

Suwinet-guidance

Handreiking ENSIA-verantwoording voor Suwinet

VNG Realisatie

Nassaulaan 12
2514 JS Den Haag

Maart 2024

Inhoud

1.	Inleiding Suwinet-guidance	3
2.	Achtergrond	3
3.	Verantwoordingsproces	3
4.	Spelers in het veld.....	4
5.	Opbouw guidance	4
6.	Suwinet guidance per BIO-control	5

1. Inleiding Suwinet-guidance

Deze handreiking is uitgegeven door het Beheerteam ENSIA van VNG Realisatie en is ontwikkeld en afgestemd met NOREA, BKWI, SUWI-team VNG-R, IBD en Ministerie van SZW.

Deze handreiking is bedoeld als guidance voor de beantwoorder van de vragen in de BIO-vragenlijst die voorzien zijn van het trefwoord "IT-audit". Het doel is richting geven voor de invuller bij het beantwoorden van IT-audit vragen en voor de auditor bij het beoordelen van de gegeven antwoorden. Het resultaat moet zijn dat gemeenten met de juiste scope de juiste antwoorden geven bij de BIO-controls en -maatregelen en bij de ENSIA-vragen.

Deze guidance wordt jaarlijks bijgesteld als gevolg van ontwikkelingen alsmede de feedback van gebruikers en de audit community (via de Suwi-vakgroep van de NOREA). Het beheer van deze handreiking ligt bij VNG Realisatie.

2. Achtergrond

Gemeenten verantwoorden zich jaarlijks over het gebruik van Suwinet volgens de ENSIA-systematiek. Zij geven zo inzicht in de mate waarin de gemeente compliant is aan de BIO. Door gemeenten wordt verantwoording afgelegd langs twee pijlers:

- Intern ten behoeve van de verantwoording van het college aan de raad over de mate waarin de gemeentelijke bedrijfsvoering in control is op het gebied van informatiebeveiliging met als norm de BIO.
- Extern ten behoeve van de verantwoording aan de toezichthouders en stelselhouders van het Rijk.

Jaarlijks wordt door de Regieraad ENSIA vastgesteld op welke wijze en met welke scope extra zekerheid verkregen wordt door het laten controleren van een deel van de uitkomsten van de ENSIA-zelfevaluatie door een bij de NOREA aangesloten auditor. Het ministerie van SZW bepaalt de selectie van normen uit de BIO voor de verantwoording Suwinet (op basis van de SUWI-regeling art. 5.2.2. en art. 6.4). Deze selectie is bij het BKWI gepubliceerd als de Verantwoordingsrichtlijn Informatiebeveiliging GeVS. Deze guidance is alleen gericht op de verantwoording Suwinet.

3. Verantwoordingsproces

Het verantwoordingsproces bestaat uit een aantal te doorlopen stappen en kent een aantal spelers. Afhankelijk van de ontvanger van de verantwoording (intern aan de gemeenteraad of extern aan het rijk) is er een aantal te volgen stappen. Voor de interne verantwoording ligt de nadruk op de (gemeentebrede) interne verantwoording. Bij de verantwoording aan het rijk ligt de nadruk op audit (assurance) van de collegeverklaring en het in te leveren/te uploaden bewijsmateriaal.

De verantwoording Suwinet vindt plaats op basis van een jaarlijkse zelfevaluatie aan de hand van de BIO-vragenlijst ENSIA. Deze fase 'zelfevaluatie' vindt plaats in de periode 1 juli tot en met 31 december. De gemeente voert de zelfevaluatie uit binnen de eigen organisatie en verwerkt de uitkomsten uit de te ontvangen Third Party Mededelingen (TPM's) van serviceorganisaties (indien van toepassing moet ook gekeken worden naar IT-organisaties (subverwerkers) waarvan een serviceorganisatie gebruik maakt). In de ENSIA-fase 'verantwoorden' (vanaf 1 januari) worden de ENSIA-uitkomsten geanalyseerd en getoetst door een IT-auditor. Voor 1 mei dienen de verantwoordingsdocumenten (vastgesteld door het College) te worden geüpload in de ENSIA tooling. De verantwoording Suwinet wordt na aanlevering door de ENSIA-coördinator automatisch

via ENSIA aangeleverd aan het BKWI. Het BKWI verwerkt de uitkomsten van de individuele gemeenten in een transparantierapportage voor het ministerie van SZW.

