Nota voor burgemeester en wethouders
Onderwerp
beveiligingsplan Suwinet gemeente Deventer 2019-2021

Team
DEV-BLD

1- Notagegevens	
Notanummer	2018-002260
Datum	31-12-2018
Programma:	
07 Inkomens-voorziening en arbeidsmarkt	
Portefeuillehouder Weth. Kolkman	

2- Bestuursorgaan	
[X]B & W	19-02-2019
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Kolkman
- Weth. Grijsen	- Weth. Rorink
- Weth. Verhaar	- Weth. Walder

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	19-02-2019	[ ]Besloten	--

Routing	d.d.
programmamanager	12-02-2019
regiemanager	12-02-2019
wethouder	11-02-2019

	par.
[X]adj.secr.	15-02-2019
[X]gem.secr.	13-02-2019
BIS Openbaar	
Status	

Bijlagen
Beveiligingsplan Suwinet gemeente Deventer 2019-2021
Bijlage 1: Specifiek normenkader Afnemers
Bijlage 2: Taakomschrijving Security Officer Suwinet
Bijlage 3: Autorisatiematrix d.d. 10 december 2018
Bijlage 4:Procedure autorisatie tot Suwinet (IDU)
Bijlage 5: Procedure controleren gebruik Suwinet
Bijlage 6: Spelregels gebruik Suwinet
Bijlage 7: 10 gouden tips bij beveiliging van persoonsgegevens
Bijlage 8: Format geheimhoudingsverklaring

B & W d.d.: 19-02-2019

Besloten wordt:
1 Het beveiligingsplan Suwinet gemeente Deventer 2019 vast te stellen.
2 de nota en het besluit openbaar te maken, m.u.v. de bijlage 'authorisatiematrix'.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[ ] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[X] De nota en het besluit openbaar te maken, behalve…
de bijlage 'authorisatiematrix' i.k.v. artikel 10 WOB
[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

gemeente Deventer

Kennisgeving/ Bekendmaking Awb	
Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

ADVIESRADEN:	
Moet een van de adviesraden gehoord worden of op de hoogte gesteld?	Nee

Toelichting

Inleiding

Informatiebeveiliging is de afgelopen jaren steeds belangrijker geworden en ook de komende jaren zal informatiebeveiliging hoog op de agenda's van bestuurders en bij medewerkers uit de uitvoering blijven staan. Met Suwinet hebben uitvoerende teams binnen de gemeente toegang tot persoonsgegevens van hun klanten, bijvoorbeeld als het gaat om het vaststellen of iemand recht heeft op een bijstandsuitkering. Omdat het werken met persoonsgegevens zorgvuldig dient te gebeuren, is het noodzakelijk dat de informatiebeveiliging op orde is. Gemeenten worden hier dan ook streng op gecontroleerd en dienen jaarlijks binnen de ENSIA-verantwoording een collegeverklaring af te geven dat de informatiebeveiliging van o.a. Suwinet op orde is. Daartoe dienen gemeenten voor wat betreft Suwinet te voldoen aan 24 normen. De uitwerking van deze normen en de beschrijving hoe in Deventer wordt omgegaan met informatiebeveiliging van Suwinet, is neergelegd in een zogenaamd beveiliginsplan.

In 2017 voldeed de gemeente Deventer aan de 13 normen waaraan destijds in het kader van informatiebeveiliging moest worden voldaan. Naast de 13 normen waarop Deventer getoetst werd, is ook een aantal speerpunten (intern) opgesteld die in 2017 opgepakt dienden te worden. Dat waren de volgende speerpunten:

- Invoering whitelist
- Beleid telewerken
- Uitbreiding spelregels
- Interne controle
- Logboek/meldingen
- Invoering breder normenkader van 26 normen

Deze acties zijn in 2017 opgepakt; zo is de whitelist op 13 februari 2017 ingevoerd, waardoor medewerkers uit de uitvoering slechts van een deel van de inwoners (namelijk alleen die inwoners waar de gemeente/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad) gegevens kan raadplegen. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde ‘escapefunctie’. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers.
Daarnaast is er binnen DOWR-verband encryptiebeleid vastgesteld waarin ook neergelegd is hoe we omgaan met telewerken. Verder zijn er spelregels opgesteld hoe medewerkers moeten omgaan met Suwinet. Ook hebben er controles plaatsgevonden en zijn er rapportages opgevraagd met betrekking tot de logging van geraadpleegde gegevens. Hieruit zijn geen onregelmatigheden geconstateerd die tot misbruik zouden kunnen leiden. Wel blijft het goed om de medewerkers uit de uitvoering bewust te maken van hun handelingen en hen kritisch te laten kijken naar wanneer zij Suwinet gebruiken of wanneer dit wellicht niet nodig is. Er is een logboek geintroduceerd waarin onregelmatigheden gemeld kunnen worden. In 2017 zijn daar geen meldingen in terecht gekomen. Tot slot zijn we in DOWR-verband gestart om ons voor te bereiden op de invoering van het normenkader van 26 normen. Het onderhavige beveiligingsplan is daar een resultante van.

Beoogd resultaat

Het vastgestelde beveiligingsplan Suwinet gemeente Deventer 2019-2021.

Kader

- ENSIA-verantwoording

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Specifiek Suwinet normenkader Afnemers

Argumenten voor en tegen

Voor

- Met het vaststellen van het Beveiligingsplan Suwinet gemeente Deventer 2019-2021 stelt het college de informatiebeveiliging voor wat betreft Suwinet voor de gemeente Deventer voor de komende 3 jaar vast en voldoet daarmee aan één van de normen van de informatiebeveiliging van Suwinet.
- Het beveiligingsplan Suwinet is in samenwerking met de gemeenten Olst-Wijhe en Raalte tot stand gekomen, zodat er met één kader gewerkt wordt binnen DOWR op het gebied van informatiebeveiliging van Suwinet.

Tegen

- Er zijn geen tegenargumenten te noemen, omdat het hebben van een door het college vastgesteld beveiligingsplan één van de normen is waaraan voldaan moet worden als het gaat om informatiebeveiliging van Suwinet.

Extern draagvlak (partners)

Het beveiligingsplan is in samenwerking met de gemeenten Olst-Wijhe en Raalte tot stand gekomen, omdat op dit thema al veel wordt samengewerkt en het wenselijk was om in gezamenlijkheid tot een nieuw beveiligingsplan te komen.

Financiële consequenties

Geen.

Aanpak/uitvoering

In het beveiligingsplan wordt aangegeven aan welke normen voldaan dient te worden als het gaat om de informatiebeveiliging van Suwinet. Bovendien wordt in het plan teruggeblikt op de resulaten van het jaar 2017. De resultaten over het jaar 2018 zullen in een aparte nota aan uw college worden aangeboden nadat de resultaten over de audit beschikbaar zijn gesteld. Op dat moment zal de raad eveneens middels een raadsmededeling geinformeerd worden over de stand van zaken aangaande informatiebeveiliging van Suwinet en hoe Deventer presteert op dit onderwerp.

Speerpunten voor de informatiebeveiliging van Suwinet in 2019 zullen qua uitvoering de volgende zijn: een diepgaander onderzoek naar de verstrekte autorisaties aan medewerkers (komt hetgeen waar zij op papier voor geautoriseerd zijn overeen met de autorisaties in de praktijk en kloppen de toegekende autorisaties bij de rollen/verantwoordelijkheden die men heeft), diepgaander onderzoek naar gebruik van de whitelist (wanneer en waarom wordt de escape-functie ingezet), wijze van archiveren van persoonsgegevens zowel door medewerkers binnen de uitvoering alsmede het bewaren en verwijderen van opgevraagde (nadere) rapportages bij BKWI waarin persoonsgegevens van medewerkers en klanten staan opgenomen, opstellen onderliggende contracten voor uitvoering Suwinet binnen DOWR-verband.

Beveiligingsplan Suwinet
gemeente Deventer 2019-2021

Deventer, 25 januari 2019

Inhoudsopgave

Hoofdstuk 1 Inleiding

Gemeenten hebben als uitvoerder van diverse wetten en regelingen te maken met veel registraties. Om de efficiency en de effectiviteit te verbeteren worden de laatste jaren steeds meer van die registraties gekoppeld en is samenwerking binnen verschillende ketens noodzakelijk.
De Gezamenlijke elektronische Voorziening Suwinet (GeVS) – vaak afgekort tot Suwinet[1] wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens.

Het Bureau Keteninformatisering werk en inkomen (BKWI), het Werkbedrijf, de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, de Dienst Uitvoering Onderwijs (DUO), de RDW (Rijksdienst voor het wegverkeer) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur. Met de faciliteit Suwinet-Inkijk worden gegevens op basis van Burger Service Nummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers.

Suwinet is tevens het netwerk waarover we de klantgegevens uitwisselen voor het Digitaal Klant Dossier. Belangrijk aspect hierbij is de Wet eenmalige gegevens uitvraag (WEU), in werking getreden op 1 januari 2008. Bij de start van de WEU is vastgelegd dat gegevens niet meerdere malen mogen worden opgevraagd. De klantgegevens die beschikbaar zijn via Suwinet moeten dus optimaal hergebruikt worden.
Suwinet-inkijk is de applicatie die op Suwinet draait. Binnen deze applicatie worden gegevens op basis van het Burgerservicenummer (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens zoals; inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, bijstandsuitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. Binnen Deventer maken de teams Inkomensondersteuning, Publiekscontacten, Belastingen en Deventer Werktalent gebruik van Suwinet.
Suwinet bevat privacygevoelige gegevens. Klanten mogen er op vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi.

1.1 Kader voor het Suwinet beveiligingsbeleid

De Inspectie SZW ging tot en met 2016 uit van zeven essentiële normen voor het waarborgen van de vertrouwelijkheid, opgenomen in het Normenkader Gezamenlijke elektronische Voorzieningen Suwi(GeVS). In het nieuwe “Specifiek Suwinet-normenkader Afnemers 2017” zijn de bestaande normen geactualiseerd.
De normen in het normenkader GeVS 2011 zijn in het kader van het programma ‘Borging veilige gegevensuitwisseling via Suwinet’ tegen het licht gehouden, aangescherpt en in lijn gebracht met de generieke bestaande baselines voor informatiebeveiliging, namelijk de normenkaders van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Rijksdienst (BIR).
Vanwege de omvang zal het “Overzicht Suwinet Normenkader 2017” als afzonderlijke bijlage (**bijlage 1**) worden toegevoegd.

De verantwoording over informatieveiligheid met betrekking tot Suwinet is met ingang van 2017 ondergebracht in de bredere gemeentelijke verantwoording over informatieveiligheid in het kader van ENSIA (Eenduidige Normatiek Single Information Audit). Suwinet is één van de onderdelen waarover de gemeente zich horizontaal aan de gemeenteraad en verticaal aan de (landelijke) toezichthouders verantwoordt. ENSIA is gemeentebreed gebaseerd op de BIG, waardoor vragen breder kunnen spelen dan bij bijvoorbeeld de onderzoeken van de Inspectie SZW, waarin de focus beperkt bleef tot Suwinet.

[1] Soms wordt de term “Suwinet” ook specifiek gebruikt voor de delen die door BKWI worden beheerd. De term “GeVS” omvat dan ook de delen die IB beheert.

Het vernieuwde normenkader Suwinet voor afnemers is integraal binnen ENSIA opgenomen. Waarbij de formulering van de vragen is afgestemd op de gehanteerde structuur en terminologie van de BIG. Op die manier is het voor gemeenten eenvoudig om te voldoen aan de eisen van transparantie en audit. Gemeenten verstrekken via ENSIA informatie aan het ministerie van SZW. Het ministerie van SZW laat vervolgens via de beheerder (BKWI) een geconsolideerde rapportage opstellen, conform het nieuwe normenkader voor afnemers. Vervolgens bundelt BKWI de verantwoording van gemeenten tot een totaal overzicht en rapporteert aan het ketenoverleg GeVS en de minister van SZW.

Er wordt opgemerkt dat informatiebeveiliging de verantwoordelijkheid is van elke gemeente afzonderlijk. De lijnverantwoordelijkheid ligt bij de teams die gebruik maken van Suwinet. Ieder college legt aan de raad verantwoording af inzake informatiebeveiliging. Gezien de DOWR samenwerking kiezen we er wel voor om hier gezamenlijk in op te trekken. Dit betekent dat we het beveiligingsplan gezamenlijk hebben opgesteld en alleen daar waar nodig is aangevuld met gemeentespecifieke informatie.

Eén van de normen is dat het beveiligingsplan eens per drie jaar moet worden geëvalueerd. In overleg met de drie Security Officers en de CISO van de DOWR gemeenten is afgesproken om het beveiligingsplan Suwinet te koppelen aan het nieuwe normenkader Suwinet 2017. Doordat er enige vertraging in het jaar 2018 is opgelopen, geldt het beveiligingsplan vanaf 2019.

1.1.2 Grondslagen waarop Suwinet gebruikt mag worden

Wettelijke grondslagen
Suwinet mag alleen gebruikt worden voor de uitvoering van de Participatiewet, het Bbz, de IOAW en de IOAZ. Daarnaast wordt Suwinet-inkijk gebruikt door de gemeentelijke Belastingdeurwaarders voor het leggen van loonbeslag. Deze taak wordt in DOWR verband uitgevoerd. Medewerkers die de inburgering verzorgen maken via Suwinet gebruik van het Inburgeringsportaal.
RMC's (Regionale Meld- en Coördinatiepunten) gebruikt Suwinet voor hulp aan voortijdig schoolverlaters. Deze taak wordt uitgevoerd door de centrumgemeente Apeldoorn. Ook wordt Suwinet in Deventer en Olst-Wijhe gebruikt door de collega's van de afdelingen Burgerzaken voor het adresonderzoeken in het kader van de BRP (Basis Registratie Personen). Hiervoor is een aparte

Met ingang van 25 mei 2018 is de AVG Algemene verordening gegevensbescherming in werking getreden. Organisaties zijn op grond van de AVG verplicht organisatorische en technische maatregelen te treffen om het gebruik van persoonsgegevens tot een minimum te beperken.
overeenkomst afgesloten.

1.1.3 Beveiligingseisen bij aanname van personeel

Vast personeel
Personeel dat in dienst is bij de gemeente valt direct onder het ambtenarenreg-lement en leggen de ambtseed af. Dit betekent dat zij bij benoeming niet apart een verklaring dienen te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit al opgenomen, vanuit de BIG en andere wet en regelgevingen wordt dit gevraagd.
Wel krijgen medewerkers na hun benoeming een gemeentebrede introductie. Tijdens deze introductie leggen zij een ambtseed af. Als ambtenaar verplicht je je dan onder meer om zaken waarvan je weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim te houden.

Tijdelijk personeel en stagiaires
Personeel dat werkzaamheden verricht bij de gemeente Deventer en niet in een ambtelijk dienstverband is benoemd, ondertekent een geheimhoudingsverklaring en verklaren daarmee, dat zij volgens de gestelde eisen omgaan met privacygevoelige informatie.

1.2 Leeswijzer

Hoofdstuk 2 betreft een overzicht van alle normen, inclusief een beschrijving op welke wij ze in Deventer (en in DOWR-verband) invulling geven aan deze informatiebeveiligingsnormen. Dit hoofdstuk vormt dan ook de kern van dit beveiligingsplan Suwinet. In dit hoofdstuk komen dan ook alle normen aan bod zaols vastgelegd in het Suwinet Normenkader Afnemers 2017, waarbij een onderscheid wordt gemaakt tussen opzet, werking en bestaan van de normen.
In hoofdstuk drie volgt het Beveiligingsplan Suwinet Gemeente Deventer 2018.
Hierna wordt in hoofdstuk 3 aangegeven op welke wijze we het zorgvuldig gebruik (en het monitoren en controleren) willen door ontwikkelen: welke zaken dienen we nog te verbeteren en hoe plannen we deze acties?
Er is een aantal bijlagen toegevoegd zoals het Suwi-normenkader 2017, de taak- en procesomschrijvingen voor de autorisaties en het controleren daarvan. Ook is informatie opgenomen over het veilig gebruik van Suwinet.
Tot slot is in één van de bijlagen een korte evaluatie van het gebruik Suwinet over de jaren 2017 en 2018 opgenomen.

Hoofdstuk 2 Beveiligingsplan Suwinet

Zoals al eerder is aangegeven is met ingang van 1 april 2017 het nieuwe Suwinet-normenkader afnemers van kracht geworden voor gemeenten. Dit normenkader vervangt het Normenkader GeVS2011. De normen in het normenkader GeVS 2011 zijn in het kader van het programma 'Borging veilige gegevensuitwisseling via Suwinet' tegen het licht gehouden, aangescherpt en in lijn gebracht met de generieke bestaande baselines voor informatiebeveiliging, namelijk de normenkaders van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Rijksdienst (BIR).

Bij de totstandkoming van het nieuwe Suwinet normenkader is eerst vastgesteld welke risico's minimaal moeten worden afgedekt. Hierna zijn de normen aangescherpt en opgenomen in het Suwinet-normenkader. De normen zijn in lijn met bovengenoemde baselines. Bij het opstellen van de normen is onderscheid gemaakt welke normen voor welke doelgroep (afnemers, beheerder en bronhouders) van toepassing zijn en is de omvang van de normen waar mogelijk gereduceerd. Daardoor zijn normen die niet van toepassing waren voor gemeenten, bijvoorbeeld ten aanzien van softwareontwikkeling ook niet opgenomen in het nieuwe normenkader. Het resultaat daarvan is dat het aantal normen voor afnemers is terug gebracht naar 26.
Het uitgangspunt van het nieuwe Suwinet Normenkader zijn de generieke bestaande baselines of normenkaders (Bir en Big). De oude Suwinet normen zijn door de "zeef" van de BIG en de BIR gehaald. De normen die al goed door deze baselines worden afgedekt zijn niet in het nieuwe Suwinet normenkader opgenomen.

In het nieuwe Suwinet normenkader zijn de normen onder gebracht binnen een drietal domeinen, namelijk beleid, uitvoering en control.
Verder wordt gesproken over criteria. Een criterium is hetzelfde als een norm. Per criterium (wie en wat) wordt het doel beschreven (waarom) en welk risico het moet afdekken. Vervolgens zijn hier conformiteitsindicatoren aan gekoppeld.
Een conformiteitsindicator kan worden opgevat als een implementatie aanwijzing.

Tot slot wordt opgemerkt dat het vernieuwde normenkader Suwinet vereist dat gemeenten de informatiebeveiliging zodanig inrichten dat wordt voldaan aan de gestelde normen. De verantwoording over Suwinet vindt plaats binnen de ENSIA vragenlijst, aangevuld met een audit op een deel van de normen (in 2017 ging het om 13 normen). In principe leggen we dan ook alleen verantwoording af over deze 13 normen. Echter, in DOWR-verband hebben we uitgangspunt genomen dat we aan alle 26 normen willen voldoen.

Dit hoofdstuk is opgebouwd aan de hand van de 26 normen. Daarbij wordt tevens stilgestaan bij de factoren opzet, bestaan en werking. Dit conform de beoordeling van de auditor.
Daar waar we nog niet (volledig) aan één van de normen voldoen, is dat meegenomen in het hoofdstuk 3 over de doorontwikkeling van de informatieveiligheid omtrent Suwinet, hoofdstuk 3.

2.1 De normen

Het Beveiligingsplan Suwinet is opgebouwd aan de hand van het beleidsdomein, uitvoeringsdomein en het Control domein.

2.1.1 Beleidsdomein

Het beleidsdomein beschrijft in het algemeen beleidsaspecten en -aansluitvoorwaarden voor het gebruik van Suwinet diensten De doelstelling van het "Beleidsdomein" is om aan te geven welke uitgangpunten en sturingsmiddelen er gelden voor het veilig gebruik Suwinet diensten.

B.01 SUWINET-AANSLUITBELEID

Met het informatiebeveiligingsbeleid geeft de organisatie richting aan de te nemen beveiligingsmaatregelen ten behoeve van een veilige dienstverlening conform wet en regelgeving. Een van de verplichtingen heeft betrekking op Suwinet. Het is daarom van belang dat de organisatie expliciet aandacht besteed aan de beveiliging van 'de eigen delen' van Suwinet.

De gemeenten Deventer, Olst-Wijhe en Raalte hebben gezamenlijk het informatiebeveiligingsbeleid opgesteld. Dit beleid is door de afzonderlijke gemeenten vastgesteld, in Olst-Wijhe vastgesteld door het college op 12 september 2017 en bevat het algemene informatiebeveiligingsbeleid.

Daarnaast heeft het college op 21 maart 2017 het Beveiligingsplan Suwinet gemeente Olst-Wijhe 2017 vastgesteld. Hierin is het beleid, specifiek geldend voor Suwinet vastgelegd. Onderhavig plan vervangt het vorige beveiligingsplan Suwinet.

In DOWR-verband hebben de security officers Suwinet afgesproken om gezamenlijk een informatiebeveiligingsplan op te stellen (met daarbij daar waar nodig onderscheid per gemeente). Echter waren de momenten waarop de drie verschillende plannen vastgesteld werden verschillend. Vanaf de vaststelling van onderhavig plan gaan we in DOWR-verband jaarlijks het beveiligingsplan herzien. Het beveiligingsplan wordt door de afzonderlijke colleges vastgesteld.

Daarnaast biedt één gezamenlijk plan ook voordelen voor het beheer van Suwinet: dit wordt door Functioneel Beheer DOWR uitgevoerd voor de drie gemeenten samen. Door gezamenlijk een beveiligingsplan op te stellen, heeft Functioneel Beheer ook slechts te maken met 1 set aan werkafspraken die we op basis van het plan afspreken (in plaats van drie verschillende plannen). Het plan wordt vastgesteld voor 3 jaren; 2019 tot en met 2021.

In dit beveiligingsplan wordt aandacht gegeven aan het stelsel van beveiligingsmaatregelen (het zogenoemde aansluitbeleid). Hierin zijn de taken en verantwoordelijkheden belegd en toegewezen aan daartoe bevoegde medewerkers. In dit beleidsplan zijn de maatregelen voor de beveiliging van de eigen delen van Suwinet beschreven. Het gaat hier om organisatorische, technische en beheersingsmaatregelen. Deze maatregelen zijn passend binnen risicoklasse II/III (is verhoogd tot hoog risico) zoals ook wordt aangegeven in de regeling wet Suwi.

Tot slot wordt in dit plan voor zover van toepassing ingegaan op de taken die zijn uitbesteed.

B.02 NALEVING EN COMPLIANCE AANSLUITBELEID

Gezien de aard van de gegevens die via Suwinet worden uitgewisseld, het uitgevaardigd beleid en wet en regelgeving is het van belang dat de organisatie inzicht geeft in de naleving van het aansluitingsbeleid en andere overeengekomen beveiligingsmaatregelen.
Het aspect compliance richt zich op het naleven van de verplichtingen die voortkomen uit (a) wet- en regelgeving en (b) door de organisatie overeengekomen beleid, richtlijnen, standaarden, en architectuur.

Met de vaststelling van dit beleidsplan zorgen we voor een kader waarmee we een correcte uitvoering en naleving van de beveiligingseisen die passen bij Suwinet borgen.
In dit plan en ook het uitvoeringsplan wordt uitgegaan van de PDCA cyclus.
Op dit moment wordt gewerkt aan de inrichting van de applicatie Key2control die ons ondersteunt in deze cyclus. De uiteindelijke verantwoording wordt afgelegd via ENSIA.

B.03 EXTERNE PARTIJEN

Zowel Bronhouders en Afnemers hebben sommige ICT diensten, vanwege gebrek aan expertise of kostenreductie, uitbesteed aan externe partijen. In deze uitbesteding is de organisatie nog steeds verantwoordelijk voor het verkrijgen van informatie op basis waarvan de organisatie assurance (dan wel transparantie) kan afgeven aan het eigen bestuur en/of aan een toezichthouder.
Voor de uitvoering van een aantal regelingen wordt gebruik gemaakt van externe partijen te weten gemeente Deventer en voor wat betreft de belastingdeurwaarder DOWR.

Deze externe partijen dienen op het juiste niveau beveiligingsmaatregelen te treffen. De afspraken hierover moeten worden vastgelegd in een bewerkersovereenkomst. Dit is nog niet in alle gevallen gedaan en wordt daarom als verbetermaatregel opgenomen in het verbeterplan.

