Vereniging van
Nederlandse Gemeenten

Stappenplan voor een veiliger gebruik van Suwinet

VEILIG SUWINET: ACHTERGROND

Stappenplan: de basis voor veilig gebruik Suwinet

Dit Stappenplan biedt gemeenten een handvat om een start te maken met een veiliger gebruik van Suwinet. Aan de hand van checklists kunt u een doorlichting uitvoeren van de wijze waarop de veiligheid van Suwinet in de gemeente nu is georganiseerd. Door de resultaten te vergelijken met referentiematerialen kunt u de verbeterpunten signaleren en een verbeterplan opstellen. Als deze basis is gelegd komt het erop aan om de nieuwe afspraken over werkwijze en organisatie te implementeren en te handhaven. En om ze bij alle betrokken medewerkers tot routine te maken: per slot is verantwoord en bewust gedrag van mensen essentieel voor een goede informatieveiligheid.

Het Stappenplan richt zich op het leggen van een basis, door overzicht te creëren en de cruciale processen Autoriseren en Controleren onder de loep te nemen. Daarna moet de doorontwikkeling Veilig Suwinet een plek krijgen in het gemeentebrede informatieveiligheidsbeleid dat in 2014 wordt vormgegeven op basis van de Baseline Informatiebeveiliging Gemeenten (BIG). Doel is dat eind 2014 gemeenten in ieder geval aan de minimale eisen van Veilig Suwinet voldoen.

Het Stappenplan is een onderdeel van het Verbetertraject dat de VNG eind 2013 is gestart en gedurende 2014 uitvoert. De VNG heeft een *Zelftest* opgesteld, als hulpmiddel om te bepalen hoe het in uw gemeente is gesteld met het basale niveau van de veiligheid van Suwinet. Wanneer uw gemeente blijkt aan minder dan de helft van de normen te voldoen, biedt dit stappenplan soelaas. Het geeft aan in welke volgorde en met welke samenhang u de verbeteracties op kunt pakken. Wanneer uw gemeente aan meer dan de helft van de zeven onderzochte normen blijkt te voldoen, kunt u ook gebruik maken van de normspecifieke tools die u aantreft op de website van het Bureau Keteninformatisering Werk en Inkomen (BKWI), de beheerder van Suwinet: www.bkwi.nl/veiligheid/veilig-gebruik-suwinet

Veilig Suwinet: organisatie en verantwoordelijkheden

Voor de organisatorische inbedding van het Verbetertraject op de korte en de langere termijn en voor informatieveiligheid in het algemeen, beschrijven we hier de relevante actoren en hun betrokkenheid.

- College van B&W: is bestuurlijk verantwoordelijk voor de informatieveiligheid, stelt het beleid vast en draagt het uit. Het College informeert de Raad, zodat die zijn controlerende taak kan waarmaken.
- De Chief Information Security Officer (CISO): is belast met de gemeentelijke informatieveiligheid en heeft onafhankelijke staffunctie (bv. bij het bureau bedrijfsvoering). Iedere gemeente gebruikt een andere functienaam, maar door de VNG wordt de benaming CISO aangehouden.[1]
- De proceseigenaar of lijnmanager (bv. afdelingshoofd): is verantwoordelijk voor de bedrijfsvoering van het betreffende gemeentelijke proces/onderdeel waar informatieveiligheid een integraal onderdeel van is.
- In sommige grotere gemeenten is een medewerker informatiebeveiliging werkzaam in een staffunctie van de afdeling Sociale Zaken. Deze kan direct onder het lijnmanagement van Sociale Zaken vallen en functioneel onder de CISO. Vaak is dit de security officer van de sociale dienst of de afdeling Sociale Zaken.
- Functioneel beheerder, zoals de beheerder van Suwinet: degene die de gebruikersadministratie van Suwinet beheert.

In het Stappenplan komen deze functionarissen/rollen terug. Veiligheid Suwinet is primair de verantwoordelijkheid van de proceseigenaar WWB/lijnmanager Sociale Zaken. Het Stappenplan is geschreven ter ondersteuning van deze lijnmanager bij het uitvoeren van het verbetertraject Veilig Suwinet. Hij kan zich daarbij op onderdelen laten adviseren en ondersteunen. De activiteiten gericht op het veiliger maken van het gebruik van Suwinet zal in praktische zin opgepakt worden door de bovengenoemde security officer van de sociale dienst of afdeling sociale zaken. De tools van het verbeterplan van de VNG zijn dan ook primair op deze functionaris gericht. De lijnmanager is en blijft verantwoordelijk, met name ook voor de koppeling naar het p&o-beleid.

