Ministerie van Sociale Zaken en
Werkgelegenheid

Handreiking Suwinet

Attentiepunten en illustratataties

Definitieve versie
17 maart 2016

Voorwoord

Hierbij ontvangt u de handreiking die we als Inspectie SZW hebben opgesteld naar aanleiding van het onderzoek naar Suwinet. In dit document worden de zeven essentiële normen uit het normenkader GeVS behandeld waarop we alle gemeenten hebben getoetst.

We zijn ons onderzoek - dat nu bijna is afgerond - in september 2015 gestart. Gemeenten die niet voldoen aan de zeven normen hebben recent een brief 'aankondiging tot aanwijzing' van de staatsecretaris van Sociale Zaken en Werkgelegenheid ontvangen.
In deze brief staat dan dat een gemeente actie moet ondernemen om alsnog zo snel mogelijk (tussen 6 en 12 weken) aan de zeven normen te voldoen.
Als Inspectie SZW bieden we met deze handreiking aanvullend informatie die gemeenten kunnen gebruiken, om alsnog aan de zeven normen te voldoen. Daarbij gaat het onder meer om operationalisatie normen, attentiepunten en illustraties.

Een individuele gemeente blijft altijd verantwoordelijk voor de manier waarop er wordt omgegaan met vertrouwelijke gegevens. Dat gaat veel verder dan het (op papier) op orde hebben van de zeven normen. Uiteraard is het van belang dat diverse plannen, procedures en controles rond Suwinet schriftelijk goed zijn vastgelegd.

Naast de 'papieren' werkelijkheid gaat het in de praktijk echter ook om het uitdragen van de juiste cultuur en het gewenste gedrag op de werkvloer. Gemeenten, individuele gebruikers en burgers lopen risico's als medewerkers die toegang hebben tot Suwinet zich onvoldoende beseffen dat het om gevoelige gegevens gaat. Met elkaar mogen we niet onderschatten welke consequenties het onzorgvuldig gebruik van deze gegevens kan hebben. Het management heeft als belangrijke rol om de betreffende medewerkers daar op te wijzen en om maatregelen te treffen die misbruik tegengaan. Dat kan door het stellen van heldere regels en door in te grijpen daar waar zaken verkeerd gaan.

Als Inspectie SZW willen we dan ook benadrukken dat het voldoen aan de zeven normen geen doel op zich is. Hoofddoel is het borgen van het veilig gebruik van persoonsgegevens die via Suwinet worden geraadpleegd.

In deze handreiking gaan we uit van de methodiek die we voor ons onderzoek hebben gebruikt. Als gemeenten de zeven normen behalen, vormt dit in de praktijk nog geen garantie voor het veilig gebruik van de persoonsgegevens. De score is slechts een momentopname. In de praktijk gaat het daarnaast om een bewust en zorgvuldig gebruik, wat continu aandacht vergt.

Verder willen we als Inspectie SZW benadrukken dat er natuurlijk verschillende manieren en mogelijkheden zijn om deze beveiliging te (blijven) waarborgen. Daarbij speelt ook de omvang van een gemeente een belangrijke rol.

We wensen u als Inspectie SZW veel succes met het veilig gebruiken van Suwinet!

Vooraf

Deze handreiking is gebaseerd op het toetsingskader van de Inspectie SZW. Dit toetsingskader bestaat uit 7 essentiële normen van de 26 essentiële normen die de Suwipartijen in de Verantwoordingsrichtijn GeVS (Gezamenlijke elektronische Voorzieningen SUWI) hebben vastgesteld. Volgens de inspectie moet tenminste aan deze 7 normen worden voldaan om te mogen veronderstellen dat de beveiliging van Suwinet voldoende is. Deze normen zijn niet alle even concreet. Bij de beoordeling heeft de inspectie daarom een operationalisatie toegepast. Het gaat daarbij om het aanwezig zijn van concrete aanwijzingen waaruit kan blijken dat aan de desbetreffende norm wordt voldaan. De zelftest die de VNG aanbiedt aan de gemeenten sluit voor een belangrijk deel aan op deze operationalisatie. Bij norm 13.5 is dat echter niet het geval. Bij de bespreking van dat onderdeel wordt hierop nader ingegaan.

De in de handreiking vermelde do's en don'ts zijn voorbeelden uit de praktijk die de inspectie in haar recente onderzoek heeft aangetroffen en die de gemeenten een houvast kunnen geven bij de invulling van het veilig gebruik van Suwinet.

Legenda:

- ☑ = Attentie-/actie-/aandachtspunten die door gemeenten kunnen worden gebruikt om zichzelf te toetsen. Let op: als een gemeente aan deze punten voldoet betekent niet per definitie dat de norm is behaald.
-  = Illustratie Do's,
-  = Illustratie Don'ts

Norm:

1.3 Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet zijn goedgekeurd door het management van de Suwi-partij.