Tabel 1: gebruik Suwinet door externen per gemeente

	SR	RMC	BBZ/IOAZ	Belastingdeurwaarder	Uitkeringsadministratie
Olst-Wijhe	X		X	X	X
Deventer		X		X	
Raalte	X	X	X	X	

B.04 BEVEILIGINGSFUNCTIE SUWINET (GEVS)
Organisatorische en technische veranderingen in de organisatie kunnen invloed hebben op het Suwinet domein binnen de organisatie van de Afnemer. Om in de Suwinetketen effectief om te kunnen gaan met deze veranderingen is het van belang dat de organisatie een Beveiligingsfunctie Suwinet heeft ingericht, daarbinnen zijn de taken en verantwoordelijkheden met betrekking tot de Suwinet aansluiting geformaliseerd.

Voor elke gemeente is er een Security Officer Suwinet aangesteld en aangemeld bij het BKWI. Deze functionaris is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document en bevordert de informatiebeveiliging en de communicatie naar de medewerkers over Suwinet. Er wordt gebruik gemaakt van de kennis én dienstverlening van het BKWI. De taakomschrijving van de Security Officer Suwinet is als **bijlage 2** in dit plan opgenomen.

Het incidentmanagementproces en responsbeleid is beschreven in DOWR verband. Dit document is te vinden op sharepoint; Incident management en responsebeleid

B.05 TAKEN, VERANTWOORDELIJKHEDEN EN FUNCTIESCHEIDING
Binnen de organisatie van de Afnemer worden verschillende type beveiligings- en beheerrollen onderkend. Deze rollen hebben specifieke taken, verantwoordelijkheden en bevoegdheden (TVB's).
De taken binnen het beheer worden verdeeld in verschillende groepen met verschillende functieprofielen. Deze profielen zijn bedoeld om enerzijds tot een effectief takenpakket te komen, anderzijds tot een adequate functiescheiding.

De taken, verantwoordelijkheden en functiescheiding zijn beschreven in de autorisatiematrix.
Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur dat de medewerker de van belang zijnde gegevens kan raadplegen.
De autorisatiematrix is als **bijlage 3** bij dit plan gevoegd.

Minimaal één keer per jaar worden de rollen, taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen geverifieerd en zo nodig geactualiseerd. In de **bijlage 4** procedure autorisaties zijn de verschillende stappen die nodig zijn voor het autoriseren van de personen voor Suwinet en de controle hierop vastgelegd.

Bij signalen over oneigenlijk gebruik van Suwinet wordt opgeschaald naar de betreffende teammanager van het team waar het signaal over het mogelijk oneigenlijk gebruik vandaan komt. De individuele medewerker wordt gevraagd zijn gedrag te verantwoorden. Indien er aanwijzingen zijn voor norm overschrijdend gedrag dan wordt gehandeld volgens het vastgestelde integriteitsbeleid.
Er wordt dan gehandeld conform artikel 16 van de CAR/UWO.
Medewerkers krijgen bij hun aanstelling de spelregels met betrekking tot het gebruik van Suwinet overhandigd (**bijlage 6**) en krijgen zij uitleg over de 10 gouden tips bij beveiliging van persoonsgegevens (**bijlage 7**). Bij hun aanstelling tekenen medewerkers een geheimhoudingsverklaring (**bijlage 8**).

B.06 SUWINET DEEL LANDSCHAP AFNEMERS (ARCHITECTUUR)
Er moet worden vastgelegd welke infrastructurele IT componenten aanwezig zijn en hoe deze met elkaar verbonden zijn. Dit verschaft inzicht in de beveiliging van de GeVs-componenten en overzicht over hun onderlinge samenhang en werking.
De organisatie heeft de actuele documentatie van de technische infrastructuur (het geheel van ICT voorzieningen) vastgelegd. Op dit moment is er niet een concrete architectuurplaat gerelateerd aan Suwinet vastgelegd. Dit punt wordt opgenomen in het verbeterplan.

2.1.2. Uitvoeringsdomein

Binnen het uitvoeringsdomein maken de Afnemers gebruik van voorzieningen die gerelateerd zijn aan specifieke Suwinet-diensten. Hierbij hebben de Afnemers enerzijds een veilige omgeving gecreëerd en anderzijds is deze omgeving zodanig georganiseerd dat zij bij uitbesteding van gedeelten van haar ICT diensten voldoende informatie van haar provider verwerft om aan de verplichtingen van verantwoording en transparantie te kunnen voldoen. Dit zal moeten plaatsvinden onder vastgestelde uitgangspunten en aansluitvoorwaarden die binnen het beleidsdomein zijn gedefinieerd.
De doelstelling van het uitvoeringsdomein is om vast te stellen of wij als Afnemer de afgesproken Suwinet diensten gebruiken conform de uitgangspunten en de aansluitvoorwaarden.

U.01 TPM EXTERNE PARTIJEN
De externe partij, de provider aan wie de Afnemer de ICT diensten heeft uitbesteed in het kader Suwi, verstrekt jaarlijks een assurance verklaring opgesteld door een Third Party Auditor geregistreerd in het register van IT auditors (NOREA), in de vorm van een Third Party Memorandum (TPM) aan de Afnemer. De afnemer verwerkt dit in zijn ICV (in control verklaring).

Op de DOWR infrastructuur wordt geen hosting Suwinet aangeboden. Juridisch gezien is DOWR geen hostende partij voor Suwinet diensten richting gemeente Deventer.
Wat wel telt is de Dienstverleningsovereenkomst, die Deventer met Raalte en Olst-Wijhe heeft over inbesteding van dienstverlening aangaande Bbz, IOAZ, werkzaamheden administratie en sociale recherche. Hierover moet een passage worden opgenomen over Suwinet diensten. Deze overeenkomst is ondergebracht bij het contractmanagement. Dit punt wordt opgenomen in het verbeterplan.

U.02 AUTORISATIE BEHEERPROCES
Het autorisatieproces zorgt ervoor dat autorisaties gestructureerd plaatsvinden. Dit proces bestaat uit sub processen zoals: toekennen (of verlenen), verwerken, wijzigen (intrekken en blokkeren), archiveren en controleren.
Dit is per gemeente vastgelegd in de procedure autorisatie Suwinet. Voor Deventer geldt de IDU-procedure. Deze is toegevoegd in **bijlage 4**.

U.03 TOEGANGSMECHANISME: GEBRUIKERSIDENTIFICATIE- EN AUTHENTICATIE (IA)
Toegang tot Suwinet diensten, bijvoorbeeld inlees-, inkijk- en Suwinet-Mail, wordt gereguleerd door de toegangsmechanismen: identificatie, authenticatie mechanisme en autorisatie.
Gezien de risicoclassificatie van de via Suwinet uitgewisselde gegevens moeten alle handelingen met betrekking tot Suwinet altijd te herleiden zijn naar natuurlijke personen. De handelingen zelf zijn beperkt tot het uitvoeren van acties die voortvloeien uit de opgedragen wettelijke taken. Anders bestaat een risico dat via Suwinet uitgewisselde gegevens onrechtmatig worden verwerkt. Ook kunnen situaties van misbruik ontstaan.
Het BKWI bepaalt de autorisatiemechanisme voor Suwinet-inkijk.
Het algemeen wachtwoordbeleid in DOWR verband is te vinden op sharepoint Wachtwoordbeleid

U.04 TOEGANGSMECHANISME: AUTORISATIE
Na het geautomatiseerde identificatie- en authenticatieproces krijgen gebruikers/beheerders verdere specifieke toegang tot Suwinet diensten. De toegangsbeperking wordt gecreëerd door middel van rollen en toegangsprofielen die voortkomen uit het Suwinet toegangsbeleid en specificaties vanuit de gebruikersorganisatie.

Op basis van functies en rollen is de autorisatiematrix vastgesteld. Dit is de basis waarmee medewerkers toegang hebben tot Suwinet. In de autorisatiematrix is rekening gehouden met doelbinding en proportionaliteit. Zo zorgen we ervoor dat medewerkers alleen die toegangsrechten hebben wat nodig voor de uitoefening van hun functie/wettelijke taak.

U.05 SUWINET-INFORMATIE
Suwinet-informatie betreft de informatie die via Suwinet wordt uitgewisseld en omvat de apparatuur waarmee gegevens verkregen via Suwinet toegankelijk worden gemaakt, zoals werkplekken en mobiele devices. De mobiele devices kunnen buiten eigen locaties gebruikt worden. Gezien het feit dat ketenpartijen risico lopen op imagoschade en aansprakelijkheid is het van belang dat zowel Suwinet-informatie als apparatuur waarop gegevens mogen worden opgeslagen aan strikte beveiligingsvoorwaarden voldoen, conform de ketenarchitectuur.

U.06 CLASSIFICATIE VAN INFORMATIE
Informatie uit authentieke bronnen die door specifieke bronhouders worden beheerd en via Suwinet ter beschikking worden gesteld aan de Afnemers, kennen verschillende risicoklassen. De bepaling van de classificatie t.b.v. de risicoklassen, waaronder gegevens ressorteren, vindt plaats op basis van wettelijke eisen, de waarde en onmisbaarheid voor de organisatie en de gevoeligheid van de gegevens (bijv. persoonsgegevens).

De risicoklasse is nog niet vastgesteld door de bronhouders. Daarmee kan niet aangegeven worden of deze classificatie aansluit.
Gezien onze eigen inschatting van de risicoklasse treffen we als afnemer beveiligingsmaatregelen die passen bij de klasse II/III.

U.07 SUWINET- INLEZEN EN DKD INLEZEN (INLEESFUNCTIONALITEIT)
Met Suwinet- Inleesfunctionaliteit kunnen medewerkers van Afnemers gegevens van diverse bronnen direct in de eigen applicatie inlezen. Het gaat alleen om gegevens die medewerkers nodig hebben voor de uitvoering van hun wettelijke taken. Suwinet-Inlezen maakt de eenmalige gegevens uitvraag en het hergebruik van gegevens mogelijk.

Deze norm is voor de DOWR gemeenten niet van toepassing omdat we geen gebruik maken van de functionaliteit Suwinet inlezen en DKD inlezen.

U.08 SUWINET-MAIL
Suwinet-Mail is een communicatiefaciliteit, in de vorm van een besloten netwerk, dat bestaat uit een centraal- deel en meerdere decentrale delen. Dit biedt gebruikers en aangesloten organisaties de mogelijkheid om vertrouwelijke informatie met elkaar uit te wisselen. Hiermee worden de risico's die zijn verbonden aan het mailen van klantgegevens aanzienlijk verkleind. Op Suwinet-Mail zijn diverse overheidsorganisaties aangesloten.

Suwinet-mail wordt gebruikt voor het uitwisselen van vertrouwelijke informatie. Deze functionaliteit is geïmplementeerd maar hierover is nog geen werkinstructie t.a.v. incidenten bij verkeerd handelen. De verdere uitrol van Suwinet-mail wordt opgenomen in het verbeterplanplan.

U.09 SCHEIDING VAN FACILITEITEN (PRODUCTIEOMGEVING)
Er wordt gebruik gemaakt van de zogeheten OTAP-omgevingen (Ontwikkel-, Test-, Acceptatie- en Productieomgeving). Binnen deze omgevingen worden specifieke activiteiten verricht. Hierbij behoren verschillende verantwoordelijkheden. Deze OTAP-omgevingen kunnen in beheer zijn bij externe providers. In het kader van het gebruik van Suwinet gegevens is het een vereiste dat de Suwinet gegevens slechts via de productie omgeving beschikbaar gesteld moet worden.

U.10 SERVER
Een server is een computer inclusief programmatuur dat diensten verleent aan clients. In de eerste betekenis wordt met server de fysieke computer aangeduid waarop een programma draait dat deze diensten verleent. In de praktijk komen verschillende combinaties van hardware en software (server programma's) voor.
De servers worden beheerd door de beheerders (van de provider). Hiervoor hebben ze vaak speciale bevoegdheden. De servers bieden over het algemeen verschillende functionaliteiten en beschikken vaak over verschillende kenmerken (features) waarmee de gewenste functionaliteiten kunnen worden aangeboden. Het is vanuit beveiligingsoogpunt van belang om de toegang tot servers adequaat te regelen en de niet noodzakelijke features uit te schakelen, te blokkeren of te elimineren. Er is geen Suwinetserver in ons eigen netwerk.

U.11 NETWERKVERBINDINGEN
Suwinet-gegevens worden beschikbaar gesteld via transport kanalen (netwerkverbindingen).
Afnemers hebben netwerkverbindingen zowel naar de Beheerder (BKWI) naar externe partijen (zoals Suwinet-Inlezen en Suwinet-Inkijk) en naar devices (Telewerken).
Er kan onderscheid gemaakt worden in logische en fysieke verbindingen. In het kader van het gebruik van Suwinet gegevens ligt de nadruk op de veiligheid van logische verbindingen. Deze verbindingen moeten voldoen aan specifieke beveiligingseisen zoals geautoriseerde toegangsbeveiliging en encryptie. Encryptie komt tot uitdrukking in de toepassing van een bepaald protocol voor de beveiliging van de verbinding.

Alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld zijn beveiligd tegen ongeautoriseerde toegang. Dit is vastgelegd ons encryptiebeleid, dit document is te vinden op sharepoint Encryptiebeleid (PKI) .

U.12 TELEWERKEN
Het breder en intensiever inzetten van e-dienstverlening, mobiele apparaten en telewerken stelt ketenpartijen in staat aan te sluiten bij de hedendaagse eisen van medewerkers en klanten. Daarnaast werken medewerkers van keten-partijen steeds meer samen met andere overheidsmedewerkers. Mobiele apparaten en netwerken die dit ondersteunen zijn extra gevoelig. Tegelijkertijd zijn de bedreigingen vanuit de buitenwereld toegenomen. Het gevolg van deze twee ontwikkelingen is dat de beveiligingsrisico's voor ketenpartijen groter zijn geworden. Daardoor bestaat meer kans op schade voor de omgeving van de Afnemers. Daarom is het van belang specifieke eisen te stellen aan telewerk voorzieningen.

Het algemeen beleid voor telewerken is vastgesteld en geïmplementeerd.
Voor wat betreft het werken in VMWare horizon (zowel BYOD regeling als Thuiswerken zonder gebruik van DOWR hardware) voldoen we aan de Big richtlijnen en er is een assessment doorlopen. Het betreft een sessie op afstand, waarbij de data in het DOWR domein blijft en de gebruikers middels multifactor authenticatie wordt toegelaten tot de VMWare omgeving.
In de gedragsregels gebruik Suwinet is opgenomen dat Suwinet alleen vanaf een thuisplek mag worden gebruikt in de DOWR omgeving. Daarbij wordt het maken van een afdruk afgeraden.

2.1.3. Control Domein
De Afnemers zullen een adequate beheerorganisatie hebben ingericht, waarin evaluatie activiteiten worden uitgevoerd en beheerprocessen zijn vormgegeven. De evaluatie activiteiten hebben betrekking op de actualisering van beveiligingsbeleid en aansluitingsbeleid. De beheer-en beheersactiviteiten betreffen o.a. evaluatie/beoordeling van aansluitingsbeleid, risicomanagement, beoordeling van toegangsrechten, wijzigingsbeheer, technisch en organisatorische naleving van IAA (identificatie, authenticatie en autorisatie).

C.01 EVALUATIE VAN AANSLUITBELEID
Het is van belang dat de gebruikersomgeving van de Afnemer continue aan de meest actuele beveiligingseisen voldoet. Het kan voorkomen dat op basis van interne of externe ontwikkelingen de aansluitvoorwaarden moet worden aangepast.

Het Suwinet beveiligingsplan wordt jaarlijks geëvalueerd en waar nodig aangepast aan de actuele ontwikkelingen. Onderdeel hiervan is de evaluatie van de uitgevoerde controles en de aandachtspunten die hieruit zijn voortgekomen. Hiervoor wordt een actielijst bijgehouden.
Jaarlijks worden medewerkers tijdens teambijeenkomsten bewust gemaakt van het gebruik van Suwinet.

C.02 RISICOMANAGEMENT
Risicomanagement omvat de activiteiten binnen de decentrale organisatie (Afnemers) die erop gericht zijn om de risico's die gerelateerd zijn 'de eigen delen' van het Suwinet te beheersen.
De risicoklasse is nog niet vastgesteld door de bronhouders. Daarmee kan niet aangegeven worden of deze classificatie aansluit.
Gezien onze eigen inschatting van de risicoklasse treffen we beveiligingsmaatregelen die passen bij de klasse II/III.

Bij de inkoop van onze eigen applicaties en systemen hanteren wij een aantal inkoopvoorwaarden. Hierbij wordt rekening gehouden met de op dat moment geldende beveiligingseisen. Deze inkoopvoorwaarden zijn te vinden op sharepoint Inkoopvoorwaarden en informatiebeveiligingseisen.

C.03 WIJZIGINGENBEHEER
Wijzigingenbeheer richt zich op het zodanig doorvoeren van wijzigingen in ICT-middelen en ICT-diensten (in relatie tot Suwinet) dat de kans op verstoring van de dienstverlening wordt geminimaliseerd en deze dienstverlening blijvend voldoet aan de functionele en beveiligingseisen van belanghebbenden. Wijzigingenbeheer is een ITIL proces, dit is belegd bij DOWR-I.

C.04 BEOORDELING VAN TOEGANGSRECHTEN
Het is nodig om de toegangsrechten van gebruikers/beheerders regelmatig te beoordelen om de toegang tot Suwinet diensten doeltreffend te kunnen beheersen. De toekenningen, wijzigingen en gebruik van toegangsrechten tot Suwinet dienen daarom periodiek gecontroleerd te worden.

De toekenningen, wijzigingen en gebruik van toegangsrechten tot Suwinet worden periodiek gecontroleerd. Dit is vastgelegd in de procedure autorisatie Suwinet (**bijlage 4**) en de Procedure controle gebruik Suwinet (**bijlage 5**).
De autorisatiematrix maakt onderdeel uit van dit beveiligingsplan (**bijlage 3**) en wordt daarmee minimaal jaarlijks geëvalueerd en waar nodig aangepast.

C.05 LOGGING
Logging is het proces voor het registreren van technische activiteiten en gebeurtenissen. Hiermee kunnen achteraf fouten of rechtmatigheid van het gebruik van en ook vroegtijdige ongeautoriseerde toegangspogingen tot Suwinet diensten worden gesignaleerd.
Het BKWI logt alle handelingen die in Suwinet plaatsvinden.
De generieke en specifieke rapportages worden maandelijks opgevraagd.
De wijze waarop deze gecontroleerd worden is beschreven in de procedure controleren gebruik Suwinet (**bijlage 5**)

De rapportages die worden opgevraagd worden momenteel maximaal twee jaar bewaard op de G-schijf.

C.06 MONITORING EN RAPPORTAGE
Onder monitoren wordt verstaan: signaleren, analyseren en rapporteren. In het kader van Suwinet is het begrip bijsturen hieraan toegevoegd.
Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot Suwinet diensten en ongeautoriseerd gebruik van deze diensten tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris.

De activiteiten zijn vastgelegd in de procedure controle gebruik Suwinet. Hierin zijn ook de normen opgenomen waaraan getoetst wordt. Daar waar nodig wordt bijgestuurd, deze acties worden vastgelegd op de actielijst.

C.07 EVALUATIE VAN IAA RAPPORTAGES (ORGANISATORISCH EN TECHNISCH)
In het Suwinet domein is het veilig inrichten en beheersen van identificatie, authenticatie en autorisatie (IAA) voor het gebruik van Suwinet diensten essentieel. Het is van belang om op basis van rapportages verkregen vanuit deze technisch en organisatorische invalshoeken te evalueren of er zich geen afwijken in de IAA beheersingsproces voordoen en of er structurele maatregelen noodzakelijk zijn.

Er wordt maandelijks een controle uitgevoerd. Per kwartaal volgt een rapportage aan het management met daarin opgenomen de verbeteracties. Een kopie van deze rapportage wordt naar de CISO gestuurd. Dit is opgenomen in de procedure controle gebruik Suwinet. De verantwoording aan het college en gemeenteraad gaat middels de ENSIA.

C.08 TRANSPARANTIE RAPPORTAGE
Transparantie en verantwoording zijn instrumentele functies ten behoeve van besturing. Het zijn relaties tussen Principal (Bestuurder) en Agent (Uitvoerder). Afnemers en Bronhouders hebben te maken met Transparantie- en/of Verantwoordingsfunctie.

Als gemeenten hebben wij onze verantwoording ingericht volgens de ENSIA lijn. En daarmee is de transparantie ingevuld. De beheerder (BKWI) kan van de ENSIA-verantwoording/controleverklaring gebruikmaken.

Hoofdstuk 3 Doorontwikkeling Suwinet

Zoals benoemd willen we in gemeente Deventer aan alle 26 normen gaan voldoen. Om dit te realiseren willen we in DOWR-verband de informatieveiligheid omtrent het gebruik van Suwinet door ontwikkelen. We spreken van een doorontwikkeling omdat we alle normen in scope hebben, alleen nog niet op alle gebieden 100% voldoen. Om dit te organiseren is onderstaand overzicht opgesteld. Zo hebben we inzichtelijk welke acties uitgezet zijn en welke zaken nog verder opgepakt moeten worden. We blijven dit gedurende het jaar monitoren (indien nodig terugkoppelen via de periodieke controlerapportages).

In onderstaande tabel zijn alle uit te voeren verbeteracties opgenomen, waarbij is aangeven wie op dit moment actiehouder is.
Opdrachtgever: Security Officer Suwinet
Opdrachtnemer: Projectgroep Suwinet

Norm	Omschrijving	Actiehouder	Uitvoerder	Status
B03	Waar liggen samenwerkingen vast? Hiervoor moeten verwerkersovereenkomsten worden opgesteld.	Security Officers DOWR (signaleringsfunctie) in samenwerking met Management betreffende onderdelen	Nader te bepalen	Format verwerkersovereenkomst is reeds verstrekt, opsteller moet aangewezen worden
U01	Check of er een TPM van de externe partijen aanwezig is/noodzakelijk is.	Contractmanagement DOWR Arjan Besselink	DOWR DOWR-I	Vraag uitgezet in interne memo aan DOWR-I d.d. 28 juni 2018 Melding in zelfservicedesk aangemaakt (verzoek DOWR-breed)
U05	Suwinet Informatie vastgelegd in algemeen DOWR-stuk m.b.t. mobile devices?	Arjan Besselink	DOWR-I	Vraag uitgezet in interne memo aan DOWR-I d.d. 28 juni 2018
U8	Suwinet-mail moet onder de aandacht gebracht worden bij medewerkers en er moet een werkinstructie komen t.a.v. incidenten bij verkeerd handelen. De technische zaken zoals het doorsturen van externe mail, viruscontrole, exclusieve toegang, open-mail-relay zal nog wel moeten worden gecheckt.	Security Officers DOWR	DOWR-I	Vraag uitgezet in interne memo aan DOWR-I d.d. 28 juni 2018
C03	Wijzigingenbeheer	Security Officers DOWR	Arjan Besselink en Wouter Franken	Vraag uitgezet in interne memo aan DOWR-I d.d. 28 juni 2018

C05	Wat moet de bewaartermijn van de rapportages worden en waar kunnen we deze opslaan?	Security Officers DOWR	Eric Grotenhuis	Mogelijkheid om dit in Key2Control te doen onderzoeken. Voorlopig op afgeschermde delen Sharepoint en/of G:schijf

Hoofdstuk 4 Evaluatie gebruik Suwinet

In voorgaande hoofdstukken hebben we voornamelijk vooruit gekeken: wat zijn alle normen waar we aan moeten voldoen, hoe organiseren we dit (ook in de toekomst) en waar moeten we nog verbeteren? Maar om effectief en efficient stappen vooruit te kunnen zetten, is het ook erg belangrijk om terug te blikken op de voorgaande periode. Eén van de normen om zorgvuldig gebruik van Suwinet te borgen, is dan ook het evalueren van het oude beveiligingsplan en hierbij ook de bevindingen van de uitgevoerde controles in mee te nemen.
Een logisch vertrekpunt om naar terug te blikken, is dan ook de ENSIA verantwoording in 2017. Wanneer we immers niet zouden voldoen aan de ENSIA-normen voor Suwinet, zou dit logischerwijs ook het vertrekpunt zijn in de te ondernemen acties voor een volgend jaar. Na deze start, kijken we in de rest van hoofdstuk 4 naar de bevindingen van de uitgevoerde controles en beschrijven we in hoofdlijnen op welke wijze we het zorgvuldig gebruik van Suwinet de afgelopen periode in de organisatie hebben opgepakt.