4. Spelers in het veld

Voor de IT-audit Suwinet zijn de volgende stakeholders zijn in beeld:

Speler	Uitleg
Gemeente	Spreekt voor zich.
Serviceorganisatie	De partij waar de gemeente in meerdere of mindere mate SUWI-taken aan uitbestede heeft. Hierbij moet ook gekeken worden naar IT-organisaties (subverwerkers) waarvan een serviceorganisatie gebruik maakt.
Lijnmanager	De eindverantwoordelijke functionaris binnen een gemeente die verantwoordelijk is voor het uitvoeren van 1 of meer SUWI-taken en zich ook daarover moet verantwoorden.
Security Officer / de gemandateerde/ intern controller	De persoon die de lijnmanager ondersteunt met het uitvoeren van controles en die gemachtigd is specifieke rapportages of gedetailleerde loginformatie op te vragen bij BKWI. Deze functionaris is bij BKWI bekend.
Gebruikersbeheerder Suwinet	De functionaris bij de gemeente/uitvoeringsorganisatie die het uitvoerende werk doet rondom afmelden, wijzigen, aanmelden van gebruikers en het onderhouden van de gebruikers autorisatiematrix.
Applicatiebeheerders	De functionaris bij de gemeente/uitvoeringsorganisatie die de rol van applicatiebeheerder (technisch en/of functioneel) van achterliggende applicaties die betrokken zijn bij de verwerking van DKD-Inlezen.
BKWI (Bureau Ketenautomatisering Werk en Inkomen)	De partij die de jaarlijkse rapportage maakt aan SZW, de beheerder van Suwinet-inkijk en Suwinet-Inlezen. BKWI weet van alle aansluitingen wie de gebruikersadministratie uitvoert. De rol van gebruikersbeheerder wordt toebedeeld door het BKWI.
Inlichtingenbureau	De partij via welke DKD-Inlezen verloopt. Zie ook: www.inlichtingenbureau.nl voor de routevoorziening Digitaal Klantdossier.

5. Opbouw guidance

Items	Uitleg
Hoofdstuk	Hoofdstuknummer en titel uit de BIO.
Paragraaf	Paragraafnummer en titel uit de BIO.
Control	Control-nummer en titel uit de BIO.
Toelichting Control	Control-tekst uit de BIO.
Maatregel	Overheidsmaatregelnummer en tekst uit de BIO.
Maatregel geldt voor	Toewijzing maatregel aan Suwinet-inkijk en/of Suwinet-Inlezen en/of DKD-Inlezen Let op: Bij DKD-Inlezen gaat het ook specifiek om de applicaties die hier gebruik van maken. Dat wil zeggen dat de maatregelen waarbij DKD-Inlezen in scope is, ook deze applicaties moeten voldoen aan deze maatregel.
Norm van toepassing op	Waar wordt de maatregel geïmplementeerd?
Nadere toelichting	Achtergrondinformatie.
Betrokken rollen	Functionarissen betrokken bij de invulling van control en maatregel.
Scope	Reikwijdte van de control en maatregel.
Aandachtspunten	Dit zijn de aandachtspunten voor de gemeente en de auditor voor waarop gecontroleerd wordt
Testaanpak	Dit zijn suggesties! Concrete aanwijzingen voor het voorbereiden en uitvoeren van de test.
Relevante documenten	Dit zijn suggesties! Documenten die als bewijslast kunnen dienen voor de auditor.

6. Suwinet-guidance per BIO-control

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.				
Maatregel	5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) De strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd f) de bevordering van het beveiligingsbewustzijn			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet Inlezen	DKD Inlezen	WGS Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	CISO, Directie, College				
Scope	Beleid				
Nadere toelichting	Let op de specifieke aandachtspunten voor de beveiliging van Suwinet gegevens en SUWI gerelateerde wetgeving (zie bijvoorbeeld het BIO OP product van de IBD - Handreiking informatiebeveiligingsbeleid, hoofdstuk 5.2) De focus ligt op de governance (incl. afspraken over de wijze van verantwoording). Er kan onderscheid gemaakt worden in een strategisch beleid en een tactisch beleid.				
Aandachtspunten	Er is een lijnmanager verantwoordelijk voor de uitvoering (van beleid en SUWI-processen). Deze verantwoordelijke lijnmanager(s) rapporteert/rapporteert aan de directie over informatiebeveiligingsaangelegenheden met betrekking tot het SUWI-stelsel Deze lijnmanager is betrokken bij de behandeling van incidenten waarbij SUWI geraakt wordt. In het beleid dient opgenomen te zijn dat de lijnmanager verantwoordelijk is voor de toegang tot de SUWI-informatie en het juiste gebruikers beheer (laat uitvoeren) bij in-dienst/wijziging van functie/uit-dienst.				
Testaanpak	Interview de verantwoordelijke functionarissen zoals opgenomen in beleid (of mandaatregister). Inspecteer het beveiligingsbeleid.				
Relevante documenten	<ul style="list-style-type: none"> Vastgesteld beleid Informatiebeveiliging, notulen collegeverklaring vaststelling. Hierbij kan gebruik gemaakt worden van een uitwerking in een specifiek informatiebeveiligingsbeleid op afdelings- of dienstniveau. Wijzigingen in algemeen beleid kunnen dan uitgewerkt worden naar beleid op afdelings- of dienstniveau zodat de verschillende documenten op elkaar blijven aansluiten. Vaststellen van strategisch beleid door college (zie bijvoorbeeld het format informatiebeveiligingsbeleid van de IBD). 				