Leeswijzer

Het Stappenplan bestaat uit drie onderdelen:

1. Allereerst wordt ingegaan op het belang van informatieveiligheid en de urgentie voor Veilig Suwinet. Ook bespreken we kort de gemeentelijke ontwikkelingen rond informatieveiligheid, hoe Veilig Suwinet daarin past en zo snel mogelijk ingepast moet worden.
2. Daarna volgt het deel met de stappen.
3. Het derde deel bevat checklists en modellen die gebruikt kunnen worden om de stappen uit te werken. Gedurende dit jaar brengt de IBD van de VNG handreikingen en modellen uit die ene generieke toepassing hebben en die dus ook voor Suwinet gebruikt moeten worden.

1 Zie de documentatie op de site van de Informatie Beveiligingsdienst (IBD): http://new.kinggemeenten.nl/informatiebeveiliging/downloads-informatiebeveiligingsdienst

1 VEILIG SUWINET: HET BELANG EN DE URGENTIE

Gemeenten moeten bewijs leveren

In november 2013 heeft de Inspectie SZW vastgesteld dat het zeer slecht gesteld is met de wijze waarop gemeenten zorgen voor de beveiliging van Suwinet en het omgaan met de gegevens die zij uit Suwinet halen.[2] De Inspectie heeft dit gemeten aan de hand van (slechts) 7 normen van de in totaal 115 normen die opgenomen zijn in het Normenkader Suwinet. Normen die sinds de start van Suwinet in 2002 gelden. Slechts 4% van de gemeenten voldeden aan de 7 getoetste normen.

VNG heeft met het ministerie van SZW afgesproken om in 2014 samen met het BKWI een verbetertraject uit te voeren. Het doel daarvan is dat eind 2014 alle gemeenten tenminste aan deze 7 normen voldoen. Begin 2015 herhaalt de Inspectie zijn meting bij een nieuwe steekproef van gemeenten en kijkt of de informatieveiligheid structureel is verbeterd. Voldoet een gemeente niet, dan volgen maatregelen. Het ministerie bereidt een Afsluitprotocol voor om gemeenten te kunnen afsluiten van Suwinet. Los daarvan gaat het College Bescherming Persoonsgegevens controles uitvoeren en kan gemeenten een dwangsom opleggen. Uw gemeente kan dus in de problemen komen als er in procedures en uitvoering geen structurele verbeteringen zijn vast te stellen. Die problemen zijn van politiek-bestuurlijke aard: het college is eindverantwoordelijke voor de gemeentelijke informatieveiligheid, als ook uitvoeringstechnisch: zonder Suwinet is de uitvoering terug bij af met al het extra administratieve handwerk van dien en de lasten voor burgers die daar nog bij komen.

Zorgvuldig omgaan met persoonsgegevens: grondrecht van de burger, pijler onder rechtstaat

De bescherming van zijn persoonsgegevens is een grondrecht van de burger, een pijler onder de rechtstaat. De overheid is de grootste dataverzamelaar. Burgers moeten er vanuit kunnen gaan dat hun privégegevens daar veilig zijn. Schendt de overheid dit vertrouwen, dat kan dat ernstige gevolgen hebben voor de relatie tussen overheid en burger. Dit geldt te meer voor gegevens die direct de persoonlijke levenssfeer raken. Zoals de gegevens die via het Suwinet worden geraadpleegd. Ook het vertrouwen van houders van de bronnen die met Suwinet worden ontsloten is in het geding. Zij hebben zich tegenover hun cliënten te verantwoorden over de gegevens die worden doorgeleverd aan gemeenten en de wijze waarop de afnemer er vervolgens mee omgaat. Dat vertrouwen hebben bronhouders op dit moment niet, omdat gemeenten niet kunnen aangeven hoe de veiligheid is geregeld.

Gemeenten krijgen nieuwe taken van het Rijk in het sociale domein. Daarvoor willen gemeenten meer gegevens van burgers kunnen raadplegen. Ook medische, die volgens de Wet Bescherming Persoonsgegevens onder de meest risicogevoelige categorie persoonsgegevens vallen. Op dit moment ontbreekt daarvoor de vertrouwensbasis. Dit zet een rem op de voortgang van de decentralisaties.