4.1 Terugblik op verantwoording ENSIA 2017

In de verantwoording over het jaar 2017 gaat het om 13 normen waarover de gemeente zich heeft verantwoord door middel van een door het college ondertekende verklaring. Deze is door de Register EDP-Auditor/RE getoetst. Deze 13 normen zijn onder andere gebaseerd op de “bekende” 7 normen zoals de inspectie die in voorgaande jaren toetste en enkele normen die uit de onderzoeken van de Autoriteit Persoonsgegeven (AP) naar voren zijn gekomen.

Norm	Beschrijving norm	Toelichting norm	Zelf evaluatie oordeel	Externe audit oordeel
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet.	VOLDOET	VOLDOET
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	Het voorkomen dat risico’s optreden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet.	VOLDOET	VOLDOET
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.	VOLDOET	VOLDOET
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor	Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken.	VOLDOET	VOLDOET

	Suwinet tijdig wordt uitgevoerd.			
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten.	VOLDOET	VOLDOET
U.11	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten.	VOLDOET	VOLDOET
C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau	VOLDOET	VOLDOET
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden.	VOLDOET	VOLDOET
C.05	Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.	Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen.	VOLDOET	VOLDOET
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).	Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie.	VOLDOET	VOLDOET
C.07	De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	Bewerkstelligen dat zich geen leemtes in de beveiliging van IAA (Identificatie, Authenticatie en Autorisatie) mechanismen voordoen.	VOLDOET	VOLDOET

Zoals uit bovenstaand overzicht blijkt, voldeden we in 2017 aan de 13 normen. Op basis dit overzicht concluderen we dan ook dat we op het gebied van informatiebeveiliging op de juiste weg zijn binnen de gemeente Deventer. Het geeft aan dat we het zorgvuldig gebruik van Suwinet voldoende binnen de organisatie geborgd hebben en biedt nu dan ook de mogelijkheid om verdere doorontwikkeling (op basis van bestaande normen) te gaan realiseren.

4.2 Evaluatie gebruik Suwinet

In deze paragraaf wordt verder ingezoomd op het gebruik van Suwinet in Deventer in 2017, de autorisaties en de beoordeling van de rapportages gebruik Suwinet.

Aanleiding
In 2015 is een projectgroep voortvarend aan de slag gegaan om de informatiebeveiliging van Suwinet op niveau te krijgen. Er is in die periode ook een Security Officer Suwinet aangesteld, die belast is met de uitvoering van een aantal taken, welke beschreven zijn in de 'Procedure veilig gebruik en beheer Suwinet'. Eén van die taken is om een jaarlijks een rapportage tbv de Chief Information Security Officer (CISO) op te stellen waarin de volgende zaken aan de orde komen:

- de uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken en toetsingen
- aanwezigheid van onverenigbare rollen;
- frauduleus gedrag van medewerkers of niet volgen van procedures;
- geconstateerde tekortkomingen in de beveiligingsvoorzieningen ;
- wijziging van procedures / afspraken / opvolgingspatroon;
- het handelen in afwijking met de vastgelegde functiescheiding;
- afwijkingen of wijzigingen op volgens de toegestane rol toegekende autorisaties.

Bovenstaande punten zijn verwerkt in de terugblik 2017 die hieronder opgenomen is. Daarnaast zijn deze punten ook als zodanig meegenomen in de ENSIA-verantwoording waar wij als Deventer goed op hebben gescoord.

Aandachtspunten voor 2017
In de jaarrapportage Suwinet over 2016 hebben wij aangegeven welke aandachtspunten wij voor 2017 zagen. Dit waren de volgende punten:

- Invoering whitelist
- Beleid telewerken
- Uitbreiding spelregels
- Interne controle
- Logboek/meldingen
- Invoering breder normenkader van 26 normen

Terugblik 2017
Hieronder staat per onderwerp beschreven wat we als projectgroep in 2017 gedaan hebben.

<u>BKWI-rapportages en onderzoeken</u>
Maandelijks[2] komt onze projectgroep Suwinet bijeen om de BKWI-rapportage van de voorgaande maand te bespreken en te analyseren. Dit doen we aan de hand van door onszelf vastgestelde normen. Komen we boven die normen, dan zullen we extra onderzoek doen. Dit geldt ook voor zaken die opvallen in de BKWI-rapportages. Opvallende zaken kunnen ook leiden tot nader onderzoek. Nader onderzoek houdt in dat we nadere rapportages bij BKWI opvragen.
De agenda's, verslagen en BKWI-rapportages worden op sharepoint op een besloten omgeving opgeslagen.

[2] Alleen in de maanden juli en september is de projectgroep Suwinet niet bijeen geweest ivm vakanties.

Nadere rapportages
In 2017 hebben we verschillende nadere rapportages opgevraagd. Bij BKWI is geregistreerd dat Peter Groot degene is die deze rapportages opvraagt. In een aantal gevallen is een gesprek gevoerd met een aantal medewerkers niet zozeer omdat sprake was van mogelijk misbruik, maar wel in het kader van bewustwording waarbij het voor een aantal medewerkers onbekend was dat iedere switch tussen pagina's op Suwinet apart wordt gelogd. Daarnaast zijn nadere rapportages opgevraagd in het kader van het aantal geblokkeerde accounts en de meest geraadpleegde BSN's per gebruiker.

Bijeenkomsten, workshops trainingen
Op 20 april 2017 heeftde Security Officer Suwinet deelgenomen aan een bijeenkomst die door BKWI is georganiseerd in het kader van 'gerichte controle'. Daarbij werd ingegaan op de ins en outs over de (nadere) rapportages om controles zo gericht mogelijk uit te voeren door het interpreteren van cijfers en op welke manier risicovol gedrag uit de rapportages gehaald kan worden. Tot slot heeft de Securuty Officer Suwinet deelgenomen aan meerdere webinars die vanuit de VNG werden georganiseerd in het kader van het voorkomen van oneigenlijk gebruik en invoering van het nieuwe normenkader.

Bewustwording
Op 30 januari 2017 zijn de medewerkers van Publiekszaken Zorg en op 15 februari 2017 zijn de medewerkers van het Jongerenloket geïnformeerd over de informatiebeveiliging van Suwinet.
Hiervan zijn korte verslagen beschikbaar en zijn op de besloten sharepoint omgeving opgeslagen.
Daarnaast is de e-learningsmodule van de VNG bij medewerkers onder de aandacht gebracht. Een aantal medewerkers heeft deze e-learningmodule gevolgd.
Tot slot weten medewerkers de leden van de projectgroep goed te vinden als zij twijfels of vragen hebben bij het mogen raadplegen van Suwinet.

Geheimhoudingsverklaringen
Iedere nieuwe medewerker (ingehuurd of in dienst van de gemeente) die een autorisatie krijgt om persoonsgegevens te raadplegen in Suwinet, krijgt bij de start in de nieuwe functie uitleg over het gebruik van Suwinet en de informatiebeveiliging daaromtrent. Daartoe wordt een geheimhoudingsverklaring ondertekend en legt het projectgroeplid - dat vanuit de uitvoering aan het projectgroepoverleg Suwinet is afgevaardigd – aan de nieuwe medewerker uit wat de spelregels zijn. De spelregels worden tevens op schrift overhandigd aan de nieuwe medewerker. In 2017 zijn de spelregels herzien en aangevuld.

Website
In het kader van bewustwording is een interne webpagina via intranet gemaakt om medewerkers op de hoogte te brengen en te houden aangaande de informatiebeveiliging van Suwinet. Hierop staat bijvoorbeeld het beleidsplan en de spelregels waaraan medewerkers zich dienen te houden.
Verder worden op een afgeschermde intranetpagina alle stukken van de projectgroep Suwinet geplaatst zoals agenda's, notulen, de IDU-lijsten en geheimhoudingsverklaringen.

Domeinen Burgerzaken en Belastingdeurwaarder
Op 20 december 2017 is door de directie van de gemeente Deventer besloten dat de Suwinet-domeinen Burgerzaken en Belastingdeurwaarder eveneens onder de verantwoordelijkheid vallen van de Security Officer Suwinet die zich bezig houdt met de informatiebeveiliging van Suwinet op het domein Werk en Inkomen. Dit betekent dat de informatiebeveiliging van Suwinet ook voor de domeinen Burgerzaken en Belastingdeurwaarder in de PDCA-cyclus op orde wordt gebracht, net zoals we hebben gedaan en nog altijd doen voor het domein Werk en Inkomen.

Whitelist

Voor het gebruik van Suwinet-Inkijk dienen medewerkers te zijn geautoriseerd. Daarmee is de toegang tot gegevens beperkt tot personen die uitvoering geven aan bovengenoemde wettelijke taken. Nadat deze toegang is verleend, kunnen geautoriseerde medewerkers in principe gegevens opvragen van iedereen die in Nederland woonachtig is. Dat betreft dan ook inwoners waar geen dienstverleningsrelatie mee is op basis van de gemeentelijke wettelijke taken. De gegevensraadpleging is dus niet begrensd tot de 'eigen' inwoners. Dit is onwenselijk omdat dit kan leiden tot het raadplegen van gegevens van inwoners waar geen dienstverleningsrelatie mee is. Om dit tegen te gaan en om het raadplegen van gegevens te begrenzen tot die 'eigen' inwoners, is het mogelijk om binnen Suwinet-Inkijk gebruik te maken van een filtermechanisme. Dit filtermechanisme is vormgegeven als een zogenaamde 'whitelist'. Een whitelist is een lijst die de BSN's bevat van alleen die inwoners waar de gemeente/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde 'escapefunctie'. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers.
Vanaf 13 februari 2017 wordt in Deventer met deze functie gewerkt.
In de generieke rapportage over 'gebruik escapefunctie' is te zien hoe vaak de escapefunctie is gebruikt, hoeveel pagina's daarvoor zijn geraadpleegd en met welke reden. In deze rapportages staan geen herleidbare gegevens naar BSN's of accounts, daarvoor moet een specifieke rapportage worden opgevraagd.

De specifieke rapportage bevat wel tot personen herleidbare gegevens. In het geval van de escapefunctie, is te zien welke medewerker op welk moment een BSN heeft benaderd via de escapefunctie, dat niet in de whitelist staat. Ook is te zien welke pagina's zijn bezocht en wat de reden was (één van de vijf beschikbare redenen);
Escape met reden: Anders
Escape met reden: Bijzonder onderzoek
Escape met reden: Nieuwe klant of aanvraag
Escape met reden: Vaststellen onderhoudsbijdrage
Escape met reden: Inkomsten 16- en 17-jarigen.

Er is in december 2017 een nadere rapportage opgevraagd inzake het gebruik van de zoekfunctie 'anders'. Gebleken is dat deze functie regelmatig wordt gebruikt. In 2018 zal een onderzoek uitgevoerd worden waarbij wordt gekeken of de geraadpleegde BSN's vanuit de whitelist voorkomen in de BPR of GWS (uitkeringssysteem).

Beveiligingsplan

Het beveiligingsplan Suwinet is in 2016 opnieuw vastgesteld. Besloten is om in 2017 het plan niet opnieuw vast te stellen, omdat er een nieuw beveilingsplan in DOWR-verband opgesteld zou worden. Echter door de komst van de ENSIA en het werk dat daarmee gepaard ging, is in DOWR-verband besloten om dit gezamenlijke beveiligingsplan in 2018 op te stellen.

IDU

Maandelijks wordt de in-uit-en-doorstroomlijst opgesteld en afgetekend door de verantwoordelijk teammanager. Op die manier wordt bijgehouden of er nieuwe autorisaties moeten worden toegekend aan nieuwe medewerkers, of dat verstrekte autorisatie bijgesteld moeten worden als gevolg van het doorstromen van een medewerker naar een andere functie of dat bepaalde autorisaties moeten worden beëindigd in verband met het vertrek van een medewerker. Op deze manier houden we grip op het aantal geblokkeerde accounts en zorgen we ervoor dat een medewerker niet langer in Suwinet kan als hij dit ook niet meer voor de uitoefening van zijn werkzaamheden nodig heeft. Daarmee wordt misbruik voorkomen.

Autorisaties
De autorisaties zijn vastgelegd in onze autorisatiematrix. Deze is in 2017 twee keer herzien; in februari en in oktober. De autorisatiematrix is terug te vinden op het besloten gedeelte van sharepoint. Met ingang van 2017 is de zogenaamde 'fijnmaziger autorisatie' doorgevoerd. Dit houdt in dat nog meer wordt gekeken wat iemand aan autorisatie echt nodig heeft voor de uitvoering van zijn/haar taak. Een fijnmaziger autorisatiestructuur bevordert 'proportionaliteit van gegevenslevering' en gaat daarmee overmatig gegevensgebruik tegen. Daarom heeft BKWI een aantal wijzigingen doorgevoerd met betrekking tot hetgeen medewerkers in een bepaalde rol binnen Suwinet kunnen raadplegen.

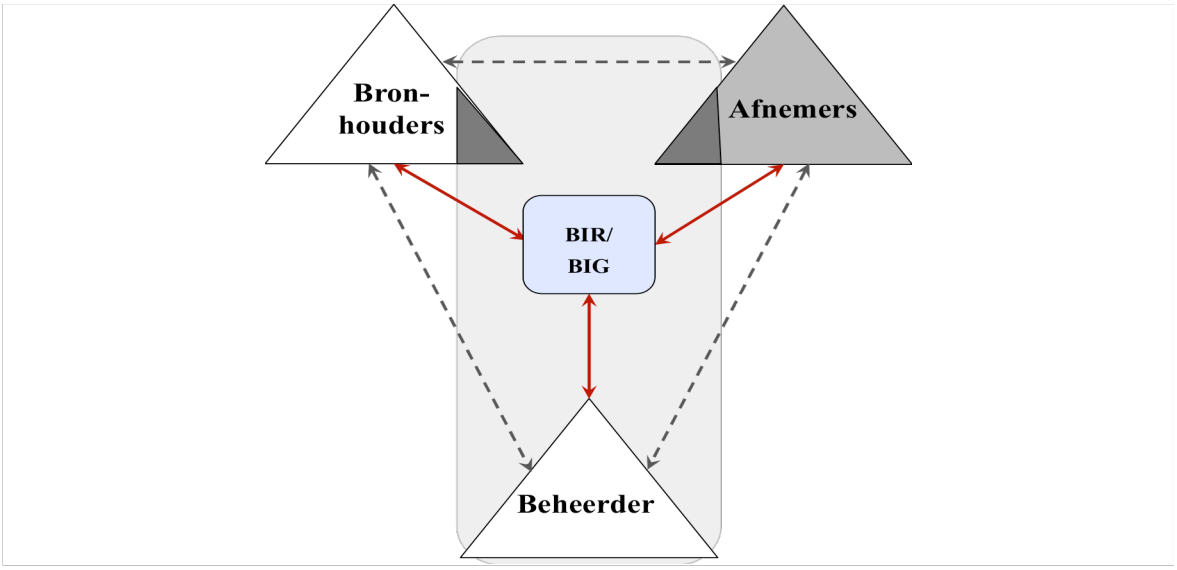
Zodra er wijzigingen in de accounts/autorisaties doorgevoerd moeten worden, dan wordt met het opstellen van de nieuwe IDU-lijst een verzoek naar Functioneel Beheer verstuurd om de wijziging door te voeren. We krijgen dan per mail een bevestiging als de wijziging is doorgevoerd. Voorbeelden van mails zijn op de besloten sharepoint site te vinden.

Single sign on
Binnen de projectgroep zijn we bezig geweest om te kijken of we één login voor samenwerkingsverbanden konden realiseren. Dit is met name handig voor medewerkers die voor Olst-Wijhe en/of Raalte werkzaamheden uitvoeren, zoals de sociaal rechercheurs. Op die manier kan voorkomen worden dat vanuit het 'verkeerde' account gegevens van klanten van een specifieke gemeente worden opgezocht. Wij hebben ons daarvoor aangemeld bij BKWI, maar helaas is er bij BKWI vertraging opgetreden in de uitrol van deze functionaliteit, waardoor het nog niet mogelijk is om deze zogenaamde single sign on konden doorvoeren.

Logboek
Er is een logboek ontwikkeld dat inzicht moet bieden aan de mogelijke incidenten die zich in de organisatie voordoen. In 2017 hebben zich geen incidenten voorgedaan, waardoor het logboek nog niet gevuld is. Daarnaast is er een aparte gemeentebrede meldknop aangemaakt voor het melden van incidenten op het gebied van informatiebeveiliging, waaronder voor Suwinet.

Conclusie
Er is over de periode januari 2017 tot 31 december 2017 (voor zover na te gaan) geen onrechtmatig gebruik gemaakt van Suwinet inkijk. Dit wordt ook bevestigd in de ENSIA-verantwoording 2017. De gemeente Deventer voldoet aan de gestelde normen die voor de informatiebeveiliging van Suwinet gesteld worden.
De invoering van de whitelist en het doorvoeren van de fijnmaziger autorisatie is daarbij zeer van belang geweest. Daardoor krijgen de daartoe bevoegde personen alleen die gegevens van klanten te zien die nodig zijn voor de uitvoering van de wettelijke taken.

Specifiek Suwinet-normenkader Afnemers 2017



Bronhouders

Afnemers

Beheerders

Versie 1.01

Voorwoord

De Gezamenlijke elektronische Voorziening Suwinet (GeVS) – vaak afgekort tot Suwinet[1] - wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. Binnen de Suwiketen participeren drie type stakeholders: Bronhouders, Beheerder van de centrale omgeving en Afnemers. De Bronhouders stellen (authentieke) gegevens beschikbaar aan Afnemers. De Afnemers hebben deze gegevens nodig voor de uitvoering van hun wettelijke taken. De Beheerder van de centrale omgeving zorgt voor de routering van deze gegevens op basis van technische en communicatie faciliteiten en IT componenten. Deze faciliteiten en IT componenten representeren het zogeheten Suwinet.

De GeVS en de informatie die via GeVS wordt uitgewisseld dienen te voldoen aan specifieke beveiligingseisen en aan de WBP. De beveiliging van GeVS kan in volle omvang alleen worden gerealiseerd wanneer de ketenpartijen gezamenlijk, ieder vanuit hun eigen verantwoordelijkheid, de juiste beveiligingsmaatregelen treffen.

Voor een adequate werking en bescherming van GeVS zijn ketenafspraken noodzakelijk op het gebied van uitgangspunten en randvoorwaarden, wijze van implementatie, beheersen en het geven van wederzijds inzicht omtrent deze afspraken. De ketenafspraken staan dan ook in het teken van de beveiligingsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Het doel van deze afspraken is een passend beveiligingsniveau van de keten te garanderen.

Om vast te stellen of de GeVS voldoet aan het afgesproken beveiligingsniveau is door de werkgroep 6 een integraal normenkader ontwikkeld dat gerelateerd is aan BIR, BIG en GeVS. Op basis van specifieke Suwinet-diensten zijn beoordelingsobjecten geselecteerd en vanuit de optiek van GeVS nader gespecificeerd. Hiernaast zijn enkele aanvullende beoordelingsobjecten in dit Suwinet-Normenkader opgenomen. Zo zijn in dit normenkader verantwoordings- of transparantie aspecten voor de Afnemer opgenomen om inzicht te geven over de sturing, implementatie en beheersingsaspecten van de gebruikte Suwinet diensten aan de ketenpartijen.

Vooralsnog bevat dit normenkader controls/normen gericht voor de Afnemer. Naderhand zullen controls/normen voor de Bronhouders en de Beheerder (BKWI) worden toegevoegd of separaat volgens dezelfde structuur worden ontwikkeld. Na de ontwikkeling van overige twee normenkaders kan worden besloten de drie normenkaders te integreren in één normenkader of separaat te houden.

Het is van belang om jaarlijks het normenkader op basis van vigerende wettelijke eisen en bedrijfseisen te evalueren en te actualiseren. De verantwoordelijkheid hiervoor ligt bij de gezamenlijke Suwi-partijen, het faciliteren van de uitvoering van deze verantwoordelijkheid zal gedaan worden door BKWI conform artikel 62 lid 2 van de wet SUWI.

Dit document beperkt zich vooralsnog tot het Afnemersdomein.

[1] Soms wordt de term “Suwinet” ook specifiek gebruikt voor de delen die door BKWI worden beheerd. De term “GeVS” omvat dan ook de delen die IB beheert.

INHOUDSOPGAVE

Onderwerp	:	*Referentiekader voor Suwinet, verantwoordelijkheidsdomein Afnemers*
Datum	:	*3 april 2017*
Uitgebracht aan:	:	*Ketenoverleg*

Uitwerking door:

Naam	**Organisatie**
Koen Wortmann	VNG
Kees Hintzbergen	IBD
Jan Breeman	BKWI
Peter de Witte	SVB
Martijn van den Berg	SVB
Joseline van Tessel	UWV
Rob Roukens	UWV
Wiekram Tewarie	UWV

Historie en versie

Versie	**Datum verzending**	**Doel verzending**	**Naam**	**Status**
Versie 0.1	19 november 2015	Review en Bespreking	Jan Breeman Wiekram Tewarie	Concept Werkdocument
Versie 0.2	20 november 2015	Review en Bespreking	Rob Roukens Wiekram Tewarie	Concept Werkdocument
Versie 0.3	23 november 2015	Review en Bespreking	Kees Hintzbergen Wiekram Tewarie	Concept Werkdocument
Versie 0.4	24 november 2015	Review en Bespreking	Peter de Witte, Jan Breeman en Wiekram Tewarie	Concept Werkdocument
Versie 0.6	1 december 2015	Review en Bespreking	Joseline van Tessel en Wiekram Tewarie	Concept Werkdocument
Versie 0.9	8 december 2015	Bespreking	Werkgroep	Concept
Versie 0.91	29 december 2015	Detail aanpassing op verzoek	Wiekram Tewarie	Concept
Versie 0.99	juli 2016	Tekstuele aanpassing	Koen Wortmann, Peter van der Zwan en Wiekram Tewarie	Concept
Versie 0.1	September 2016	Tekstuele aanpassing en verwerking commentaar SZW	Rob Roukens, Kees Hintzbergen en Wiekram Tewarie	Concept
Versie 1.0	9 maart 2017	Goedkeuring door Ketenoverleg	Marc Woltering	Definitief
Versie 1.01	4 april 2017	Aanpassing titelblad	Marc Woltering	Definitief

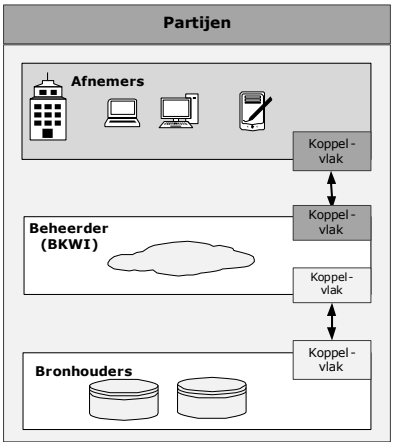
1. Inleiding

1.1. Organisatie GeVS

De Gezamenlijke elektronische Voorzieningen Suwi (GeVS) zijn voorzieningen waarin drie type partijen participeren: Bronhouders, Beheerders van de centrale (BKWI) en decentrale (Inlichtingenbureau) omgeving en Afnemers.

- *Bronhouders* – Bronhouders zijn de partijen die - ten behoeve van Afnemers - authentieke gegevens beschikbaar stellen aan de Beheerders via de centrale omgeving. De bronhouders vormen de zogeheten leveranciers van gegevens, zoals UWV, SVB en de Gemeenten, BRP, RDW, Kadaster, HR (KvK).
- *Beheerders* - Beheerder van de centrale omgeving (BKWI) is de partij die - conform de ketenafspraken en –standaarden zorg draagt voor het beschikbaar stellen van de centrale omgeving Suwi en voor de transformatie, autorisatie, transport en verdere routering van gegevens/berichten.
  Hiertoe stelt de Beheerder van de centrale omgeving instrumenten, zoals applicaties beschikbaar. De Beheerder van de centrale omgeving is BKWI.
  De Beheerder van de decentrale omgeving[2] (IB) is de partij die voor de routering van 'berichten-op-maat' tussen de centrale omgeving en de gemeenten zorg draagt, gegevens van de gemeenten verzamelt en als Bron voor de uitwisseling van gegevens met de ketenpartijen fungeert. Hiertoe stelt de Beheerder van de decentrale omgeving instrumenten (voorzieningen en applicaties) beschikbaar. De Beheerder van de decentrale omgeving is Inlichtingenbureau.
- *Afnemers* - Afnemers zijn de partijen die via de GeVS - voor hun bedrijfsvoering en uitvoering van hun wettelijke taken - gegevens betrekken uit gegevensbronnen van bronhouder.

