Nota voor Burgemeester en Wethouders

Team: Beleid
Onderwerp:
Beveilingsplan Suwinet 2022-2026

Notagegevens		
Bestuursorgaan	:	B-en-W 7-12-2021
Notanummer	:	2021-324
Datum	:	7-12-2021
Programma	:	07-Inkomensvoorziening en arbeidsmarkt
Portefeuillehouder	:	Wethouder De Geest,
Bijlage(n)	:	Beveiligingsplan Suwinet 2022-2025.docx,Format geheimhoudingsverklaring.doc,Specifiek Suwinet-normenkader Afnemers.1.01.2017.pdf,Suwinet_autorisatiematrix_deel I.pdf,Taakomschrijving security officer suwinet.docx,Tien gouden tips bij beveiliging van persoonsgegevens.docx

Parafering

01-12-2021: Programmamanager
30-11-2021: Wethouder

Agendering

* 02-12-2021: Gemeentesecretaris/algemeen directeur

Definitieve akkoord

8-12-2021

B & W d.d.: 7-12-2021

Besluit

1. Het beveiligingsplan Suwinet 2022-2026 gemeente Deventer vast te stellen
2. De nota en het besluit openbaar te maken, met uitzondering van de bijlage "autorisatiematrix"

De nota en het besluit openbaar te maken met uitzondering van de bijlage "autorisatiematrix" in het kader van artikel 10 WOB

Inleiding

Voor een goede uitvoering van de Participatiewet, de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW) en de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) heeft de gemeente gegevens nodig van andere partijen. Bijvoorbeeld bij het vaststellen van het recht op een uitkering. Partijen, waaronder gemeenten, UWV en de Belastingdienst, maken hiervoor gebruik van Suwinet. Dit is een informatiesysteem dat een veilige omgeving biedt voor het delen van gegevens. Het gaat hier om privacygevoelige gegevens, zoals inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, bijstandsuitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering.

Behandeling van deze gegevens moet op zorgvuldige en controleerbare wijze geschieden. Over het gebruik van Suwinet dient dan ook verantwoording afgelegd te worden. Dit gebeurt op basis van 14 normen. Deze normen worden afzonderlijk in het onderhavige beveiligingsplan beschreven, waarbij per norm wordt

toegelicht welke beveiligingsmaatregelen worden genomen.

Het laatst vastgestelde beveiligingsplan dateert uit 2019. Het plan is voor drie jaar vastgesteld. Omdat de werkingstermijn van een beveiligingsplan Suwinet op dat moment drie jaar was (nu is dit vier jaar) moet nu een nieuw beveiligingsplan met ingang 2022 vast te laten stellen.

De belangrijkste normen worden hieronder kort toegelicht:

1. Inrichten van een Beveiligingsfunctie Suwinet

De gemeente Deventer heeft twee Security Officers. Deze functionarissen zijn verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document en bevorderen de informatiebeveiliging en de communicatie naar de medewerkers over het gebruik van Suwinet.

2. Scheiding van taken, verantwoordelijkheden en functies

Er is een autorisatiematrix, waarin de scheiding van taken, verantwoordelijkheden en functies staat beschreven. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur, dat de medewerker alleen die gegevens kan raadplegen die van belang zijn voor zijn/haar werkzaamheden.

3. Monitoring, rapportage en controle

Alle handelingen die in Suwinet plaatsvinden worden door het Bureau Keteninformatisering werk en inkomen (BKWI) gelogd. Deze informatie wordt maandelijks in een rapportage door BKWI beschikbaar gesteld. Het is de taak van de Security Officers om deze informatie te controleren en te analyseren op het zorgvuldig gebruik van Suwinet. Tevens wordt in een controle beoordeeld of alle autorisaties nog overeenkomstig de matrix zijn afgegeven. Signalen van mogelijk onrechtmatig gebruik worden vastgelegd en onderzocht. Ieder half jaar wordt over de uitkomsten van de maandelijkse controles en de eventuele verbeteracties gerapporteerd aan de teammanager Werk&Inkomen en de CISO.

4. Verantwoording

Jaarlijks moet door middel van beantwoording van de ENSIA-vragenlijst (in de digitale omgeving van de ENSIA-tool) verantwoord worden hoe de gemeente Deventer invulling geeft aan de gestelde normen. Hiermee voldoen we aan de eisen van transparantie. De beheerder (BKWI) kan van de ENSIA-verantwoording/controleverklaring gebruikmaken. Over 2021 is de ENSIA-vragenlijst ingevuld door de Security Officers. Verantwoording aan het college en de gemeenteraad over de normen geschiedt tevens via de ENSIA-tool.

Dit beveiligingsplan is in gezamenlijkheid met de gemeente Raalte en Olst-Wijhe opgesteld.

Beoogd maatschappelijk resultaat

Vaststellen van onderhavig beveiligingsplan, waarmee de gemeente Deventer een kader biedt voor een correcte uitvoering en naleving van de beveiligingseisen die passen bij Suwinet.

Kader
* Ensia verantwoording
* Baseline Informatiebeveiliging Overheid (BIO).
* Specifiek Suwinet normenkader Afnemers

Betrokken partijen en participatie
Dit beveiligingsplan is in gezamenlijkheid met de gemeente Deventer en Olst-Wijhe opgesteld omdat op dit thema al veel wordt samengewerkt en het wenselijk is om in gezamenlijkheid tot een nieuw beveiligingsplan te komen.

Argumenten voor en tegen
Voor

Een vastgesteld beveiligingsplan is voorwaardelijk om aangesloten te kunnen zijn op Suwinet. Zonder deze aansluiting kunnen wij geen gebruik maken van een beveiligde omgeving waarin gegevens met andere instanties binnen de SUWI-keten kunnen worden gedeeld. Dit heeft gevolgen voor het beoordelen van de rechtmatigheid op grond van de Participatiewet.