Operationalisatie:

Deze norm gaat uit van het bestaan van een algemeen gemeentelijk informatiebeveiligingsbeleid en een beveiligingsplan van het Suwinet dat op het informatiebeveiligingsbeleid gebaseerd is. De Inspectie SZW controleert of de gemeente beschikt over een document dat specifiek aandacht besteedt aan het veilig gebruik van Suwinet binnen de eigen gemeente. De Suwi-specifieke aandacht mag ook blijken uit een afzonderlijk onderdeel van het beleid/plan dat generiek is gericht op informatiebeveiliging gemeentebreed.

Het college van burgemeester en wethouders van de gemeente is volgens de Wet bescherming persoonsgegevens (Wbp) de verantwoordelijke voor de verwerking van persoonsgegevens en dus ook voor een veilig en rechtmatig gebruik van Suwinet. Die verantwoordelijkheid komt o.a. tot uitdrukking in een goedkeuring van het beleid/plan. De goedkeuring moet blijken uit ondertekening van het betreffende document en/of uit het verslag van een vergadering van het management waarin het document is besproken en akkoord bevonden. Kortom: er moet sprake zijn van een formele vastlegging van de goedkeuring door het management.

Onder management verstaan wij het college van B&W, de wethouder, managementteam of de manager (directeur/afdelingshoofd) van de gemeente.

Attentiepunten:

- ☑ Er moet een Suwinet beveiligingsbeleid/plan of een specifiek op Suwinet gerichte passage zijn.
- ☑ Het moet duidelijk zijn door wie en wanneer het beleid/plan formeel is vastgesteld.
- ☑ Het moet duidelijk blijken dat het beleid/plan gaat over de betreffende gemeente.
- ☑ Ook bij het gebruik van een (algemeen BIG) plan moet er een specifieke uitwerking voor Suwinet zijn.

Do:

- 👍 Een specifiek opgesteld beleid/plan voor Suwinet. Dit is bij voorkeur een onderdeel van een gemeentebreed informatiebeveiligingsplan gebaseerd op de Baseline Informatiebeveiliging Nederlandse gemeenten (BIG).
- 👍 Eén beleid/plan met alle procedures.
- 👍 Duidelijke vermelding van de gemeente in het beleid/plan.
- 👍 Bij samenwerkingsverbanden zijn alle gemeenten duidelijk genoemd in het beleid/plan.
- 👍 Schriftelijke bewijsvoering (bijvoorbeeld notulen) van de accordering en ondertekening door het management inclusief naam, datum en eventueel functie.
- 👍 Het toevoegen van een besluitenlijst waaruit een formele vastlegging door het management blijkt.
- 👍 Aparte goedkeuring van elke gemeente in een samenwerkingsverband voor het beleid, plan of passage.

Don't:

- 👎 Een informatie beveiligingsbeleid/plan gebaseerd op de BIG waarbij het beleid geldt voor alle bedrijfsapplicaties en waarin niet specifiek wordt ingegaan op Suwinet.
- 👎 Het beveiligingsplan beslaat enkel de zeven normen en gaat niet in op andere aspecten.
- 👎 Meerdere afzonderlijke documenten vormen samen het beleid/plan.
- 👎 Een krabbel op het voorblad van het beleid/plan zonder naam en datum.
- 👎 Bewijs van een ondertekend informatiebeveiligingsplan waarbij de bijlagen niet onderdeel van het plan (geen één document) zijn, waardoor de bijlagen niet officieel zijn vastgesteld.

Norm:

1.4 Het informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet worden uitgedragen in de organisatie.

Operationalisatie:

Het management moet het bewustzijn van de medewerkers op het gebied van informatiebeveiliging stimuleren. Dit vindt plaats door het beleid/plan actief uit te dragen in de organisatie.

Of het beleid/plan wordt uitgedragen in de organisatie wordt vastgesteld door te kijken of

- het beleid/plan voor alle medewerkers beschikbaar is (bijvoorbeeld aan iedereen gemaild, op intranet gepubliceerd of via een handboek verspreid) en (daarnaast) of er in het afgelopen jaar minimaal twee keer een actie is geweest om de medewerkers (opnieuw) te attenderen op het bestaan van het beleid/plan (bijvoorbeeld in afdelingsoverleggen, trainingen en/of presentaties).

Het is daarbij van belang dat de ondernomen activiteiten zijn vastgelegd. Het uitdragen van het beleid/plan moet niet alleen onder de direct bij de beveiliging betrokken medewerkers plaatsvinden, maar bij alle mensen in de organisatie die Suwinet gebruiken.

Attentiepunten:

- ☑ Het Suwinet beveiligingsbeleid/plan moet aantoonbaar centraal beschikbaar zijn voor alle gebruikers. Bijvoorbeeld beschikbaar op intranet of op de afdelings-/organisatieschijf.
- ☑ Er moeten minimaal 2 acties in één jaar geweest te zijn om veilig gebruik van Suwinet uit te dragen in de organisatie.
- ☑ Acties moeten betrekking hebben op de informatiebeveiliging van Suwinet.
- ☑ De ondernomen acties moeten zijn vastgelegd (denk bijvoorbeeld aan schermafdrukken van intranet of verzonden e-mails).
- ☑ Het uitdragen van het veilig gebruik van Suwinet vindt plaats in de gehele organisatie, niet alleen bij de medewerkers die betrokken zijn bij de beveiliging.