Figuur 1 geeft de relaties tussen de partijen weer. Iedere partij heeft vanuit haar eigen perspectief de verantwoordelijkheid om adequate beveiligingsmaatregelen te treffen voor de beveiliging van het koppelvlak met de GeVS dat onderdeel uitmaakt van de infrastructuur. Zo is de Beheerder verantwoordelijk voor die infrastructurele componenten binnen het koppelvlak die de uitwisseling van Suwi-gegevens mogelijk maken (koppelvlak Bronhouder-Beheerder en Beheerder-Afnemer). Zie figuur 1.



Figuur 1 Relatie tussen de betrokken partijen

2 UWV is voor KBS en Sonar de decentrale beheerder.

1.2. Suwinet Services

De Suwinet-Services omvat centraal voorzieningen in de vorm van applicaties die specifieke functionaliteiten bieden aan de Afnemers, zoals:

- Suwinet-Broker (Broker functie);
- Suwinet-Inlezen (pull berichten, antwoord op vragen) t.b.v. inlezende voorzieningen, zoals: Suwinet-Inkijk, Klantbeeld (onderdeel van Portlets), Mens Centraal, GWS4All, enz.);
- Suwinet-Meldingen (push berichten, doorgeven van informatie) t.b.v. Correctie en Terugmeld service);
- Suwinet-Mail (ongestructureerde gegevens uitwisseling) d.m.v. de Centrale- en Decentrale Suwinet-Mail voorzieningen);
- Suwinet Rapportages (stuurinformatie in de vorm van rapporten en bestanden).

De Suwinet-Services omvat ook decentraal voorzieningen in de vorm van applicaties die specifieke functionaliteiten bieden aan de Afnemers, zoals:

- IBSI sector loket;
- Inlees webservices;
- GSD Leveringen Suwi;
- DKD Inlezen.

1.3. Organisatie van het Suwinet Normenkader

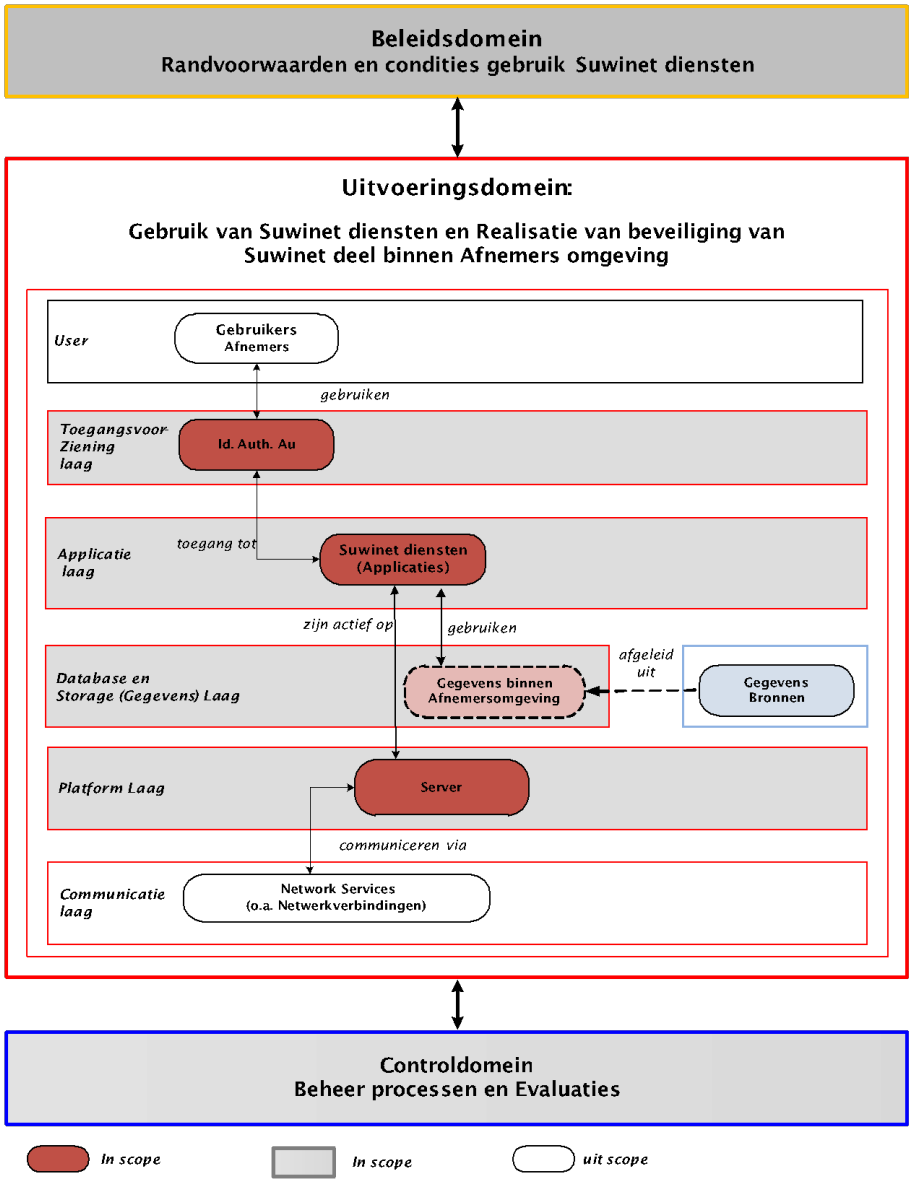
In deze paragraaf wordt de indeling van dit normenkader toegelicht. Het nomenkader is georganiseerd in drie hoofdstukken: beleids-, uitvoering- en control domein (ook wel beheersingsdomein genoemd). Figuur 2 geeft de relatie tussen de objecten die op de verschillende lagen kunnen voorkomen.

Deze lagenstructuur geeft door middel van drie onderkende domeinen een indeling van conditionele -, inrichtings- en beheersingsaspecten. Deze aspecten worden hiermee in juiste contextuele samenhang gepositioneerd. Figuur 3 geeft een overzicht van de lagenstructuur en enkele bijbehorende relevante kenmerken. De betekenissen die aan de lagen worden toegekend zijn:

Beleidsdomein – Dit domein bevat uitgangspunten voor het gebruik van Suwinet services binnen de Afnemers organisatie.

Uitvoeringsdomein – Dit domein bevat de implementatie van componenten die voor het veilig gebruik van gegevens noodzakelijk zijn, zoals toegangsvoorziening, koppelingen met voorzieningen zoals applicaties, eventuele servers waarop de decentrale applicatie actief op zijn.

Controldomein – Dit domein bevat evaluatie-, meet- en beheersingsaspecten op basis waarvan beheerst en bijgestuurd kan worden. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen en/of aanpassen van de eerder geformuleerde conditionele elementen die gebaseerd zijn op aannames, visies en uitgestippeld beleid en ook op het geven van inzicht over de Suwinet omgeving aan andere keten partijen.



Figuur 2 Indeling van de Suwinet-aspecten vanuit Afnemers perspectief

1.4. Beschrijving van de controls en onderliggende maatregelen

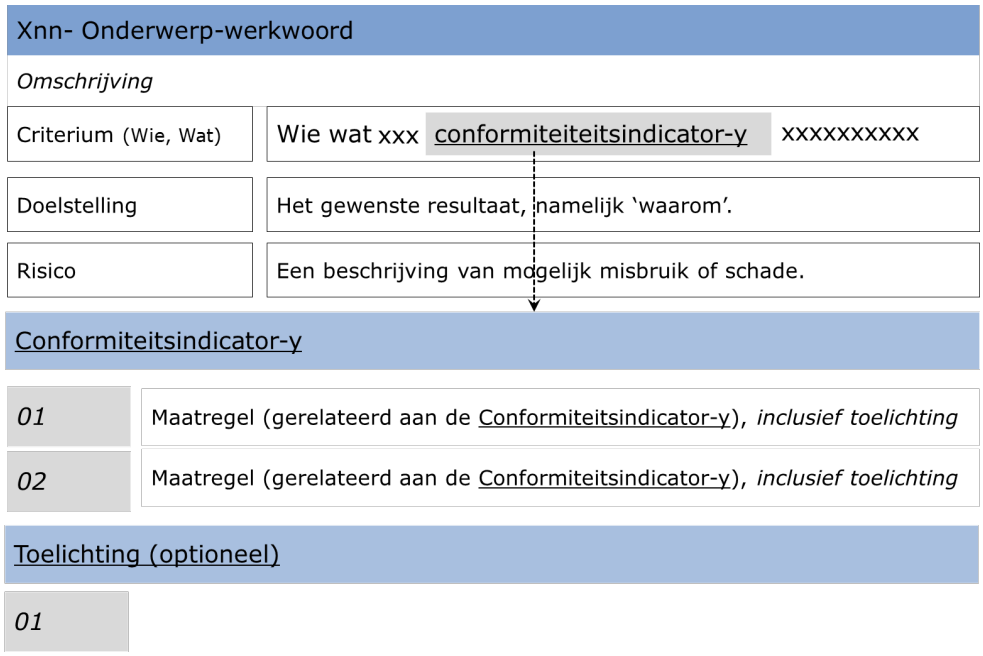
Binnen elk domein bevinden zich onderwerpen die bij de implementatie danwel bij een beoordeling van een onderzoeksobject een rol spelen. Per onderwerp wordt een criterium (of hoofdnorm) geformuleerd. Het criterium is beschreven in een vorm waarin de elementen wie, wat en waarom geadresseerd worden. Het waarom deel representeert een doelstelling die per criterium bereikt moet worden en/of wat men beoogd te bereiken. Hiernaast wordt per criterium een risico vermeld.

Hiermee is vastgelegd wat het criterium is, wie waarvoor verantwoordelijk is en de reden dat dit criterium opgenomen is.

Vervolgens wordt per criterium een aantal conformiteitsindicatoren gegeven. Met deze indicatoren wordt bereikt (implementatie) of vastgesteld (audit) hoe aan het criterium invulling kan worden gegeven. De hoofdnormen worden in een enkelvoudige zin zodanig beschreven dat deze voorzien worden met specifieke werkwoorden en trefwoorden. De werkwoorden geven bepaalde acties weer die ondernomen worden door betrokken functionarissen (actoren) binnen specifieke domeinen. De trefwoorden fungeren als conformiteitsindicatoren.

De conformiteitsindicatoren zijn nader gedetailleerd in maatregelen die deelaspecten beschrijven waaraan invulling gegeven moet worden ten aanzien van het criterium. Waar noodzakelijk zijn maatregelen voorzien van een nadere toelichting.

Bij de uitwerking van het criterium is gebruik gemaakt van een template, waarbij het element ”wie” vaak achterwege is gelaten. De elementen “wat” en “waarom” zijn separaat vermeld. Het gebruikte template wordt in Figuur 3 weergegeven.



Figuur 3 Template voor het beschrijven van een criterium

1.5. Aanpak en herkomst van criteria Afnemers Suwinet-Services

Het te ontwikkelen referentiekader voor het Suwinet domein (Afnemers) is gefaseerd aangepakt:

- vaststellen eisen,
- identificeren van objecten,
- matchen en (her)benoemen objecten,
- projectie van objecten op de domeinen: Beleid, Uitvoering en Control (BUC),
- herformuleren van criteria (controls) gerelateerd aan de geïdentificeerde objecten.

De volgende activiteiten zijn in fases uitgevoerd:

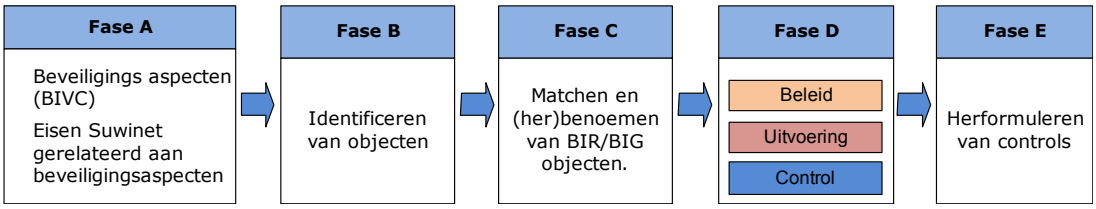
A. *Vaststellen eisen* – Bij deze fase zijn, uitgaande van de informatiebeveiligingsaspecten: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid (BIVC) (Regeling Suwi: Art. 6.4 en Art. 5.22) en kennis van de Suwinet-omgeving, op basis van een creatief proces, enkele globale relevante eisen geïdentificeerd voor het gebruik van Suwinet-services binnen Afnemersorganisatie.

B. *Identificeren van objecten* – Op basis van de geïdentificeerde eisen zijn in deze fase objecten benoemd waar de eisen aan kunnen worden gelinkt,

C. *Matchen en (her)benoemen objecten* – In deze fase zijn uitgaande van de geïdentificeerde en aanvullende eisen vanuit het project en globale objectenanalyse connecties gelegd met objecten uit BIR en BIG.

D. *Projectie van objecten op BUC domein*– In deze fase zijn de geïdentificeerde objecten geprojecteerd op de domeinen: Beleid, Uitvoering en Controle (BUC). Met de afronding van deze fase is het objecten-landschap voor het Suwinet domein (Afnemers) gecompleteerd.

E. *Herformuleren* – In deze fase zijn de formuleringen van controls die gerelateerde waren aan de geïdentificeerde objecten bestudeerd. Waar mogelijk zijn de oorspronkelijke controls geadopteerd, waar het een specifiek object van onderzoek betrof, namelijk GeVS, zijn de meeste controls geherformuleerd.



Figuur 4 De sequentie van de gehanteerde fases

Figuur 4 geeft een overzicht van de gehanteerde volgorde. De resultaten van stap D (*Projectie van objecten op BUC domein*) ziet als volgt uit:

Beleidsdomein

- *Aansluitbeleid* — Het aansluiten op de centrale- en decentrale omgeving van de GeVS voor het gebruik van Suwinet gegevens geschiedt op basis van vooraf vastgestelde randvoorwaarden,
- *Taken*, *Verantwoordelijkheden* — Alle type rollen zijn onderkend en de daarbij behorende de taken en verantwoordelijkheden zijn vastgesteld en vastgelegd,

- *Functiescheiding* — Alle noodzakelijke functiescheidingen zijn vastgesteld en beschreven,
- *Beveiligingsfunctie* — De noodzakelijke beveiligingsfunctie is benoemd en adequaat gepositioneerd,
- *Classificatie* — Gegevens die via Suwinet worden gedistribueerd zijn geclassificeerd,
- *Uitbesteding* — Uitbesteding van ICT diensten worden vastgelegd in een overeenkomst inclusief bewerkersovereenkomst,
- *Architectuur* — Het Suwinet-landschap inclusief de ICT is in kaart gebracht en beschreven.

Uitvoeringsdomein

- *Informatie Externe partijen* — Externe partijen aan wie ICT diensten zijn uitbesteed verstrekken aan de Afnemer jaarlijks een assurance verklaring (TPM),
- *Suwinet-Informatie* — Alle Suwinet-informatie (tijdens transport, bij interne of externe opslag) wordt beveiligd volgens de geldende standaarden,
- *Autorisatiebeheerproces*— Autorisaties worden beheerst op basis van een vastgesteld autorisatie beheerproces,
- *Identificatie en authenticatie mechanisme* — Toegang tot informatiesystemen is slechts mogelijk op basis een uniek identificatie en authenticatie mechanisme,
- *Autorisatie-mechanisme* — Gebruikers krijgen alleen die autorisaties die noodzakelijk zijn voor de wettelijke uitvoering van hun taken (principes: need to have en least privilege) en mogen alleen gegevens opvragen op basis van doelbindingprincipe),
- *Scheiding faciliteiten* — De Suwinet-gegevens worden alleen in een veilige omgeving gebruikt, zoals de productie omgeving binnen de OTAP indeling;
- *Communicatiefaciliteiten* — Uitwisseling van informatie tussen Suwi-partijen via het gebruik van verschillende typen communicatiefaciliteiten (bijv. mail) vindt beveiligd plaats, zoals de
- *Inleesfunctionaliteit* — Gestructureerde gegevens worden met web-applicaties uitgewisseld via een specifieke Inleesfunctionaliteit,
- *Technische componenten* — De technische componenten zijn veilig ingericht (Suwinet services, Servers),
- *Netwerkverbindingen* — GeVS is een besloten netwerk, waarbij alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld zijn beveiligd,
- *Telewerken* — De Suwinet-omgeving moet via veilige mobiele apparatuur en veilige verbindingen toegankelijk zijn.

Controledomein

- *Evaluatie Aansluitingsbeleid* — De vastgestelde randvoorwaarden worden periodiek[3] geevalueerd,

[3] Periodiek kan worden opgevat als zich in tijd herhalende activiteiten met een minimaal maandelijkse frequentie.

- *Risicomanagement* — Periodiek worden risicoanalyses uitgevoerd op de implementatie van Suwinet diensten en op de gerelateerde IT componenten,
- *Beheerprocessen* — Veranderingen/Wijzigingen worden procesmatig en procedureel doorgevoerd,
- *Organisatorisch evaluatie IAA mechanismen* — Periodiek wordt het IAA mechanisme organisatorisch geëvalueerd (Beoordeling van toegangsrechten),
- *Technisch evaluatie IAA mechanismen* — Periodiek wordt het IAA mechanisme technisch en het rechtmatig gebruik van Suwinet geëvalueerd (Logging en Monitoring),
- *Evaluatie van IAA rapportages* — Organisatorische en technische rapportages worden periodiek geëvalueerd,
- *Transparantie* — Periodiek wordt inzicht gegeven in de opzet bestaan en werking van de maatregelen ten aanzien van organisatorische, implementatie (technische)- en beheersingsaspecten aan ketenpartijen en hogere management.

De resultaten van fase D (Projectie van objecten op BUC domein) en fase E (Herformuleren) worden in hoofdstuk 2 uitgewerkt.

2. Beleidsdomein

Inleiding

Het beleidsdomein beschrijft in het algemeen beleidsaspecten en -aansluitvoorwaarden voor het gebruik van Suwinet diensten (bijv. Suwinet-Inlezen, Suwinet-Inkijk, Suwinet-Mail). De Afnemers hanteren in het algemeen hun eigen baselines (normenkader). Zo zullen organisaties die 'BIR-plichtig' zijn de BIR hanteren en de gemeenten de BIG en aan de BIG gerelateerde operationele producten. Alle overige organisaties zullen de ISO 27001/2 norm hanteren.

Naast de BIR, BIG en ISO 27001/2 zijn een aantal specifieke en op stelselrisico's gebaseerde maatregelen vereist vanuit de bronhouders, UWV, SVB, gemeentes. De specifieke en op stelselrisico's gebaseerde maatregelen zijn aanvullend op de genoemde baselines. Tevens zijn enkele uitgangspunten (controls) uit deze baselines, vanuit de optiek van het Suwinet, specifieker geformuleerd.

Doelstelling

De doelstelling van het "Beleidsdomein" is om aan te geven welke uitgangpunten en sturingsmiddellen er gelden voor het veilig gebruik Suwinet diensten.

Risico's

Door het ontbreken van een door het management van de Bronhouders uitgevaardigd beleid richting Afnemers bestaat het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van de Suwinet-omgeving. Dit zal een negatieve impact hebben op veilig gebruik van Suwinet diensten.

Onderwerpen

Binnen het beleidsdomein zijn normen opgenomen die gerelateerd zijn aan bepaalde onderwerpen (objecten). De normen drukken handelingen uit die gerelateerd zijn aan verantwoordelijkheden van een beschikkende functionaris (hogere management). Per onderwerp worden conformiteitsindicatoren uitgewerkt. Deze conformiteitsindicatoren representeren een vast te stellen set van maatregelen. De onderwerpen zijn afgeleid uit BIR, BIG en GeVS. Hiernaast zijn enkele onderwerpen incidenteel aangevuld met onderwerpen uit de NCSC beveiligingsrichtlijn of Standaard of Good practice (ISF). Tabel 1 geeft overzicht van de uit te werken onderwerpen binnen het Beleidsdomein.

Domein	Nummer	Objecten	Herkomst	
Beleidsdomein	B.01	Suwinet aansluitbeleid	BIG, GeVS	5.1
	B.02	Naleving en Compliance aansluitbeleid	BIG/BIR	15.2.1/SoGP
	B.03	Externe Partijen	BIG/BIR	6.2.3
	B.04	Beveiligingsfunctie Suwinet	BIG	6.1.7/6.1.2
	B.05	Taken, Verantwoordelijkheden en Functiescheiding	BIG, GeVS	6.1.3/10.1.3
	B.06	Suwinet deel landschap Afnemers (Architectuur)	x	x

Tabel 1 Te behandelen onderwerpen in beleidsdomein

B.01 Suwinet-aansluitbeleid

Elke organisatie ontwikkelt voor de beveiliging van haar ICT omgeving een informatiebeveiligingsbeleid. Met dit informatiebeveiligingsbeleid geeft de organisatie enerzijds richting aan de te nemen beveiligingsmaatregelen ten behoeve van een veilige dienstverlening conform wet en regelgeving. Anderzijds geeft dit beleid handvatten om aan te geven dat de organisatie aantoonbaar aan de verplichtingen uit de wet en regelgeving voldoet.

Een van de verplichtingen rond de wet en regelgeving heeft betrekking op Suwinet en de Suwinet diensten. Het is daarom van belang dat de organisatie expliciet aandacht besteed aan de beveiliging van 'de eigen delen' van Suwinet.

Het is gewenst dat de organisatie vanuit haar ICT omgeving adequate beveiligingsmaatregelen treft ten aanzien van Suwinet treft en dat zij deze ook aantoonbaar transparant maakt.

Het is daarom van belang een specifiek aansluitingsbeleid op Suwinet, als onderdeel van haar beveiligingsbeleid, te formuleren. Een aansluitbeleid is het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens.

B.01 Suwinet- aansluitbeleid		
Criterium/ (wie en wat)	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	BIG 5.1/5.1.1
Doelstelling (waarom)	Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet.	
Risico	*Het risico bestaat dat de bescherming van de aansluiting op Suwinet, in tegenstelling tot bescherming van haar eigen ICT omgeving, onvoldoende aandacht krijgt.*	

Conformiteitsindicatoren en maatregelen

Afnemer		
01	De Afnemer neemt in haar informatiebeveiligingsbeleid op, op welke wijze invulling wordt gegeven aan het Suwinet aansluitingsbeleid.	BIR/BIG 5.1 1 BIR/BIG 15.2.1
02	De Afnemer heeft de taken en verantwoordelijkheden ten aanzien van coördinatie van aansluitingsbeveiliging en ontwikkeling van aansluitingsbeleid belegd en toegewezen aan daartoe bevoegde functionarissen.	BIR/BIG 6.1.2
Aansluitingsbeleid		
03	Het aansluitingsbeleid is gericht op de, door de bronhouders vastgestelde, risicoklasse van de gegevens die uitgewisseld worden.	5.1 1 aanvullend
04	Het aansluitingsbeleid geeft inzicht in het type maatregelen voor de beveiliging van de eigen delen van Suwinet (bijv.: (organisatorische-, technisch- en, beheersingsmaatregelen)	5.1 1 aanvullend
05	In het aansluitingsbeleid werkt de Afnemer de vanuit Suwinet gestelde eisen uit voor de eigen organisatie.	5.1 1 aanvullend
07	Wanneer besloten wordt tot uitbesteden van taken en diensten in relatie tot Suwinet, legt Afnemer in de overeenkomst vast dat de aan haar gestelde beveiligingseisen voor Suwinet onverkort van toepassing zijn bij deze uitbesteding	BIG 6.2.3

08	In het beveiligingsbeleid is vastgelegd hoe de beveiligingsmaatregelen door de uitbestedende partij gecontroleerd worden (bijv. audits en penetratietests) en hoe het toezicht is geregeld.	BIG 6.2.1.6 (c)

B.02 Naleving en Compliance aansluitbeleid

Gezien de aard van de gegevens die via Suwinet worden uitgewisseld, het uitgevaardigd beleid en wet en regelgeving is het van belang dat de organisatie inzicht geeft in de naleving van het aansluitingsbeleid en andere overeengekomen beveiligingsmaatregelen.

Het aspect compliance richt zich op het naleven van de verplichtingen die voortkomen uit (a) wet- en regelgeving en (b) door de organisatie overeengekomen beleid, richtlijnen, standaarden, en architectuur.