Het beveiligingsplan is in samenwerking met de gemeente 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.

Financiële consequenties en dekking
Het Beveiligingsplan Suwinet heeft geen financiële consequenties.

Openbaarmaking en communicatie
Het beveiligingsplan wordt gecommuniceerd met de teammanager Inkomensondersteuning, de security - en privacy officer.

Aanpak en uitvoering
n.v.t.

Beveiligingsplan Suwinet 2022-2025

Domein Sociaal gemeente Deventer

Deventer, november 2021

Inhoudsopgave

Hoofdstuk 1	**Inleiding**	**2**
1.1	Kader voor het Suwinet beveiligingsbeleid	2
1.2	Grondslagen op grond waarvan Suwinet gebruikt mag worden	3
1.3	Leeswijzer	3
Hoofdstuk 2	**Beveiligingsplan Suwinet**	**4**
Hoofdstuk 3	**Evaluatie 2020**	**8**

Bijlagen

Bijlage 1	Specifiek Suwinet-normenkader afnemers
Bijlage 2	Benoeming en taakomschrijving Security Officer Suwinet
Bijlage 3	Autorisatiematrix
Bijlage 4	Autorisatieprocedure Suwinet
Bijlage 5	Procedure uitvoeren periodieke controles Suwinet
Bijlage 6	De tien ‘gouden’ gedragsregels gebruik Suwinet
Bijlage 7	Geheimhoudingsverklaring medewerkers
Bijlage 8	Protocol inzage Suwinet door cliënt

Hoofdstuk 1 Inleiding

Gemeenten hebben als uitvoerders 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), de stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, de Dienst Uitvoering Onderwijs (DUO), de Sociale Verzekeringsbank (SVB), 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 Burgerservicenummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers.

Een belangrijk aspect bij het opvragen, opslaan en delen van gegevens is de Wet eenmalige gegevens uitvraag (WEU). 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.

Zoals genoemd worden gegevens binnen de applicatie Suwinet-Inkijk op basis van het 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.
Omdat Suwinet dergelijke privacygevoelige gegevens bevat, moeten klanten erop kunnen vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft dan ook al bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Uiteraard zijn er op het gebied van gegevensbeveiliging sindsdien vele (grote) ontwikkelingen geweest. Dit beveiligingsplan dient dan ook als kader waarbinnen we het zorgvuldig gebruik van Suwinet willen borgen.

1.1 Kader voor het Suwinet beveiligingsbeleid

Vanaf 1 januari 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO voorziet in een uniform en uitgebreid normenkader informatiebeveiliging voor de gehele overheidssector. Organisaties die de BIO (moeten) implementeren werken daarmee aan het verzekeren van een adequaat niveau van informatiebeveiliging. Jaarlijks vindt op basis van het normenkader van de BIO verantwoording plaats. Voor Suwinet geldt dat we met ingang van 2020 over 14 normen verantwoording moeten afleggen. Het “Normenkader GeVS” is afzonderlijk in bijlage 1 toegevoegd.

De verantwoording over informatieveiligheid met betrekking tot Suwinet is met ingang van 2017 ondergebracht in de bredere gemeentelijke verantwoording over informatieveiligheid en wordt ENSIA (Eenduidige Normatiek Single Information Audit) genoemd. Suwinet is één van de onderdelen waarover de gemeente zich horizontaal aan de gemeenteraad en verticaal aan de (landelijke) toezichthouders verantwoordt. ENSIA is in 2017 ontstaan op initiatief van gemeenten en de ministeries van BZK en SZW en is in het leven geroepen om een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te bieden. Gemeenten gebruiken ENSIA om zich te verantwoorden over de staat van informatiebeveiliging op basis van de BIO (Baseline Informatiebeveiliging Overheid).

Via het ENSIA-platform stellen gemeenten op digitale wijze rapportages en informatie beschikbaar over de zelfevaluatie, de Collegeverklaring ENSIA en het Assurancerapport aan de minister van BZK ten behoeve van het toezicht op de BRP en Reisdocumenten, DigiD, de BAG, de BGT en de BRO. Namens de minister van BZK verwerkt Logius de verantwoordingsinformatie over DigiD. Verder bieden gemeenten via ENSIA transparantie aan de beheerder van de centrale omgeving van de GeVS4

[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.

(BKWI)5 ten behoeve van het jaarlijks opstellen van een totaaloverzicht van de beveiliging van de GeVS. Deze rapportage wordt uitgebracht aan het ketenoverleg GeVS en de minister van SZW. De Inspectie SZW houdt onafhankelijk signalerend toezicht op het functioneren van het stelsel werk en inkomen. Met ingang van 2021 wordt via de Waarderingskamer verantwoording afgelegd aan de minister van Financiën met betrekking tot de WOZ. Toezichthouders kunnen, indien nodig, nader onderzoek doen. Hiervoor zijn protocollen aanwezig bij de betrokken ministeries

Om de bredere focus van informatieveiligheid beter te borgen, is het strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022 vastgesteld. Dit beveiligingskader dient dan ook als kapstok waaraan het specifiek voor Suwinet opgestelde plan opgehangen kan worden. Het beveiligingsplan Suwinet geeft dan ook aan hoe we uitvoering geven op het terrein van Suwinet aan de kaders zoals gesteld in het genoemde beleidskader.