Do:

- Het plan is centraal beschikbaar op intranet of op de afdelings- of organisatieschijf (bewijs: schermafdruk van de locatie).
- E-mail aan alle gebruikers met daarin een vermelding van/link naar het Suwinet beveiligingsbeleid/plan.
- Notulen van het overleg (incl. notitie van aanwezigen en afwezigen) waarin aandacht is geschonken aan informatiebeveiliging Suwinet. Hierbij is het van belang dat alle Suwinet gebruikers aanwezig waren of op de hoogte zijn gesteld van deze vergadering, bijvoorbeeld door het verspreiden van deze notulen.
- Formats van PO's en/of beoordelingsgesprekken waaruit blijkt dat het beleid/plan een standaard agendapunt vormt.
- Campagnes rond informatiebeveiliging Suwinet (bijvoorbeeld: eLearnings, animatiefilmpjes, nieuwsbrieven).

Don't:

- Er zijn alleen acties met betrekking tot informatiebeveiliging in het algemeen, niet specifiek Suwinet.
- Alleen het beleid/plan uitreiken aan *nieuwe* medewerkers.
- Alleen (ondertekende) geheimhouding- of zorgvuldigheidsverklaring als bewijs voor het uitdragen van veilig gebruik.
- Niet bewijsbare verwijzing naar het uitdelen van de BKWI kalender.
- Alleen de resultaten van de VNG-zelftest gebruiken om aan te tonen dat men met Suwinet bezig is.
- Aanwezig zijn bij Bijeenkomsten Veilig gebruik Suwinet VNG/ISZW meetellen als actie om veilig gebruik uit te dragen (aangezien dit vaak alleen wordt bezocht door de SO en niet alle gebruikers van Suwinet).

Norm:

1.5 Het informatie beveiligingsbeleid en het beveiligingsplan van het Suwinet worden jaarlijks geëvalueerd en indien nodig geactualiseerd.

Operationalisatie:

Organisaties en werkwijzen veranderen continu. Dit kan van invloed zijn op de wijze waarop Suwinet wordt gebruikt. Daarom is het van belang om minimaal jaarlijks het algemene informatiebeveiligingsbeleid en het beveiligingsplan van het Suwinet te evalueren en na te gaan of het informatiebeveiligingsbeleid en het beveiligingsplan nog steeds voldoen aan de beveiligingseisen en –randvoorwaarden. Ook is de vraag relevant of risico's voldoende gereduceerd worden. Wanneer dat nodig is leidt de evaluatie tot aanpassing (actualisatie) van het informatiebeveiligingsbeleid en het beveiligingsplan.

Zoals aangegeven onder norm 1.3 let de Inspectie SZW met name op het beveiligingsplan van het Suwinet. De evaluatie hiervan moet een concrete actie zijn geweest van alle direct betrokkenen en is vastgesteld door het management. Er zijn bewijsstukken dat deze evaluatie heeft plaatsgevonden en is geaccordeerd door het management (bijvoorbeeld plan van aanpak evaluatie, enquêteformulier, resultaat van de evaluatie en verslagen van vergaderingen waarin de evaluatie is besproken en goedgekeurd door het management).

Als het afgelopen jaar een (nieuw) informatiebeveiligingsplan is vastgesteld wordt dit ook beschouwd als een actualisatie.

Attentiepunten:

- ☑ De laatste evaluatie moet minder dan één jaar oud zijn.
- ☑ Het moet aantoonbaar zijn dat er een evaluatie heeft plaatsgevonden en deze is vastgesteld door het management.
- ☑ De evaluatie moet een concrete actie van alle direct betrokkenen zijn (bijvoorbeeld: security officer, managers, gebruikers en beheerders).

Do:

- Ondertekende versiehistorie op het document waaruit blijkt dat het document periodiek formeel geëvalueerd is.
- Verslag met daarin melding van de goedkeuring door het management.
- Een beschreven procedure voor het evalueren van het beleid/plan.
- Mailwisseling als bewijs dat de evaluatie een gezamenlijke actie is geweest.

Don't:

- Niet documenteren wanneer een evaluatie niet tot aanpassing van het beleid/plan leidt.
- Een verslag waarin wordt gemeld dat het beleid/plan een update krijgt, maar onduidelijk laten wat er vervolgens is aangepast.
- Een audit met aanbevelingen van een extern bedrijf gebruiken als bewijs voor evaluatie, waarna geen herleidbare opvolging wordt gegeven aan deze aanbevelingen.
- Evaluatie is geen brede actie geweest, maar een solo-actie uitgevoerd door de beveiligingsfunctionarissen.
- De zelftest van VNG gebruiken als reden om geen formele evaluatie te laten plaatsvinden.

Norm:

2.2 De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinet gegevens, applicaties, processen en infrastructuur moeten zijn beschreven en duidelijk en gescheiden zijn belegd.