Vanuit de optiek van de functionele en beveiligde inrichting van Suwinet diensten is het van belang om via naleving en compliance management proces vast te stellen in welke mate de gerealiseerde Suwinet diensten voldoen aan de verplichtingen die voorvloeien uit de wet en regelgeving en vooraf overeengekomen beleid, architectuur en standaarden (naleving).

De resultaten van de compliancy-check worden vastgelegd in een rapportage vergezeld van een Interne Control Verklaring (ICV) ten behoeve van transparantie en verantwoording.

Wanneer duidelijk wordt dat niet aan de overeengekomen verplichtingen wordt voldaan en of dat de geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen, zijn nadere afspraken tussen de Beheerder en de Afnemer en opvolging met corrigerende acties noodzakelijk.

In de loop van de tijd veranderen technieken en inzichten. Ook zal het Suwinet landschap gaandeweg veranderen. Deze ontwikkelingen kunnen aanleiding zijn het beleid bij te stellen en de controles aan te passen. Elke (groep van) verandering(en) is aanleiding om een compliancy-check uit te voeren.

Tot slot kunnen (vermoedens van) incidenten aanleiding geven tot het uitvoeren van ad hoc compliancy checks.

B.02 Naleving en compliance aansluitingbeleid		
Criterium/ *(ISO:Control)* *(wie en wat)*	De Afnemer bewerkstelligt dat het aansluitingsbeleid correct wordt uitgevoerd en dat de vereisten hieruit worden nageleefd.	BIG 15.2.1
Doelstelling *(waarom)*	Bereiken dat het eigen deel van Suwinet aantoonbaar voldoet aan de gestelde eisen passend bij het gewenste beveiligingsniveau.	
Risico	*Het risico bestaat dat zowel de Suwinet omgeving als de gegevens die worden uitgewisseld onvoldoende worden beschermd.*	

Conformiteitsindicatoren en maatregelen

Correct		
01	Afnemer is verantwoordelijk voor de uitvoering van het aansluitingsbeleid en de hieraan gerelateerde beveiligingsprocedures	~BIG 15.2.1.1
02	Afnemer heeft een compliance management proces, bestaande uit de subprocessen planning, evaluatie en registratie, rapportering, en implementatie van verbetervoorstellen vastgesteld en gedocumenteerd.	SoGP

Nageleefd		
03	Regulier worden (zelf)evaluatierapportages van compliance checks op aansluitingsbeleid Suwinet, Suwinet architectuur en wet en regelgeving samengesteld en beschikbaar gesteld aan de Stelselverantwoordelijke (SZW).	~BIG 15.2.1.2

B.03 Externe partijen

Zowel Bronhouders en Afnemers hebben sommige ICT diensten, vanwege gebrek aan expertise of kostenreductie, uitbesteed aan externe partijen. In deze uitbesteding is de organisatie nog steeds verantwoordelijk voor het verkrijgen van informatie op basis waarvan de organisatie assurance (dan wel transparantie) kan afgeven aan het eigen bestuur en/of aan een toezichthouder.

Derhalve moet bij uitbesteding van taken en/of diensten (of delen hiervan) de beveiligingseisen van de organisatie expliciet in de overeenkomst met de dienstverlener benoemd worden.

De informatie die de Afnemer in het kader van de assurance verklaring van de externe partij nodig heeft, wordt verkregen op basis van een ISAE 3402 of ISAE 3000 verklaring. Een alternatief hierbij is dat de assurance informatie van de externe partij verkregen wordt op basis van een specifiek Suwinet gerelateerd referentiekader die tussen de Afnemer en Externe partij is overeengekomen.

B.03 Externe partijen		
Criterium/ *(ISO:Control)* *(wie en wat)*	De organisatie stelt als Afnemer met externe partijen in een overeenkomst, waarvan een bewerkersovereenkomst onderdeel uitmaakt, minimaal vast dat de aan haar gestelde beveiligingseisen voor Suwinet onverkort van toepassing zijn op de dienstverlening die door deze externe partijen worden geleverd.	BIG 6.1.2
Doelstelling (waarom)	Bewerkstellingen dat de externe partij het juiste niveau van beveiligingsmaatregelen treft en de gewenste diensten biedt.	
Risico	*Bij het ontbreken van een overeenkomst waarin de wederzijdse verantwoordelijkheden ten aanzien van de te leveren diensten worden vermeld bestaat het risico dat de geleverde diensten niet voldoen aan het gewenste beveiligingsniveau en of dat de ICT omgeving van de Afnemer de werking van Suwinet negatief beïnvloed.*	

Conformiteitsindicatoren en maatregelen

Overeenkomst		
01	In de overeenkomst wordt ten aanzien van Suwinet beveiligingseisen vastgelegd dat de provider en haar onderaannemers de beveiligingseisen zullen implementeren en dat beveiligingsincidenten onmiddellijk aan de aanbesteder gerapporteerd worden.	BIG 6.2.1.6 (b)
02	De overeenkomst vermeldt dat de vanuit Suwinet aan de organisatie gestelde eisen onverkort van toepassing zijn voor de externe partij en eventuele onderaanbesteders.	BIG 6.2.3.7
03	De overeenkomst bevat een verplichting dat de externe dienstverlener zich jaarlijks verantwoordt over de opzet bestaan en werking van de beveiliging van de uitbestede diensten op basis een normenkader waarin o.a. Suwinet Aansluitvoorwaarden zijn verwerkt.	BIG 6.2.1.7

Bewerkersovereenkomst		
04	In de bewerkersovereenkomst worden de beveiligingseisen voor het verwerken van persoonsgegevens vastgelegd.	BIG 6.2.1.5
Beveiligingseisen voor Suwinet		
05	De scope van de technische omgeving waarvoor de beveiligingseisen gelden is inzichtelijk gemaakt op basis van een conceptuele architectuur (ontwerp documentatie).	~Cobit
06	De beveiligingseisen voor Suwinet waar de Afnemer verantwoordelijk voor is, zijn formeel vastgelegd en inzichtelijk gemaakt op basis van een conceptuele architectuur.	B06

B.04 Beveiligingsfunctie Suwinet (GeVS)

Organisatorische en technische veranderingen in de organisatie kunnen invloed hebben op het Suwinet domein binnen de organisatie van de Afnemer. Om in Suwinet keten verband effectief om te kunnen gaan met deze veranderingen is het van belang dat de organisatie een Beveiligingsfunctie Suwinet heeft ingericht, daarbinnen zijn de taken en verantwoordelijkheden met betrekking tot de Suwinet aansluiting geformaliseerd.

Binnen de Beveiligingsfunctie Suwinet is geregeld dat contact wordt onderhouden met de Security Officer van de Beheerder (BKWI) wanneer sprake is van beveiligingsincidenten die het stelsel aangaan.

B.04 Beveiligingsfunctie Suwinet		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS)benoemd en taken en verantwoordelijkheden vastgesteld.	BIG 6.1.7 BIG 6.1.2
Doelstelling (waarom)	Het voorkomen dat risico's plaatsvinden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet.	
Risico	Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan.	

Conformiteitsindicatoren en maatregelen

Taken en verantwoordelijkheden		
01	Binnen de Beveiligingsfunctie worden activiteiten welke impact hebben op de bescherming van de Suwinet-keten of de bescherming van de via Suwinet uitgewisselde gegevens doorgegeven aan de Security Officer van BKWI (beveiligingsincidenten).	Gevs SoGP
02	De verantwoordelijke binnen de Beveiligingsfunctie controleert regulier in welke mate de getroffen maatregelen in relatie tot Suwinet volstaan en/of escalatie of aanvullende maatregelen nodig zijn.	Gevs SoGP

B.05 Taken, Verantwoordelijkheden en Functiescheiding

Binnen organisatie van de Afnemer worden verschillende type beveiligings- en beheerrollen onderkend. Deze rollen hebben specifieke taken, verantwoordelijkheden en bevoegdheden (TVB's).

De taken binnen het beheer worden verdeeld in verschillende groepen met verschillende functieprofielen. Deze profielen zijn bedoeld om enerzijds tot een effectief takenpakket te komen, anderzijds tot een adequate functiescheiding.

Met behulp van functiescheiding worden de taken binnen een organisatie van de Afnemer verdeeld, zodat tegengestelde belangen ontstaan. Door deze tegengestelde belangen wordt getracht misbruik van een functie te voorkomen. Hierbij worden taken en verantwoordelijkheidsgebieden gescheiden en tegengestelde belangen gecreëerd en worden ongewenste functiecombinaties voorkomen. Zo wordt ervoor gezorgd dat taken, bevoegdheden en verantwoordelijkheden niet bij één persoon komen te liggen, maar bij meerdere personen met tegengesteld belang.

B.05 Taken, Verantwoordelijkheden en Functiescheiding		
Criterium/ *(ISO:Control)* *(wie en wat)*	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	BIG 6.1.3 BIG 10.1.3
Doelstelling *(waarom)*	Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.	
Risico	*Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:* - *misbruik van bevoegdheden,* - *te ruim toegekende bevoegdheden,* - *over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen.*	

Conformiteitsindicatoren en maatregelen

Type rollen		
01	De organisatie heeft rollen met betrekking tot beschikkende functie (lijnmanagement), uitvoerende functie (functioneel beheer) en controlerende functie (interne controle) onderkend en toegewezen aan verschillende functionarissen.	BIR/BIG 6.1.3
Taken, verantwoordelijkheden		
02	De taken, verantwoordelijkheden en bevoegdheden van de geïdentificeerde rollen en de betrokken functionarissen zijn beschreven.	BIR/BIG 8.1.1.
03	Verantwoordelijkheden en bevoegdheden zijn verwerkt in autorisatie matrices.	BIR/BIG 6.1.3. (aanvullend)
04	Periodiek worden de rollen, taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen geverifieerd en zo nodig geactualiseerd.	BIR/BIG 6.1.3 (aanvullend)
Functiescheiding		
05	Taken en verantwoordelijkheden binnen de onderkende rollen en de betrokken functionarissen zijn gescheiden.	BIR/BIG 10.1.3

B.06 Suwinet deel landschap Afnemers (architectuur)

In het deel van het Suwinet landschap dat behoort tot de verantwoordelijkheid van de Afnemer, legt de Afnemer vast welke infrastructurele IT componenten aanwezig zijn en hoe deze met elkaar verbonden zijn. Dit verschaft inzicht in de beveiliging van de GeVS-componenten en overzicht over hun onderlinge samenhang en werking. Tevens verschaft dit inzicht in hoe de componenten de bedrijfsprocessen van de decentrale organisatie ondersteunen.

Belangrijk onderdeel van het Suwinet landschap is een documentatie waarin de koppelingen van de Suwinet componenten worden weergegeven inclusief de beveiligingsmaatregelen en/of beveiligingscomponenten.

B.06 Suwinet deel landschap Afnemers (architectuur)		
Richtlijn (wie en wat)	De Afnemer heeft de actuele documentatie van de technische infrastructuur[4] Suwinet landschap, voor het deel waar de Afnemer verantwoordelijk voor is, vastgelegd.	SoGP Cobit NCSC
Doelstelling (waarom)	Het geven van inzicht in de relatie tussen techniek en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het Suwinet deel landschap inzicht in de beveiliging, interactie en relaties tussen Suwinet componenten.	
Risico	Dagelijkse operatie, die betrekking hebben op Suwinet componenten, is niet in lijn met het geformuleerde aansluitingsbeleid en de impact van toekomstige innovaties kan niet in volle omvang en geïntegreerd in beeld worden gebracht.	

Conformiteitsindicatoren en maatregelen

Documentatie		
01	De Afnemer heeft de samenhang van technische infrastructuur van het Suwinet, die bij het gebruik van Suwinet diensten een rol spelen, benoemd en vastgelegd in een 'Suwinet landschap' document.	SoGP Cobit NCSC
02	Het 'Suwinet landschap' document wordt actief onderhouden.	SoGP,Cobit NCSC
Technische infrastructuur		
03	De beveiligingsmaatregelen van de technische infrastructuur die gerelateerd zijn aan Suwinet zijn beschreven.	SoGP Cobit NCSC

4 *Technische infrastructuur* : Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden (Zie definitie BIG)

3. Uitvoeringsdomein

Inleiding

Binnen het uitvoeringsdomein maken de Afnemers gebruik van voorzieningen die gerelateerd zijn aan specifieke Suwinet-diensten. Hierbij hebben de Afnemers enerzijds een veilige omgeving gecreëerd en anderzijds is deze omgeving zodanig georganiseerd dat zij bij uitbesteding van gedeelten van haar ICT diensten voldoende informatie van haar provider verwerft om aan de verplichtingen van verantwoording en transparantie te kunnen voldoen. Dit zal moeten plaatsvinden onder vastgestelde uitgangspunten en aansluitvoorwaarden die binnen het beleidsdomein zijn gedefinieerd

Doelstelling

De doelstelling van het uitvoeringsdomein is om vast te stellen of de Afnemer de afgesproken Suwinet diensten gebruikt conform de uitgangspunten en de aansluitvoorwaarden.

Risico's

Door het ontbreken van adequate beveiligingsmaatregelen binnen de organisatie van de Afnemer bestaat het risico o.a.:

- dat misbruik wordt gemaakt van Suwinet-gegevens door onbevoegdheden of dat de Suwinet-gegevens op andere wijze onrechtmatig worden gebruikt;
- dat de Afnemer onvoldoende informatie heeft om aan haar verantwoording en transparantie verplichtingen te kunnen voldoen.

Inrichtings- en beveiligingscomponenten

Binnen dit domein worden volgende thema's als inrichtings- en beveiligingscomponenten behandeld.

Domeinen	Nummer	Objecten	Herkomst	
Uitvoerings-domein	U.01	TPM Externe partijen	BIG/BIR	6.2.3
	U.02	Autorisatie beheerproces	BIG/BIR	8.2.2 /11.2
	U.03	Toegangsmechanisme: Gebruikersidentificatie- en authenticatie (IA)	BIG/BIR	11.5.2, 11.2.3, 11.3.1
	U.04	Toegangsmechanisme: Autorisatie	BIG/BIR	11.6.1
	U.05	Suwinet-informatie	BIG/BIR	10.8.5
	U.06	Classificatie van informatie	BIG/BIR	7.2.1
	U.07	Suwinet-Inlezen en DKD Inlezen	BIG/BIR GeVS	10.9.2
	U.08	Suwinet-Mail	BIG/BIR GeVS	10.8
	U.09	Scheiding van faciliteiten (productieomgeving)	BIG/BIR	10.1.4
	U.10	Server (Intern BKWI)	SoGP	
	U.11	Netwerkverbindingen (BKWI)	BIG/BIR	11.4.6
	U.12	Telewerken	BIG/BIR	11.7.2

U.01 TPM Externe partijen

De externe partij, de provider aan wie de Afnemer de ICT diensten heeft uitbesteed in het kader Suwi, verstrekt jaarlijks een assurance verklaring opgesteld door een Third Party Auditor geregistreerd in het register van IT auditors (NOREA), in de vorm van een Third Party Memorandum (TPM) aan de Afnemer. De afnemer verwerkt dit in zijn ICV.

De jaarlijkse assurance verklaring van de externe partij verschaft voldoende informatie aan de Afnemer opdat deze aan haar verantwoordingsverplichtingen kan voldoen. De verantwoordingsverplichtingen hebben betrekking op opzet, bestaan en werking[5] van de beveiliging van uitbestede diensten; enerzijds generiek in relatie tot BIR/BIG en anderzijds specifiek in relatie tot Suwinet aansluitvoorwaarden.

U.01 TPM Externe partijen		
Criterium/ *(ISO:Control)* *(wie en wat)*	Externe partij verstrekt jaarlijks een verklaring aan de Afnemer over de aan hen aanbestede diensten in relatie tot Suwinet.	BIG 6.2.3
Doelstelling *(waarom)*	Bewerkstellingen dat de Afnemer aan hun assurance verplichtingen in relatie tot Suwinet kan voldoen.	
Risico	*Mogelijk kan de Afnemer niet of in onvoldoende mate aantonen dat opzet bestaan en werking van de beveiliging van de uitbestede diensten voldoen aan de gestelde eisen*	

Conformiteitsindicatoren en maatregelen

Jaarlijkse verklaring		
01	De jaarlijks assurance verklaring van de externe partij is gericht op opzet, bestaan en werking van de beveiliging van de uitbestede diensten.	BIG 6.2.1.6 (a)
02	Binnen de scope van de verklaring worden in ieder geval de volgende type maatregelen opgenomen: organisatorische-, technische- en beheersingsmaatregelen in relatie tot Suwinet.	aanvullend
03	De assurance verklaring wordt geleverd over de door de Afnemer vastgestelde verantwoordingsperiode binnen de afgesproken periode en termijn.	aanvullend

Toelichting 01: Opzet, bestaan en werking

De beoordeling van de uitbestede diensten richt zich op de aspecten *opzet*, *bestaan* en *werking*

- *opzet* – Heeft betrekking op de formele inrichting en beschrijving van de wijze waarop de provider de ICT diensten zal gaan uitvoeren. Veelal treft de ICT-auditor de opzet aan in handboeken, beleidsplannen, architectuurbeschrijvingen, etc.
- *bestaan* – Heeft betrekking op de wijze waarop ICT diensten, processen en maatregelen daadwerkelijk in de organisatie van de externe provider zijn geïmplementeerd. Deze situatie kan afwijken van hetgeen in de aanwezige beschrijvingen en plannen (de opzet) is vermeld.

5 Zie toelichting 01

- *de werking* – Heeft betrekking op de implementatie van de ICT diensten en het bestaan van processen gedurende een bepaalde periode. Hierbij wordt vastgesteld op welke wijze een organisatie een proces bij voortduring heeft uitgevoerd.

De opzet wordt veelal beoordeeld tijdens de ontwerpfase, het bestaan tijdens de implementatiefase en de werking tijdens de uitvoering van de processen. De controle op de werking wordt periodiek (veelal jaarlijks) uitgevoerd. Hierbij wordt eerst beoordeeld of opzet en bestaan ten opzichte van het voorgaande jaar zijn gewijzigd.

Het vaststellen van de werking vereist dat gedurende de controleperiode bij de betreffende Suwi-partij wordt nagegaan of de procedures en maatregelen worden nageleefd.

Toelichting 02: Type maatregelen

Met organisatorische maatregelen worden beleidsmatige maatregelen bedoeld(condities of randvoorwaarden), zoals informatiebeleid, aansluitingsbeleid en architectuur (zie onderwerpen in beleidsdomein),

Met technische maatregelen worden bedoeld maatregelen met betrekking tot de technisch inrichting van de ICT componenten die gerelateerd zijn aan Suwinet. Zie onderwerpen uit het uitvoeringsdomein,

Met beheersingsmaatregelen worden bedoeld maatregelen met betrekking tot de inrichting van beheerprocessen. Zie onderwerpen uit het controldomein.

U.02 Autorisatie beheerproces

Het autorisatieproces zorgt ervoor dat autorisaties gestructureerd plaatsvinden. Dit proces bestaat uit subprocessen zoals: toekennen (of verlenen), verwerken, wijzigen (intrekken en blokkeren), archiveren en controleren. Deze subprocessen zijn gerelateerd aan de fasen: instroom, doorstroom en uitstroom.

U.02 Autorisatiebeheerproces		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	8.3.3 11.2.
Doelstelling (waarom)	Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken.	
Risico	Het risico bestaat dat medewerkers onrechtmatig toegang hebben tot Suwinet of tot de via Suwinet beschikbaar gestelde gegevens. Voor Suwinet geldt een verhoogd risico omdat het Suwinet account van een organisatie ook toegang tot Suwinet kan krijgen vanuit het domein van een ander op Suwinet aangesloten organisatie.	

Conformiteitsindicatoren en maatregelen

Formeel autorisatiebeheer proces		
01	De toegang tot Inlezen en Inkijk wordt uitgevoerd op basis een autorisatie beheerproces bestaande uit: verlenen, (toekennen), verwerken, intrekken, blokkeren, archiveren en controleren.	Norea
Wijzigen toegangsrechten		
02	Bij wijzigen van functies of uitdiensttreding is de toegang tot Suwinet per mutatiedatum (uiterlijk de eerst volgende werkdag) aangepast of geblokkeerd of verwijderd.	~8.3.1.3 11.2.2
03	Een verantwoordelijke functionaris controleert in opdracht van de systeemeigenaar de toegekende autorisaties en bevestigt de juistheid van de gewijzigde autorisatie bij functiewijzigingen aan de registrerende partij.	8.3.3

U.03 Toegangsmechanisme: Gebruikersidentificatie- en authenticatie (IA)

Toegang tot Suwinet diensten, bijvoorbeeld inlees-, inkijk- en Suwinet-Mail functie[6], wordt gereguleerd door de toegangsmechanismen:

- gebruikers identificatie – een naam waarmee een gebruiker zichzelf bekend maakt aan een Suwinet dienst (user-ID);
- authenticatie - Na het zich bekend maken moet de gebruiker een bij het user-ID bijbehorend wachtwoord (of password) invoeren om toegang te krijgen tot het systeem. Een geheime code die alleen de gebruiker mag weten;
- autorisatie – Na het zich bekend maken aan de Suwinet dienst, via (user-ID en password) krijgt de gebruiker op basis van zijn/haar functieprofiel toegang tot de Suwinet dienst om handelingen te verrichten.

De identificatie, authenticatie mechanisme en autorisatie worden verder uitgewerkt in:

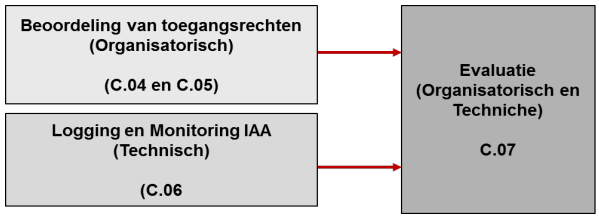
- U.03 Toegangsmechanisme: Identificatie- en authenticatie en
- U.04 Toegangsmechanisme: Autorisatie.

Gezien de risicoclassificatie van de via Suwinet uitgewisselde gegevens moeten alle handelingen met betrekking tot Suwinet altijd te herleiden zijn naar natuurlijke personen. De handelingen zelf zijn beperkt tot het uitvoeren van acties die voortvloeien uit de opgedragen wettelijke taken. Anders bestaat een risico dat via Suwinet uitgewisselde gegevens onrechtmatig worden verwerkt. Ook kunnen situaties van misbruik ontstaan.

Om bovenstaande risico's te voorkomen is het van belang dat:

a. de Afnemer zorgt dat het gebruik van de inkijkfunctie gecontroleerd wordt door het maandelijks opvragen van de logging over de inkijkfunctie bij BKWI. Zie verder de *onderwerpen 'Logging en Monitoring' (C.04 – C.06)* in het *Control domein.*
b. de Afnemer zorgt dat het gebruik van de ingelezen gegevens vastgelegd (gelogd) wordt. Hierbij zal de Afnemer op basis van de vastleggingen kunnen vaststellen wie welke handelingen heeft verricht. Zie verder de *onderwerpen 'Logging en Monitoring' (C.04 – C.06)* in het *Control domein.*
c. Rapportages opgesteld worden ten behoeve van controledoeleinden. Hierbij zal de afnemer op basis van de vastleggingen evaluatie rapportages op het gebruik/misbruik van IAA moeten opstellen. Zie verder het onderwerp 'Beoordeling van autorisaties, C.06)in het Control domein.
d. de Afnemer zorgt dat het gebruik van autorisaties gecontroleerd wordt. Hierbij zal de Afnemer aandacht schenken aan het gebruik (a) en de evaluatie rapportages (b) en dat noodzakelijke verbeteracties worden geformuleerd. Zie verder het onderwerp *Evaluatie van IAA rapportages, C.07'* in het Control domein.
e. de Afnemer zorgt dat maatregelen worden genomen bij misbruik of oneigenlijk gebruik van de beschikbaar gestelde gegevens. Zie verder het onderwerp *Evaluatie van IAA rapportages, C.07'* in het Control domein. Figuur 5 geeft de relatie tussen de aandachtgebieden.

