Guidance voor de toepassing van de BIO bij het gebruik van Suwinet[1]

1. Inleiding

Met ingang van 2020 zijn alle overheidsorganisaties gebonden aan de Baseline Informatiebeveiliging Overheid (BIO). Het Ketenoverleg, dat verantwoordelijk is voor het beheer van Suwinet, heeft in de Verantwoordingsrichtlijn Informatiebeveiliging GeVS aangegeven over welke BIO-normen (controls) het verantwoording vraagt aan de op Suwinet aangesloten partijen. Deze Suwinet-guidance geeft voor ieder van die normen een nadere toelichting, die gebruikt kan worden bij de implementatie van de norm en eventueel ook bij de controle daarvan door de auditor. Daarbij is ernaar gestreefd de aangesloten partijen zoveel mogelijk ruimte te laten voor hun eigen risico-sturing en -invulling.

Het gaat hierbij telkens om de toepassing van de BIO-normen bij processen en systemen, inclusief koppelvlakken, die Suwinet-gegevens verwerken of uitwisselen. De nadere toelichting is gericht op de aantoonbaarheid van de naleving van de maatregelen met betrekking tot Suwinet-gerelateerde gegevens.

Deze guidance[2] is opgesteld op verzoek van het Ministerie van Sociale Zaken en Werkgelegenheid en bestemd voor alle afnemers van Suwinet-services.

Speciaal voor gemeenten heeft de VNG een SUWI-guidance op maatregelniveau gemaakt, die is afgestemd op de ENSIA-verantwoordingssystematiek. Ook heeft de NOREA een nieuwe Handreiking Suwinet opgesteld, die is afgestemd op de ENSIA-verantwoordingssystematiek. Zowel de VNG SUWI-guidance als de NOREA- handreiking zijn te beschouwen als een verdere uitwerking van deze Suwinet-guidance.

[1] Deze tekst is vastgesteld door het Ketenoverleg op 17 september 2020.

[2] Het format van deze Suwinet-guidance is afgeleid van de VNG Suwinet-guidance en ingevuld met Suwinet-specifieke aandachtspunten. Hierbij is gebruikt gemaakt van de NEN-ISO27002-2017 toelichting.

2. Opbouw guidance

Items	**Uitleg**
Hoofdstuk	Hoofdstuknummer en titel uit de BIO
Paragraaf	Paragraafnummer en titel uit de BIO
Control	Controlnummer en titel uit de BIO
Toelichting Control	Controltekst uit de BIO
Control/ Norm geldt voor	Norm geldig voor Suwinet-inkijk en/of Suwinet-inlezen en/of DKD-inlezen
Norm van toepassing op	Waar zijn maatregelen geïmplementeerd om aan te tonen dat wordt voldaan aan de norm?
Scope	Reikwijdte van de control
Nadere toelichting	Context ter toelichting en aandachtspunten