Hierbij moet wel opgemerkt worden dat informatiebeveiliging de verantwoordelijkheid is van elke gemeente afzonderlijk. De lijnverantwoordelijkheid ligt bij de teams die Suwinet gebruiken. Het College legt hierover verantwoording af. 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 gemeente specifieke informatie.

1.2 Grondslagen op grond waarvan Suwinet gebruikt mag worden

Voordat aangegeven kan worden op welke wijze we het zorgvuldig gebruik van Suwinet borgen, moet vastgelegd worden in welke gevallen en door wie Suwinet gebruikt mag worden.
Suwinet mag alleen gebruikt worden door medewerkers voor de uitvoering van de Participatiewet, de Bbz, de IOAW, de IOAZ en sinds medio 2021 ook voor de uitvoering van de Wgs.
Daarnaast kan Suwinet gebruikt worden door de gemeentelijke belastingdeurwaarders voor het leggen van loonbeslag. Deze taak wordt in DOWR verband uitgevoerd.
Tot slot mogen de medewerkers die de inburgering verzorgen via Suwinet het Inburgeringsportaal gebruiken.

1.3 Leeswijzer

Hoofdstuk 2 betreft een overzicht van alle normen, inclusief een beschrijving op welke wijze we in Deventer (en in DOWR-verband) invulling geven aan deze beveiligingsnormen. Dit hoofdstuk vormt dan ook de kern van dit beveiligingsplan Suwinet.
Hierna wordt in hoofdstuk 3 terug geblikt op de audit ENSIA van 2020. Beschreven staat aan welke normen we voldoen, welke aandachtspunten er waren en hoe we hier in 2021 invulling aan hebben gegeven.

In onderhavig plan wordt meerdere malen verwezen naar de verscheidene bijlagen. Deze, in totaal acht, bijlagen zijn onlosmakelijk onderdeel van dit beveiligingsplan. Voor wat betreft de autorisatiematrix wordt opgemerkt dat deze gedurende het jaar aan verandering onderhevig kan zijn. Bijvoorbeeld op basis van richtlijnen van het BKWI of van nieuwe inzichten naar aanleiding van de halfjaarlijkse controles. Het mandaat om de autorisatiematrix vast te stellen ligt bij de teammanager van Werk&Inkomen.

Hoofdstuk 2 Beveiligingsplan Suwinet

In dit hoofdstuk gaan we nader in op hoe we uitvoering geven aan de 14 BIO-normen, die in het normenkader zijn vastgesteld (zie bijlage). Gemeenten moeten zich verantwoorden over opzet, bestaan en werking van deze normen. Hierin is echter een groeipad bepaald: vooralsnog hoeven we ons alleen te verantwoorden over opzet en bestaan van de normen.
In de volgende onderdelen is de norm schuingedrukt. De nummering verwijst naar de BIO-normen. Bij iedere norm wordt kort een toelichting geschetst. Vervolgens wordt uiteengezet op welke wijze we invulling geven aan de beschreven norm.

5.1.1 Beleidsregels voor informatiebeveiliging

> Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.

De gemeenten Deventer, Olst-Wijhe en Raalte hebben gezamenlijk het informatiebeveiligingsbeleid opgesteld. Dit beleid (strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2020-2022) is door de afzonderlijke gemeenten vastgesteld en bevat het algemene informatiebeveiligingskader. Onderhavig plan betreft het uitvoeringsbeleid, specifiek geldend voor Suwinet. Dit beleidsplan heeft een werkingstermijn van vier jaar. Dit plan is gezamenlijk met de Security Officers Suwinet in DOWR-verband opgesteld. Het beveiligingsplan wordt wel door de afzonderlijke colleges vastgesteld.

Een gezamenlijk plan biedt meerdere voordelen voor het beheer van Suwinet. Het beheer 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 één set aan werkafspraken die we op basis van het plan afspreken (in plaats van drie verschillende plannen).

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.

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

> Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.

Het Suwinet beveiligingsplan wordt voor een periode van vier jaar vastgesteld. Ieder jaar wordt het plan beleidsmatig geëvalueerd en waar nodig aangepast aan de actuele ontwikkelingen. Van de bevindingen stellen we een memo op en stemmen deze af met de teammanager en CISO. Onderdeel van de periodieke beoordeling is de halfjaarlijkse evaluatie van de uitgevoerde controles en de aandachtspunten die hieruit zijn voortgekomen. Hiervan wordt een actielijst bijgehouden. Deze evaluatie wordt opgesteld in overleg met de teammanager en CISO. Dit moment wordt tevens aangegrepen om medewerkers bewust te maken van het gebruik van Suwinet.

6.1.1. Rollen en verantwoordelijkheden bij informatiebeveiliging

> Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.

Voor elke gemeente is er een Security Officier Suwinet aangesteld en aangemeld bij het BKWI. In Deventer hebben we, in het kader van vervangbaarheid, op dit moment twee Security Officers benoemd. Deze functionarissen zijn verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document en bevorderen de informatiebeveiliging en de communicatie naar de medewerkers over het gebruik van Suwinet.
De taakomschrijving is als bijlage 2 in dit plan opgenomen.

Ook hebben we een incidentmanagementproces en responsbeleid, welke is beschreven in DOWR-verband en heeft de titel ‘ Beleid Incident management en response DOWR-gemeenten’.

De drie DOWR-gemeenten hebben gezamenlijk een CISO aangesteld, die zich op strategisch niveau bezighoudt met informatieveiligheid. Voor privacy is er een Functionaris Gegevensbescherming aangesteld voor de drie DOWR-gemeenten.

6.1.2. Scheiding van taken

> Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

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 alleen die gegevens kan raadplegen die van belang zijn voor zijn/haar werkzaamheden.
De autorisatiematrix is als bijlage bij dit plan gevoegd.

