VNG Realisatie

Handreiking Implementatie Specifiek Suwinet-normenkader Afnemers 2017

Versie 2.0 van mei 2019

Inhoud

1 Inleiding

Met ingang van 1 april 2017 is het nieuwe Suwinet-normenkader afnemers van kracht geworden voor gemeenten. Dit normenkader vervangt het Normenkader GeVS 2011. De normen in het normenkader GeVS 2011 zijn in het kader van het programma 'Borging veilige gegevensuitwisseling via Suwinet' tegen het licht gehouden, aangescherpt en in lijn gebracht met de generieke bestaande baselines voor informatiebeveiliging, namelijk de normenkaders van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de Baseline Informatiebeveiliging Rijksdienst (BIR).
Momenteel (mei 2019) worden er analyses uitgevoerd om het Suwinet-normenkader in lijn te brengen met de Baseline Informatiebeveiliging Overheid (BIO). Dit document zal daar t.z.t. op aangepast worden.

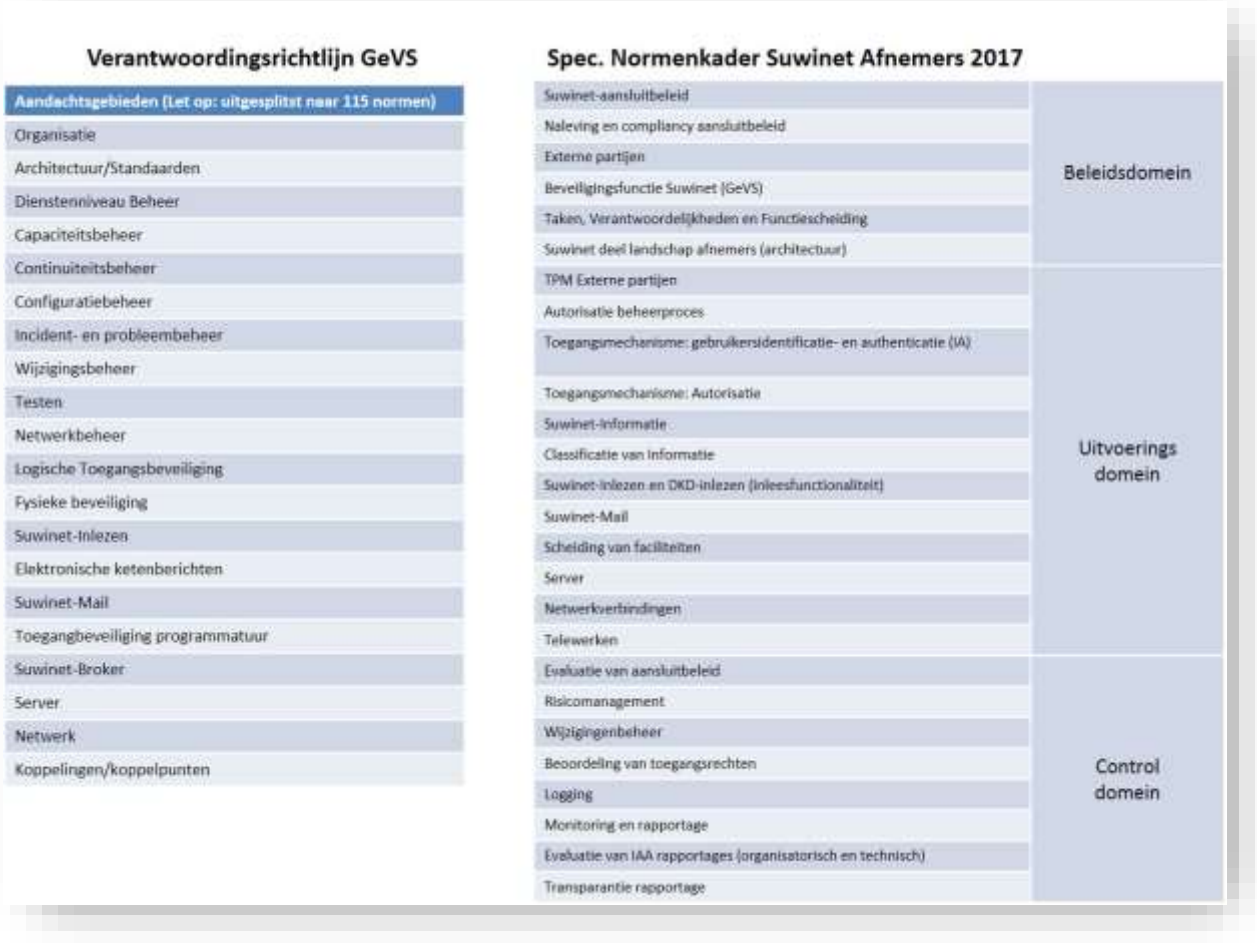
Bij de totstandkoming van het nieuwe Suwinet-normenkader is eerst vastgesteld welke risico's minimaal moeten worden afgedekt. Hierna zijn de normen aangescherpt en opgenomen in het Suwinet-normenkader. De normen zijn in lijn met bovengenoemde baselines.