- *Operationeel beheer*
- *Functioneel beheer*
- *Technisch beheer*
- *Aansturing ICT-leveranciers*
- *Security Officer*
- *Autorisatiebeheer*
- *Eigenaarschap Suwinet*

Operationalisatie:

Een adequaat ingerichte organisatie is een belangrijke voorwaarde voor het realiseren van een voldoende beveiligingsniveau voor Suwinet. Norm 2.2 ziet in dit verband toe op de functiescheiding. Zo zullen in principe de functies *gebruik van Suwinet*, *beheer van autorisaties Suwinet*, *controle op het gebruik van Suwinet* en *beslissen over wie welke functies krijgt in Suwinet* gescheiden moeten zijn. Door middel van functiescheiding worden risico's beperkt. Wanneer functiescheiding niet of onvoldoende is geïmplementeerd verhoogt dit de kans op oneigenlijk gebruik en/of misbruik zonder dat dit wordt ontdekt.

Bij deze norm wordt gekeken of de diverse functies schriftelijk zijn vastgelegd, of er een heldere overweging ten grondslag ligt aan de toedeling van taken en of er functiescheiding is toegepast. Het is daarbij van belang dat er een splitsing is tussen beschikkende, controlerende en uitvoerende taken. U kunt de functiescheiding aantonen door de functies duidelijk te omschrijven en vast te leggen.

Er wordt door de Inspectie SZW gekeken naar vier gescheiden functies (in plaats van de zeven zoals deze formeel in de norm worden genoemd). Beoordeeld wordt of minimaal de volgende functies bij verschillende personen zijn belegd:

- uitvoering van taken (het gebruik van Suwinet zoals door de klantmanager);
- beheer van autorisaties (toegang verlenen tot Suwinet, de applicatiebeheerder van Suwinet);
- kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet, bijvoorbeeld de Security Officer);
- management (beslissen over bevoegdheden van functiegroepen en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet)

Sommige kleinere gemeenten hebben door de beperkte omvang van het ambtelijk apparaat diverse functies binnen één persoon gecombineerd. In dergelijke gevallen wordt het (gedeeltelijk) ontbreken van functiescheiding geaccepteerd als de gemeente aangeeft zich bewust te zijn van de risico's en aantoonbaar aanvullende maatregelen heeft getroffen (bijvoorbeeld door extra controles waar functiescheiding niet of minder goed mogelijk is). Ook hier is het belangrijk dat u dit schriftelijk vastlegt.

Attentiepunten:

- ☑ De specifiek op Suwinet gerichte functies moeten schriftelijk zijn vastgelegd en duidelijk omschreven zijn.
- ☑ Er is functiescheiding tussen de beschikkende, beherende, uitvoerende en controlerende taken met betrekking tot Suwinet. Er zijn minimaal 4 gescheiden functies:
    1. Uitvoering van taken
    2. Beheer van autorisaties
    3. Controle op rechtmatigheid
    4. Management
- ☑ Wanneer er geen functiescheiding is tussen de vier hierboven genoemde functies dan moet worden toegelicht waarom dit het geval is en hoe de gemeente de bijbehorende taken waarborgt (extra maatregelen).

Do:

- Schriftelijke vastlegging van de verantwoordelijkheden per functie.
- Schriftelijke onderbouwing wanneer functiescheiding niet volmaakt is.
- Extra controles plaats laten vinden wanneer functiescheiding niet of minder volmaakt is.

Don't:

- Functies zijn in het algemeen beschreven en niet specifiek op Suwinet gericht.
- Verschillende namen gebruiken voor dezelfde functie.
- Functies verspreid vastleggen in verschillende procedures en documenten.
- De medewerker die bevoegdheden toewijst, voert ook de controle uit.
- Functies en taken van het management ontbreken.

Norm:

2.3

- De Security Officer beheert en beheerst beveiligingsprocedures en –maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.

- De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt rapportages over de status en controleert dat de beveiliging van de Suwinet maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.

- De Security Officer rapporteert rechtstreeks aan het hoogste management.

Operationalisatie:

Naast de functiescheiding (zie norm 2.2) is ook van belang de aanstelling van een persoon die verantwoordelijk is voor het gemeentelijk informatiebeveiligingsbeleid en de naleving daarvan. Deze medewerker bevordert, controleert en adviseert over de beveiliging van Suwinet.

In het normenkader wordt voor deze functie de naam 'security officer' gebruikt. De functie kan ook een andere naam hebben. Waar het om gaat is dat er een functionaris is die bovengenoemde taken in zijn pakket heeft en onafhankelijk van andere functionarissen kan werken. Deze persoon is deskundig op het terrein van informatiebeveiliging, controleert planmatig en periodiek (minimaal twee keer per jaar) of wordt voldaan aan de regels en analyseert eventuele incidenten. Daarnaast rapporteert hij rechtstreeks aan het management of het bestuur van de organisatie. Onder *rechtstreeks* verstaat de inspectie tevens de situatie waarin deze functionaris als CISO ressorteert onder een CIO en deze laatste rapporteert aan het management of het bestuur van de organisatie.