Informatieveiligheid: gemeentebreed geldt de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Gemeenten moeten hun informatieveiligheidsbeleid voor de hele gemeente beter regelen. Hiervoor is eind 2013 in VNG-verband een resolutie aangenomen.[3] Gemeenten hebben daarin afgesproken dat ze zichzelf toetsen aan de hand van een normenkader. Dit normenkader is de zogenaamde Baseline Informatiebeveiliging Gemeenten (BIG).[4] De BIG geldt gemeentebreed als basis. Daarnaast moeten extra maatregelen genomen worden voor een aantal risicogevoelige systemen, onder andere voor Suwinet. Voor Suwinet worden die zogenaamde "plus"-maatregelen worden vastgelegd in een bijlage bij de BIG. Alle risico's dan zijn afgedekt. Met de inhaalslag op de 7 onderzochte normen voor het gebruik van suwinet wordt inhoudelijk geen dubbel werk verricht ten opzichte

2 http://www.inspectieszw.nl/Images/NvB-Veilig-gebruik-Suwinet_tcm335-346931.pdf
http://www.gemeenteloket.minszw.nl/dossiers/werk-en-inkomen/wwb/nieuwsberichten/Opvragen-persoonsgegevens-door-gemeenten-niet-goed-bewaakt.html

3 De Resolutie Informatieveiligheid, 31 oktober 2013 http://www.vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/informatiebeveiliging/brieven/resolutie-informatieveiligheid-randvoorwaarde-voor-de-professionele-gemeente

4 Meer informatie over de BIG: https://new.kinggemeenten.nl/informatiebeveiliging/downloads-informatiebeveiligingsdienst

van de BIG: de normen komen er een op een in terug. De Suwi- en de BIG-normen zijn naast elkaar gezet in de bijlage van de zelftest. De gemeenten hebben afgesproken hun gemeentelijk informatiebeveiligingsplan per 1/2015 gereed te hebben. Daarin wordt aangegeven op welke punten zij hun veiligheid op orde hebben conform de normen uit de BIG, op welke punten dat niet het geval is en hoe zij de BIG-normen willen bereiken. Veilig Suwinet moet daarin worden meegenomen.

De opdracht om het gemeentelijk informatieveiligheidsbeleid tot stand te brengen (en uiteindelijk te toetsen op naleving) is belegd bij de zogenaamde Chief Information Security Officer (CISO) van de gemeente. Hij is verantwoordelijk voor de gemeentelijke informatiebeveiliging. De CISO is een staffunctionaris die direct onder B&W of de gemeentesecretaris opereert en zelfstandig kan rapporteren aan het college van B&W. Voor de uitvoering van dit Stappenplan moet de lijnmanager/systeemeigenaar Suwinet nauwe samenwerking zoeken met de CISO, omdat Veilig Suwinet uiteindelijk integraal onderdeel uitmaakt van de BIG.

Suwinet: alleen voor de uitvoering van de bijstand en dan ook nog proportioneel

In dit Stappenplan gaat het om het veilig gebruik van Suwinet voor de uitvoering van de WWB, IOAW, IOAZ.

Suwinet: alleen WWB en voorzieningen

Suwinet mag door gemeenten *alleen* worden gebruikt voor de uitvoering van de in de Suwiwet genoemde wetten (art. 62.2). Dat is voor de gemeente op dit moment:

- WWB (inclusief BBZ), IOAW, IOAZ.

Gebruik voor andere doeleinden is dus absoluut niet toegestaan. Dat geldt ook voor het doorleveren van gegevens. Denk aan de Wmo, jeugdzorg, welzijn, achterdevoordeur-projecten, schuldhulpverlening, Veiligheidshuizen, Parkeerbeheer ed. Ook al gaat het om cliënten WWB en ook al "is het handig".