Waarom een handreiking voor de implementatie van het nieuwe normenkader?

Na vaststelling en publicatie van het nieuwe Suwinet normenkader in april 2017 zijn veel vragen binnengekomen bij het toenmalige implementatieteam 'Borging veilige gegevensuitwisseling via Suwinet'. Bijvoorbeeld: wat is het verschil tussen het oude en nieuwe normenkader en hoe komt de BIG terug in het nieuwe normenkader? Hoe kan het geïmplementeerd worden? Wat is de relatie met ENSIA en hoe kun je de conformiteitsindicatoren duiden?
Met deze handreiking beogen wij de relatie tussen de verschillende onderwerpen uit te leggen en gaan wij in op de verschillen tussen het oude en nieuwe normenkader. Wij bieden handvatten om het nieuwe Suwinet normenkader te implementeren en gaan tenslotte in op de relatie van het nieuwe normenkader met ENSIA.

2 Algemene verschillen:
Verantwoordingsrichtlijn GeVS 2011 en Specifiek Normenkader Suwinet Afnemers 2017

In volgend schema zijn de 'oude' verantwoordingsrichtlijn GeVS 2011 en het Specifiek Normenkader Suwinet Afnemers tegenover elkaar gezet. Belangrijk verschil bij de totstandkoming van het nieuwe Suwinet normenkader is dat een andere methodiek is gebruikt. In het oude normenkader zijn de 115 normen voor afnemers, bronhouders en de beheerder samengevoegd en vervolgens onderverdeeld in 20 aandachtsgebieden.



Verantwoordingsrichtlijn GeVS

Aandachtsgebieden (Let op: uitgesplitst naar 115 normen)
Organisatie
Architectuur/Standaarden
Dienstenniveau Beheer
Capaciteitsbeheer
Continuiteitsbeheer
Configuratiebeheer
Incident- en probleembeheer
Wijzigingsbeheer
Testen
Netwerkbeheer
Logische Toegangsbeveiliging
Fysieke beveiliging
Suwinet-Inlezen
Elektronische ketenberichten
Suwinet-Mail
Toegangbeveiliging programmatuur
Suwinet-Broker
Server
Netwerk
Koppelingen/koppelpunten

Spec. Normenkader Suwinet Afnemers 2017

Suwinet-aansluitbeleid	Beleidsdomein
Naleving en compliancy aansluitbeleid	
Externe partijen	
Beveiligingsfunctie Suwinet (GeVS)	
Taken, Verantwoordelijkheden en Functiescheiding	
Suwinet deel landschap afnemers (architectuur)	
TPM Externe partijen	Uitvoerings domein
Autorisatie beheerproces	
Toegangsmechanisme: gebruikersidentificatie- en authenticatie (IA)	
Toegangsmechanisme: Autorisatie	
Suwinet-Informatie	
Classificatie van informatie	
Suwinet-Inlezen en DKD-inlezen (inleesfunctionaliteit)	
Suwinet-Mail	
Scheiding van faciliteiten	
Server	
Netwerkverbindingen	
Telewerken	
Evaluatie van aansluitbeleid	Control domein
Risicomanagement	
Wijzigingenbeheer	
Beoordeling van toegangsrechten	
Logging	
Monitoring en rapportage	
Evaluatie van IAA rapportages (organisatorisch en technisch)	
Transparantie rapportage	

In het algemeen geldt dat het nieuwe normenkader in basis dezelfde risico's afdekt als het oude normenkader.