3. Suwinet-guidance per BIO-norm

Hoofdstuk	5	Informatiebeveiligingsbeleid		
Paragraaf	5.1	Aansturing door de directie van de informatiebeveiliging		
Control	5.1.1	Beleidsregels voor informatiebeveiliging		
Toelichting control		Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.		
Norm/Control geldt voor			**Norm van toepassing op**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	n.v.t.
Scope		Beleid		
Nadere toelichting		Organisaties behoren op het hoogste niveau een informatiebeveiligingsbeleid te definiëren dat is goedgekeurd door de directie en dat de aanpak van de organisatie beschrijft om haar doelstellingen inzake informatiebeveiliging te bereiken. De focus ligt op de governance (incl. afspraken over de wijze van verantwoording). Onder andere is met het beleid: • Uiteengezet hoe de organisatie van de informatiebeveiligingsfunctie er uit ziet, waaronder verantwoordelijkheden, taken en bevoegdheden; • Helder wie in de organisatie als verantwoordelijke proceseigena(ar)(ren) is/zijn aangewezen voor de processen waar op basis van een basis beveiligingsniveau (BBN) niveau en classificatie op beschikbaarheid, integriteit en vertrouwelijkheid (BIV) met geclassificeerde Suwinet gerelateerde gegevens wordt gewerkt. • Voor elk proces waar informatie wordt verwerkt of uitgewisseld, is een verantwoordelijke persoon toegewezen die zorg draagt voor de benodigde beveiligingsfunctie, waaronder ook ten behoeve van de Suwinet gerelateerde gegevens. Er kan onderscheid gemaakt worden in een strategisch beleid en een tactisch beleid. • Strategische uitgangspunten zijn beschreven, ingebed in en afgestemd op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. • Op een lager niveau kan een tactisch kader voor beveiliging zijn opgesteld en wordt het strategische informatiebeveiligingsbeleid ondersteund door onderwerpspecifieke beleidsregels die de implementatie van beheersmaatregelen inzake informatiebeveiliging verplicht stelt, in dit geval specifieke Suwinet context bevat en taken/verantwoordelijkheden specifiek voor beveiliging rondom Suwinet gerelateerde gegevens beschreven zijn. Beleidsregels voor informatiebeveiliging kunnen worden uitgevaardigd als een enkelvoudig document inzake ‘informatiebeveiligingsbeleid’ of als een reeks individuele maar gerelateerde documenten. termen voor deze beleidsdocumenten, zijn bijvoorbeeld ‘beleid’, ‘normen’, uitgangspunten, richtlijnen’ of ‘regels’.		

Hoofdstuk	5	Informatiebeveiligingsbeleid		
Paragraaf	5.1	Aansturing door de directie van de informatiebeveiliging		
Control	5.1.2	Beoordeling van het informatiebeveiligingsbeleid		
Toelichting control		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.		
Norm/Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	n.v.t.
Scope		Beleid		
Nadere toelichting		De focus ligt op de frequentie van bijstelling. De organisatie dient het (strategisch) beleid regelmatig te beoordelen en zo nodig bij te stellen. Veranderingen in de omgeving van de organisatie, de bedrijfsomstandigheden, juridische voorwaarden, technische omgeving of andere externe ontwikkelingen kunnen leiden tot wijzigingen in beleid. Het beleid dient daarom periodiek te worden bijgewerkt en aan te sluiten bij een (bestaande) bestuurs- en P&C-cyclus en op basis daarvan beoordeeld en zo nodig bijgesteld te zijn, en wel minimaal één keer per drie à vier jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdelingen. Voor nieuw en herzien beleid behoort de goedkeuring van de directie te worden verkregen. NB: indien een afnemer in een structuur werkt van strategisch en tactisch beleid, dan kan het strategisch beleid ouder zijn, als dit generiek van opzet is.		

Hoofdstuk	6	Organiseren van informatiebeveiliging		
Paragraaf	6.1	Interne organisatie		
Control	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging		
Toelichting control		Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.		
Norm/Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	n.v.t.
Scope		Beleid, implementatie		
Nadere toelichting		Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie 5.1.1). De leiding/het management van de organisatie heeft vastgelegd en vastgesteld wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie en in het bijzonder de verantwoordelijkheden voor het accepteren van restrisico's. Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren. Niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht. De verantwoordelijkheden en rollen worden ook ingevuld in de organisatie. Indien een Chief Information Security Officer (CISO) is aangesteld, dienen de rol en de verantwoordelijkheden van de CISO vastgelegd en vastgesteld te zijn in een CISO-functieprofiel. Bij voorkeur wordt hierbij gebruik gemaakt van het 'BIO OP product Handreiking functieprofiel CISO'		