Suwinet: onder extra voorwaarden

Daarnaast *kunnen* onder speciale voorwaarden toegang krijgen: de gemeentelijke belastingdeurwaarders, specifieke GBA-medewerkers en de RMC-functionarissen[5]. Dit zijn niet-Suwipartijen waarvoor aparte procedures gelden. Later wordt toegang mogelijk voor de gemeentelijke onderdelen die de Wet gemeentelijke schuldhulpverlening uitvoeren. Het gebruik van Suwinet door deze gemeentelijke onderdelen is niet de verantwoordelijkheid van de proceseigenaar/lijnmanager sociale zaken, maar van de proceseigenaar /lijnmanager die voor deze onderdelen is aangewezen. Sociale zaken moet er als suwipartij wel van op aan kunnen dat ook voor deze gemeentelijke taken een zorgvuldig gebruik goed is geregeld en of die afspraken ook in de praktijk worden nagekomen. Het is dus zaak dat hierover informatie wordt uitgewisseld tussen beide functionarissen. Het gebruik door deze gemeentelijke niet-Suwi-taken valt buiten dit Stappenplan. Het Stappenplan kan wel gebruikt worden om te toetsen of aan de meest noodzakelijke voorwaarden wordt voldaan, maar zoals gezegd gelden hier aanvullende eisen.[6]

Proportioneel

Toegang tot de specifieke persoonsgegevens in Suwinet is afhankelijk van de rol van een medewerker. De ene medewerker heeft voor zijn taken meer gegevens nodig dan de andere. Belangrijk is dat de gemeente permanent in beeld heeft of een medewerker nog wel de juiste toegang (autorisatierollen) heeft. En dat de gemeente controleert of een medewerker gegevens van zijn eigen cliënt raadpleegt of van burgers die niet in zijn caseload zitten. Het raadplegen van BN-ers, plaatselijke politici, een ex of een nieuwe partner van een ex, familie, de buren of een hele buurt zijn excessen die helaas voorkomen. We komen later terug op autoriseren en controleren.

5 Regionale Meld- en Coördinatiefuncties Voortijdig Schoolverlaters.
6 Raadpleeg hiervoor het BKWI.

Intergemeentelijke sociale diensten en andere intergemeentelijke gemeentelijke samenwerkingsverbanden: iedere gemeente zelf verantwoordelijk

Gemeenten die op onderdelen van de WWB of geheel samenwerken met andere gemeenten zijn allemaal zelf verantwoordelijk voor de informatieveiligheid. Dat wil zeggen dat iedere gemeente (te zijner tijd) de bijlage Suwinet bij de BIG moet laten vaststellen door het College van B&W, ook al zijn dat inhoudelijk identieke bijlagen. Datzelfde geldt voor alle verantwoordingen, controles, evaluaties etc. Een Verbeterplan Veilig Suwinet hoort dus zaak te zijn van alle aangesloten gemeenten en op de agenda van alle betrokken wethouders Informatieveiligheid (en Sociale Zaken) te staan. En natuurlijk op de agenda van het AB en DB van een gemeenschappelijke regeling.

Gebruik Suwinet door niet-gemeenteambtenaren en externe bureaus voor de uitvoering van de WWB: gemeenten zijn verantwoordelijk

Gemeenten die incassobureaus, ZZP-ers, gedetacheerden, flexwerkers etc. inschakelen zijn integraal verantwoordelijk voor het gebruik van Suwinet door deze ingehuurde krachten. Voor het beleid, controles, autorisaties, maatregelen etc. worden deze inhuurkrachten als onderdeel van de gemeente beschouwd. Het ligt voor de hand deze externen extra te wijzen op geheimhouding, hun verantwoordelijkheid en het maatregelenregime dat geldt bij geconstateerde overtredingen. Laat ze daarvoor als bureau en als individuele inhuurkracht persoonlijk tekenen. Voer extra controles uit op het zoekgedrag van externe krachten, zeker als deze buiten de gemeente (uit het zicht) werken. De gemeente hoort hen uiteraard ook te informeren over de uitgevoerde controles.

2 VERBETERAANPAK VEILIG SUWINET: DE STAPPEN

Stap 1: Organiseren en plannen Verbeterplan

- Doe de Zelftest van de VNG.
  De *zelftest* geeft aan hoe de gemeente op dit moment de veiligheid Suwinet voor wat betreft de 7 Inspectienormen heeft geregeld. Bekijk aan de hand van de resultaten wat de grootste risico's zijn. Richt je dan in het vervolg meteen daarop.

- Bepaal opdrachtgeverschap, opdrachtnemerschap Verbeterplan. Een teleurstellende uitkomst van de zelftest kan de trigger zijn om aandacht te vragen. Zorg ervoor dat het Verbeterplan wordt ingebed in de reguliere besluitvormingsprocessen van de gemeente. Wij beschouwen de proceseigenaar WWB (lijnmanager) als degene die opdrachtnemer is van het Verbeterplan. Zoek allereerst contact met de CISO om gezamenlijk op te trekken en zo snel mogelijk af te stemmen met de BIG. B&W is opdrachtgever in de persoon van de portefeuillehouder informatieveiligheid en die voor sociale zaken. Bespreek het proces, tijdpad en de procedure met deze portefeuillehouders. De Raad wordt via de reguliere besluitvormingsprocessen op de hoogte gesteld.