Deze functie/taken moeten zijn belegd in de organisatie. Een schriftelijke vastlegging van de taken in een functieomschrijving is daarvoor een belangrijk bewijsmiddel. Ook wordt er gekeken naar het daadwerkelijk planmatig en periodiek uitvoeren van de functie/taken: is er minimaal twee keer per jaar naar de beveiliging van Suwinet gekeken en is er rechtstreeks gerapporteerd aan het hoogste management (minimaal 1 rapportage per jaar). Verder wordt door de Inspectie SZW onderzocht of de functionaris ook andere activiteiten op het gebied van de beveiliging van Suwinet heeft verricht (bijvoorbeeld incidenten waarop de security officer heeft gereageerd). Belangrijk is dat er een schriftelijke neerslag is van de uitgevoerde controles en van rapportages aan het hoogste management.

Attentiepunten:

- ☑ De taken van de Security Officer (SO) moeten schriftelijk zijn vastgelegd in een functieomschrijving.
- ☑ De taken moeten betrekking hebben op de informatiebeveiliging van Suwinet:
  - De SO controleert minimaal 2x per jaar de beveiliging van Suwinet.
  - De SO is vereist periodiek (aan) het hoogste management te adviseren en te rapporteren.
- ☑ Bewijs van uitvoering van bovenstaande taken moet duidelijk zijn vastgelegd.

Do:

- Een specifiek op Suwinet gerichte taakomschrijving (eventueel als onderdeel van een algemene omschrijving van taken) inclusief periodiciteit van de controles en rapportages aan het hoogste management.
- De SO rapporteert minimaal 1x per jaar aan het hoogste management.
- Het is aantoonbaar dat het verslag ontvangen is door het management. Bijvoorbeeld: er is een verantwoordingsverslag aan het hoogste management dat het verslag ter kennisneming heeft ondertekend.
- GSD rapportages worden met geplande de periodiciteit (zoals vermeld in de werkwijze) opgevraagd.

Don't:

- Functieomschrijving van SO met algemene beveiligingstaken, waar niet uit blijkt of dit ook op Suwinet van toepassing is.
- Enkel rapporteren aan een teamleider (wanneer deze niet het hoogste management is).
- Alleen rapporteren aan het hoogste management wanneer er opvallendheden zijn geconstateerd.
- De SO rapporteert mondeling aan het hoogste management, waarvan bewijs ontbreekt.
- Alleen een opgesteld rapport van controle overhandigen aan de Inspectie zonder bewijs dat deze met het management is gedeeld.
- Rapporten van externe audits waarbij de algemene informatieveiligheid van de gemeente is gecontroleerd en die niet specifiek op Suwinet zijn gericht, gebruiken als bewijs.

Norm:

13.1 De Suwi-partij autoriseert en registreert de gebruikers die toegang hebben tot de Suwinet applicaties op basis van een formele procedure waarin is opgenomen.

- *Het verlenen van toegang tot de benodigde gegevens op basis van de uit te voeren functie/taken*
- *Het uniek identificeren van elke gebruiker tot één persoon*
- *Het goedkeuren van de aanvraag voor toegangsrechten door de manager of een gemandateerde*
- *Het tijdig aanpassen of wijzigen van de autorisatie bij functiewijziging of vertrek*
- *Het benaderen van de Suwi-databestanden door gebruikers mag alleen plaatsvinden via applicatieprogrammatuur (tenzij sprake is van calamiteiten)*

Operationalisatie:

Deze norm en norm 13.5 hebben betrekking op de bescherming van de informatiehuishouding en de te verwerken gegevens tegen ongeautoriseerde toegang en gebruik.

De gemeente is verantwoordelijk voor het beheer van de toegang tot Suwinet. Autorisatie van medewerkers moet plaatsvinden met behulp van een schriftelijk vastgelegde procedure waarin functies aan autorisaties - en in het verlengde daarvan aan Suwinet-rollen - worden gekoppeld. Concreet gaat het om het aanwezig zijn van een autorisatieprocedure en een autorisatiematrix die onderdeel uitmaakt van de procedure. Uit de autorisatiematrix blijkt dat de gemeente heeft nagedacht over welke functionarissen welke informatie via Suwinet mogen raadplegen, met andere woorden een opzet van de wijze waarop de gemeente de accounts en rollen toekent. . Door een uitdraai uit Suwinet hiermee te vergelijken kan de gemeente controleren of de daadwerkelijk uitgereikte accounts en rollen overeenkomen met de in opzet bedachte accounts en rollen.

De autorisatieprocedure moet ervoor zorgen dat alle gebruikers uniek identificeerbaar zijn. Groepsautorisaties mogen dus niet worden afgegeven. Hierdoor kunnen gebruikers persoonlijk worden aangesproken op hun gebruik van Suwinet. Door aan te geven welke persoon welke functie(s) uitoefent, kan op een gestandaardiseerde en controleerbare wijze de autorisatie voor een persoon binnen Suwinet worden verleend en gecontroleerd. Het toekennen van rollen in Suwinet moet volgens een logische procedure plaats te vinden. Uit de autorisatieprocedure moet duidelijk worden op basis van welke afwegingen, welke medewerker welke gegevens mag zien.