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.				
Maatregel	5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	CISO, Directie, College				
Scope	Beleid				

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.	
Nadere toelichting	De organisatie dient het (strategisch) beleid regelmatig te beoordelen en zo nodig bij te stellen. De focus ligt op de frequentie van bijstelling.	
Aandachtspunten	NB: Als een gemeente in een structuur werkt van strategisch en tactisch beleid, dan kan het strategisch beleid ouder zijn, want het is dan generiek van opzet. Het beleid dient aan te sluiten bij een verkiezingscyclus (maximaal 5 jaar oud).	
Testaanpak	<ul style="list-style-type: none"> Controleer de datum van vaststelling van het informatiebeveiligingsbeleid. Stel vast of het beleid wordt geëvalueerd Past dit binnen de wijzigingscyclus? Zo ja, dan hoeft het centrale beleid niet jonger te zijn dan 4 jaar. 	
Relevante documenten	<ul style="list-style-type: none"> Beleid Informatieveiligheid, Notulen collegeverklaring vaststelling. Indien gebruik gemaakt wordt van een specifiek informatiebeveiligingsbeleid (beleidskader op dienstniveau incl. gelijke release. Vaststellen van strategisch beleid (zie bijvoorbeeld IBD OP product). Ondertekening van het beleid conform mandaatregister of document waarin bevoegdheden zijn ingericht. 	

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.	
Maatregel	6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
Maatregel geldt voor:		
Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen
		WGS- Inlezen
		Eigen organisatie
		Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x
		x
		N.v.t.
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), IT-leverancier	
Scope	Beleid, afdelingsbeleid	
Nadere toelichting	De governance dient in het informatiebeveiligingsbeleid een plek te hebben. Maar specifiek voor Suwinet zijn er een aantal rollen die mogelijk niet in het centrale beleid uitgewerkt hoeven te zijn. Hiervoor dient de afdelingsmanager mogelijk aanvullend beleid te schrijven of in een afdelingsnotitie te hebben uitgewerkt welke rollen er onderkend zijn en wie deze uitvoeren.	
Aandachtspunten	De invulling van de specifieke Suwinet-rollen kan op meerdere plekken uitgewerkt zijn. Niet alleen voor Suwinet-Inkijk en Suwinet-Inlezen maar ook achterliggende applicaties die gebruik maken van DKD-Inlezen. Tenminste de volgende rollen moeten belegd zijn: <ul style="list-style-type: none"> Wie autoriseert toegang Wie controleert het gebruik van Suwinet Wie controleert de actualiteit van de gebruikersadministratie Wie meldt of verwerkt incidenten in relatie tot Suwinet. 	
Testaanpak	Controleer de beschikbare documentatie op het aanwezig zijn van hierboven genoemde en belegde Suwinet-rollen en verantwoordelijkheden.	
Relevante documenten	<ul style="list-style-type: none"> Suwinet-Inkijk: Vastgestelde autorisatiematrix (rolbepaling), gebruikersadministratie. Suwinet-Inlezen: uit de logging van het systeem moet blijken dat de autorisatiematrix in lijn is met de logging. DKD-Inlezen: uit de logging van het systeem moet blijken dat de autorisatiematrix in lijn is met de logging. 	

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.	
Maatregel	6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.

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.				
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Bestuur, HRM				
Scope	Personeelsbeleid, informatiebeveiligingsbeleid				
Nadere toelichting	De governance dient in het informatiebeveiligingsbeleid een plek te hebben. De rol en de verantwoordelijkheden van de CISO dient beschreven te zijn in het beleid en de CISO is aangesteld (zie voorbeeld functieprofiel van de IBD). Als de gemeente gebruik maakt van HR21 (functiewaarderingssysteem voor gemeenten), dan is er gebruik gemaakt van de indelingsmotivering uit bijlage 1 van het BIO OP product Handreiking functieprofiel CISO van de IBD (aanwijzing, geen verplichting).				
Aandachtspunten	Tenminste de onafhankelijke positie moet zijn uitgewerkt: <ul style="list-style-type: none"> • Mandaat • Adviesfunctie • Controle naleving beleid • Rapportage in de lijn • Ondersteuning in de lijn 				
Testaanpak	Controleer het functieprofiel of het HR21 indelingsmotiveringsbesluit op de aanwezige punten. Er dient functiescheiding te zijn aangebracht daar waar sprake is van tegengestelde maatregelen, daar waar de functionaris meerdere rollen bekleedt.				
Relevante documenten	Functieprofiel CISO				

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.				
Maatregel	6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Bestuur, HRM				
Scope	Informatiebeveiligingsbeleid				
Nadere toelichting	De rol van CISO en de bijbehorende verantwoordelijkheden en bevoegdheden moeten formeel bij een medewerker zijn belegd.				
Aandachtspunten	De verantwoordelijkheden en bevoegdheden moeten aan een persoon zijn toegewezen en het moet binnen de organisatie bekend zijn wie de CISO is en wat hij doet.				
Testaanpak	Interview de verantwoordelijke functionarissen en stel vast dat taken, bevoegdheden en verantwoordelijkheden ten aanzien van de CISO-functie formeel zijn toegewezen en dat binnen de organisatie bekend is wie de CISO is en waarvoor hij/zij staat.				
Relevante documenten	Functieprofiel CISO. Organogram.				