  ISD/RSD of andere constructie: de praktische opdracht ligt bij de gemeente of GR die de WWB uitvoert. Maak afspraken over de uitvoering van het Verbeterplan, wie welke rol heeft wordt en maak afspraken over de bestuurlijke betrokkenheid.

- Maak een actielijst van de punten die geregeld moeten worden.
  Geef per actiepunt aan wanneer je die af hebt, wie je daarvoor nodig hebt en wanneer je het eindresultaat aan de opdrachtgever oplevert. Voor de actiepunten kun je de punten nemen uit dit Stappenplan. Neem dit op in het Verbeterplan.

- Informeer het personeel gedurende het hele traject.
  Bespreek de uitkomst van de zelftest en het Verbetertraject in de werkoverleggen. Dit is meteen aanleiding om nog eens de spelregels Suwinet te bespreken, onder de aandacht te brengen dat het zoekgedrag van elke medewerker gelogd wordt, en dus iedereen voor de raadplegingen onder zijn autorisatierollen verantwoordelijk is. Kondig de extra controles aan die op basis van het Verbeterplan gaan plaatsvinden. Vraag naar ideeën, check of de medewerkers zijn doordrongen van de impact en urgentie.

- Werk door tijdens verkiezingstijd en de onderhandelingsperiode.
  Zorg dat de basis onder Veilig Suwinet gereed is zodra de nieuwe portefeuillehouder aantreedt. Veilig suwinet is namelijk niet aan een politieke kleur gebonden: het is altijd noodzakelijk. Informatieveiligheid in den brede is evenmin politiek bepaald: niet voor niets heeft 95% van de lokale bestuurders op de ALV van 29 november 2013 ingestemd met de resolutie.

Stap 2. Verzeker je van bestuurlijke verantwoordelijkheid: betrek de portefeuillehouder(s) en raad

- Breng het voorstel Verbeterplan in B&W.
  Leg het voorstel Verbeterplan via de portefeuillehouder voor aan B&W voor akkoord. Verwijs naar de brief van de VNG van 12 november 2013.[7]
  ISD/RSD of andere constructie: overleg met de portefeuillehouders van de aangesloten gemeenten en leg het voorstel voor het Verbeterplan voor bij de afzonderlijke colleges of het AB wanneer hier alle portefeuillehouders van de participerende gemeenten in vertegenwoordigd zijn. Geef nadrukkelijk aan dat iedere gemeente

7 Brief 12 november 2013 van de VNG aan de leden, t.a.v. het college en de raad: https://www.vng.nl/files/vng/brieven/2013/20131112_ledenbrief_veilig_gebruik-van-suwi-net-reactie-op-inspectierapportage-en-verbetertraject-voor-gemeenten.pdf

afzonderlijk bestuurlijk verantwoordelijk is en dat de AB-leden dit geacht worden daar terug te leggen.

- Wijs op de bestuurlijke eindverantwoordelijkheid.
  Wijs op de urgentie: bij geen verbetering volgen maatregelen, zoals afsluiting van Suwinet en/of een dwangsom van het CBP.
  Betrek naast de brieven van de VNG ook die van staatssecretaris Klijnsma van 8 en 13 november 2013 en van 19 dec. 2013[8]. Overleg de VNG-publicatie 'Naar veiliger gebruik van Suwinet'.[9]

- Informeer de portefeuillehouders over de voortgang.

- Doe in afstemming met de portefeuillehouder melding aan de Raad.
  In enkele gemeenten heeft de Raad naar aanleiding van het Inspectierapport en/of publicaties in de pers vragen gesteld. Houd de Raad via de reguliere kanalen op de hoogte van het verbetertraject. VNG en SZW zullen ook de raden blijven informeren.

Stap 3. Verzamel (werkendeweg) de documenten die betrekking hebben over Veilig Suwinet

- Verzamel gedurende het traject alle relevante documenten, ook de documenten waarin naar Veilig Suwinet wordt verwezen (bv verantwoordingsverslagen).

- Inventariseer ze met behulp van de Checklist (zie bijlage 1).