Bij het opstellen van het nieuwe normenkader is een grote inspanning gepleegd om onderscheid te maken welke normen voor welke doelgroep (afnemers, beheerder en bronhouders) van toepassing zijn en is de omvang van de normen waar mogelijk gereduceerd. Het resultaat hiervan is dat het aantal normen voor afnemers is teruggebracht naar 26. Daardoor zijn normen die niet van toepassing waren voor gemeenten, bijvoorbeeld eisen ten aanzien van softwareontwikkeling, ook niet opgenomen in het nieuwe normenkader.

Het uitgangspunt van het nieuwe Suwinet Normenkader zijn de generieke bestaande baselines of normenkaders (BIR en BIG). De oude Suwinet normen zijn door de "zeef" van de BIG en de BIR gehaald. De normen die al goed door deze baselines worden afgedekt zijn niet in het nieuwe Suwinet normenkader opgenomen.

3 Het nieuwe normenkader

In het nieuwe Suwinet-normenkader zijn de normen ondergebracht binnen een drietal domeinen, namelijk beleid, uitvoering en control.

Verder spreekt het nieuwe Suwinet-normenkader over criteria. Een criterium is hetzelfde als een norm. Per criterium (wie en wat) wordt het doel beschreven (waarom) en welk risico het moet afdekken. Vervolgens zijn hier conformiteitsindicatoren aan gekoppeld.

Een conformiteitsindicator kan worden opgevat als een implementatie-aanwijzing. Met andere woorden, u kunt het inzetten om de norm te implementeren. Het is echter geen verplichting. U kunt dus ook op een andere manier aan de norm voldoen. Het belangrijkste is dat het risico volledig is afgedekt en daarmee aan de norm wordt voldaan. De conformiteitsindicatoren vormen samen wel een goede richting om te voldoen aan de normen.

3.1 Highlights

Het nieuwe Suwinet normenkader bevat een aantal onderwerpen waar gemeenten vragen over hebben gesteld. De meeste vragen zijn te herleiden tot een aantal termen en onderwerpen.

1. Aansluitbeleid

Het aansluitbeleid verwijst naar het gemeente-breed informatiebeveiligingsbeleid met daarin specifieke aandacht voor ‘het aansluiten op’ Suwinet. Aansluitbeleid en informatiebeveiligingsbeleid zijn in die zin vergelijkbaar. Overigens, gemeenten noemen dit ook vaak het “beveiligingsbeleid Suwinet”.

2. Risico-klasse/classificatie van informatie

In het nieuwe normenkader wordt verwezen naar een door de bronhouders vast te stellen risicoklasse. Deze vaststelling heeft nog niet plaatsgevonden. Dat betekent dat de oude klasse geldt vanuit het voorgaande normenkader (classificatie 2). De IBD heeft hiervoor een praktische ‘Handreiking Dataclassificatie’ ontwikkeld. Deze vindt u op www.informatiebeveiligingsdienst.nl

3. Suwinet deel landschap afnemers

Dit betreft de IT-componenten die vanuit de gemeente een relatie hebben met Suwinet. Denk bijvoorbeeld aan de gemeentelijke kantoorautomatisering, het netwerk, de firewall en ook de applicatieserver. Indien men DKD-inlezen gebruikt, dan vallen ook de bijbehorende applicaties, waar gegevens uit Suwinet-Inkijk in komen te staan, onder het Suwinet deel landschap afnemers.

4. TPM

TPM staat voor ‘Third Party Memorandum’. Dit is een middel om de betrouwbaarheid op gebied van informatiebeveiliging van een derde partij te kunnen vaststellen. Een TPM wordt opgesteld door een externe auditor.

5. Eisen aan wachtwoorden

De scope van deze norm betreft zowel de eisen aan wachtwoorden aan Suwinet-zijde (door BKWI vast te stellen) als de (logische) toegangsbeveiliging aan gemeentezijde. Hierbij moet worden gedacht aan de toegang tot de gemeentelijke kantoorautomatisering/applicaties/netwerk.