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.				
Maatregel	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x

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 misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), HRM	
Scope	Personeelsbeleid, proces en procedurecontrole gegevensgebruik	
Nadere toelichting	Voor deze maatregel worden de beveiligingsrollen uit 6.1.1.3 getoetst.	
Aandachtspunten	Scheiding van taken (<i>segregation of duties</i>) Onafhankelijke controle van het gegevensgebruik en autorisatiebeheer	
Testaanpak	Toets of het gebruik van gegevens uit Suwinet (incl. de gegevens aangeleverd door het Inlichtingenbureau voor DKD-Inlezen) door iemand anders wordt gecontroleerd dan een gebruiker.	
Relevante documenten	Functie- en taakomschrijvingen.	

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.				
Maatregel	7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager)				
Scope	Bewustwording				
Nadere toelichting	Bewustwording is essentieel in het werken met persoonsgegevens. De organisatie dient een bewustwordingsprogramma te hebben.				
Aandachtspunten	Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma, dit is ook goed. Zijn specifieke Suwinet-risico's ook meegenomen in het bewustwordingstraject?				
Testaanpak	<ul style="list-style-type: none"> • Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. • Onderzoek de agenda van de organisatie op het aanwezig zijn van bewustwordingsactiviteiten. • Mogelijk financiële uitgaven in het kader van bewustwording. 				
Relevante documenten	Huisregels, e-learning, domeinspecifieke verplichtingen in aanvulling op huisregels (voor zover niet elders in de organisatie uitgewerkt).				

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.				
Maatregel	7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager)				
Scope	Bewustwording				
Nadere toelichting	Bewustwording is essentieel in het werken met persoonsgegevens. Medewerkers moeten opleidingen en trainingen volgen zodat ze zich in hun werk bewust zijn van hun				

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.	
	verantwoordelijkheden en weten hoe ze op een juiste manier met vertrouwelijke (persoons)gegevens moeten omgaan.	
Aandachtspunten	Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma, dit is ook goed.	
Testaanpak	<ul style="list-style-type: none"> • Interview een willekeurige gebruiker (ten minste 3) en vraag hem wanneer hij/zij iets gedaan heeft aan bewustwording. • Bewijs van deelname aan e-learning en/of bewustzijns campagne. • Controleer dat nieuwe medewerkers binnen drie maanden na hun indiensttreding een bewustzijnstraining succesvol hebben gevolgd. 	
Relevante documenten	Verstreckte certificaten van deelname, registratie van trainingen en deelnemers.	

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.				
Maatregel	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), HRM, gebruikersbeheerder				
Scope	Toegangsverlening Suwinet				
Nadere toelichting	Hangt samen met maatregel 6.1.1.1 Worden gebruikers van Suwinet gegevens altijd op dezelfde manier geautoriseerd tot de Suwinet-omgeving en is dat proces mogelijk organisatie-breed uitgewerkt? De afdelingsmanager heeft een belangrijke rol, hij moet toezien op het juiste gebruik van Suwinet en ervoor zorgen dat er niet te veel mensen toegang hebben, en ook dat ze niet te lang toegang hebben.				
Aandachtspunten	<ul style="list-style-type: none"> • Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). • Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma (bijvoorbeeld Identity and Access Management (IAM)-programma bij HR en of IT), dit is ook goed. • Deze maatregel heeft betrekking op de processen voor In dienst, doorstroom en uitstroom. • In het proces van nieuwe accounts geeft de manager opdracht om een account aan te maken. Hierbij wordt opgegeven welke rol moet worden toegekend. Als dit een aanvullende rol betreft op de bestaande autorisatiematrix, dan dient deze te worden opgenomen. 				
Testaanpak	<ul style="list-style-type: none"> • Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. • De lokale Suwinet-administratie voor gebruikersbeheer dient synchroon te zijn aan de autorisatiematrix bij Suwinet-Inkijk. Controleer hoe ervoor gezorgd wordt dat de lijnmanager periodiek controleert welke gebruikers waartoe geautoriseerd zijn, en of de beide administraties synchroon lopen. 				
Relevante documenten	Autorisatiematrix in vergelijking met de autorisatie tot Suwinet-Inkijk				

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.				
Maatregel	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.			
Maatregel geldt voor:			Norm van toepassing op:		

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.				
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), IT, leverancier				
Scope	Toegangsverlening Suwinet, gebruikersaccounts				
Nadere toelichting	Hangt samen met 6.1.1.1 en 9.2.1.1				
Aandachtspunten	<ul style="list-style-type: none"> Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure. Indien gebruik gemaakt wordt van groepsaccount dient de afdelingsmanager Suwinet/sociaal domein speciaal toegang geven. 				
Testaanpak	<ul style="list-style-type: none"> Interview de verantwoordelijke voor de processen met Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. Onderzoek de organisatie of er een specifieke procedure is voor het aan- en afmelden van gebruikers met toegang tot de gegevens van Suwinet. Onderzoek de AD/LDAP/SSO op het bestaan van groepsaccounts. Onderzoek of de leverancier gebruik maakt van speciale beheer accounts. 				
Relevante documenten	Autorisatiematrix (bestaan groepsaccounts), gebruikersoverzicht.				