Stap 4. Controleer de huidige autorisaties voor de uitvoering van de WWB en schoon op

- Inventariseer alle autorisaties die op dit moment voor de uitvoering van de WWB zijn uitgegeven.
  Doe dit samen met de gebruikersbeheerder Suwinet. Laat de gebruikersbeheerder een listing maken van de autorisatierollen in Suwinet. Leg de relatie naar de medewerkers waar het om gaat en de functies/taken die zij vervullen waarvoor hij/zij Suwinet nodig heeft. U kunt daarvoor het Overzicht autorisaties gebruiken (zie bijlage 2).

- Controleer op functie en taak medewerker:
  - Is de medewerker nog in dienst bij de gemeente?

  Zo nee: sluit dit account onmiddellijk af.
  - Is de medewerker nog belast met de uitvoering van de WWB, IOAW, IOAZ?

  Zo nee: sluit dit account onmiddellijk af.
  - Passen de uitgegeven autorisatierollen nog wel bij de taken die de medewerker uitvoert, gegeven doelbinding en proportionaliteit?

  Zo nee: sluit niet noodzakelijke rollen af, wijs evt. een andere rol toe. Informeer de medewerker.
  - Wordt het account nog wel gebruikt?

  Zo nee: ga na waarom niet. Sluit af tenzij er een goede reden is om dit niet te doen. Informeer de medewerker.

- Actualiseer het Overzicht autorisaties.
  - Beheerder Suwinet en proceseigenaar WWB (lijnmanager) tekenen beiden voor akkoord.

---

8 Brief 8 november 2013 van de staatssecretaris: http://www.gemeenteloket.minszw.nl/dossiers/werk-en-inkomen/wwb/nieuwsberichten/Opvragen-persoonsgegevens-door-gemeenten-niet-goed-bewaakt.html
Brief 13 november 2013 van de staatssecretaris: http://www.gemeenteloket.minszw.nl/binaries/live/gemeenteloket/hst%3Acontent/documents/gemeenteloket/documenten/dossiers/financieel/naleving-handhaving/kamerstukken/2013-11-13/nadere-informatie-beveiliging-Suwinet-door-gemeenten
Brief 19 december 2013 van de staatssecretaris: https://www.vng.nl/onderwerpenindex/sociale-zaken/samenwerken-op-de-arbeidsmarkt/nieuws/staatssecretaris-schrijft-gemeenten-aan-over-veilig-gebruik-van-suwinet

9 http://www.vng.nl/files/vng/nieuws_attachments/2013/20131202-veilig-suwinet.pdf

Stap 5. Controleer het recente gebruik aan de hand van gebruiksrapportages en bepaal eventuele vervolgstappen.

- Haal de meest recente Gebruiksrapportage Suwinet op.
  Dit kan alleen door degene met het account Gebruiksrapportage Suwinet. Dit is de proceseigenaar om functievermenging met die van de beheerder Suwinet te voorkomen. Dit account is aan te vragen bij BKWI. NB: deze taak kan ook in opdracht van de proceseigenaar/lijnmanager worden uitgevoerd door een intern controleur of een medewerker beveiligingsbeleid van Sociale Zaken, mits deze geen rol als gebruiker of beheerder in Suwinet hebben.

- Bestudeer de tabellen en signaleer afwijkende patronen.
  Hiervoor kunt u de Leeswijzer gebruiken die bij de Gebruiksrapportages is gevoegd.

- Geef op het Controleoverzicht aan of er afwijkingen zijn, of daar een verklaring voor is of niet. Voor het Controleoverzicht zie bijlage 3.

- Voer een extra controle uit op raadplegingen van niet-cliënten.
  Deze extra controle heeft bij veel gemeenten geleid tot meer verantwoord zoekgedrag van de medewerkers. Vraag BKWI om advies om deze controle uit te voeren. Het is aan te bevelen om deze extra controle als reguliere controle in te bouwen.

- Geef op het Controleoverzicht aan of er maatregelen genomen moeten worden, zo ja: welke maatregelen dat zijn (bv. gesprek met een team voor verklaringen van het gebruik) en wanneer deze zijn doorgevoerd.

- Indien de Gebruiksrapportages daartoe aanleiding geven kan er een rapportage van het zoekgedrag van een specifieke medewerker worden opgesteld door BKWI. Dit kan alleen worden gedaan door degene die daartoe is gemachtigd (proceseigenaar / lijnmanager). Indien deze persoonlijke rapportage daartoe aanleiding geeft, kan een specifieke procedure gestart worden, die moet zijn beschreven. Bijvoorbeeld: de betreffende medewerker wordt gehoord om zijn zoekgedrag te verklaren. Leg vast wat de uitkomsten zijn en of er wordt opgeschaald naar procedures uit het Integriteitsbeleid (P&O/HRM).