6 Zie hoofdstuk 1.2



Figuur 5 Aandachtgebieden IAA vanuit de Afnemer

U.03 Toegangsmechanisme: Identificatie en authenticatie		
Criterium (wie en wat)	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	11.5.2, 11.2.3 11.3.1
Doelstelling (waarom)	Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten.	
Risico	*Onbevoegde gebruikers kunnen toegang krijgen tot Suwinet diensten.*	

Conformiteitsindicatoren en maatregelen

Authenticatietechniek (wachtwoorden)		
01	Bij uitgifte van authenticatie middelen wordt minimaal de identiteit vastgesteld evenals het feit dat de gebruiker voor de uitvoering van wettelijke taken recht heeft op het authenticatie middel.	11.5.2.1
02	Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats (telewerken).	BIR 11.6.1.3 (R en A)
03	Wachtwoorden worden interactief beheerd en voldoen aan gespecificeerde kwaliteit in het toegangsbeleid op basis van BIG/BIR.	BIG 11.5.3
Identificatiecode		
04	Bij het gebruik van Suwinet diensten worden gebruikers minimaal geauthentiseerd op basis van User-ID en wachtwoorden die voldoen aan daaraan gestelde eisen.	BIR 11.5.2. 2

U.04 Toegangsmechanisme: Autorisatie

Na het geautomatiseerde identificatie- en authenticatieproces krijgen gebruikers/beheerders verdere specifieke toegang tot Suwinet diensten. De toegangsbeperking wordt gecreëerd door middel van rollen en toegangsprofielen die voortkomen uit het Suwinet toegangsbeleid en specificaties vanuit de gebruikersorganisatie (business).

U.04 Toegangsmechanisme: Autorisatie		
Criterium (wie en wat)	Toegang tot Suwinet diensten door gebruikers en beheerders behoort te worden beperkt overeenkomstig het vastgestelde (Suwinet) toegangsbeleid gebaseerd op de WBP.	BIG, BIR: 11.6.1
Doelstelling (waarom)	Bewerkstelligen dat invulling wordt gegeven aan doelbinding en proportionaliteit.	
Risico	Door het niet beperken van toegang door middel van gespecificeerde autorisaties tot Suwinet diensten wordt niet voldaan aan doelbinding en proportionaliteit principes.	

Conformiteitsindicatoren en maatregelen

Toegang		
01	In de toegangsregels ten behoeve van Suwinet diensten wordt ten minste onderscheid gemaakt tussen lees- en schrijf, en beheerbevoegdheden.	11.6.1.1
02	De toegangsregels tot Suwinet diensten worden beperkt op basis van juiste rollen en autorisatieprofielen	~ 8.1.1
Suwinet toegangsbeleid		
03	Het Suwinet toegangsbeleid, mede gebaseerd op de WBP, geeft richting aan het specificeren van autorisatieprofielen.	ISO 11.6.1 Impl. richtlijn

U.05 Suwinet-informatie

Suwinet-informatie betreft informatie die via Suwinet wordt uitgewisseld en omvat de apparatuur waarmee gegevens verkregen via Suwinet toegankelijk worden gemaakt, zoals werkplekken en mobiele devices. De mobiele devices kunnen buiten eigen locaties gebruikt worden. Gezien het feit dat ketenpartijen risico lopen op imagoschade en aansprakelijkheid is het van belang dat zowel Suwinet-informatie als apparatuur waarop gegevens mogen worden opgeslagen aan strikte beveiligingsvoorwaarden voldoen, conform de ketenarchitectuur.

U.05 Suwinet-informatie		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer heeft alle Suwinet-informatie (bij transport) binnen en buiten de eigen locaties en apparatuur waarmee Suwinet-informatie toegankelijk wordt gemaakt, beveiligd volgens de geldende standaarden.	10.8.5
Doelstelling (waarom)	Bewerkstelligen dat de beveiliging van Suwinet gegevens aan de vereiste beveiliging voldoet.	
Risico	Ongeautoriseerde personen kunnen zich toegang verschaffen tot Suwinet gegevens welke opgeslagen zijn op apparatuur of op mobiel apparatuur welke zich buiten de eigen locatie(s) van de op Suwinet aangesloten organisaties bevinden.	

Conformiteitsindicatoren en maatregelen

Suwinet-Informatie		
01	Gegevens die via Suwinet en via mobiele devices worden verstuurd worden op basis van veilige protocollen (tweezijdig versleuteld, sterke authenticatie) verstuurd conform geldende standaarden (Forum standaardisatie).	aanvullend
02	De Suwinet data op alle mobiele apparatuur welke zich buiten de eigen locatie(s) van de organisatie bevinden en waarop via Suwinet verkregen gegevens worden verwerkt moeten zijn versleuteld.	aanvullend

03	De techniek van versleuteling van de gegevens wordt uitgevoerd op basis van pas-toe-of-leg-uit lijst van het forum standaardisatie (zie toelichting).	Big/Bir
04	Alle apparatuur welke zich buiten de eigen locatie(s) van de organisatie bevindt is voorzien van adequate[7] bescherming.	aanvullend

Toelichtingen

Toelichting : 0.3 pas-toe-of-leg-uit lijst

Overheden en semi-overheden zijn verplicht de open standaarden, die op de lijst met 'pas toe of leg uit'-standaarden staan, bij aanschaf of (ver)bouw van ICT-systemen/-diensten te eisen ('pas toe'). Afwijken mag alleen met zwaarwegende redenen en verantwoording hierover worden afgelegd in het jaarverslag ('leg uit'). 'Pas toe of leg uit'-standaarden zijn open standaarden waarvoor breed draagvlak bestaat maar die nog niet breed geadopteerd zijn. Daarom krijgen deze standaarden de status van 'pas toe of leg uit'.

U.06 classificatie van informatie

Informatie uit authentieke bronnen die door specifieke bronhouders worden beheerd en via Suwinet ter beschikking worden gesteld aan de Afnemers, kennen verschillende risicoklassen. De bepaling van de classificatie t.b.v. de risicoklassen, waaronder gegevens ressorteren, vindt plaats op basis van wettelijke eisen, de waarde en onmisbaarheid voor de organisatie en de gevoeligheid van de gegevens (bijv. persoonsgegevens).

Deze gegevens worden door Afnemers via Suwinet gebruikt en ook geregistreerd binnen hun eigen technische domein.

In verband met het risico op imagoschade voor de gehele keten en voor de Minister moet de classificatie van de via Suwinet uitgewisselde gegevens bij het verwerken door de Afnemer minimaal hetzelfde niveau hebben als de classificatie die bronhouder voor deze gegevens heeft aangegeven.

Dit impliceert ook dat de organisatie - in lijn hiermee - de juiste maatregelen heeft genomen aangaande het aanvaardbaar gebruik van bedrijfsmiddelen en persoonsgegevens.

U.06 Classificatie van Informatie		
Criterium/ (ISO:Control) (wie en wat)	De organisatie van de Afnemer classificeert de informatie, in relatie tot de via Suwinet uitgewisselde gegevens, op basis van een classificatie-voorschrift die gerelateerd is aan de classificatie-indicatie van de bron-houders.	7.2.1
Doelstelling (waarom)	Te voorkomen dat gegevens op een lager niveau beschermd worden dan aangegeven door de bronhouder(s).	
Risico	Gegevens worden op een lager niveau beschermd, dan welke door de betreffende bronhouder(s) is vastgesteld en waardoor gegevens onvoldoende zijn beschermd.	

7 Adequate bescherming duidt in het kader van WBP op passende beveiligingsmaatregelen hetgeen betekent rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.

Conformiteitsindicatoren en maatregelen

Classificatie-indicatie		
01	De organisatie past een classificatie (of een rubricering) toe dat aansluit op de classificatie-indicatie van de bronhouder	BIG 7.2.1.1
02	De organisatie treft overeenkomstig het classificatieprofiel van de uit te wisselen gegevens de juiste technische beveiligingsmaatregelen in overeenstemming met de risicoclassificatie die door de betreffende bronhouder(s) is aangegeven.	BIG 7.2.2. (1 en 2) aanvullend

U.07 Suwinet- Inlezen en DKD Inlezen (inleesfunctionaliteit)

Met Suwinet- Inleesfunctionaliteit kunnen medewerkers van Afnemers gegevens van diverse bronnen direct in de eigen applicatie inlezen. Het gaat alleen om gegevens die medewerkers nodig hebben voor de uitvoering van hun wettelijke taken. Suwinet-Inlezen maakt de eenmalige gegevens uitvraag en het hergebruik van gegevens mogelijk.

Het uitgangspunt is dat de aangesloten partijen voor het raadplegen en verwerken van persoonsgegevens gestructureerde berichten uitwisselen via het beveiligd netwerk (veilige kanalen), conform de ketenstandaarden en slechts nadat de identiteit, authenticiteit en autorisatie van Afnemer zijn vastgesteld.

Inlezen via de GeVS wordt op twee manieren mogelijk gemaakt:
- De gegevenslevering verloopt via het IB (dit noemen we DKD-Inlezen).
- De gegevenslevering verloopt via het BKWI (dit noemen we Suwinet-Inlezen).

DKD-Inlezen is met name ontwikkeld om gemeenten te ondersteunen bij de uitvoering van hun taken in het domein werk en inkomen. In alle andere situaties vindt de levering plaats via het BKWI.

DKD inlezen is equivalent aan Suwinet-Inlezen' en wordt door IB aangeboden aan de gemeenten via een Firewall van Inlichtingen Bureau (IB). DKD inlezen wordt eveneens technisch beheerd door BKWI. Hiermee is het normenkader Afnemers ook an toepassing voor afnemers welke gebruik maakt van DKD inlezen. De Brongegevens worden aangeboden via een Klantbeeldserver die in de Bronhoudersomgeving is gepositioneerd.

U.07 Suwinet- Inlezen en DKD Inlezen		
Criterium/ (ISO:Control) (wie en wat)	De aangesloten partijen wisselen onderling gestructureerde gegevens uit via de service Suwinet-Inlezen die direct worden ingelezen in een applicatie (inlees applicatie).	BIR 10.9.2 (aangepast)
Doelstelling (waarom)	Dat de juistheid, volledigheid, tijdigheid en contoleerbaarheid van de berichten tijdens het gebruik binnen de Inleesapplicatie is gewaarborgd.	
Risico	Informatie raakt corrupt of is onbetrouwbaar en/of via Suwinet beschikbaar gestelde gegevens worden onrechtmatig verwerkt.	

Conformiteitsindicatoren en maatregelen

applicatie		
01	Het online uitwisselen van gegevens en het verwerken in de inleesapplicatie vindt plaats conform Suwinet aansluitbeleid.	GeVS 15.1 BIR/BIG 10.8 (?).
02	Binnen de applicatie van de Afnemer wordt de vertrouwelijkheid van Ingelezen gegevens gewaarborgd, ongeautoriseerd gebruik van de gegevens is niet mogelijk, ook niet tijdens transport.	GeVS 15.3 BIR/BIG 10.8(~)
03	Binnen de applicatie van de Afnemer wordt de integriteit van de gegevensuitwisseling gewaarborgd (ongeautoriseerde wijzigingen, toevoegingen en weglatingen door derden is niet mogelijk ten tijde van het transport).	GeVS 15.4 BIR/BIG 10.9.1(~) BIR/BIG 12.2.3
04	Vanaf het moment van het verzoek van inlezen wordt er gelogd zodat er een controlemogelijkheid is op rechtmatig gebruik (wie heeft welke gegevens geraadpleegd)	Big 10.10.2

U.08 Suwinet-Mail

Suwinet-Mail is een communicatiefaciliteit, in de vorm van een besloten netwerk, dat bestaat uit een centraal- deel en meerdere decentrale delen. Dit biedt gebruikers en aangesloten organisaties de mogelijkheid om vertrouwelijke informatie met elkaar uit te wisselen. Hiermee worden de risico's die zijn verbonden aan het mailen van klantgegevens aanzienlijk verkleind. Op Suwinet-Mail zijn diverse overheidsorganisaties aangesloten.

Het gehanteerde uitgangspunt is dat Afnemer/Bronhouder/Beheerder ongestructureerde berichten met persoonsgegevens en/of gevoelige bedrijfsgegevens niet via het publieke internet uit, maar via het beveiligd Suwinet-Mail netwerk uitwisselen.

U.08 Suwinet-Mail		
Criterium ISO: Control (Wat)	Het beschermen van de uitwisseling van informatie via Suwinet-Mail wordt uitgevoerd conform formeel beleid- en procedures en beheersmaatregelen.	BIR/BIG 10.8 GeVS
Doelstelling (waarom)	Voorkomen dat door via Suwinet-Mail uitgewisselde berichten de integriteit en vertrouwelijkheid van de ontvanger in gevaar brengen.	BIR/BIG 10.8
Risico	*Ondanks de beslotenheid van Suwinet kan de zender onbedoeld besmette berichten verspreiden, waardoor de ontvanger, wanneer deze hierop geen maatregelen treft last van heeft.*	

Conformiteitsindicatoren en maatregelen

Beleid en procedures		
01	De e-mail uitwisseling vindt plaats conform vastgestelde richtlijnen en handreiking Suwinet-Mail	GeVS 18.1
02	Het e-mail gebruik is gebaseerd op richtlijnen ten aanzien van: - bescherming tegen ongeautoriseerd gebruik en, - het rapporteren over gedetecteerde ongewenste events	GeVS 18.3 BIR/BIG 10.9.1 ~ BIR/BIG 13.1.1
Beheersmaatregelen		
03	De e-mail-voorziening (centraal en decentraal) bevat een filterfunctie voor het controleren van e-mail berichten op schadelijke inhoud en of attachments.	GeVS 18.2 BIR/BIG 10.4.1
04	Het is niet mogelijk e-mail-berichten te versturen die afkomstig zijn uit ander dan uit het eigen domein (open-mail relay).	GeVS 18.4(?) BIR/BIG 11.4.7)
05	Het doorsturen van externe e-mail berichten via Suwinet-Mail is niet mogelijk.	BIR/BIG 10.8.1.5
06	De inrichting van Suwinet-Mail waarborgt, behalve voor viruscontrole en back--up doeleinden, de exclusieve toegang tot de inhoud van e-mailberichten door uitsluitend de eigenaar van het e-mail account en de geadresseerde.	GeVS 18.5 BIR/BIG 12.5.4)

U.09 Scheiding van faciliteiten (productieomgeving)

De Afnemer maakt gebruik van de zogeheten OTAP-omgevingen (Ontwikkel-, Test-, Acceptatie- en Productieomgeving). Binnen deze omgevingen worden specifieke activiteiten verricht. Hierbij behoren verschillende verantwoordelijkheden. Deze OTAP-omgevingen kunnen in beheer zijn bij externe providers.. In het kader van het gebruik van Suwinet gegevens is het een vereiste dat de Suwinet gegevens slechts via de productie omgeving beschikbaar gesteld moet worden.

U.09 Scheiding van faciliteiten (productieomgeving)		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer behoort de via Suwinet geleverde gegevens alleen via de productieomgeving beschikbaar te stellen.	~10.1.4 Wbp
Doelstelling (waarom)	Voorkomen dat productgegevens beschikbaar zijn of verwerkt worden in andere omgevingen dan in de productie omgevingen.	
Risico	Handelen in strijd met de wet (WBP), in relatie tot het rechtmatig toegang verlenen tot of verwerken van persoonsgegevens	

Conformiteitsindicatoren en maatregelen

Suwinet geleverde gegevens		
01	De via Suwinet geleverde gegevens bevinden zich alleen in de productie omgeving	Bir/Big Ir~10.1.4
Productieomgeving		
02	Medewerkers hebben alleen toegang tot de omgevingen waarvoor ze geautoriseerd zijn.	Bir/Big ~10.1.4
03	Alleen geautoriseerde medewerkers binnen de productieomgeving hebben toegang tot persoonsgegevens	Bir/Big ~10.1.4
04	De ontwikkel, test en acceptatievoorzieningen omgevingen zijn gescheiden van de productievoorzieningen (OTAP).	Bir/Big ~10.1.4 (1,2, 3)

U.10 Server

Een server is een computer inclusief programmatuur dat diensten verleent aan clients. In de eerste betekenis wordt met server de fysieke computer aangeduid waarop een programma draait dat deze diensten verleent. In de praktijk komen verschillende combinaties van hardware en software (server programma's) voor.

De servers worden beheerd door de beheerders (van de provider). Hiervoor hebben ze vaak speciale bevoegdheden. De servers bieden over het algemeen verschillende functionaliteiten en beschikken vaak over verschillende kenmerken (features) waarmee de gewenste functionaliteiten kunnen worden aangeboden. Het is vanuit beveiligingsoogpunt van belang om de toegang tot servers adequaat te regelen en de niet noodzakelijke features uit te schakelen, te blokkeren of te elimineren.

U.10 Server		
Criterium ISO:Control) (wie en wat)	De Suwinet Servers worden gehardend volgens een vastgestelde configuratiebaseline.	SoGP
Doelstelling (waarom)	Zeker te stellen dat servers opereren zoals het gewenst is en dat de beveiliging van computer omgevingen niet wordt gecompromitteerd.	
Risico	*Van de zwakheden in de Suwinet servers kan misbruik gemaakt worden.*	

Conformiteitsindicatoren en Maatregelen

Servers		
01	Suwinet Servers zijn voorzien van antivirus software en updates	GeVS 20.6
02	Het is voor ongeautoriseerden niet mogelijk om de inhoud van het filesysteem van de Suwinet Servers op te vragen.	SoGP
hardening		
03	Suwinet Servers zijn gehardend en beschermd tegen ongeautoriseerd toegang door: - uitschakelen van onnodige en onveilige user accounts, - veranderen van beveiliging gerelateerde parameters (zoals passwords) - gebruik van time-out faciliteiten, - beperken van toegang tot krachtige systeem faciliteiten - beperken van het gebruik van protocollen die gevoelig zijn voor misbruik	GeVS 20.3 SoGP
configuratiebaseline		
04	De parametrisering (hardening) van de Suwinet Servers worden uitgevoerd op basis van een formeel configuratiedocument.	GeVS 20. SoGP 1

U.11 Netwerkverbindingen

Suwinet-gegevens worden beschikbaar gesteld via transport kanalen (netwerkverbindingen). Afnemers hebben netwerkverbindingen zowel naar de Beheerder (BKWI) naar externe partijen (zoals Suwinet-Inlezen en Suwinet-Inkijk) en naar devices (Telewerken).

Er kan onderscheid gemaakt worden in logische en fysieke verbindingen. In het kader van het gebruik van Suwinet gegevens ligt de nadruk op de veiligheid van logische verbindingen. Deze verbindingen moeten voldoen aan specifieke beveiligingseisen zoals geautoriseerde toegangsbeveiliging en encryptie. Encryptie komt tot uitdrukking in de toepassing van een bepaald protocol voor de beveiliging van de verbinding.

U.11 Netwerkverbindingen		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	BIG 11.4.6.
Doelstelling (waarom)	Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten	
Risico	Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd.	

Conformiteitsindicatoren en maatregelen

Beveiligd		
01	De Suwinet verbindingen zijn tweezijdig versleuteld (met TLS).	12.3.1 10.6.1.(2 en3)
02	De techniek van versleuteling van de gegevens wordt uitgevoerd op basis van pas-toe-of-leg-uit lijst van het forum standaardisatie	B.01

Toelichting

Zie toelichting ' pas-toe-of-leg-uit lijst 'op pagina 21.

U.12 Telewerken

Het breder en intensiever inzetten van e-dienstverlening, mobiele apparaten en telewerken stelt ketenpartijen in staat aan te sluiten bij de hedendaagse eisen van medewerkers en klanten. Daarnaast werken medewerkers van keten-partijen steeds meer samen met andere overheidsmedewerkers. Mobiele apparaten en netwerken die dit ondersteunen zijn extra gevoelig. Tegelijkertijd zijn de bedreigingen vanuit de buitenwereld toegenomen. Het gevolg van deze twee ontwikkelingen is dat de beveiligingsrisico's voor ketenpartijen groter zijn geworden. Daardoor bestaat meer kans op schade voor de omgeving van de Afnemers. Daarom is het van belang specifieke eisen te stellen aan telewerk voorzieningen.

U.12 Telewerken		
Criterium/ (ISO:Control) (wie en wat)	Afnemer heeft beleid, operationele richtlijnen en procedures voor telewerken ontwikkeld en geïmplementeerd.	11.7.2
Doelstelling (waarom)	Bewerkstelligen van Suwinet gegevensbeveiliging bij transport en gebruik van telewerkvoorzieningen	
Risico	Ongeautoriseerde personen kunnen toegang krijgen tot gegevens behorend tot een verhoogde risico klasse.	

Conformiteitsindicatoren en maatregelen

Beleid		
01	De Afnemer heeft in haar beleid uitgewerkt welke Suwinet diensten wel/niet vanuit de thuiswerkplek of vanuit andere telewerkvoorzieningen mogen worden geraadpleegd.	BIG
02	Afnemer heeft in haar beleid onder andere gedragsregels aangaande het transport en gebruik van de Suwinet-gegevens opgenomen.	BIG
03	Het telewerkbeleid wordt, in relatie tot Suwinet gegevens, ondersteund door een MDM-oplossing (Mobile Device Management).	
04	De telewerkvoorzieningen zijn, in relatie tot Suwinet, zo ingericht dat op de werkplek (thuis of op een andere locatie) geen Suwinet-informatie wordt opgeslagen. ('zero footprint').	Big [A]
05	De telewerkvoorzieningen zijn, in relatie tot Suwinet zo ingericht dat mogelijke malware vanaf de werkplek niet via Suwinet verspreid kan worden.	Big 11.7.1.2
Operationele richtlijnen en procedures		
06	Afnemer heeft geschikte implementatie richtlijnen opgesteld voor de toe te passen producten en technieken.	Big
07	Afnemer heeft deze richtlijnen vertaald naar procedures aangaande het aanvaardbaar gebruik van producten en technieken.	aanvullend

4. Control

Inleiding

De Afnemers zullen een adequate beheerorganisatie hebben ingericht, waarin evaluatie activiteiten worden uitgevoerd en beheerprocessen zijn vormgegeven. De evaluatie activiteiten hebben betrekking op de actualisering van beveiligingsbeleid en aansluitingsbeleid. De beheer- en beheersactiviteiten betreffen o.a. evaluatie/beoordeling van aansluitingsbeleid, risicomanagement, beoordeling van toegangsrechten, wijzigingsbeheer, technisch en organisatorische naleving van IAA.

Deze beheerprocessen - en beheersactiviteiten zorgen ervoor dat deze ICT-componenten steeds veilig zijn geconfigureerd en dat het gewenste beveiligingsniveau behouden blijft. Deze ICT-beheerprocessen moeten op basis van service managementbeleid zijn ingericht.

Doelstelling

De doelstelling van de laag control (beheersing) is erop gericht te zorgen en/of vast te stellen dat:

- de Afnemer haar omgeving zodanig heeft ingericht dat kwetsbaarheden binnen haar infrastructurele omgeving niet doorwerken in overige delen van Suwinet,
- de Afnemer het juiste beveiligingsniveau van technische componenten ten aanzien van toegangsvoorziening, applicatie, koppelingen, platformen en servers en netwerken heeft geïmplementeerd,
- de Afnemer evaluatieactiviteiten verricht om blijvend aan de overeengekomen condities en randvoorwaarden te kunnen voldoen,
- de Afnemer aantoonbaar de via Suwinet verkregen gegevens slechts rechtmatig gebruikt

Risico's

Door het ontbreken van noodzakelijke maatregelen binnen het beheersingsdomein is het niet zeker dat de -omgeving aan de beoogde beveiligingsvoorwaarden voldoet.

Beveiligingsrichtlijnen

Binnen de laag 'Beheersing' worden onderstaande richtlijnen beschreven en per richtlijn worden Conformiteitsindicatoren en de betreffende implementatie en audit elementen uitgewerkt.

Domein	Nummer	Objecten	Herkomst	
Controldomein	C.01	Evaluatie op Aansluitbeleid	BIR/BIG	5.1.2
	C.02	Risicomanagement	BIR/BIG	H4
	C.03	Wijzigingenbeheer	BIR/BIG/NCSC	10.1.2
	C.04	Beoordeling van toegangsrechten	BIR/BIG	11.2.4
	C.05	Logging	BIR/BIG	10.10.1, 10.10.4,
	C.06	Monitoring en Rapportage	BIR/BIG	10.10.1
	C.07	Evaluatie van IAA rapportages	Project W6	
	C.08	Transparantie rapportage		

C.01 Evaluatie van aansluitbeleid

Het is van belang dat de gebruikersomgeving van de Afnemer continue aan de meest actuele beveiligingseisen voldoet. Het kan voorkomen dat op basis van interne of externe ontwikkelingen de aansluitvoorwaarden moet worden aangepast.