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.				
Maatregel	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), IT, leverancier				
Scope	Toegangsverlening Suwinet-gegevens (incl. DKD-Inlezen), gebruikersaccounts				
Nadere toelichting	Hangt samen met 6.1.1.1 en 9.2.1.1				
Aandachtspunten	Het gaat om het controleren van de administratie van toegangsverlening en of de lijnmanager inderdaad de toegang tot Suwinet autoriseert of laat autoriseren. Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure.				
Testaanpak	Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel.				
Relevante documenten	Vastgestelde autorisatiematrix, gebruikersoverzicht.				

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.				
Maatregel	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager)				

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.	
Scope	<ul style="list-style-type: none"> Toegangsverlening Suwinet, speciale Suwinet-accounts (speciale bevoegdheden zijn het kunnen zoeken met andere zoek sleutels dan het BSN zoals bijv. op naam of kenteken). Andere speciale accounts zijn: die van de gebruikersbeheerder, die kan accounts aanmaken en verwijderen en rollen maken. Die van de Security Officer of de gemandateerde, die kan specifieke rapportage opvragen (die is niet geanonimiseerd)). Achterliggende applicaties die gebruik maken Suwi-gegevens dmv DKD-Inlezen 	
Nadere toelichting	Hangt samen met 6.1.1.1 en 9.2.1.1	
Aandachtspunten	Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-brede procedure voor toegangsverlening. Let op bij kleine gemeenten en afdelingen: de kans bestaat dat sommige controletaken niet goed gescheiden worden.	
Testaanpak	<ul style="list-style-type: none"> Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. Onderzoek of er rollen binnen de Suwinet-autorisatie zijn die eigenlijk niet samen kunnen gaan en waarom dat dit zo is. Zie ook: www.bkwi.nl voor het 'Overzicht autorisaties op Suwinet-Inkijk voor GSD'. Hierbij zijn ook de autorisaties relevant van achterliggende systemen die gebruik maken van Suwinet gegevens via DKD-Inlezen. Controleer of de lijnmanager voldoende waarborgen of mitigerende maatregelen genomen heeft om de risico's van het mogelijk samengaan van beheren functies en/of beschikken functies en/of controleren functies te beheersen (vier ogen principe, extra interne controle, controle via een andere afdeling). 	
Relevante documenten	Autorisatiematrix.	

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.				
Maatregel	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager)				
Scope	Toegangsverlening Suwinet. Achterliggende applicaties die gebruik maken Suwi-gegevens dmv DKD-Inlezen				
Nadere toelichting	Hangt samen met 6.1.1.1 en 9.2.1.1				
Aandachtspunten	Er moet een register zijn van personen die bevoegd zijn om autorisatiemutaties aan te vragen. Uit het overzicht moet blijken welke toegangsrechten deze personen mogen aanvragen.				
Testaanpak	<ul style="list-style-type: none"> Interview de verantwoordelijke voor Suwinet en vraag hoe hij/zij binnen zijn afdeling omgaat met deze maatregel. Onderzoek of de lijst met gemandateerde personen actueel is (er mogen geen namen op voorkomen die niet langer voor de gemeente werken). 				
Relevante documenten	Mandaatregister.				

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.	
Maatregel	9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.

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.				
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager)				
Scope	<ul style="list-style-type: none"> Toegangsverlening Suwinet, speciale Suwinet-accounts (speciale bevoegdheden zijn het kunnen zoeken met andere zoek sleutels dan het BSN zoals bijv. op naam of kenteken. Andere speciale accounts zijn: die van de gebruikersbeheerder, die kan accounts aanmaken en verwijderen en rollen maken. Die van de Security Officer of de gemandateerde, die kan specifieke rapportage opvragen (die is niet geanonimiseerd)). Ook de achterliggende applicaties die gebruik maken van Suwinet-gegevens via DKD-Inlezen zijn onderdeel van deze scope. 				
Nadere toelichting	Het Ministerie van SZW heeft in haar selectie voor verantwoording eveneens maatregel 9.2.5.1 opgenomen (BBN1). Maatregel 9.2.5.3 vergt een halfjaarlijkse controle. Hiermee wordt eveneens aan maatregel 9.2.5.1 (jaarlijkse controle) voldaan. Hangt samen met 6.1.1.1 (inrichting) en 9.2.1.1 (procedure)				
Aandachtspunten	Geen				
Testaanpak	Controleer of de afdelingsmanager minimaal 1 keer per 6 maanden de toegangsrechten (laat) controleren. Dit moet blijken uit een rapportage van de controle aan of van de lijnmanager.				
Relevante documenten	Rapportage controle toegangsrechten.				