6. OTAP

OTAP staat voor Ontwikkel-/Test-/Acceptatietest-/Productie-omgeving. Dit betreft de scheiding van IT-omgevingen voor de verschillende stadia van software-ontwikkeling of bijvoorbeeld in productie name van software van derden. Deze norm ziet toe op procedures voor testen ten aanzien van de betrouwbaarheid van software, alvorens deze in productie wordt genomen. De inzet van nieuwe gemeentelijke software mag in die zin niet leiden tot beveiligingsrisico's voor Suwinet.
Een tweede onderdeel van deze norm is het voorkomen van gebruik van Suwinet-productiegegevens buiten de reguliere productie-omgeving. Dat betekent dat gegevens uit Suwinet-Inkijk niet mogen worden gebruikt voor het testen van nieuwe software. Dit kan bijvoorbeeld het geval zijn als men gebruik maakt van een applicatie voor DKD-Inlezen.

7. Suwinet-Servers

Onder Suwinet-servers worden de servers van de gemeente (of de hosting partij) verstaan die gekoppeld zijn aan en/of gebruik maken van het Suwinet. Bijvoorbeeld de applicatieserver waar de internet browser draait, de mailserver met Suwi-Mail of de applicatieserver voor de applicatie die gebruik maakt van DKD-inlezen.

8. Scope logging

De scope van deze norm betreft zowel de logging door BKWI (denk aan de generieke en specifieke rapportages) maar ook de logging van handelingen voor zover deze plaatsvindt op en binnen de gemeentelijke IT-omgeving (werkplek, beheer). Het gaat bij logging dus vooral om de vraag: 'wie heeft wanneer welk persoonsgegeven verwerkt en voor welk doel?'.

3.2 Hoe kun je het normenkader implementeren?

De InformatieBeveiligingsDienst (IBD) heeft voor de implementatie van de BIG een handreiking ontwikkeld om binnen de gemeente te toetsen of en in welke mate de gemeente voldoet aan de maatregelen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

De stappen die zijn beschreven in de handreiking om de BIG te implementeren kunnen ook worden aangehouden voor de implementatie van het nieuwe Suwinet normenkader.

Zoals aangegeven zijn ook de conformiteitsindicatoren inzetbaar om de normen te implementeren

4 Het specifieke normenkader Suwinet voor afnemers en ENSIA

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

Het effectief en efficiënt inrichten van de beveiliging van de informatievoorziening vraagt om eenduidige normen (en verantwoording). Dat geldt voor Suwinet en ook voor de basis registratie personen (BRP), de paspoortwet (PUN), DigiD en gebouwenregistraties (BAG/BGT). De basis voor de controle van al deze normen en de verantwoording daarover, is gelegd in ENSIA.

ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren. Dit doet ENSIA door het toezicht te bundelen en aan te laten sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier beter op sturen.

Binnen ENSIA is gewerkt aan één integrale set van vragen die alle bestaande normen en maatregelen in één keer uitvraagbaar maakt. Dit is inclusief een eindrapportage, een met DigiD gecombineerde controle door een auditor en een verantwoording (horizontaal en verticaal).

Het vernieuwde normenkader Suwinet voor afnemers is integraal binnen ENSIA opgenomen. Waarbij de formulering van de vragen is afgestemd op de gehanteerde structuur en terminologie van de BIG. Op die manier is het voor gemeenten eenvoudig om te voldoen aan de eisen van transparantie en audit. De vragenset van ENSIA is ontwikkeld door BZK, I en M, SZW, VNG en een aantal gemeenten. De vragenset is per 1 juli 2017 beschikbaar gesteld. Meer informatie is te vinden op de website van ENSIA en VNG-Realisatie.

Verantwoording nieuwe Suwinet normenkader via ENSIA

Gemeenten verstrekken via ENSIA informatie aan het ministerie van SZW. Het ministerie van SZW laat vervolgens via de beheerder (BKWI) een geconsolideerde rapportage opstellen, conform het nieuwe normenkader voor afnemers (C08 – transparantie-eis). Vervolgens bundelt BKWI de verantwoording van gemeenten tot een totaal overzicht en rapporteert aan het ketenoverleg GeVS en de minister van SZW.

Suwinet en ENSIA in de praktijk

In de afgelopen jaren was er al de eis aan gemeenten zich te verantwoorden aan het BKWI als beheerder van Suwinet op grond van het (volledige) normenkader GeVS 2011. Daarnaast heeft de Inspectie SZW een aantal opeenvolgende onderzoeken uitgevoerd naar de kwaliteit van de

informatiebeveiliging van Suwinet door gemeenten. De Inspectie SZW heeft deze onderzoeken afgebakend tot een selectie van zeven normen.