Enerzijds is het daarom van belang dat het aansluitbeleid, in samenwerking met belanghebbenden, geëvalueerd wordt. Anderzijds is het van belang om periodiek vast te stellen in hoeverre aan de verplichtingen uit het aansluitbeleid wordt voldaan en/of in hoeverre die worden nagekomen.

C.01 Evaluatie van aansluitbeleid		
Criterium/ *(ISO:Control)* *(wie en wat)*	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologiën.	BIG 5.1.2
Doelstelling *(waarom)*	Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau.	
Risico	*De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën.*	

Conformiteitsindicatoren en Maatregelen

Periodiek	
01	De organisatie beoordeelt minimaal jaarlijks of anders wanneer risico's zodanig zijn gewijzigd of de toereikendheid van de bescherming van eigen delen Suwinet moet worden aangepast
Verandering	
02	Periodiek wordt geëvalueerd of wet- en regelgeving of de risicoklasse van de via Suwinet beschikbaar gestelde gegevens zodanig zijn gewijzigd, dat de bescherming van eigen delen van Suwinet moet worden aangepast.
03	De organisatie evalueert regulier op basis van inzicht van haar eigen ICT omgeving, technologie ontwikkelingen (en waar mogelijk in ontwikkelingen op het gebied van cyber security) of de geïmplementeerde technische maatregelen adequaat zijn.
04	Het aansluitbeleid, wordt periodiek geactualiseerd op basis van evaluaties van de geïmplementeerde aansluitvoorziening, veranderingen in technologische vereisten, veranderingen in aan wetgeving en keten-brede afspraken (aansluitingsvoorwaarden).

C.02 Risicomanagement

Risicomanagement omvat de activiteiten binnen de decentrale organisatie (Afnemers) die erop gericht zijn om de risico's die gerelateerd zijn 'de eigen delen' van het Suwinet te beheersen. De risico's zijn weer afhankelijk van de kwetsbaarheden van de Suwinet componenten en de infrastructuur waarin deze kwetsbaarheden zich bevinden. Het is dan ook belangrijk dat de beveiligingsbehoeften aan de hand van een risicoanalyse worden bepaald. Een risicoanalyse is het systematisch beoordelen van:

- de schade die kan ontstaan door een beveiligingsincident als de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie en andere bedrijfsmiddelen wordt geschonden.

- de waarschijnlijkheid dat een beveiligingsincident optreedt rekening houdend met de aanwezige bedreigingen, kwetsbaarheden en de getroffen maatregelen.

Het is belangrijk om de beveiligingsrisico's en geïmplementeerde maatregelen periodiek te evalueren, om:

- in te kunnen spelen op wijzigingen in bedrijfsbehoeften en prioriteiten,
- nieuwe bedreigingen en kwetsbaarheden te bepalen,
- te bevestigen dat maatregelen nog steeds effectief en geschikt zijn,
- het geaccepteerd risico te kunnen vaststellen.

Bij het vaststellen van de risico's is het van belang dat de Afnemer rekening houdt met de risicoklasse van de gegevens van de bronhouders.

C.02 Risicomanagement		
Criterium/ *(ISO:Control)* *(wie en wat)*	Bij de beoordeling van de te treffen maatregelen ofwel risicomanagement houdt de Afnemer rekening met de risicoklasse van de berichten die worden uitgewisseld.	Bir H4
Doelstelling *(waarom)*	Voorkomen dat partijen een lager risicoklasse niveau hanteren aangaande de Suwinet beschikbaar gestelde gegevens, dan door de bronhouders is aangegeven.	
Risico	*Door het niet beheren en beheersen van risico's bestaat de mogelijkheid dat partijen onacceptabele schade leiden.*	

Conformiteitsindicatoren en maatregelen

Risico-klasse		
01	Bij aanschaf en of wijziging van informatiesystemen in relatie tot Suwinet wordt rekening gehouden met de risico-klasse van de bronhouder(s).	Bir/Big
02	De organisatie ziet erop toe dat via de Suwinet ontvangen gegevens beschermd zijn op minimaal het door de bronhouder(s) aangegeven niveau.	Bir/Big

C.03 Wijzigingenbeheer

Wijzigingenbeheer richt zich op het zodanig doorvoeren van wijzigingen in ICT-middelen en ICT-diensten (in relatie tot Suwinet) dat de kans op verstoring van de dienstverlening wordt geminimaliseerd en deze dienstverlening blijvend voldoet aan de functionele en beveiligingseisen van belanghebbenden.

C.03 Wijzigingenbeheer		
Richtlijn *(wie en wat)*	Afnemer heeft wijzigingenbeheer procesmatig en procedureel zodanig ingericht dat wijzigingen in relatie tot Suwinet tijdig, geautoriseerd en getest worden doorgevoerd.	NCSC Big/Bir 10.1.2 SoGP/Cobit
Doelstelling *(waarom)*	Zeker stellen dat wijzigingen in relatie tot Suwinet op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van Suwinet gegarandeerd blijft.	
Risico	Ongeautoriseerde acties kunnen worden doorgevoerd of acties zijn onvoldoende op elkaar afgestemd, waardoor de betrouwbaarheid van Suwinet in gevaar kan komen.	

Conformiteitsindicatoren en maatregelen

Procesmatig en procedureel		
01	Alle wijzigingen doorlopen formeel en systematisch alle processtappen: intake, acceptatie, impactanalyse, prioritering en planning, uitvoering (OTAP), bewaking en afsluiting.	Big/Bir 10.1.2 SoGP/Cobi
Tijdig		
02	Alle wijzigingen worden tijdig en geautoriseerd doorgevoerd in de verschillende OTAP-omgevingen.	Big/Bir 10.1.2 SoGP/Cobi
03	Landschap beïnvloedende wijzigingen worden tijdig gemeld bij de beveiligingsfunctionaris van de Beheerder.	Big/Bir 10.1.2 SoGP/Cobi
Geautoriseerd		
04	Alleen geautoriseerde wijzigingsverzoeken (Request for Change (RFC)) worden in behandeling genomen.	Big/Bir 10.1.2 SoGP/Cobi
Testen		
05	Alle wijzigingen worden altijd eerst getest voordat deze in productie genomen.	Big/Bir 10.1.2 SoGP/Cobi

C.04 Beoordeling van toegangsrechten

Het is nodig om de toegangsrechten van gebruikers/beheerders regelmatig te beoordelen om de toegang tot Suwinet diensten doeltreffend te kunnen beheersen. De toekenningen, wijzigingen en gebruik van toegangsrechten tot Suwinet dienen daarom periodiek gecontroleerd te worden. Hiertoe dienen maatregelen te worden getroffen in de vorm:

- Het voeren van controle activiteiten op de validiteit van de toegekende autorisaties en het gebruik en misbruik van deze autorisaties,
- het uitbrengen van rapportages aan het management over deze controle activiteiten.

C.04 Beoordeling van toegangsrechten		
Criterium (wie en wat)	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig[8] te beoordelen in een formeel proces (cyclisch proces).	BIG/BIR: 11.2.4
Doelstelling (waarom)	Het vaststellen of: – de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, – de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, – oneigenlijk autorisatie-toekenningen hebben plaatsgevonden.	

[8] Uitgangspunt is dat deze beoordeling maandelijks plaatsvindt; in specifieke situaties kan hiervan worden afgeweken, hetgeen in dat geval in de verantwoordings-/transparantierapportage dient te worden toegelicht.

C.04 Beoordeling van toegangsrechten

Risico	*Bij het ontbreken van controle op de toegangsrechten worden afwijkingen in het autorisatieproces niet gesignaleerd worden.* *Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd.*

Conformiteitsindicatoren en maatregelen

Toegangsrechten		
01	Afnemer heeft een actuele matrix waaruit blijkt welke gebruikers/beheerders welke rechten hebben op Suwinet diensten.	
02	Uit de actuele autorisatiematrix blijkt aan welke type functionaris welke rol(len) zijn toegekend en voor welk doel.	
Beoordelen		
03	Afnemer controleert periodiek de toegangsrechten van gebruikers/beheerders.	Big/BirR 11.2.4 1
04	De beoordelingsrapportage bevat kwetsbaarheden, zwakheden, mogelijk misbruik en verbetervoorstellen en wordt gecommuniceerd met verantwoordelijk management.	
05	Kwetsbaarheden, zwakheden worden toegelicht en verbetervoorstellen worden geprioriteerd op basis van risico's en hierover wordt een actielijst samengesteld	
06	Afnemer controleert regulier de rechtmatigheid van het gebruik van toegekende autorisaties.	
Formeel cyclisch proces		
07	De Afnemer heeft een formeel controle proces vastgelegd en vastgesteld welk onder andere behandelt: planning, uitvoering van scope, rapporteren en bespreken van verbetervoorstellen.	
08	De Afnemer heeft de taken en verantwoordelijkheden van functionarissen die betrokken zijn bij het evaluatieproces vastgelegd en vastgesteld.	
09	De autorisatiematrix wordt minimaal jaarlijks op juistheid, tijdigheid en volledigheid beoordeeld en formeel bekrachtigd door het verantwoordelijk management.	

C.05 Logging

Logging is het proces voor het registreren van technische activiteiten en gebeurtenissen. Hiermee kunnen achteraf fouten of rechtmatigheid van het gebruik van en ook vroegtijdige ongeautoriseerde toegangspogingen tot Suwinet diensten worden gesignaleerd.

Het loggen in relatie tot Suwinet spitst zich toe tot de rechtmatigheid van toegekende rechten en het gebruik hiervan.

C.05 Logging		
Criterium/ (ISO:Control) (wie en wat)	Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.	BIR 10.10.1 en 10.10.4
Doelstelling (waarom)	Alle handelingen die betrekking hebben op gebruikers en beheerders moeten herleidbaar zijn naar individuele personen.	
Risico	Zonder vastlegging en bewaking kan achteraf niet worden vastgesteld wie bepaalde handelingen heeft uitgevoerd.	

Conformiteitsindicatoren en maatregelen

Activiteiten van gebruikers en beheerders		
01	Alle activiteiten van gebruikers die gerelateerd zijn aan het gebruik van Suwinet diensten worden gelogd.	BIG/BIR 10.10.4
02	Alle Activiteiten van beheerders en gebruikers met speciale bevoegdheden worden gelogd.	
Audit-Logbestanden		
03	Logbestanden van het autorisatiebeheersysteem bevatten informatie over wanneer en door wie welke handelingen zijn uitgevoerd.	BIR 10.10.4
04	Alle uitzonderingen en informatiebeveiligingsgebeurtenissen worden vastgelegd in audit-logbestanden.	BIR 10.10.
06	Een logregel aangaande een handeling bevat minimaal: – De datum en het tijdstip van de handeling; – Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID; – Waar mogelijk de identiteit van het werkstation of de locatie; – De handeling; – Het object waarop de handeling werd uitgevoerd; – Het resultaat van de handeling.	BIG/BIR 10.10.4
07	Een logregel aangaande een gebeurtenis bevat minimaal: – De datum en het tijdstip van de gebeurtenis; – De gebeurtenis; – Het object en identiteit van het object waarop de gebeurtenis plaatsvond; – Het resultaat van de gebeurtenis.	BIG/BIR 10.10.4
08	Log-faciliteiten en informatie in logbestanden worden beschermd tegen onbevoegde toegang.	
Bewaard		
09	De logbestanden worden zodanig beschermd dat de informatie in deze bestanden zo nodig ontvankelijk is voor de rechtbank.	
10	De logbestanden worden gedurende een overeengekomen periode bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.	

C.06 Monitoring en rapportage

Onder monitoren wordt verstaan: signaleren, analyseren en rapporteren. In het kader van Suwinet is het begrip bijsturen hieraan toegevoegd.

Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot Suwinet diensten en ongeautoriseerd gebruik van deze diensten tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris.

Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd en te worden gerapporteerd (alerting). Alerting kan ook geautomatiseerd plaats vinden op basis van vastgestelde overschrijding van drempelwaarden.

Een deel van de logging (Suwinet inkijkfunctie) is in het bezit van de centrale beheerder en dient voor controle doeleinden maandelijks te worden opgevraagd.

C.06 Monitoring en rapportage		
Richtlijn (wie en wat)	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen)	Big/Bir 10.10.1
Doelstelling (waarom)	Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie.	
Risico	Afwijkingen niet worden gesignaleerd en derhalve niet kunnen worden aangepakt.	

Conformiteitsindicatoren en maatregelen

Signaleren, analyseren		
01	Afnemer analyseert periodiek (maandelijks[9]) en actief: - de gelogde gebruikersgegevens ten aanzien van het gebruik van Suwinet diensten - het optreden van verdachte[10] gebeurtenissen en mogelijke schendingen van de beveiligingseisen; - eventuele ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.	Big/Bir 10.10.1
02	De verzamelde log-informatie wordt in samenhang geanalyseerd.	Big/Bir 10.10.1
03	Periodiek worden de geregistreerde gebruikers- en beheerdersactiviteiten en systeemacties geanalyseerd.	Big/Bir 10.10.1
04	Periodiek worden de geanalyseerde en beoordeelde gelogde (gesignaleerde) gegevens aan de systeemeigenaren en/of aan het management gerapporteerd.	
Rapporteren		
05	De rapportages uit de beheerdisciplines compliancymanagement, vulnerability assessment, penetratietest en logging en monitoring worden op aanwezigheid van structurele risico's geanalyseerd en geëvalueerd.	Big/Bir 10.10.1

9 Uitgangspunt is dat de controle op de logging rapportages maandelijks plaatsvindt; in specifieke situaties kan hiervan worden afgewerken, hetgeen in dat geval in de verantwoordingsrapportage dient te worden toegelicht.

10 Verdachte gebeurtenissen zijn afwijkend en opmerkelijk gedrag ten aanzien gangbare patronen en geldende (beleids)regels.

06	De rapportage bevat informatie over kwetsbaarheden, zwakheden en misbruik en wordt gecommuniceerd met verantwoordelijk management.	Big/Bir 10.10.1
07	Op basis van analyses worden verbeteringsvoorstellen gedaan.	
Bijsturen		
08	Afnemer geeft aantoonbaar opvolging aan verbeteringsvoorstellen vanuit de analyse-rapportages.	Big/Bir 10.10.1
09	Het beveiligingsplan wordt jaarlijks conform P&C cyclus, of als uit geconsolideerde rapportages aanleiding toe is, geactualiseerd.	Big/Bir 10.10.1
10	De afnemer heeft de verantwoordelijkheid voor het realiseren van (delen) van het geactualiseerd beveiligingsplan in relatie tot Suwinet belegd.	Big/Bir 10.10.1

C.07 Evaluatie van IAA rapportages (organisatorisch en technisch)

In het Suwinet domein is het veilig inrichten en beheersen van identificatie, authenticatie en autorisatie (IAA) voor het gebruik van Suwinet diensten essentieel. Het is van belang om op basis van rapportages verkregen vanuit deze technisch en organisatorische invalshoeken te evalueren of er zich geen afwijken in de IAA beheersingsproces voordoen en of er structurele maatregelen noodzakelijk zijn.

Aan IAA wordt aandacht geschonken vanuit zowel organisatorisch perspectief (C.03 Beoordeling van toegangsrechten) als technisch perspectief (C.04 Logging C.05 Monitoring en rapportage).

C.07 Evaluatie van IAA (organisatorisch en technisch)		
Criterium/ (ISO:Control) (wie en wat)	De Afnemer voert periodiek[11] evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	obv notitie project
Doelstelling (waarom)	Bewerkstelligen dat zich geen leemtes in de beveiliging van IAA mechanismen voordoen.	
Risico	Zonder evaluaties van beide type rapportages bestaat het risico dat IAA mechanismen niet ingericht zijn conform de beveiligingseisen en dat zich afwijkingen en of bedreigingen hebben voorgedaan waartegen maatregelen moeten worden getroffen.	

Conformiteitsindicatoren en maatregelen

Periodiek evaluaties		
01	De systeem-verantwoordelijke rapporteert periodiek over de beveiliging en het rechtmatig gebruik van zijn systeem aan de bestuurlijk verantwoordelijke (portefeuille houder) aan de hand van o.a. beoordelings- en logging en monitoringsrapportages.	obv notitie project
02	De systeem-verantwoordelijke, die de controle uitvoert op de implementatie van de toegangsrechten, rapporteert periodiek de controlerapportages aan de Suwinet - procesverantwoordelijke of aan het verantwoordelijke management.	obv notitie project
Verbeteracties		
03	De verantwoordelijke functionaris evalueert deze rapportages, bespreekt de eindrapportages over de inrichting van IAA mechanismen met het management en neemt noodzakelijke verbeteracties.	obv notitie project
04	Vermoedens van misbruik (bijv. van autorisaties) worden met de betrokkene(n) besproken en bij het vaststellen van misbruik worden passende maatregelen getroffen.	obv notitie project

[11] Uitgangspunt is dat de uitvoering van deze evaluaties maandelijks plaatsvindt; in specifieke situaties kan hiervan worden afgeweken, hetgeen in dat geval in de verantwoordings-/transparantierapportage dient te worden toegelicht

C.08 Transparantie rapportage

Transparantie en verantwoording zijn instrumentele functies ten behoeve van besturing. Het zijn relaties tussen Principal (Bestuurder) en Agent (Uitvoerder). Afnemers en Bronhouders hebben te maken met Transparantie- en/of Verantwoordingsfunctie.

Transparantie is gericht op het "bieden van informatie" over de sturing, implementatie en beheersingsaspecten van de gebruikte Suwinet-diensten aan BKWI. BKWI beschouwt de 'Transparantie rapportage' als kennisgeving (Principe: recht tot het vernemen van kennis).

Verantwoording is een middel om over de 'mate van in control zijn' een verklaring af te geven. Met deze zogeheten 'In Control verklaring (ICV)' verstrekt de RvB (bijv. ZBO) aan de minister van SZW of het College (bij een Gemeente) aan de Gemeenteraad het signaal greep te hebben op de sturing van de dienstverlening en de informatiebeveiliging". Vaak gaat een ICV gepaard met een door een onafhankelijke instantie opgesteld getrouwheidsverklaring (GV) over de juistheid van de ICV

Een (bij de NOREA) geregistreerde IT auditor beoordeelt de ICV, en mogelijke bijbehorende TPM's, op getrouwheid en geeft daarmee een getrouwheidsverklaring (GV) af.

De GV en de ICV maken onderdeel uit van het Jaarverslag . (Principe: 'recht tot het ontvangen van een uitspraak' en 'laten acteren n.a.v. de uitspraak').

In het kader van Suwinet kunnen we onderscheid maken tussen verschillende type Bronhouders en Afnemers. Tabel 2 geeft een overzicht van de transparantie en verantwoording verplichtingen.

Organisatie	Afnemers/ Bronhouders	Instrumentele functie	Ontvanger van Verantwoording-/Transparantie Rapportages
Gemeenten	Type-G	Uitvoering door	College B&W
		Verantwoording aan	Gemeenteraad
		Transparantie aan	BKWI
ZBO	Type-Z	Uitvoering door	RvB
		Verantwoording aan	Min. SZW
		Transparantie aan	BKWI
Overigen	Type-O	Uitvoering door	Directie
		Verantwoording aan	Eigen bestuurlijk verantwoordelijke
		Transparantie aan	BKWI

Tabel 2 Overzicht horizontale en verticale informatie verschaffing (Transparantie en Verantwoording)

Zowel Transparantie- als de Verantwoordingsrapportage bevatten relevante informatie over de onderwerpen die in de voornoemde domeinen zijn beschreven. Het doel is de onderwerpen in samenhang te evalueren vanuit zowel organisatorische als vanuit technische invalhoek en de resultaten samenvattend weer te geven in een rapportage. Deze rapportage moet informatie bevatten over de opzet, bestaan en werking van de maatregelen die bij elke criterium behoren.

C.08 Transparantie rapportage	
Criterium/ (ISO:Control) (wie en wat)	Het management van de Afnemer (in geval van gemeenten is dit het college van B&W) publiceert en/of levert aan de Beheerder jaarlijks een transparantierapportage conform een afgesproken format.
Doelstelling (waarom)	Het geven van inzicht dat het interne deel van het Suwinet-domein juist is ingericht en dat er gehandeld wordt binnen de afgesproken uitgangspunten en aansluitingsvoorwaarden.
Risico	Onvoldoende onderling vertrouwen tussen ketenpartners in de toereikendheid van de geïmplementeerde- en beheerste maatregelen.

Conformiteitsindicatoren en maatregelen

Management		
01	Het management monitort en evalueert de transparantierapportage en ziet toe op de juistheid van de inhoud van de rapportage en dat deze tijdig wordt uitgebracht.	obv notitie project
Transparantierapportage		
02	De transparantierapportage geeft inzicht in evaluaties van de beleids-, implementatie- en beheersingsmaatregelen met betrekking tot opzet, bestaan en werking.	obv notitie project
03	De samenstelling van de transparantie- en verantwoordingsrapportage komt tot stand op basis van informatie verkregen uit interne- en externe bronnen (Externe uitbestede partij) en beoordelingen die binnen verschillende domeinen zijn verricht.	
04	De Transparantierapportage wordt vergezeld van een ICV	

Toelichting Transparantierapportage

Gemeenten leggen jaarlijks verantwoording af aan de gemeenteraad. Een afschrift wordt beschikbaar gesteld aan de beheerder. De beheerder maakt op basis daarvan de samengestelde rapportage. Voor gemeenten die volgens de ENSIA lijn hun verantwoording hebben ingericht, geldt dat transparantie middels de ENSIA lijn wordt ingevuld en de beheerder kan hiervan gebruik maken.