Bij iedere halfjaarlijkse controle wordt een actueel overzicht van alle gebruikers in Deventer opgevraagd. De autorisaties worden dan per medewerker vergeleken met de autorisatiematrix om vast te stellen dat medewerkers de juiste autorisaties hebben binnen Suwinet.
In de autorisatie procedure Suwinet (bijlage) zijn de verschillende stappen beschreven die doorlopen worden bij het toekennen, muteren of beëindigen van autorisaties voor Suwinet.

Bij signalen over oneigenlijk gebruik van Suwinet wordt opgeschaald naar de teammanager Werk&Inkomen. De individuele medewerker wordt gevraagd zijn gedrag te verantwoorden. Indien er aanwijzingen zijn voor norm overschrijdend gedrag, wordt gehandeld volgens het vastgestelde integriteitsbeleid. Er wordt dan gehandeld conform artikel 16 van de CAR/UWO.

7.2.2. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

> Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.

Bij indiensttreding moet iedere nieuwe medewerker die de bevoegdheid krijgt om met Suwinet te werken een E-learning van de VNG volgen. Daarnaast verhogen we de bewustzijn omtrent het gebruik van Suwinet door posters met algemene tips over het veilig omgaan met (persoons)gegevens op de afdeling te hangen en door periodiek het onderwerp Suwinet te bespreken met de gebruikers in het teamoverleg.

9.2.1. Registratie en afmelden van gebruikers

> Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

Dit is per gemeente vastgelegd in de procedure autorisatie Suwinet. Deze is toegevoegd in bijlage 3.

9.2.2. Gebruikers toegang verlenen

Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.

Op basis van functies en rollen is de autorisatiematrix vastgesteld, zie bijlage 2. Dit is de basis op grond waarvan medewerkers toegang verkrijgen tot Suwinet. In de autorisatiematrix is rekening gehouden met doelbinding en proportionaliteit. Zo zorgen we ervoor dat medewerkers alleen die toegangsrechten hebben die ze nodig hebben voor de uitoefening van hun functie/wettelijke taak. Als onderdeel van de autorisatiematrix zijn dan ook afwegingen vastgelegd op grond waarvan we risicovolle zoekpagina's hebben toegekend.

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 is in DOWR-verband vastgesteld.

9.2.5. Beoordeling van toegangsrechten van gebruikers

Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.

De toekenningen, wijzigingen en gebruik van toegangsrechten tot Suwinet worden periodiek gecontroleerd als onderdeel van de controles die we ieder half jaar uitvoeren aan de hand van de gebruikersrapporten Suwinet die door het BKWI worden opgesteld. We doen dit door een overzicht van alle gebruikers op te vragen en daarbij de verstrekte autorisaties te vergelijken met de autorisatiematrix. Eventuele verschillen worden dan geconstateerd en gecorrigeerd.
De autorisatiematrix maakt onderdeel uit van dit beveiligingsplan (bijlage) en wordt daarmee minimaal jaarlijks geëvalueerd en waar nodig aangepast.

9.2.6. Toegangsrechten intrekken of aanpassen

De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

Bij uitdiensttreding van een medewerker wordt de toegang tot Suwinet beëindigd. Bij verandering van functie worden de toegangsrechten aangepast of, indien de medewerker in diens nieuwe functie geen gebruik meer hoeft te maken van Suwinet, beëindigd. Minimaal ieder half jaar worden de autorisaties gecontroleerd en beoordeeld of deze nog actueel zijn.

10.1.1. Beleid inzake het gebruik van cryptografische beheersmaatregelen

Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.

Alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld zijn beveiligd tegen ongeautoriseerde toegang. Dit is in DOWR-verband vastgelegd 'Beleid_Encryptie DOWR- gemeenten'. Gemeente Deventer maakt geen gebruik van de functionaliteit DKD-inlezen en Suwinet-inlezen.

12.1.1. Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.

De bedieningsprocedures betreffen 1) de handleiding voor gebruikers van Suwinet (hierbij valt te denken aan handleidingen Suwinet die door BKWI beschikbaar gesteld worden) en 2) de handleiding voor de beheerders van de applicaties. Hierbij valt te denken aan specifieke handleidingen voor Suwinet, en bij DKD-inlezen of Suwinet-inlezen algemene bedieningshandleidingen ten aanzien van installatie, beheer, back-up, etc. Deze norm is nieuw. Met ingang van 2022 gaan de Security Officers deze handleidingen met de gebruikers delen.

12.4.1. Gebeurtenissen registreren

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

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 in een controlerapport en terugkoppeling vindt plaats in het volgende controlerapport (controlecyclus).

12.4.2. Beschermen van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.

Het BKWI logt alle handelingen die in Suwinet plaatsvinden. De generieke en specifieke rapportages worden maandelijks beschikbaar gesteld en door de Security Officers gedownload via Suwinet Inkijk.
De wijze waarop deze gecontroleerd worden is beschreven in de procedure uitvoeren periodieke controles Suwinet (bijlage).
De rapportages die worden opgevraagd worden momenteel maximaal twee jaar bewaard op de eigen omgeving op Sharepoint van de Security Officer, zodat onbevoegden geen toegang hebben tot deze gegevens.

18.1.4. Privacy en bescherming van persoonsgegevens

Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.

Twee keer per jaar vindt afstemming plaats tussen de Security Officers Suwinet van de drie DOWR-gemeenten, de CISO en de Privacy Officer over naleving van privacy en bescherming van persoonsgegevens.