Hoofdstuk	6	Organiseren van informatiebeveiliging		
Paragraaf	6.1	Interne organisatie		
Control	6.1.2	Scheiding van taken		
Toelichting control		Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbedoeld of wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.		
Norm/Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Personeelsbeleid, proces en procedurecontrole gegevensgebruik		
Nadere toelichting		Maatregelen zijn getroffen om onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waar te nemen of voorkomen. Hierbij is scheiding van taken/functiescheiding van belang zoals t.a.v. invoerende en controlerende taken. Onafhankelijke controle van het gegevensgebruik en autorisatiebeheer vindt plaats. Gebruik van gegevens uit Suwinet wordt door een andere persoon gecontroleerd dan een gebruiker van Suwinetgegevens. Indien gebruik wordt gemaakt van tactisch kader voor beveiliging, zou de scheiding van taken hierin opgenomen moeten zijn. De volgende taken dienen gescheiden te zijn en worden minimaal verwacht en aanzien van: • Autoriseren van toewijzing van toegang tot Suwinet gerelateerde gegevens • Controleren van gebruik van Suwinet gerelateerde gegevens • Controleren van de actualiteit van de gebruikersadministratie • Melding van incidenten gerelateerd aan Suwinetgegevens. • Gebruik van Suwinet gerelateerde gegevens als gebruiker Wanneer het moeilijk is om taken te scheiden, behoren andere beheersmaatregelen zoals het monitoren van activiteiten, audittrajecten en supervisie door de directie te worden overwogen. Deze afweging dient o.b.v. een risico-analyse en -acceptatie te zijn vastgesteld.		

Hoofdstuk	7	Veilig personeel		
Paragraaf	7.2	Tijdens het dienstverband		
Control	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging		
Toelichting control		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.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	n.v.t.
Scope		Bewustwording		
Nadere toelichting		Bewustwording is essentieel in het werken met vertrouwelijke gegevens en kwetsbare processen. De organisatie dient een bewustwordingsprogramma te hebben, waarbij alle medewerkers (intern en extern) gewezen worden op hun verantwoordelijkheid ten aanzien van informatiebeveiliging. Onder ander is continu aandacht voor de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen, zoals de SUWI-omgeving. Opleiding en training voor informatiebeveiliging behoort periodiek plaats te vinden. De basisopleiding en -training geldt ook voor personen die worden overgeplaatst naar nieuwe functies of rollen met substantieel verschillende eisen ten aanzien van informatiebeveiliging, niet alleen voor nieuwe starters, en behoort plaats te vinden voordat de rol actief wordt. Voor nieuwe medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten, met name SUWI-gerelateerd, geldt dat zij binnen drie maanden na indiensttreding een training I-bewustzijn en/of specifiek een SUWI-gebruikstraining met aandacht voor informatiebeveiliging succesvol hebben gevolgd.		

Hoofdstuk	9	Toegangsbeveiliging		
Paragraaf	9.2	Beheer van toegangsrechten van gebruikers		
Control	9.2.1	Registratie en afmelden van gebruikers		
Toelichting control		Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Toegangsverlening Suwinet		
Nadere toelichting		Een gebruiker/account is uitsluitend toewijsbaar aan één uniek identificeerbaar natuurlijk persoon, zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties. Toewijzing, wijziging of onttrekking van toegangsrechten op Suwinetgegevens (bijv. o.b.v. rollen) gebeurt op een controleerbare manier. Gebruik van gemeenschappelijke accounts (groepsaccounts) om Suwinet gerelateerde gegevens in te zien, te wijzigen en/of te verwijderen is niet toegestaan, tenzij dit om bedrijfs- of operationele redenen noodzakelijk is, en is vastgelegd o.b.v. een risico-analyse en geaccordeerd door een daartoe bevoegde functionaris. In dergelijke gevallen dient monitoring plaats te vinden. Controle vindt periodiek plaats op toegewezen autorisaties o.b.v. toegepaste functiescheiding (norm 6.1.1 en 6.1.2).		

Hoofdstuk	9	Toegangsbeveiliging		
Paragraaf	9.2	Beheer van toegangsrechten van gebruikers		
Control	9.2.2	Gebruikers toegang verlenen		
Toelichting control		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.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Toegangsverlening Suwinet, gebruikersaccounts		
Nadere toelichting		Deze norm hangt samen met 6.1.1 (inrichting), 6.1.2 (functiescheiding), 9.2.1 (procedure). Alleen gebruikers die op basis van hun rol recht hebben op Suwinet gerelateerde gegevens hebben een toegangsrecht op deze gegevens. De toegangsrechten zijn bepaald o.b.v. een risico-afweging. In de afweging is rekening gehouden met scheiding van taken. Er is uitsluitend toegang verleend tot informatiesystemen met Suwinet gerelateerde gegevens na autorisatie door een bevoegde functionaris. De profielen van rollen die toegang verschaffen tot Suwinet gerelateerde gegevens worden geautoriseerd door een daartoe bevoegde functionaris/proceseigenaar. De bevoegdheden worden bijgehouden in een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en –diensten.		