- Vraag bijzondere rapportages op als daar een bepaalde aanleiding voor is. Bijvoorbeeld naar aanleiding van publiciteit rond een publiek of politiek figuur uit de gemeente of een persoon die in de pers is genoemd. Laat BKWI dan rapporteren of deze perso(o)n(en) in Suwinet is/zijn geraadpleegd.

- Informeer het personeel over de uitkomsten van de controle.

Stap 6. Analyseer de organisatie van Veilig Suwinet en de verantwoordelijkheden

Voor het beheer, gebruik en toezicht op Suwinet zijn verschillende taken en processen te onderscheiden. Verschillende functionarissen hebben daarbij een rol. Het uitschrijven van de taken, processen en betrokken functies zorgt ervoor dat zichtbaar wordt, zowel voor medewerkers intern als voor externen, hoe zaken precies zijn geregeld, wie waarvoor verantwoordelijk is. Het uitschrijven van de processen zorgt er ook voor dat deze worden ingebed in de organisatie. Dit vormt de basis voor de controles die in opdracht van de CISO uitgevoerd worden om te kijken of processen nog wel lopen zoals afgesproken. Ook de Inspectie toetst of processen op papier staan. Net zoals voor de reguliere uitvoeringsprocessen geldt ook voor deze processen dat ze navolgbaar en controleerbaar moeten zijn.

Net als bij de uitkeringsprocessen is bij de organisatie van Suwinet functiescheiding cruciaal. We onderscheiden:

- Gebruikers van Suwinet: de medewerkers die zijn belast met werkzaamheden om de WWB, IOAW en IOAZ uit te voeren en die daarvoor via een of meerdere autorisatierollen Suwinet moeten raadplegen;

- Beheerder van Suwinet: degene die de gebruikersadministratie beheert, medewerkers in Suwinet opvoert via een rol als gebruiker cf. de beslissing van de proceseigenaar of die een account na opdracht daartoe afsluit, en die periodiek rapporteert over de gebruikers, rollen en het gebruik van de accounts;
- De proceseigenaar/lijnmanager: degene die invulling geeft aan het informatieveiligheidsbeleid en verantwoordelijk is voor de uitvoering conform de normen. Hieronder valt o.a.: het zorgdragen voor de organisatie rond Suwinet, zoals het toedelen van taken, vaststellen van processen rond Suwinet, beslissen over de bevoegdheden in Suwinet van functiegroepen en individuele medewerkers, bijsturen naar aanleiding van signalen over (oneigenlijk) gebruik, optreden na misbruik, uitdragen belang goed gebruik, het rapporteren aan de gemeentesecretaris en aan B&W over de uitvoering van de informatieveiligheidsbeleid als onderdeel van de bedrijfsvoering in de managementrapportages.
- Medewerker informatiebeveiligingsbeleid sociale zaken. In sommige gemeenten heeft afdeling sociale zaken een aparte medewerker informatiebeveiligingsbeleid. Deze heeft een staffunctie en staat los van de lijn en rapporteert aan de proceseigenaar/lijnmanager.
- Intern controleur. Een proceseigenaar kan de controle voorlopig door middel van de Gebruiksrapportages laten uitvoeren door een intern controleur die vervolgens zijn bevindingen aan de proceseigenaar rapporteert. Een intern controleur heeft een staffunctie en staat los van de lijn.

Deze onderscheiden taken moeten bewust bij verschillende functionarissen en medewerkers worden belegd. Het is niet toelaatbaar dat de beheerder van de autorisaties ook nog zelf een account heeft voor uitvoerende taken. Datzelfde geldt voor een beheerder die ook de controles uitvoert. Ook in kleine gemeenten zijn er mogelijkheden om deze functies te scheiden, bv. door het inschakelen van de intern controleur. De verdere ontwikkeling van het gemeentelijke informatiebeleid conform de BIG moet aangegrepen worden om functiescheiding definitief en in lijn met de BIG door te voeren.

De volgende stappen bieden een handvat om inzicht te krijgen in hoe de processen nu lopen en wie daarbij als verantwoordelijken zijn betrokken. Gebruik het Overzicht proces Autoriseren (bijlage 4) en het Overzicht proces Controleren (bijlage 5).