Hoofdstuk 3 Evaluatie 2020

Zoals benoemd, worden we beoordeeld in hoeverre we voldoen aan de 14 normen. Eén van de normen om zorgvuldig gebruik van Suwinet te borgen, is het evalueren van het beveiligingsplan en hierin ook de bevindingen van de uitgevoerde controles mee te nemen.
Omdat we de evaluatie jaarlijks gaan uitvoeren, is het logisch om terug te blikken naar de laatst afgeronde audit in 2020.

Hieronder zijn de bevindingen van de auditor ten aanzien van Suwinet opgenomen. Hieruit blijkt dat we in 2020 aan bijna alle normen voldeden, met een paar aandachtspunten:

Bevindingen SUWI - Deventer

BIO HFD	Criterium BIO		Bevinding Pre-audit
5. Informatiebeveiligingsbeleid	5.1.1 Beleidsregels voor informatiebeveiliging (was B01)	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Voor 2020 is het beveiligingsbeleid nog niet aangepast naar de BIO. De Suwi-coördinatoren hebben bevestigd dat dit op de actielijst voor 2021 is opgenomen.
	5.1.2 Beoordeling van het informatie-beveiligingsbeleid (was C01)	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Binnen Deventer, Suwi, heeft deze beoordeling nog niet plaatsgevonden. Dit zal i.s.m. de CISO verder worden opgepakt.
6. Organiseren van informatiebeveiliging	6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging (was B04)	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen. Nieuw is het beschrijven van de rol en verantwoordelijkheden in een functieprofiel voor de CISO en het aanstellen van deze functionaris.	Voldoet, met aandachtspunt De overdacht van werkzaamheden van de vorige Suwi-officer naar haar opvolgers had niet of nauwelijks plaatsgevonden en was niet gedocumenteerd.
	6.1.2. Scheiding van taken (was B04)	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Voldoet
7. Veilig personeel	7.2.2. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging (was AP).	Alle medewerkers van de organisatie en, voorzover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie	Voldoet
9. Toegangsbeveiliging	9.1.2. Registratie en afmelden van gebruikers (was U02/03)	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Voldoet.
	9.2.2. Gebruikers toegang verlenen (was U02)	Een formele gebruikers toegangs-verleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in trekken.	Voldoet

	9.2.5. Beoordeling van toegangsrechten van gebruikers (was U02)	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Voldoet
	9.2.6. Toegangsrechten intrekken of aanpassen (was U02)	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband , contract of overeenkomst te worden verwijderd en bij wijzigingen behoren ze te worden aangepast.	Voldoet.
10. Cryptografie	10.1.1. Beleid inzake het gebruik van crypto grafische beheersmaatregelen (was U11).	Ter bescherming van informatie behoort een beleid voor het gebruik van crypto grafische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	NVT voor Suwi inkijk.
12. Beveiliging bedrijfsvoering	12.1.1. Gedocumenteerde bedieningsprocedure (nieuw).	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Voldoet.
	12.4.1. Gebeurtenissen registreren (was C06).	Logbestanden van gebeurtenissen die gebruikers-activiteiten, uitzonderingen en informatiebeveili-gingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Voldoet.
	12.4.2. Beschermen van informatie in logbestanden (was C05).	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang,	NVT voor Suwi inkijk.

Uit het overzicht blijkt dat er een paar aandachtspunten waren. Hieronder gaan we in op de afzonderlijke aandachtspunten en hoe we hier in 2021 uitvoering aan hebben gegeven:

- Het beveiligingsplan Suwinet was in 2020 nog niet geactualiseerd naar de BIO-normen. Het laatst vastgestelde beveiligingsplan dateert uit 2019. In goed overleg met de auditor is besloten om pas met ingang van 2022 een nieuw beveiligingsplan vast te laten stellen, waarbij we ook de actualisatieslag zouden meenemen. Dit plan is hier het resultaat van.

- De periodieke controlerapporten die we ieder half jaar opstellen moeten niet alleen uitgevoerd en gedocumenteerd worden en worden ondertekend voor akkoord door de (gemandateerde) teammanager, maar ook worden afgestemd met de CISO. Inmiddels hebben we met de CISO de afspraak gemaakt dat we deze controlerapporten met hem afstemmen. Hiermee is geborgd dat eventuele aandachtspunten of verbeteracties gericht op Suwinet aangehaakt zijn op de informatiebeveiliging in bredere zin.

- Periodiek moet er afstemming zijn tussen Security Officers, de CISO en FG. Sinds dit jaar (2021) hebben we afgesproken dat we 2 x per jaar een afstemmingsoverleg hebben. Het doel van het overleg is om ontwikkelingen op het gebied van informatiebeveiliging in algemenere zin en Suwinet specifiek te bespreken.

Conclusie
Op basis van bovenstaand overzicht concluderen we 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 op dit moment voldoende binnen de organisatie geborgd hebben. Door jaarlijks dit beveiligingsplan te evalueren en het gebruik van Suwinet periodiek te controleren borgen we dat we ook in de toekomst bovenop dit proces zitten.

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

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 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.