Hoofdstuk	9	Toegangsbeveiliging		
Paragraaf	9.2	Beheer van toegangsrechten van gebruikers		
Control	9.2.5	Beoordeling van toegangsrechten van gebruikers		
Toelichting control		Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Toegangsverlening tot Suwinet-gerelateerde gegevens door reguliere gebruiker accounts en speciale Suwinet accounts3		
Nadere toelichting		Deze norm hangt samen met 6.1.1 (inrichting), 9.2.1 (procedure) en 12.4.1 (incident) Toegangsrechten (dus ook voor Suwinet gerelateerde gegevens) worden minimaal halfjaarlijks beoordeeld. Autorisatieprocedures worden minimaal jaarlijks beoordeeld op bevoegde toegang tot Suwinet-gerelateerde gegevens. Het halfjaarlijks beoordelen van toegangsrechten in generiek verband op bevoegde toegang tot Suwinet gerelateerde gegevens wordt als adequaat genoeg gezien. Dit geldt ook voor beoordeling van het doorlopen van in- en uittredingsprocedures. Beoordeling van speciale Suwinet accounts met speciale bevoegdheden (beheerderaccounts) worden minimaal elk kwartaal beoordeeld op bevoegdheid tot aanmaken, verwijderen en muteren gebruikers/rollen/instellingen die gerelateerd zijn aan inzien of gebruik van Suwinet-gegevens. Toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen. Van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden. Deze controle compenseert mogelijke zwakke plekken in de uitvoering van beheersmaatregelen 9.2.1, 9.2.2 en 9.2.6. Indien issues worden gevonden ten aanzien van toegang tot Suwinet-gerelateerde gegevens worden die als beveiligingsincident gerapporteerd.		

[3] Speciale Suwinet-accounts kunnen betrekking hebben op speciale bevoegdheden zoals het kunnen zoeken met andere zoeksleutels dan het BSN zoals bijv. op naam of kenteken.

Andere speciale Suwinet accounts zijn bijvoorbeeld:

- Een gebruikersbeheerder, die accounts kan aanmaken en verwijderen en rollen kan muteren.
- Een Security Officer of de gemandateerde, die specifieke (niet geanonimiseerde) rapportages kan opvragen.

Hoofdstuk	9	Toegangsbeveiliging		
Paragraaf	9.2	Beheer van toegangsrechten van gebruikers		
Control	9.2.6	Toegangsrechten intrekken of aanpassen		
Toelichting control		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.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Toegangsverlening Suwinet		
Nadere toelichting		Deze norm hangt samen met 6.1.1 (inrichting) en 9.2.1 (procedure). Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering en/of beëindiging van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie. Vastgesteld zal moeten worden dat deze procedure wordt gevolgd. De toegangsrechten tot Suwinet gerelateerde gegevens en systemen dienen adequaat (tijdig, juist en volledig) te zijn verwijderd na vertrek of functiewijziging van de medewerker / externe gebruikers / contractanten.		

Hoofdstuk	10	Cryptografie		
Paragraaf	10.1	Cryptografische beheersmaatregelen		
Control	10.1.1	Gedocumenteerde bedieningsprocedures		
Toelichting control		Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
n.v.t.	x	x	x	n.v.t.
Scope		Cryptografie Suwinet inlezen en DKD inlezen		
Nadere toelichting		Cryptografie is een essentiële maatregel om de vertrouwelijkheid te waarborgen van Suwinet gegevens. De organisatie heeft cryptografiebeleid opgesteld en vastgesteld, waarin de inzet van cryptografie is voorgeschreven en als zodanig toepast op Suwinet-gerelateerde gegevens. De organisatie heeft aantoonbaar gemaakt dat cryptografie wordt toegepast op transport en opslag van Suwinet-gerelateerde gegevens indien dat vanuit haar beleid en classificatie is vereist. Het vereiste beschermingsniveau behoort te worden geïdentificeerd op basis van een risicobeoordeling. Besluitvorming over het punt of een cryptografische oplossing passend is, behoort te worden beschouwd als deel van het totale proces van risicobeoordeling en het kiezen van beheersmaatregelen. Deze beoordeling kan vervolgens worden gebruikt om vast te stellen of een cryptografische beheersmaatregel passend is, welk type beheersmaatregel behoort te worden toegepast en voor welk doel en voor welke bedrijfsprocessen. De organisatie past bij de cryptografie best practices toe en voldoet aan de relevante standaarden van het Forum Standaardisatie.		