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.				
Maatregel	9.2.6.1	Deze control kent in de BIO geen maatregel. NB: voor deze control is een aanvullende maatregel opgesteld in de ENSIA-vragenlijst: Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering 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.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet- Inkijk	Suwinet- Inlezen	DKD- Inlezen	WGS- Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), HRM, IT				
Scope	Toegangsverlening Suwinet				
Nadere toelichting	Deze maatregel hangt samen met 6.1.1.1 en 9.2.1.1. Worden de toegangsrechten van gebruikers bij wijziging van functie aangepast? Worden alle gebruikers van Suwinet-gegevens altijd binnen een dag afgemeld uit het systeem als ze de toegang tot Suwinet-gegevens niet meer nodig hebben? Omdat de control geen verplichte overheidsmaatregelen kent, is er een zekere keuzevrijheid bij de organisatie over de exacte uitwerking van deze control in maatregelen.				
Aandachtspunten	<ul style="list-style-type: none"> Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma voor toegangsbeleid (HR en of IT). Rechten dienen in tijd goed volgordekelijk doorgevoerd te worden bij wijziging van functie om te voorkomen dat een te brede set aan rechten aan de gebruiker wordt toegekend. 				
Testaanpak	<ul style="list-style-type: none"> Interview de verantwoordelijke voor Suwinet en vraag hoe hij binnen zijn afdeling omgaat met deze maatregel. Onderzoek de organisatie of er een generieke procedure is voor het aan- en afmelden van gebruikers. Laat een uitdraai maken van de huidige lijst van geautoriseerde gebruikers, controleer of deze gebruikers nog werkzaam zijn binnen het SUWI-domein. Neem een willekeurige steekproef van 5% van de gebruikers. 				

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.	
Relevante documenten	Procedure in dienst, uit dienst en bij wijziging van functie, gebruikersoverzicht, autorisatiematrix.	

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.				
Maatregel	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum* worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld. *www.forumstandaardisatie.nl			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
N.v.t.	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Cryptografie Suwinet-Inlezen en DKD inlezen				
Nadere toelichting	Cryptografie is een essentiële maatregel om de vertrouwelijkheid te waarborgen van Suwinet-gegevens. Cryptografie wordt toegepast op vele vlakken: opslag, transport en daar waar het niet kan worden gegarandeerd dat de vertrouwelijkheid van de gegevens kan worden gewaarborgd. Voor Suwinet-Inkijk geldt dat de webpagina die gehost wordt door BKWI al voorzien is van HTTPS, deze pagina is onder beheer van BKWI en is dus buiten scope. In scope zijn de applicaties die Suwinet-Inlezen of DKD-Inlezen gebruiken en het transport naar die applicaties. De maatregel richt zich op het bestaan van cryptografiebeleid.				
Aandachtspunten	Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma (HR en of IT), dit is ook goed.				
Testaanpak	<ul style="list-style-type: none"> Interview de verantwoordelijke voor Suwinet of zijn (IT) beveiligingsmanager en vraag hoe cryptografie wordt toegepast in het kader van Suwinet bij DKD-Inlezen en Suwinet-Inlezen. Als gegevens verwerkt worden in de cloud of het bedrijfsproces is uitbesteed, is het ook van belang te onderzoeken hoe bij het transport van gegevens de vertrouwelijkheid van de gegevens gewaarborgd is. Onderzoek de organisatie of er een cryptografiebeleid is dat voldoet aan de punten genoemd in de BIO. 				
Relevante documenten	Cryptografiebeleid.				

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.				
Maatregel	10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
N.v.t.	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Cryptografie Suwinet-Inlezen en DKD inlezen				

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.
Nadere toelichting		De gehanteerde technologie voor cryptografie moet voldoen aan de standaarden die "veilig" worden beschouwd.
Aandachtspunten		Focus specifiek op de afdeling die gebruik maakt van Suwinet (Afdeling Sociale Zaken, maar mogelijk ook Burgerzaken, RMC en gemeentelijk Gerechtsdeurwaarders). Het kan zijn dat de afdeling meeloopt in een organisatie-breed programma (HR en of IT), dit is ook goed.
Testaanpak		<ul style="list-style-type: none"> • Observeer de (wijze van) encryptie van gegevens. • Inspecteer de TLS-configuratie. Deze moet voldoen aan de laatste stand der techniek. • Inspecteer voor webapplicaties de HTTPS-configuratie. Zie hiervoor de testaanpak voor DigiD bij norm U/PW.02. • Interview de verantwoordelijke voor Suwinet of zijn (IT) beveiligingsmanager en vraag hoe cryptografie wordt toegepast in het kader van Suwinet bij DKD-Inlezen en Suwinet-Inlezen.
Relevante documenten		Cryptografiebeleid.