De Inspectie SZW controleert of de gemeente een autorisatieprocedure en -matrix heeft. Zijn alle stappen in het autorisatieproces aanwezig, helder beschreven en toegewezen aan bevoegde functionarissen binnen de gemeente? En kan de gebruiker met behulp van de autorisatiematrix en gebruikersadministratie tot een persoon worden herleid? Daarnaast wordt bekeken of de autorisatiematrix specifiek ingaat op Suwinet en of deze gebaseerd is op onderkende/aanwezige functieprofielen en aanwezige rollen in Suwinet.

Van belang is dat het accountbestand meerdere keren (minimaal twee keer) per jaar wordt gecontroleerd en dat aansluitend inactieve accounts worden verwijderd. Om dit te kunnen aantonen is een schriftelijke vastlegging van zowel de procedure als de uitvoering van de controles belangrijk.
Of er sprake is van een goed werkend accountbeheer wordt in beginsel over een periode van een jaar bekeken. Dit gebeurt op basis van maandelijkse gegevens van het BKWI naar het percentage inactieve accounts en naar het percentage geblokkeerde accounts bij een gemeente. Het BKWI verstaat onder een inactieve account een account waarmee niet tenminste 1x is ingelogd in een maand en onder een geblokkeerde account een account dat meer dan 90 dagen niet is gebruikt of waarmee 5x foutief is ingelogd.

Een combinatie van een hoog percentage geblokkeerde accounts samen met een hoog percentage niet actieve accounts is een indicatie van een niet goed werkend accountbeheer en vormt een reden tot nadere vragen aan de gemeente. Als richtsnoer wordt gehanteerd dat bij meer dan 80% actieve accounts er goed gebruik wordt gemaakt van Suwinet. Bij 60% tot 80% wordt het twijfelachtig en bij minder dan 60% lijkt er echt iets aan de hand te zijn. Dit zijn geen harde grenzen maar zoals aangegeven een richtsnoer en kan er toe leiden dat er nadere vragen worden gesteld aan de gemeente.

Ook is het belangrijk dat zware rollen beperkt zijn uitgedeeld. Dit zijn de rollen waarvan het BKWI aangeeft dat het "risicovolle autorisaties" betreft. Beperkt betekent dat aan een klein percentage medewerkers van de gemeente deze rollen zijn toebedeeld. Het te ruim verstrekken van zware autorisaties vergroot het risico op onrechtmatige raadplegingen van de bestanden, omdat het voor een medewerker eenvoudiger is om - zonder te beschikken over een BSN - gegevens van personen te raadplegen. Hierbij wordt gekeken naar de verhouding aantal accounts/accounts met zware rollen en de verhouding medewerkers sociale dienst/sociale recherche. Concreet wordt naar de volgende zware rollen gekeken: G018 (LRD/GBA zoeken), G030 (LRD/GBA zoeken uitgebreid) en G021/R1920 (RDW+ Fraude). Van belang is dat per functie (en per toegekende zware rol) moet worden gemotiveerd waarom er één of meerdere zware rollen zijn toegekend en dan met name waarom het noodzakelijk (proportioneel en subsidiair) is voor de uitoefening van de werkzaamheden. Voorts zijn aanvullende controles noodzakelijk. Ook moet hier sprake te zijn van functiescheiding: wanneer een gemeente 100 consulenten heeft dan wordt niet verwacht dat alle 100 dan ook over zware rollen kunnen beschikken omdat dit binnen hun functie zou passen.

Medewerkers die belast zijn met de uitvoering van de wettelijke taken die vallen onder de Participatiewet, IOAW en IOAZ hebben na autorisatie toegang tot Suwinet. Daarnaast heeft slechts een zeer beperkte groep toegang tot Suwinet: de gemeentelijke belastingdeurwaarders, burgerzaken of de regionale meld- en coördinatiefunctie voortijdig schoolverlaten. Voor deze groep moet een apart contract worden afgesloten met het BKWI. Gebruik van Suwinet door overige functionarissen zoals WMO-medewerkers, medewerkers parkeerbeheer of andere hiervoor niet genoemde medewerkers is niet toegestaan.

Attentiepunten:

- ☑ Er moet een formeel vastgelegde en specifiek op Suwinet gerichte autorisatieprocedure zijn.
- ☑ De gemeente moet kunnen aantonen dat deze procedure in de praktijk wordt gevolgd.
- ☑ Door middel van een autorisatiematrix moet het duidelijk zijn welke organisatorische rollen worden gekoppeld aan Suwinet gebruikersrollen.
- ☑ Er moet een specifiek op Suwinet gerichte periodieke controle zijn op inactieve en geblokkeerde accounts. Daarnaast moet de gemeente kunnen aantonen dat deze controle plaatsvindt.
- ☑ Zware rollen moeten beperkt worden uitgedeeld en er moet een verklaring zijn waarom een persoon of functie zo'n risicovolle autorisatie krijgt toegediend.
- ☑ Alleen aan die personen waarvoor het strikt noodzakelijk is voor het uitoefenen van hun functie mag een zware rol worden toegekend.
- ☑ Wanneer er veel zware rollen zijn, moet hiervoor een toereikende verklaring worden gegeven en zijn aanvullende controles vereist.
- ☑ Voor gemeentelijke belastingdeurwaarders, burgerzaken en de regionale meld- en coördinatiefunctie moet een apart contract worden afgesloten.