Hoofdstuk	12	Beveiliging bedrijfsvoering		
Paragraaf	12.1	Bedieningsprocedures en verantwoordelijkheden		
Control	12.1.1	Gedocumenteerde bedieningsprocedures		
Toelichting control		Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
X .	x	x	x	x
Scope		Beheerprocedures		
Nadere toelichting		De focus ligt op beheeractiviteiten en -procedures (o.a. de verschillende ITIL-processen). Bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten behoren te worden behandeld als formele documenten en wijzigingen behoren door de directie te worden goedgekeurd. Voor beheeractiviteiten die samenhangen met informatieverwerkende en communicatiefaciliteiten, zoals de procedures van ITIL-processen die betrekking hebben op verwerking en behandeling van Suwinet gerelateerde informatie en het monitoren van deze activiteiten, behoren gedocumenteerd te zijn. Functionele en technische beheerhandboeken zijn beschikbaar en actueel m.b.t. de Suwinet-gerelateerde applicaties. Dit kunnen bijvoorbeeld zijn: Installatie en configuratie van systemen, Back-up, Restore, Monitoring, Afhandeling van fouten met betrekking tot Suwinet, ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden; procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen. Naast de bedieningsprocedures zijn de belangrijkste beheerprocessen in relatie tot Suwinet: • Change management; • Asset en configuration management • Incident management • Release en deploy management • Availability management • IT service Continuity management Let op: het gaat om het beschikbaar hebben van deze procedures en het aantoonbaar hebben van implementatie op basis van deze procedures. Gebruikersprocedures zijn bij deze control buiten scope: het gaat alleen om beheer. Alleen beheer procedures bij de IT-afdeling en eventueel bij functioneel beheer zijn in scope.		

Hoofdstuk	12	Beveiliging bedrijfsvoering		
Paragraaf	12.4	Verslaglegging en monitoren		
Control	12.4.1	Gebeurtenissen registreren		
Toelichting control		Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	x
Scope		Logging		
Nadere toelichting		Onderstaande toelichting ten aanzien van loggingvereisten is niet van toepassing bij gebruik van Suwinet Inkijk. De toelichting ten aanzien van security incidenten is wel van toepassing op Suwinet Inkijk. Logging is essentieel voor het vastleggen van gebruikers en systeembeheer handelingen, maar ook voor het vastleggen uitzonderingen, gebeurtenissen en alles wat maar relevant kan zijn voor een gecontroleerde werking van het systeem en dat achteraf kunnen aantonen. Logbestanden van gebeurtenissen vormen de basis van geautomatiseerde monitorsystemen die geconsolideerde rapporten en waarschuwingen over systeembeveiliging kunnen verzamelen. De logging bevat minimaal relevante gegevens om een gebeurtenis dat samenhangt met het inzien, wijzigen of verwijderen van Suwinet gerelateerde informatie te herleiden is tot een gebruiker (natuurlijk persoon). Tevens bevat de logging informatie over wat aan activiteiten aan systemen en data met vermelding van datum en tijdstippen heeft plaatsgevonden, onder andere in- en uitlogtijden, registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem, systeemconfiguratieveranderingen, gebruik van speciale bevoegdheden, alarmen die worden afgegeven door het toegangsbeveiligingssysteem, verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd. Logbestanden van gebeurtenissen kunnen gevoelige gegevens en persoonsgegevens bevatten. Ter bescherming van de privacy behoren passende maatregelen te worden genomen (zie ook 18.1.4). De logging wordt gemonitord door een Security Incident & Event Management Systeem (SIEM) en/of Security Operations Center (SOC) of een vergelijkbaar tool/proces middels detectie-voorzieningen, om beveiligingsincidenten tijdig te signaleren en daarop actie te ondernemen via het incidentproces. Security incidenten waarbij Suwinet gerelateerde gegevens zijn betrokken, worden gekenmerkt als SUWI-incident in de incidentregistratie, zoals met de SLA-afspraken is afgestemd (par. 2.4 ketenSLA). Deze worden tevens gemeld aan de Suwidesk van BKWI. Minimaal eens per jaar is het incident beheerproces beoordeeld op juiste, tijdige en volledige verwerking van Suwinet gerelateerde security-incidenten.		