Onderwerpen tbv: Bronhouders en Beheer

Bronhouders

Beleidsdomein

Nr	*Onderwerpen*	
1	Classificatiebeleid	

Uitvoeringsdomein

Nr	*Onderwerpen*	
1	Externekoppelingen (DMZ)	

Controldomein

Nr	*Onderwerpen*	
	Incident en Probleembeheer	
2	Beschikbaarheidsbeheer	
3	Continuiteitsbeheer	

Beheerder (BKWI)

Beleidsdomein

Nr	*Onderwerpen*	
1	Suwi-Aansluitbeleid	
2	GeVS toegangsbeleid	
3	Naleving en Compliancy aansluitbeleid	
4	Externe partijen	
5	Taken, Verantwoordelijkheden en Functiescheiding	
6	GeVS beveiligingsfunctie	
7	Transparantie	
8	Suwi-landschap (architectuur	

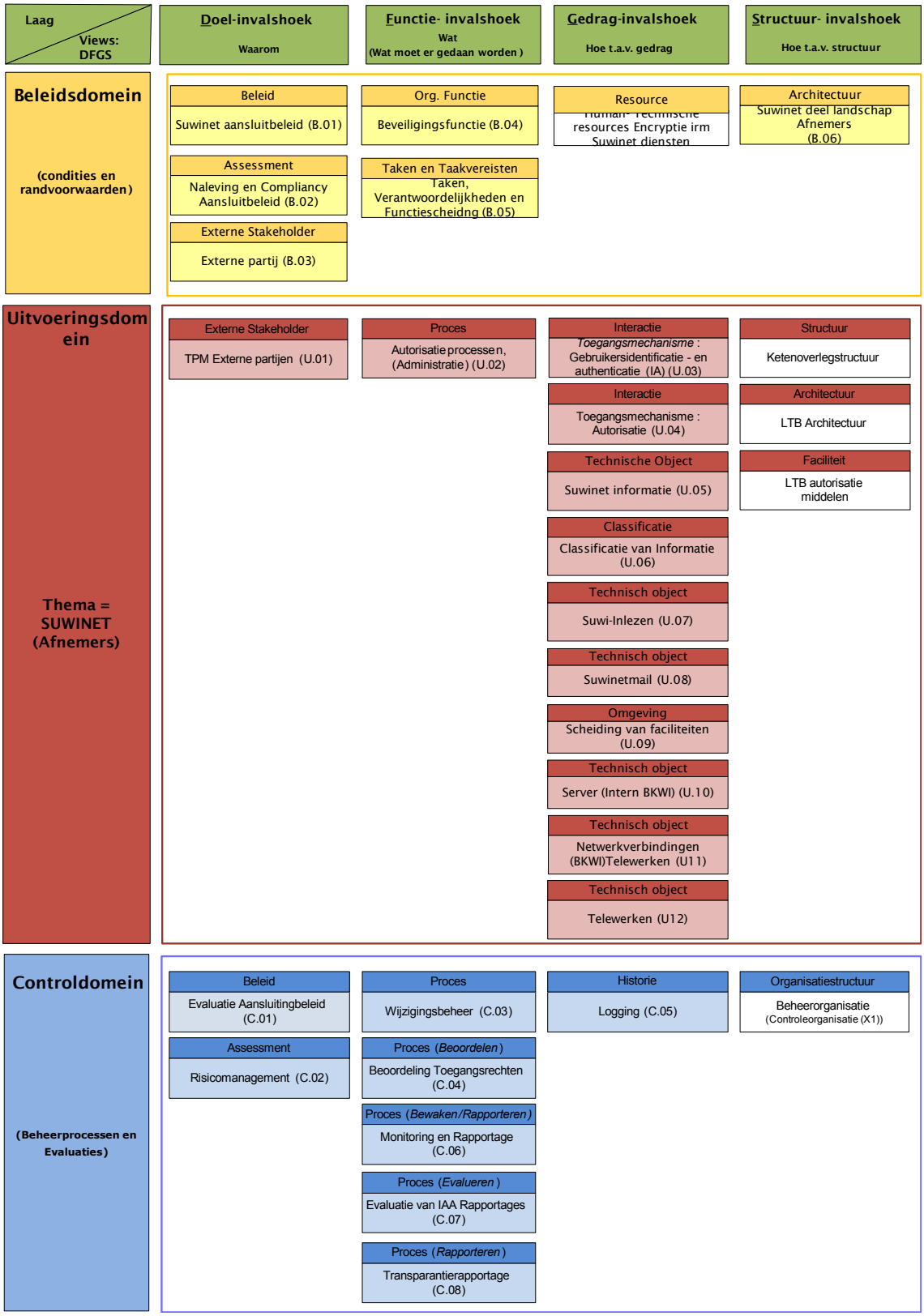
Uitvoeringsdomein

Nr	*Onderwerpen*	
1	Ketenstandaarden	
2	TPM Externe partijen	
3	Autorisatie beheerproces tbv Suwipartijen	
4	Toegangsmechanisme: Gebruikersidentificatie- en authenticatie (IA)	
5	Toegangsmechanisme: Autorisatie	
6	Suwi-berichtenuitwisseling(10.8.4)	
7	Suwinet-Mail	
8	Suwinet-Inlezen en DKD Inlezen (inleesfunctionaliteit)	
9	Suwinet-Inkijk (Inzien Suwi gegevens)	
10	Suwi-Meldingen	
11	Scheiding van faciliteiten	

12	Classificatie van informatie	
13	Server	
14	Netwerkverbindingen	
15	Telewerken	

Controldomein		
Nr	***Onderwerpen***	
1	Evaluatie van aansluitsbeleid	
3	Risicomanagement	
4	Incidentmanagement	
5	Wijzigingenbeheer	
6	Beoordeling van toegangsrechten	
7	Logging	
8	Monitoring en rapportage	
9	Evaluatie van IAA rapportages (organisatorisch en technisch)	
10	Transparantie	
11	Totaalrapportage	

Overzicht van objecten binnen Beleids-, Uitvoerings-, en Control domein



Bijlage 2: Taakomschrijving security officer Suwinet

Naam functionaris	**Security Officer Suwinet**
Functie medewerker	**Beleidsmedewerker team beleid**
Datum beschrijving	**3 december 2018**
Taakbenaming	**Security Officer Suwinet**
Plaats in organisatie	**Team beleid**

Algemene beschrijving
De security officer Suwinet is verantwoordelijk voor:

- het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen rond het gebruik van Suwinet.
- het toetsen op de uitvoering van regelgeving en procedures ten aanzien van Suwinet.
- het houden en evalueren van controles, toetsen en steekproeven en het verzorgen van een managementrapportage aan het MT Sociaal Domein.

Organisatie van de beveiliging binnen Suwinet
De werkzaamheden als security officer Suwinet omvatten ten minste de volgende onderdelen:

- het (laten) verzorgen van voorlichting en stimuleren van risicobewust gedrag bij medewerkers die gebruik maken van Suwinet (minimaal 1x per jaar).
- het (laten) verzorgen van een introductie over het veilig gebruik van Suwinet voor nieuwe medewerkers.
- het (laten) verzorgen van rapportage over de verleende autorisaties aan de betreffende leidinggevenden (minimaal 1x per kwartaal).
- het steekproefsgewijs uitvoeren van controles op de uitvoering en naleving van beveiligingsprocedures binnen Suwinet (minimaal 1x per kwartaal).
- het periodiek opvragen van logging-gegevens over het gebruik van Suwinet bij het BKWI en het analyseren van deze gegevens om mogelijk misbruik of oneigenlijk gebruik te signaleren (minimaal 1x per kwartaal).
- het direct signaleren van misbruik en/of oneigenlijk gebruik van Suwinet aan de eigen leidinggevende en aan de informatiebeveiligingscoördinator zodat deze maatregelen kunnen nemen.
- het actueel houden van het overzicht waarbij de door het BKWI gedefinieerde Suwinet-rollen worden gekoppeld aan functies/personen die werkzaam zijn voor de gemeente Deventer.
- het controleren van verleende autorisaties - toets of de juiste rol is toegekend aan een persoon – in overleg met de betreffende leidinggevenden (minimaal 1x per kwartaal).
- het toetsen op onverenigbare rollen – combinatie van niet te verenigen rollen die aan een persoon zijn toegekend – (minimaal 1x per kwartaal).
- het toetsen of de beveiligingsprocedures rond Suwinet aangepast dienen te worden op basis van gewijzigde wet- en regelgeving en/of organisatiewijzigingen (minimaal 1x per jaar).
- het zo nodig (laten) ontwikkelen en/of actualiseren van beveiligingsprocedures.
- het regelmatig toetsen van gemelde incidenten die binnen Suwinet voorkomen en zo nodig ondernemen van acties.
- het bespreken van beveiligingsonderwerpen met betrokken organisaties en/of derden met betrekking tot het gebruik van Suwinet.
- het controleren of de medewerkers binnen Suwinet beschikken over voldoende kennis en vaardigheden.
- het gevraagd en ongevraagd adviseren van de eigen organisatie ten aanzien van technische, organisatorische of fysieke verbeteringen m.b.t. het gebruik van Suwinet.
- het periodiek (één keer per kwartaal) bespreken van beveiligingsonderwerpen met de informatiebeveiligingscoördinator.
- het rapporteren over de beveiliging en het gebruik van Suwinet aan het MT Sociaal Domein en de informatiebeveiligingscoördinator (minimaal 1x per jaar).

Rapportage en verantwoording
Tenminste 1x per jaar wordt over de beveiligingsstatus van Suwinet gerapporteerd aan het MT Sociaal Domein. Deze rapportage bevat minimaal informatie over:

- de uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken en toetsingen;
- aanwezigheid van onverenigbare rollen.
- frauduleus gedrag van medewerkers of niet volgen van procedures.
- geconstateerde tekortkomingen in de beveiligingsvoorzieningen.
- wijziging van procedures / afspraken / opvolgingspatroon.
- het handelen in afwijking met de vastgelegde functiescheiding.
- afwijkingen of wijzigingen op volgens de toegestane rol toegekende autorisaties.

Functietypering

Functietypering:	• Kennis van de werkprocessen waarbij gebruik wordt gemaakt van Suwinet; • Bekendheid met beveiligingseisen & procedures; • Redactionele en communicatieve vaardigheden; • Organisatorisch inzicht; • Probleemoplossend vermogen.
Contacten:	Gebruikers van Suwinet binnen de gemeente Deventer, informatiebeveiligingscoördinator, vertrouwenspersoon, leveranciers, BKWI en Inspectie SZW.

Bijlage 4: Procedure Autorisatie tot Suwinet (IDU)

De procedure voorziet in het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet en de controle hierop.
Met een autorisatie wordt bedoeld het door het bevoegd gezag verstrekken van een gelegitimeerde toegang tot één of meerdere informatiesystemen van de gemeente.

Achtergrond
Op basis van de autorisatiematrix waarin rollen staan omschreven, wordt de toegang tot het Suwinet geregeld. Maandelijks wordt er aan de hand van een IDU lijst (in- door- en uitstroomlijst) gecontroleerd of een ieder nog gebruik mag maken van het Suwinet.

Wachtwoorden
Suwinet is voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes De wachtwoorden voor Suwinet zijn maximaal 90 dagen geldig. Wanneer een gebruiker gedurende 90 dagen achtereen niet heeft ingelogd wordt het wachtwoord automatisch geblokkeerd. Na drie maal foutief inloggen wordt het account automatisch geblokkeerd.

Proces controle IDU
Er wordt op een 4 tal punten een controle uitgevoerd;

1. Nieuwe gebruikers die zijn toegevoegd worden met Groen gearceerd;
2. Oude gebruikers die worden verwijderd worden met Rood gearceerd;
3. Geblokkeerde accounts (langer dan drie maanden geen gebruik) worden beëindigd en met Rood gearceerd.
4. Gebruikers welke andere werkzaamheden krijgen en waarvan de rol op Suwinet gewijzigd wordt, worden met Geel gearceerd.

De IDU lijst wordt voor de 1ste van de maand opgesteld en verwerkt

Beheer
Om toegang te kunnen krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie(s) tevens een bevoegdheid nodig op netwerk- en/of het systeemniveau. Deze bevoegdheden worden beheerd door de systeembeheerder. De bevoegdheden binnen Suwinet worden beheerd door de applicatiebeheerder Suwinet.

Proceseigenaar
De overkoepelende proceseigenaar is de teammanager van het team Inkomensondersteuning. De proceseigenaar is ervoor verantwoordelijk dat per de 1e van de maand een definitieve IDU-lijst is opgesteld met daarin alle werkzame personen binnen de teams en daarbij de juiste profielen met de daarbij behorende autorisaties.

Verantwoordelijkheid
De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het college van B&W en namens dit college bij de teammanager van het team Inkomensondersteuning.
De verantwoordelijkheid om toegang te verlenen tot de gegevens, behorend bij Suwinet, berust bij de teammanager van het team Inkomensondersteuning. De uitvoering hiervan en het up-to-date houden van de procedure ligt bij de Security Officer Suwinet.

Uitvoering

Stap1
De IDU lijst (lijst met alle gebruikers en beheerders, de rol en status account) wordt door de administratief ondersteuner van team IO opgevraagd, middels een call in Topdesk;

Stap 2
De IDU lijst, wordt doorgezet aan werkgroep lid Suwinet (gebruiker)/ gemachtigde Suwinet.

Stap 3
Door het werkgroep lid/ gemachtigde wordt bij de betreffende teammanagers/senioren uitgevraagd of de betrokken collega's nog steeds werkzaamheden uitvoeren waarvoor het suwinet noodzakelijk is. (m.u.v. team manager IO, de ontwikkelingen binnen het team zijn bekend en deze manager zal de IDU lijst goedkeuren).

Stap 4
De IDU lijst wordt n.a.v. de managers/senioren opgesteld en alle mutaties worden op de IDU lijst doorgegeven.

Stap 5
De IDU lijst wordt verstuurt naar de administratief medewerker van team IO. Zij zorgt ervoor dat de lijst door de overstijgend manager van team IO akkoord wordt bevonden.

Stap 6
De administratief medewerker van team Inkomensondersteuning stuurt de ondertekende lijst door naar functioneel beheer en de Security Officer Suwinet.

Stap 7
De wijzigingen worden door functioneel beheer verwerkt en koppelt doorgevoerde wijziging terug aan de administratief medewerker en Security Officer Suwinet via afsluiten melding in Topdesk als melding via dat kanaal is binnengekomen.

Stap 8
De Security Officer Suwinet archiveert de ondertekende IDU lijst.

Periodieke controle autorisaties

Maandelijks worden lijsten met de gegevens over in-uit-en-doorstroom opgesteld en gecontroleerd. Jaarlijks wordt de autorisatiematrix gecontroleerd op rollen en toebedeelde taken/autorisaties. Beoordeeld wordt of de geïmplementeerde autorisaties overeenkomen met de toegekende autorisaties. Daarnaast wordt gecontroleerd of de geregistreerde gebruikers en de aan hen toegekende autorisaties op inhoud correct zijn.

Wanneer geconstateerd wordt dat een medewerker 3 maanden of langer geen gebruik heeft gemaakt van zijn/haar Suwinet-account, zal de autorisatie beëindigd worden door Functioneel beheer. Wanneer sprake is van beëindiging agv een inactief account, wordt dit door Functioneel beheer aangegeven op de lijst.

Bijlage 5: Procedure controleren gebruik Suwinet

Door het BKWI worden generieke (anonieme) 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. In deze generieke rapportages worden kengetallen van de gemeente naast die van het landelijke gemiddelde gelegd.

Maandelijks worden deze generieke rapportages door het BKWI beschikbaar gesteld.
De gegevens van deze rapportages bevatten de volgende gegevens:

- Aantal bevragingen met een gevulde zoeksleutel, anders dan Burgerservicenummer per maand;
- Aantal bevragingen van unieke Burgerservicenummers per maand;
- Aantal bevragingen met een gevulde zoeksleutel, anders dan Burgerservicenummer per pagina per maand;
- Aantal bevragingen binnen/ buiten kantooruren per maand;
- Aantal bevragingen en aantal gebruikers per maand;
- Top 5 opgevraagde Burgerservicenummers per maand;
- Aantal inlogpogingen per maand;
- Top 5 gebruikers met het hoogste aantal bevragingen per maand;
- Aantal accounts per gebruikersrol per maand;
- Aantal geregistreerde accounts per afdeling;
- Aantal accounts per account status
- Aantal gebruikers die langer dan 90 dagen niet ingelogd hebben;
- Aantal verzonden Suwinet e-mails;
- Aantal ontvangen Suwinet e-mails;
- Verzonden Suwinet e-mails naar domein;
- Ontvangen Suwinet e-mails van domein;
- Whitelist gebruik (geraadpleegde BSN die geen relatie hebben met de participatiewet of ioaw/z bbz).

Periodiciteit
Jaarlijks worden normen opgesteld waarlangs de resultaten van de maandelijkse generieke rapportages worden beoordeeld. Deze normen worden vastgesteld door de leden van het Suwinet-overleg, bestaande uit de Security Officer Suwinet, de functioneel beheerder en de gemandateerde (medewerker(s) uit de uitvoering). Maandelijks wordt tijdens het Suwinet-overleg de generieke rapportage van de afgelopen maand besproken. De functioneel beheerder voegt de resultaten van de generieke rapportages in een excelbestand, zodat per maand de resultaten zichtbaar zijn en vergeleken kunnen worden. Daarnaast zijn de gemiddelde resultaten van de afgelopen jaren zichtbaar.
Indien een overschrijding van één of meerdere normen plaatsvindt, dan wordt in beginsel een nadere rapportage opgevraagd door de gemandateerde. De resultaten van de nadere rapportage worden tijdens het volgende Suwinet-overleg besproken.
De controle en conclusies met betrekking tot de generieke en nadere rapportages worden vastgelegd in notulen. Deze notulen worden op een afgesloten plek op intranet opgeslagen, welke eveneens toegankelijk zijn voor de CISO. Jaarlijks wordt hierover gerapporteerd in de “Evaluatie gebruik Suwinet”.

Omwille van de privacy worden de opgevraagde specifieke rapportages en eventuele andere documenten waarin persoonsgegevens zijn opgenomen bewaard in een afgesloten omgeving.

Het informeren over de rapportages en adviseren over vervolgstappen;
Zijn er signalen over oneigenlijk gebruik dan wordt opgeschaald naar de betreffende teammanager. De Individuele medewerker wordt gevraagd zijn/haar zoekgedrag te verantwoorden.

Indien blijkt dat de medewerker het zoekgedrag niet kan verantwoorden en er zijn aanwijzingen voor norm overschrijdend gedrag dan wordt gehandeld volgens het vastgestelde integriteitsbeleid. Team ASK (onderdeel P&O) wordt in dat geval ingeschakeld. Er wordt dan gehandeld conform artikel 16 van de CAR/UWO.

Periodieke rapportage over controles, resultaten en maatregelen aan bestuur.
In het beveiligingsplan Suwinet, dat jaarlijks moet worden vastgesteld, is een hoofdstuk Evaluatie gebruik Suwinet opgenomen. In dit hoofdstuk worden de resultaten van de uitgevoerde controles vermeld.

Termijn bewaren gegevens
De gegevens worden maximaal twee jaar bewaard op de G-schijf.
Dit wordt jaarlijks gecontroleerd.

Bijlage 6: Spelregels gebruik Suwinet

Gebruikers van Suwinet hebben toegang tot privacygevoelige gegevens. Uiteraard moet zorgvuldig worden omgegaan met de via Suwinet verkregen gegevens. Op het gebruik van Suwinet wordt toezicht uitgeoefend door het Bureau Keteninformatisering Werk en Inkomen (BKWI) en de gemeente.

Omdat u gebruiker wordt van Suwinet staan hieronder relevante regels in het kader van privacy en correct gebruik Suwinet.

U bent verplicht om zorgvuldig en correct met de informatie om te gaan waarover u de beschikking heeft. U mag de verkregen informatie niet ten eigen bate of ten behoeve van uw persoonlijke betrekkingen gebruiken. De gegevens die opgevraagd worden via Suwinet mogen niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd (uitvoering participatiewet ioaw, ioaz en bbz).

Kortom:
- U mag alleen gegevens opvragen die u nodig heeft om uw werk te kunnen doen. Gebruik voor andere doeleinden (privé, vereniging etc.) is niet toegestaan.
- U heeft geheimhoudingsplicht inzake de via Suwinet verkregen gegevens.
- De gegevens mogen niet worden uitgewisseld met derden zonder toestemming van de cliënt (uitgezonderd bijzonder onderzoek wanneer dat wordt ingezet).
- U draagt er zorg voor dat de print van de gegevens niet ter inzage kan komen van onbevoegden: de print is opgeborgen wanneer u uw bureau verlaat en de print wordt opgeborgen in het dossier wanneer het werkproces is afgesloten. Dit geld ook wanneer u thuis werkt.
- U draagt er zorg voor dat niet-geautoriseerde geen gebruik kunnen maken van Suwinet.
- U sluit dus het programma af wanneer u uw (thuis)werkplek verlaat.

Op het gebruik van Suwinet wordt toezicht uitgeoefend door het Bureau Keteninformatisering Werk en Inkomen (BKWI). Het BKWI is verplicht om gegevens bij te houden (te loggen) waarmee het gebruik van Suwinet inkijk per medewerker van o.a. de gemeente kan worden nagegaan.

De volgende gegevens worden bijgehouden (gelogd) in een tabel:
- Aantal bevragingen met een gevulde zoeksleutel, anders dan Burgerservicenummer per maand;
- Aantal bevragingen van unieke Burgerservicenummers per maand;
- Aantal bevragingen met een gevulde zoeksleutel, anders dan Burgerservicenummer per pagina per maand;
- Aantal bevragingen binnen/ buiten kantooruren per maand;
- Aantal bevragingen en aantal gebruikers per maand;
- Top 5 opgevraagde Burgerservicenummers per maand;
- Aantal inlogpogingen per maand;
- Top 5 gebruikers met het hoogste aantal bevragingen per maand;
- Aantal accounts per gebruikersrol per maand;
- Aantal geregistreerde accounts per afdeling;
- Aantal accounts per account status
- Aantal gebruikers die langer dan 90 dagen niet ingelogd hebben;
- Aantal verzonden Suwinet emails;
- Aantal ontvangen Suwinet emails;
- Verzonden Suwinet emails naar domein;
- Ontvangen Suwinet emails van domein;
- Whitelist gebruik (geraadpleegde bsn die geen relatie hebben met de participatiewet of ioaw/z bbz).

Het doel van deze logs is tweeledig:
1. Tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking;
2. Wetenschappelijke en/of statistische doeleinden.

De gemeente vraagt periodiek het rapport “gebruik van SUWI Services” op. Het gaat hierbij om een rapportage die geen op persoon herleidbare gegevens bevat. De project groep suwinet beoordeelt deze gegevens. Zodra een score in een van de hierboven vermelde tabellen daar aanleiding toegeeft, zullen op medewerker herleidbare gegevens worden opgevraagd. Hiertoe vraagt de gemandateerde een specifieke rapportage op bij de beheerder (BKWI).

Wanneer blijkt dat een specifieke medewerker de hierboven gestelde eisen niet naleeft, wordt de desbetreffende medewerker hierover door zijn teammanager gehoord. Die beziet of al naar gelang de ernst en de gevolgen van de overtreding of overgegaan wordt tot het geven van een waarschuwing of tot het treffen van disciplinaire maatregelen in het P&O-spoor.

Wij vragen je de e-learning module te volgen op de site van de VNG. Een kopie van het certificaat overleg je aan l.de.waal@deventer.nl;

Link naar de e-learning module https://www.vngacademie.nl/e-learning

Bijlage 7: Tien gouden tips bij beveiliging van persoonsgegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving.
Als handvat hierbij 10 gedragsregels voor medewerkers van de teams Inkomensondersteuning, Publiekscontacten, Belastingen en Deventer Werktalent.

1. Beheren van wachtwoorden
De gebruiker moet het door functioneel beheer uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Periodiek vervalt dat wachtwoord. De gebruiker beheert dus het eigen wachtwoord.
Zodra een medewerker de gemeente verlaat, wordt het account verwijderd door de applicatiebeheerder.
Wanneer het account niet wordt gebruikt, vervalt het account automatisch.

2. Melden van beveiligingsincidenten
Het is belangrijk dat beveiligingsincidenten worden gemeld bij de ICT Servicedesk. De medewerkers van de Servicedesk kunnen vervolgens een andere functionaris die daartoe is bevoegd is, inschakelen om dat incident te onderzoeken.
Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht
Binnen de afdeling wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Algemene Verordening Gegevensbescherming (AVG)). In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens alleen gebruikt mogen worden voor de uitoefening van de functie.

4. Gedragscode internet- en e-mailgebruik
De gemeente hanteert een protocol voor gebruik van e-mail en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe e-mail en internet wordt geobserveerd.

5. Kennisnemen van het informatiebeveiligingsbeleid
Het binnen de gemeente geldende informatiebeveiligingsbeleid (inclusief instructies en protocollen) is op iedereen binnen het team van toepassing die gebruik maakt van Suwinet-Inkijk. Bestaande gebruikers zijn op de hoogte; nieuwe gebruikers worden op de hoogte gesteld.
Gebruikers van Suwinet-Inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers.

6. Gegevensverstrekking aan derden via de telefoon
Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen.
Het voeren van telefoongesprekken brengt namelijk de risico's met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben.
In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging.
Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien afkomstig van een vaste contactpersoon.

7. Clean desk en clear screen policy
De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven.
Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers.
Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord), zodra de medewerker de werkplek verlaat.

8. Geen vertrouwelijke gegevens in de prullenbak
De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk binnen de afdeling. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Binnen de gemeente is geregeld hoe vertrouwelijke stukken worden verzameld en vernietigd en iedereen is daarvan op de hoogte. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een prullenbak of een bak die bestemd is voor oud papier.

9. Aanspreken van onbekende personen
Als je een onbekende persoon in de gang tegenkomt waar officieel geen publiek zonder begeleiding mag komen, spreek je deze persoon aan. Je vraagt deze persoon zichzelf voor te stellen en vraagt wat hij/zij hier doet. Personen die niet bevoegd zijn, wordt beleefd maar duidelijk begeleid naar het publieke gedeelte van het gebouw.

10. De dagelijkse werkzaamheden vs. Informatiebeveiliging
Informatiebeveiliging is uitermate belangrijk voor het werk binnen een afdeling waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook inwoners vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom in het werkoverleg geregeld aandacht aan dit onderwerp wordt gegeven.

GEHEIMHOUDINGSVERKLARING

Ondergetekende :

Geboren op :

Wonende te :

Werkzaam in de functie van :

Bij het team :

Vast/tijdelijk dienstverband :
(ingeval van een tijdelijk dienstverband dient de periode te worden vermeld)

VERKLAART

zich hierbij te verplichten tot geheimhouding van hetgeen hem/haar tijdens de uitoefening van zijn/haar functie ter kennis komt.

Bij schending van deze geheimhoudingsverplichting ontstaat het risico strafrechtelijk vervolgd te worden op basis van artikel 272 van het Wetboek van Strafrecht.

(artikel 272 Wetboek van Strafrecht luidt: "Hij, die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel vroeger ambt, beroep of wettelijk voorschrift verplicht is te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.")

Deventer,

Naam:

Handtekening