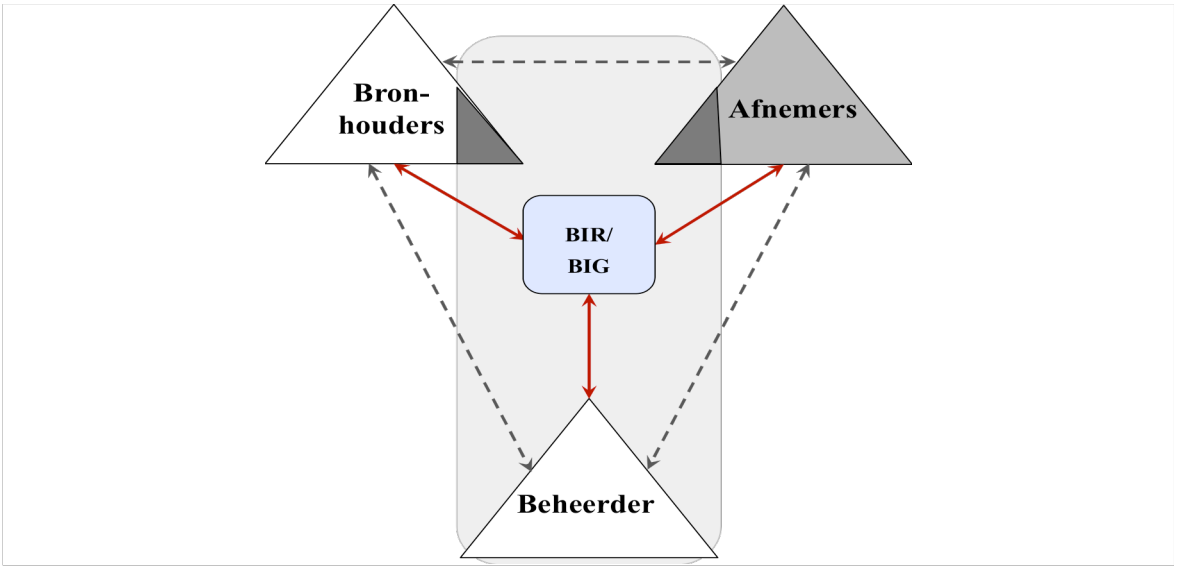
Het informeren over de rapportages en adviseren over vervolgstappen;
Zijn er signalen over oneigenlijk gebruik dan wordt opgeschaald naar de betreffende teammanager. De Individuele medewerker wordt gevraagd zijn/haar zoekgedrag te verantwoorden.

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.