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.				
Maatregel	12.1.1.1	Deze control kent in de BIO geen maatregel NB: voor deze control is een aanvullende maatregel opgesteld in de ENSIA-vragenlijst: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.				
Maatregel geldt voor:			Norm van toepassing op:			
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt	
x	x	x	x	x	x	
Betrokken rollen	IT-manager, functioneel beheer, manager I&A.					
Scope	Beheer procedures					
Nadere toelichting	Bedieningsprocedures bestaan op alle gebieden, functioneel en technisch. Voor Suwinet geldt dat de organisatie niet zonder bedieningsprocedures kan, zo moet er voor alle handelingen waarbij Suwinet gebruikt wordt ook een bedieningshandleiding of werkinstructie aanwezig zijn. Idealiter worden deze gemaakt op basis van beleid, maar daar ligt hier niet de focus. 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. Omdat de control geen maatregelen kent is er een zekere keuzevrijheid bij de organisatie over de exacte uitwerking van deze control in maatregelen.					
Aandachtspunten	Dit is een kapstokartikel dat binnen 12.1 in diverse controls uitgewerkt is. Focus specifiek op de IT-afdeling en functioneel beheer					
Testaanpak	Interview de verantwoordelijke voor IT/FB en vraag welke bedieningsprocedures aanwezig zijn voor het gebruik van Suwinet-gegevens, dit kunnen zijn: functioneel beheer procedures. Bijvoorbeeld: Installatie van systemen, Back-up, Restore, Monitoring, Afhandeling van fouten met betrekking tot Suwinet.					
Relevante documenten	Bedieningsprocedures voor beheer.					

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.				
Maatregel	12.4.1.1	Een logregel bevat minimaal: <ul style="list-style-type: none"> (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; 				

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.				
		(e) een datum en tijdstip van de gebeurtenis.			
Maatregel geldt voor:				Norm van toepassing op:	
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Logging				
Nadere toelichting	Dit is een kapstokartikel, deze control is de inleiding op de andere controls van 12.4 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.				
Aandachtspunten	<ul style="list-style-type: none"> Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet-gegevens. Dit zal veelal binnen applicaties geregeld zijn, let op mogelijke overlap met 18.1.4 De logging op de servers van BKWI voor Suwinet-Inkijk is niet in scope. Accountgegevens van medewerkers die de logging controleren dienen altijd persoonsgebonden te zijn. 				
Testaanpak	<ul style="list-style-type: none"> Interview het hoofd IT en vraag hoe logging geregeld is binnen de organisatie, hoe het wordt opgeslagen, welke gebeurtenissen worden vastgelegd en hoe de logregel opgebouwd is. Onderzoek de logging van Suwinet-Inlezen of DKD-Inlezen (servers en applicaties). 				
Relevante documenten	Logbeleid, autorisatiematrix, logbestanden.				

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.				
Maatregel	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.			
Maatregel geldt voor:				Norm van toepassing op:	
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Logging				
Nadere toelichting	Een logregel mag bijvoorbeeld geen inloggegevens bevatten of andere informatie die een kwaadwillende in staat stellen om beveiligingsmaatregelen te omzeilen.				
Aandachtspunten	<ul style="list-style-type: none"> Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet-gegevens. Dit zal veelal binnen applicaties geregeld zijn, let op mogelijke overlap met 18.1.4 De logging op de servers van BKWI voor Suwinet-Inkijk is niet in scope. 				
Testaanpak	<ul style="list-style-type: none"> Interview het hoofd IT en vraag hoe de logregel opgebouwd is. Onderzoek de logging van Suwinet-Inlezen of DKD-Inlezen (servers en applicaties). 				
Relevante documenten	Logbeleid, logbestanden.				

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.				
Maatregel	12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/ of SOC middels detectievoorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor			

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.				
	rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.				
Maatregel geldt voor:				Norm van toepassing op:	
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Intrusion Detection, Firewall				
Nadere toelichting	Het netwerk moet mogelijke aanvallen kunnen detecteren en blokkeren.				
Aandachtspunten	Controleer het netwerkschema op de aanwezigheid van firewalls / IDS.				
Testaanpak	Interview het hoofd IT en vraag welke maatregelen zijn getroffen om tijdig mogelijke aanvallen te detecteren (monitoring, SIEM, SOC). Als deze er niet zijn, moet een expliciete risicoafweging zijn gemaakt en bekend gesteld aan het verantwoordelijke management (GS/dir. Bedrijfsvoering) en deze risicoafweging mag maximaal een jaar oud zijn.				
Relevante documenten	Netwerkschema, risicoacceptatie.				

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.				
Maatregel	12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.			
Maatregel geldt voor:				Norm van toepassing op:	
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
N.v.t.	x	x	x	x	x
Betrokken rollen	IT-manager				
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.				
Aandachtspunten	<ul style="list-style-type: none"> Focus specifiek op de IT-afdeling. Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet-gegevens. 				
Testaanpak	<ul style="list-style-type: none"> Interview het hoofd IT en vraag welke logging wordt bewaard. De logging op de servers van BKWI voor Suwinet-Inkijk zijn niet in scope. 				
Relevante documenten	Logbeleid, overzicht van logbestanden.				