Do:

- 👍 Er is een duidelijke autorisatieprocedure die stapsgewijs laat zien op welke wijze en door wie autorisaties worden toegewezen. Bijvoorbeeld: waarbij de applicatiebeheerder autorisaties toewijst na akkoord van SO en teamleider.
- 👍 Er is bewijsmateriaal waaruit de praktische uitvoering van de formele autorisatieprocedure blijkt. Bijvoorbeeld: ingevulde autorisatie formulieren van de laatste drie autorisaties.
- 👍 Door middel van de autorisatiematrix en gebruikersadministratie kan de gemeente de gebruiker tot een persoon herleiden.

Don't:

- 👎 Documentatie waarbij de medewerkers niet herleidbaar zijn of waarin de rollen onduidelijk zijn beschreven.
- 👎 Meerdere medewerkers die autorisaties kunnen toekennen wat niet in overeenstemming is met hun functie.
- 👎 Als bewijs voor de autorisatiematrix een uitdraai uit Suwinet leveren van de huidige accounts met rollen.
- 👎 De rollen in de autorisatiematrix komen niet overeen met die benoemd zijn in de sectie over functiescheiding.
- 👎 Geen procedure met betrekking tot inactieve accounts. De gemeente laat accounts verlopen in plaats van het op te zeggen.

- Accounts verwijderen bij uitdiensttreding van medewerkers.
- Controle op inactieve accounts vindt minimaal 2x per jaar plaats.
- Gemiddeld zijn er meer dan 80% actieve accounts.
- Beschikbaar bewijs van de uitgevoerde controles. Bijvoorbeeld: mails of gebruikersadministratie met notities.
- Een goede beargumenteerde reden om aan medewerkers zware rollen toe te wijzen.

- Geen beschikbaar bewijs van de controle op inactieve accounts.
- Zware rollen zijn gemakshalve uitgereikt aan veel medewerkers die deze zware rollen niet nodig hebben voor hun werkzaamheden.
- Zware rollen zijn uitgeven aan veel medewerkers met als reden dat fraudepreventie een rol is van alle medewerkers.
- Medewerkers hebben toegang tot Suwinet voor het uitvoeren van gemeentelijke taken waar Suwinet niet voor is bedoeld / wettelijke titel ontbreekt (bijvoorbeeld: integratie en schuldhulpverlening).

Norm:

13.5 De controle op verleende toegangsrechten en gebruik vindt meerdere keren per jaar plaats.

- *Interne controle op rechten en gebruik van Suwinet*
- *Analyseren van de van het BKWI verkregen informatie over het gebruik van Suwigegevens*

Operationalisatie:

Deze norm gaat over het belang om periodiek te controleren of de verleende toegangsrechten (wie mag wat en waarom?) en het gebruik van Suwinet (wat heeft de gebruiker geraadpleegd en was dat noodzakelijk?) in overeenstemming zijn met de vooraf bepaalde uitgangspunten. Zeker voor de zogenaamde zware rollen is de periodieke controle op uitgave van rechten en gebruik van die rollen belangrijk. Bij geconstateerde afwijkingen waarbij sprake is van onregelmatigheden zal de gemeente corrigerende maatregelen moeten nemen. Afhankelijk van de soort onregelmatigheden zal de maatregel variëren van beperking van toegangsrechten tot disciplinaire maatregelen bij geconstateerd misbruik van persoonsgegevens.

Interne controle en analyse kan op verschillende wijzen worden vormgegeven. In de lichtste variant bestaat deze uit het op hoofdlijnen analyseren van het gebruik op gemeenteniveau en in een zware variant worden de opvragingen per gebruiker structureel op rechtmatigheid beoordeeld. De norm kan dan ook op verschillende wijzen worden uitgelegd en toegepast. Daarom moet de norm worden vertaald naar een praktische toepassing. De Inspectie SZW heeft er voor gekozen om het gebruik van Suwinet door een gemeente evenals de door de gemeente ingezette controlemethoden te vergelijken en te beoordelen. Gemeenten moeten daarbij het gebruik van Suwinet tot op accountniveau (steekproefsgewijs) controleren. Het alleen controleren door middel van de generieke rapportages kan voldoende zijn maar geeft geen zicht op individuele opvragingen. Voor het onderzoek wordt gebruik gemaakt van een aantal zoeksleutels anders dan op BSN. Wanneer binnen een gemeente opvallend vaak gebruik wordt gemaakt van dit soort zoeksleutels en de gemeente de controle uitsluitend heeft gebaseerd op basis van een generieke rapportage van het BKW, dan wordt dit als onvoldoende beoordeeld. Een gemeente moet beter zicht hebben op het gebruik van Suwinet door individuele medewerkers om oneigenlijk gebruik vroegtijdig te signaleren en te voorkomen.
Het BKWI biedt maandelijks een generieke rapportage aan, waarin geaggregeerde en geanonimiseerde gegevens staan. Voor gemeenten is dit – een mogelijk niet afdoende – handvat bij de controle. Ook het opvragen van specifieke rapportages bij het BKWI is van belang. Een specifieke rapportage kan - in tegenstelling tot een generieke - gegevens bevatten over individuele medewerkers en/of cliënten.