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 **3**

1. INLEIDING **4**

1.1. ORGANISATIE GEVS ***4***

1.2. SUWINET SERVICES ***5***

1.3. ORGANISATIE VAN HET SUWINET NORMENKADER ***5***

1.4. BESCHRIJVING VAN DE CONTROLS EN ONDERLIGGENDE MAATREGELEN ***7***

2. BELEIDSDOMEIN **11**

B.01 SUWINET-AANSLUITBELEID 12

B.02 NALEVING EN COMPLIANCY AANSLUITBELEID 13

B.03 EXTERNE PARTIJEN 14

B.04 BEVEILIGINGSFUNCTIE SUWINET (GEVS) 15

B.05 TAKEN, VERANTWOORDELIJKHEDEN EN FUNCTIESCHEIDING 16

B.06 SUWINET DEEL LANDSCHAP AFNEMERS (ARCHITECTUUR) 17

3. UITVOERINGSDOMEIN **18**

U.01 TPM EXTERNE PARTIJEN 19

U.02 AUTORISATIE BEHEERPROCES 21

U.03 TOEGANGSMECHANISME: GEBRUIKERSIDENTIFICATIE- EN AUTHENTICATIE (IA) 22

U.04 TOEGANGSMECHANISME: AUTORISATIE 23

U.05 SUWINET-INFORMATIE 24

U.06 CLASSIFICATIE VAN INFORMATIE 25

U.07 SUWINET- INLEZEN EN DKD INLEZEN (INLEESFUNCTIONALITEIT) 27

U.08 SUWINET-MAIL 28

U.09 SCHEIDING VAN FACILITEITEN (PRODUCTIEOMGEVING) 28

U.10 SERVER 30

U.11 NETWERKVERBINDINGEN 30

U.12 TELEWERKEN 31

4. CONTROL **33**

C.01 EVALUATIE VAN AANSLUITBELEID 34

C.02 RISICOMANAGEMENT 34

C.03 WIJZIGINGENBEHEER 35

C.04 BEOORDELING VAN TOEGANGSRECHTEN 36

C.05 LOGGING 37

C.06 MONITORING EN RAPPORTAGE 38

C.07 EVALUATIE VAN IAA RAPPORTAGES (ORGANISATORISCH EN TECHNISCH) 41

C.08 TRANSPARANTIE RAPPORTAGE 42

ONDERWERPEN TBV: BRONHOUDERS EN BEHEER 44

OVERZICHT VAN OBJECTEN BINNEN BELEIDS-, UITVOERINGS-, EN CONTROL DOMEIN 46

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

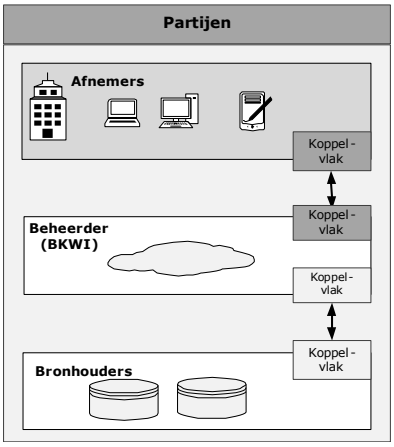
1. Inleiding

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

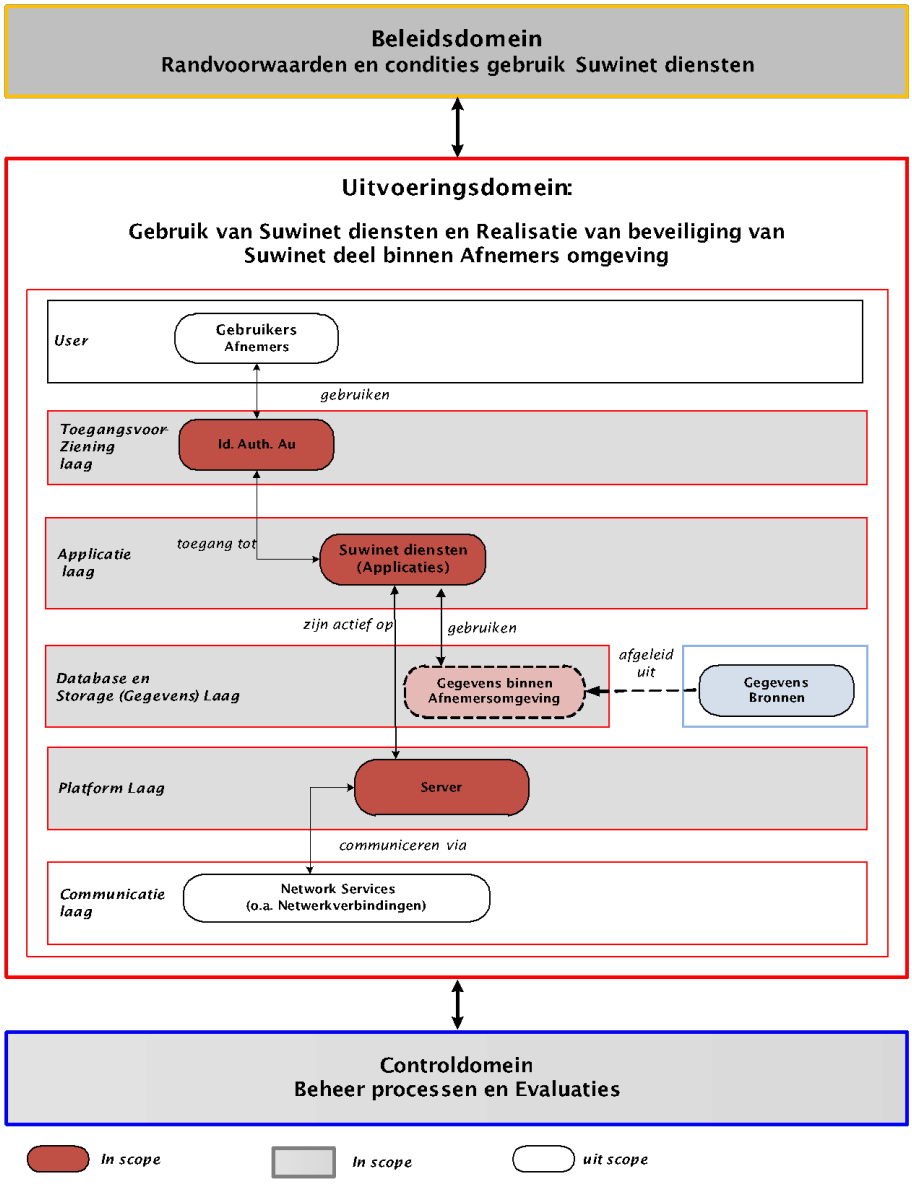
In deze paragraaf wordt de indeling van dit normenkader toegelicht. Het nomenkader is georganiseerd in drie hoofdstukken: beleids-, uitvoering- en control domein (ook wel beheersingsdomein genoemd). Figuur 2 geeft de relatie tussen de objecten die op de verschillende lagen kunnen voorkomen.

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

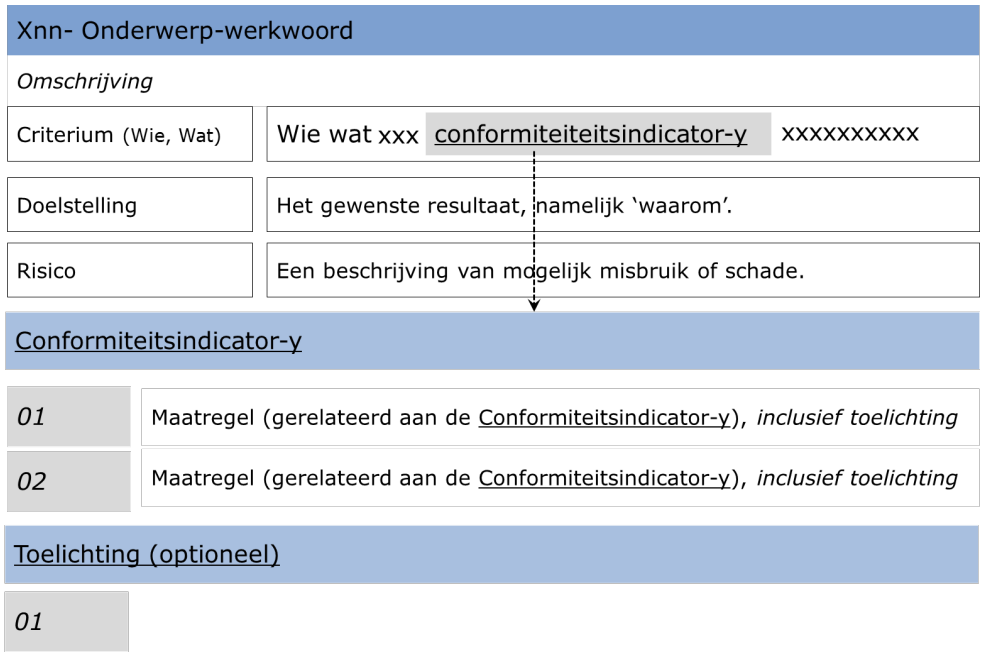
Binnen elk domein bevinden zich onderwerpen die bij de implementatie danwel bij een beoordeling van een onderzoeksobject een rol spelen. Per onderwerp wordt een criterium (of hoofdnorm) geformuleerd. Het criterium is beschreven in een vorm waarin de elementen wie, wat en waarom geadresseerd worden. Het 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:

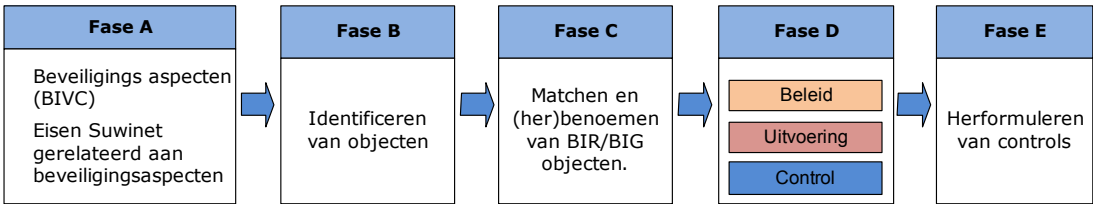
A. *Vaststellen eisen* – Bij deze fase zijn, uitgaande van de informatiebeveiligingsaspecten: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid (BIVC) (Regeling Suwi: Art. 6.4 en Art. 5.22) en kennis van de Suwinet-omgeving, op basis van een creatief proces, enkele globale relevante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

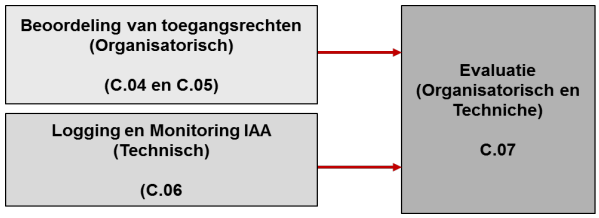
- U.03 Toegangsmechanisme: Identificatie- en authenticatie en
- U.04 Toegangsmechanisme: Autorisatie.

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	

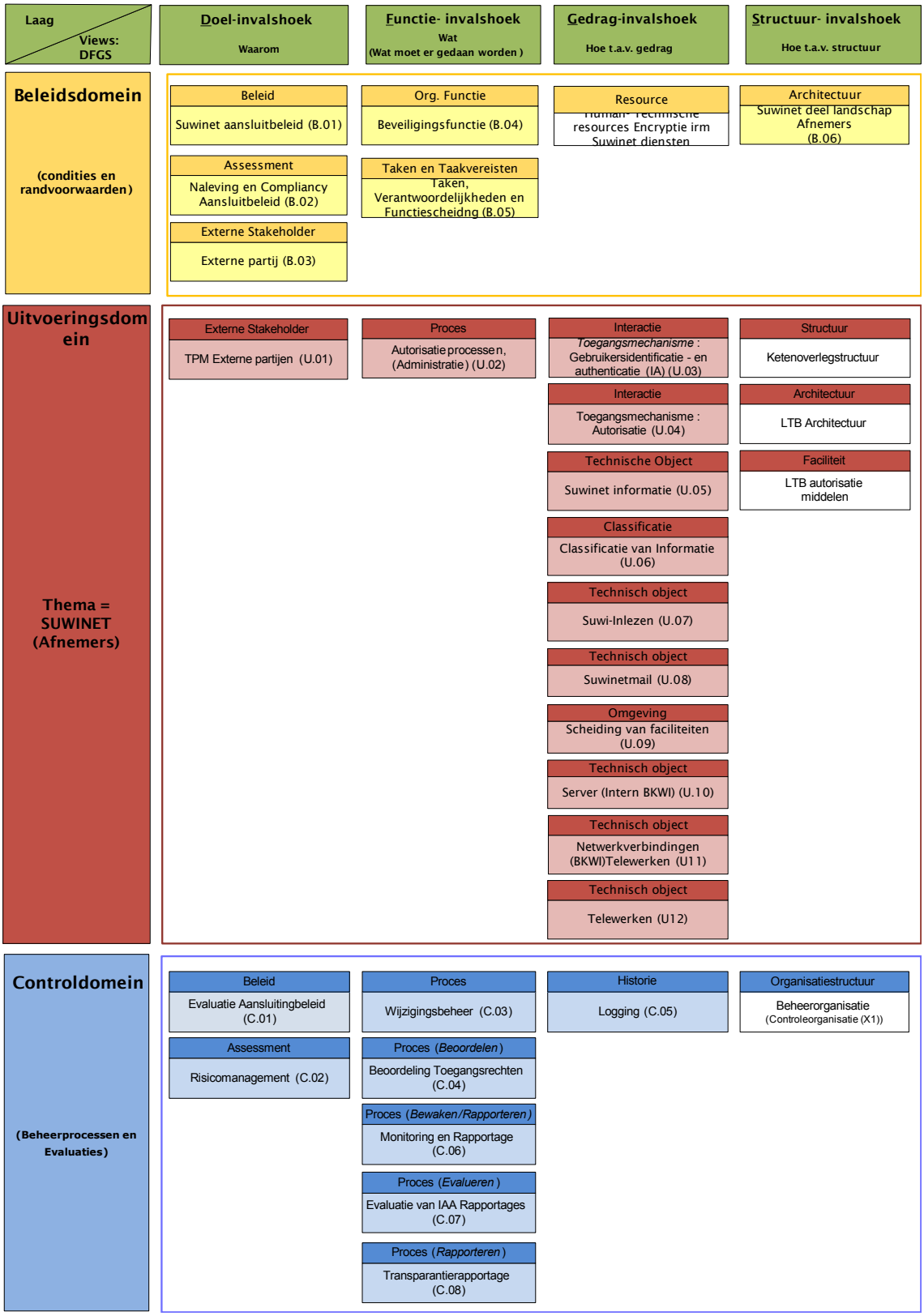
Uitvoeringsdomein

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 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 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 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.