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.				
Maatregel	12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.			
Maatregel geldt voor:				Norm van toepassing op:	
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
N.v.t.	x	x	x	x	x
Betrokken rollen	IT-manager				
Scope	Logging				

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.	
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.	
Aandachtspunten	<ul style="list-style-type: none"> • Focus specifiek op de IT-afdeling • Controleer ook logging met betrekking van de toegang van gebruikers tot Suwinet-gegevens. 	
Testaanpak	<ul style="list-style-type: none"> • Interview het hoofd IT en vraag hoe lang logging wordt bewaard en hoe het wordt bewaard. • Onderzoek alleen de logging van Suwinet-Inlezen of DKD-Inlezen (servers en applicaties en eventuele message broker). • Onderzoek of de logging adequaat wordt beschermd tegen ongewenste manipulatie. • De logging op de servers van BKWI voor Suwinet-Inkijk zijn niet in scope. 	
Relevante documenten	Logbeleid.	

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.				
Maatregel	12.4.2.3	Er is een (onafhankelijke) interne auditprocedure die minimaal halfjaarlijks toetst op het ongewijzigd bestaan van logbestanden.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
N.v.t.	x	x	x	x	x
Betrokken rollen	IT-manager, interne auditor/controller				
Scope	Logging				
Nadere toelichting	De logging moet periodiek gecontroleerd worden op uitzonderingen. Het interne auditproces waarborgt dat gecontroleerd wordt dat dit daadwerkelijk gebeurt.				
Aandachtspunten	<ul style="list-style-type: none"> • Focus specifiek op de IT-afdeling. 				
Testaanpak	<ul style="list-style-type: none"> • Interview het hoofd IT en vraag naar het auditrapport en de controleverslagen. • Onderzoek of getoetst is dat de logging halfjaarlijks is gecontroleerd. 				
Relevante documenten	Intern auditrapport, controleverslagen				

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.				
Maatregel	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Bestuur, HRM.				
Scope	Personeelsbeleid, privacybeleid.				
Nadere toelichting	Het is essentieel dat er onafhankelijk toezicht is op het rechtmatig gebruik van Suwinet. Hiervoor moet een Functionaris Gegevensbescherming aangesteld zijn.				
Aandachtspunten	Tenminste de onafhankelijke positie moet zijn uitgewerkt: <ul style="list-style-type: none"> • Mandaat • Adviesfunctie • Controle naleving beleid • Rapportage in de lijn • Ondersteuning in de lijn. 				

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.
Testaanpak		Controleer het functieprofiel of het HR21 indelingsmotiveringsbesluit op de aanwezige punten. Er dient functiescheiding te zijn aangebracht daar waar sprake is van tegengestelde maatregelen, daar waar de functionaris meerdere rollen bekleedt.
Relevante documenten		Functieprofiel Functionaris Gegevensbescherming.

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.			
Maatregel	18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.			
Maatregel geldt voor:			Norm van toepassing op:		
Suwinet-Inkijk	Suwinet-Inlezen	DKD-Inlezen	WGS-Inlezen	Eigen organisatie	Serviceorganisatie en onderliggende IT-organisaties (subverwerkers) waarvan gebruik wordt gemaakt
x	x	x	x	x	N.v.t.
Betrokken rollen	Verantwoordelijke voor Suwinet (lijnmanager), Security Officer, gemandateerde, intern controleur, privacyfunctionaris Suwinet.				
Scope	Privacy controle, Suwinet-Inlezen en Suwinet-Inkijk				
Nadere toelichting	Het is essentieel om het gebruik van persoonsgegevens te monitoren, te loggen en regelmatig te beoordelen. Het betreft systemen waarbinnen Suwinet-gegevens verwerkt worden.				
Aandachtspunten	Focus op applicatie specifieke logging, zoals die van Suwinet-Inkijk, maar let vooral op de (zaak)systemen achter Suwinet en DKD-Inlezen. Controleer of deze logging regelmatig beoordeeld wordt op het rechtmatig verwerken van persoonsgegevens. Zie hiervoor de handreiking van VNG Realisatie. Als nog niet voldoende privacy logging aanwezig is, vraag dan aan de organisatie op welke termijn maatregelen genomen worden in (zaak)systemen.				
Testaanpak	Interview de Suwinet-verantwoordelijke lijnmanager en de privacyfunctionaris Suwinet op het bestaan van logging en de controle daarop Is het privacybeleid vastgesteld? Onderzoek de procedures voor controle van de applicatie logging.				
Relevante documenten	Het gaat natuurlijk om meer dan alleen logging: een goed uitgangspunt is de controle of de organisatie beschikt over een actueel en vastgesteld privacybeleid. In het kader van naleving: controle generieke gebruikersrapportage en mogelijk opgevraagde specifieke rapportages bij BKWI. Zie ook de 'Handreiking Gebruikersrapportage Suwinet-Inkijk' op https://vng.nl/projecten/ensia				