Van een gemeente wordt verwacht dat deze minimaal twee keer per jaar een generieke rapportage opvraagt bij het BKWI, dat er een procedure is aan de hand waarvan de generieke rapportages worden beoordeeld en dat er rapportages aanwezig zijn waaruit blijkt dat de gemeente deze controles heeft uitgevoerd.

Verder wordt op basis van gegevens van het BKWI en een statistische bewerking daarvan bekeken of er sprake is van bovengemiddeld veel opvragingen buiten het BSN (opvallend zoekgedrag). Dat wil overigens niet zeggen dat er iets aan de hand is, maar dat in die gevallen wel nader onderzoek moet worden verricht. Aan de gemeente wordt aanvullend gevraagd of men dit zelf ook heeft geconstateerd en of hiervoor een verklaring is.

Ten slotte wordt van gemeenten verwacht dat zij naast generieke rapportages ook specifieke rapportages bij hun controle inzetten. Overigens is het minimaal 2 keer per jaar opvragen van een generieke rapportage geen harde eis voor de beoordeling van de Inspectie SZW. Het komt bijvoorbeeld ook voor dat een gemeente alleen specifieke rapportages opvraagt en daarmee gerichte controles uitvoert. Deze gemeente heeft in dat geval een eigen vorm gevonden om de controle in te richten.

De inspectie wil in dit verband niet onvermeld laten dat haar operationalisatie van deze norm afwijkt van de invulling die de VNG geeft in haar zelftest. Die invulling komt er op neer dat controle op het gebruik in beginsel ook kan plaatsvinden door uitsluitend een generieke rapportage te gebruiken. Met behulp van deze rapportage kunnen gemeenten in absolute zin zien hoeveel zij afwijken van het gemiddelde. Vanuit de VNG is gemeenten steeds geadviseerd om vanuit kennis van de eigen werkprocessen de afwijkingen van het gemiddelde te interpreteren en zo te beoordelen of dit aanleiding geeft tot nader onderzoek. De inspectie is zoals gezegd van mening dat het voor een sluitende controle, zoals bedoeld in deze norm, van belang is dat ook (steekproefsgewijs) tot op accountniveau gecontroleerd wordt. Ook als er geen generieke indicaties zijn dat er iets mis is. Generieke rapportages zijn een hulpmiddel maar niet als sluitend controlemiddel te gebruiken. In essentie is volgens de inspectie dus altijd een (steekproefsgewijze) controle op het gebruik op accountniveau nodig. Het gaat er om dat gemeenten verder kijken dan alleen generiek.

Attentiepunten:

- ☑ Minimaal 2x per jaar moet een generieke rapportage worden opgevraagd bij het BKWI en worden beoordeeld.
- ☑ Er moet een procedure zijn aan de hand waarvan een medewerker (bijvoorbeeld de SO) deze rapportages controleert.
- ☑ Van de controle moet schriftelijk verslag worden gemaakt.
- ☑ Wanneer nader onderzoek gewenst is (bijvoorbeeld bij opvallendheden of afwijkingen) moet een specifieke rapportage worden opgevraagd.
- ☑ Bijzonderheden zijn opgemerkt door de gemeente en moeten worden vermeld in verslagen.
- ☑ Naast de generieke rapportages voert de gemeente extra controles uit op het gebruik van Suwinet.

Do:

- 👍 Meer dan 1x per jaar is een generieke rapportage bij het BKWI opgevraagd.
- 👍 Een procedure waarin is beschreven door wie en langs welke criteria de generieke rapportages worden beoordeeld.
- 👍 De specifieke criteria waarnaar moet worden gekeken is vastgesteld door het management en mogelijke afwijkingen zijn uitvoerig beschreven.
- 👍 Van de controles is verslaglegging beschikbaar.
- 👍 Volgens de vastgestelde criteria wordt een specifieke rapportage opgevraagd.
- 👍 Extra controle (voorbeeld): uitdraai maken van de opgevraagde BSN nummers en deze matchen met het klantbestand.

Don't:

- 👎 Enkel het voorblad van een generieke BKWI-rapportage aanbieden als bewijs voor controle.
- 👎 Alleen wanneer er bijzonderheden zijn een verslag maken.
- 👎 Geen specifieke rapportages opvragen bij bijzonderheden (bijvoorbeeld bij veel raadplegingen op zoeksleutel anders dan BSN).
- 👎 Opvragingen van bepaalde groepen, zoals Sociaal Rechercheurs, niet onderzoeken omdat deze "altijd gerechtvaardigd" zouden zijn.
- 👎 Onvoldoende verklaring geven bij opvallende zoekresultaten (anders dan BSN).
  Nader onderzoek naar opvallendheden of afwijkingen niet documenteren.

- Extra controle (voorbeeld): steekproefsgewijs controleren of wethouders en het hoger management zijn geraadpleegd.
- Extra controle (voorbeeld): aantal keer per jaar in een steekproef de zoeksleutels van willekeurige medewerkers controleren.
- Van de extra controles is ook verslaglegging beschikbaar.