke actualisatie van het beveiligingsplan Suwinet wordt besproken in de overleggroep Informatiebeveiliging Suwinet. Dit kan plaatsvinden in een regulier MT-overleg. De Suwinet SO zorgt voor de input voor dit overleg. Mocht bijstelling van het beveiligingsplan Suwinet noodzakelijk zijn, zal de Suwinet SO zorgdragen voor een aangepast beveiligingsplan en deze ter vaststelling aanbieden aan het ~~MUO~~/MT-overleg en ter kennisname aan het Dagelijks Bestuur.

Taken Suwinet SO

De Suwinet SO:

- Bevordert en adviseert op het gebied van de informatiebeveiliging;
- Controleert of en in hoeverre beveiligingsmaatregelen worden nageleefd;
- Voert periodieke controles uit op een rechtmatig gebruik van Suwinet;
- Doet voorstellen tot implementatie of aanpassing van plannen en werkprocessen op het gebied van de beveiliging;
- Houdt toezicht op het feit dat nieuwe medewerkers (ook extern personeel) worden geïntroduceerd en bekend gemaakt met de beveiligingsprocedures;
- Zorgt voor ondertekening van de zorgvuldigheidsverklaring door nieuwe medewerkers;
- Fungeert als centraal aanspreekpunt op het gebied van informatiebeveiliging en in het bijzonder voor het gebruik van Suwinet;
- Onderneemt actie voor de jaarlijkse evaluatie en het actueel houden van het beveiligingsplan.