Het nieuwe normenkader Suwinet vereist dat gemeenten de informatiebeveiliging zodanig inrichten dat wordt voldaan aan de gestelde normen. De verantwoording vindt plaats in de ENSIA vragenlijst, aangevuld met een audit op een deel van de normen. In ENSIA kunnen gemeenten conform de structuur van de BIG aangeven hoe de informatieveiligheid voor Suwinet is georganiseerd. De ENSIA-vragen die zijn gerelateerd aan het normenkader Suwinet bevatten een verwijzing naar de betreffende norm (is opgenomen in de toelichting bij de vragen). Let er op dat door de vraagstelling (ja/nee vragen) het aantal vragen groter is dan het aantal normen. Een norm kan in meerdere vragen in ENSIA terugkomen en een vraag kan betrekking hebben op meer domeinen dan alleen het SUWI domein.

Over welke normen legt de gemeente verantwoording af aan het ministerie van SZW?
In de verantwoording gaat het om 13 normen waarover de gemeente zich verantwoordt in de collegeverklaring die uiteindelijk door de Register EDP-Auditor/RE wordt getoetst. Deze 13 normen zijn onder andere gebaseerd op de ‘bekende’ 7 normen zoals de inspectie die in voorgaande jaren toetste en enkele normen die uit de onderzoeken van de Autoriteit Persoonsgegeven (AP) naar voren zijn gekomen. In onderstaande tabel zijn deze normen opgenomen.

BIG	**Suwinet**[1]
Generieke controls met specifieke objectgerichte aanvullingen	
5.1.1 Beleidsdocument voor informatiebeveiliging	x (B01)
5.1.2 Beoordeling van het informatiebeleid x	x
6.1.1 Betrokkenheid van het college van B en W bij informatiebeveiliging x	x
6.1.2 Coördineren van informatiebeveiliging	x (B01, B03, B04)
6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging	x (B05)
Objectgerichte controls	
8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging x	
10.1.3 Functiescheiding	x (B05)
10.10.1 Aanmaken auditlogbestanden	x (C05)
10.10.2 Controle van het systeemgebruik	x (C06)
11.2.1 Registratie van gebruikers	x (U03)
11.2.4 Beoordeling van toegangsrechten van gebruikers	x (U03, C04)
11.5.2 Gebruikersidentificatie en -authenticatie	x (U03)
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen	x (U11)

De bovenstaande 13 normen zijn in de ENSIA vragenlijst gekoppeld aan 36 hoofdvragen. Het verschil in aantal komt doordat de normen als eenduidige vragen zijn geformuleerd in de vragenlijst. De beantwoording van deze vragen vormt de basis voor de verantwoording van het College aan het Rijk.

[1]Wanneer er geen verwijzing naar een Suwinetnorm is aangegeven is, betekent dit dat de vraag vanuit de BIG is toegevoegd. Daarmee wordt het meegenomen in de beoordeling van de informatiebeveiliging rondom Suwinet.

In totaal zijn in de vragenlijst 36 vragen opgenomen die relevant zijn voor suwi. De volledige set van antwoorden wordt meegenomen in de verantwoording van het College aan de raad d.m.v een paragraaf in het jaarverslag.

5 Nieuwe Suwinet normenkader i.r.t. Samenwerkingsverbanden

Er zijn in de eerste periode veel vragen gesteld hoe vanuit het normenkader voor Suwinet om te gaan met de verschillende vormen van samenwerking en hoe zich dit verhoudt tot (gemandateerde en gedelegeerde) overgedragen bevoegdheden. Het Ministerie van SZW heeft de grondslag voor (alle) verantwoording Suwinet toegelicht.

De gemeente is en blijft verantwoordelijk voor het aantoonbaar voldoen aan de normen voor Suwinet, ook al zijn de taken overgeheveld naar een samenwerkingsverband, in wat voor vorm dan ook. De verantwoording van de gemeente over het voldoen aan het specifieke normenkader Suwinet omvat derhalve ook de activiteiten binnen het samenwerkingsverband.