Hoofdstuk	12	Beveiliging bedrijfsvoering		
Paragraaf	12.4	Verslaglegging en monitoren		
Control	12.4.2	Beschermen van informatie in logbestanden		
Toelichting control		Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
n.v.t.	x	x	x	x
Scope		Logging		
Nadere toelichting		Logging is essentieel voor het vastleggen van gebruikers en systeembeheer handelingen, maar ook voor het vastleggen uitzonderingen, gebeurtenissen en alles wat maar relevant kan zijn voor een gecontroleerde werking van het systeem en dat achteraf kunnen aantonen. De loggegevens dienen adequaat te zijn beveiligd tegen manipulatie. Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van: a) veranderingen aan de soorten berichten die worden vastgelegd; b) bewerken of verwijderen van logbestanden; c) overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven. Het is noodzakelijk dat systeemverslagen worden beschermd, want indien gegevens ervan kunnen worden gewijzigd of verwijderd, kan hun bestaan een vals gevoel van veiligheid creëren. Real time kopiëren van bestanden naar een systeem buiten het beheer van een systeembeheerder of –operator kan worden toegepast om bestanden te beveiligen. Minimaal halfjaarlijks dient te worden vastgesteld dat logbestanden beveiligd zijn tegen manipulatie. Daartoe dient inzicht te zijn in logbestanden die gegevensverwerking en/of -uitwisseling van Suwinet gerelateerde gegevens loggen. Ten behoeve van loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. Bij constatering dat loggegevens oneigenlijk zijn gewijzigd of verwijderd is dit als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten gemeld (zie norm 12.4.1).		

Hoofdstuk	18	Naleving		
Paragraaf	18.1	Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.		
Control	18.1.4	Privacy en bescherming van persoonsgegevens		
Toelichting control		Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met de relevante wet- en regelgeving.		
Norm / Control geldt voor:			**Norm van toepassing op:**	
Suwinet Inkijk	Suwinet Inlezen	DKD Inlezen	Eigen organisatie	Dienstenleverancier
x	x	x	x	n.v.t.
Scope		Privacycontrole, inlezen en inkijk		
Nadere toelichting		Het is essentieel dat rechtmatig gebruik van Suwinet gerelateerde gegevens is geborgd. De organisatie heeft toezicht op privacy in haar organisatie ingericht. Vaak wordt dit bereikt door een persoon te benoemen die hiervoor verantwoordelijk is, zoals een privacyfunctionaris, die richtlijnen behoort te geven aan managers, gebruikers en aanbieders van diensten over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Ten behoeve van processen/systemen/projecten waar Suwinet gerelateerde gegevens worden verwerkt /uitgewisseld, worden Privacy Impact analyses (PIA) en/of Gegevensbeschermings Effect Beoordelingen (GEB) uitgevoerd en onderhouden. Een actueel privacybeleid is beschikbaar en vastgesteld door een daartoe bevoegde functionaris. Deze nalevingsnorm vraagt aantoonbaarheid van de werking van de normen betreffende autorisatiebeheer en logging. Autorisatiebeheer dient op orde te zijn (norm 9.2.1, 9.2.2, 9.2.5 en 9.2.6) en o.b.v. logging dient signalering te kunnen plaatsvinden (norm 12.4.4 en 12.4.2) om het gebruik van persoonsgegevens te monitoren, te loggen en regelmatig te beoordelen. Het betreffen systemen waarbinnen Suwinet gegevens verwerkt worden. De periodieke controles binnen een jaar, op beoordeling van autorisatiebeheer, gebruik Suwinet gerelateerde persoonsgegevens, logging en incidentbeheer, zijn aantoonbaar uitgevoerd.		