- Breng in het overzicht aan hoe het proces Autoriseren verloopt:
  - De achtereenvolgende stappen,
  - De functionaris die die stap zet,
  - Wie dat is,
  - Of daarbij gebruik wordt gemaakt van formulieren.

- Breng in het overzicht aan hoe het proces Controleren verloopt:
  - De achtereenvolgende stappen,
  - De functionaris die die stap zet,
  - Wie dat is,
  - Of daarbij gebruik wordt gemaakt van formulieren.

- Analyseer deze processen aan de hand van de criteria: logische volgorde van de stappen, zijn de stappen compleet, functiescheiding, benodigde formulieren.

Stap 7. Doe aan de hand van alle uitgevoerde doorlichtingen en opschoningsacties voorstellen voor nieuwe processen, de verdeling van verantwoordelijkheden en geef aan wat de vervolgstappen zijn in samenhang met de BIG

- Analyseer de beschreven processen, procedures en relevante documenten
  De inventarisatie van documenten en procedures, de uitgevoerde opschoningacties en de procesbeschrijvingen bieden een basis voor het signaleren van dubbels, hiaten en verbeteringen.

- Beschrijf de verbeterde processen/procedures, taken/verantwoordelijkheidsverdeling.
- Stel de periodiciteit vast waarmee het proces doorlopen moet worden.
- Stel documenten op die onderdeel zijn van deze procedures.
- Stel met de CISO vast wat de vervolgstappen moeten zijn in afstemming met de BIG en op welke termijn die gezet moeten worden om eind 2014 te voldoen aan tenminste de 7 normen van de Inspectie.

Stap 8. Leg het pakket met verbetervoorstellen voor ter besluitvorming aan de gemeentesecretaris en aan B&W

- Bespreek de verbetervoorstellen met de gemeentesecretaris, portefeuillehouder(s), DB van de ISD/RSD.
- Leg ze voor voor besluitvorming door B&W ('s).
- Zorg voor mededeling aan de raad.
- Publiceer de nieuwe processen, procedures etc.

Stap 9. Implementeer de nieuwe processen autoriseren en controleren in de organisatie

- Organiseer werkoverleggen etc. om de nieuwe procedures door te spreken met het personeel.
- Laat zo nodig (nieuwe) zorgvuldigheidsverklaringen ondertekenen, ook door externen.
- Plan in dat Suwinet periodiek onderwerp van de werkoverleggen is, bv. naar aanleiding van uitgevoerde controles.

Stap 10. Voer onder regie van de CISO de vervolgstappen Veilig Suwinet uit als onderdeel van de BIG.

3 BIJLAGEN

1 Checklist documenten Suwinet (of documenten waarin wordt verwezen naar Veilig Suwinet)

Onderwerp	Naam document/ verwijzing Datum:	Opgesteld door: … Vastgesteld door: …	Vindplaats	Opmerking/actie-punt
Beleidsplan veiligheid Suwinet (afzonderlijk of als onderdeel van gemeentelijke informatieveiligheidsplan)				
Document(en) waaruit blijkt dat beleidsplan Suwinet is vastgesteld door B&W				
Beschrijving procedure opstellen/evaluatie beleidsplan				
Procesbeschrijving/Beschrij-ving procedure autorisatie Suwinet				
Autorisatiematrix				
Schema functies(groepen) en rollen				
Aanvraagformulier Autorisatie				
Procesbeschrijving/ Beschrijving procedure controle op gebruik, inclusief procedure maatregelen				
Rapportage over de bevindingen naar aanleiding van de Gebruiksrapportages BKWI				
Document(en) met een samenvatting en conclusies van uitgevoerde controles voor College(s) en Raad (Raden) [maraps, beraps, jaarrekeing]				
Document(en) waarin functiescheiding is vastgelegd [bv. functiebeschrijving]				
Document waarin deze functiescheiding is onderbouwd				
Document voor medewerkers om ze attent te maken op belang zorgvuldig omgaan met Suwinet, bekendmaking van controles op gebruik, maatregelen en sanctieregime bij oneigenlijk gebruik [bv. Zorgvuldigheidsverklaring]				
Document waaruit blijkt dat Suwinet onderdeel vormt van HRM-beoordelingscyclus				
Document waaruit blijkt dat logging en controle Suwinetgebruik deel uit maakt van het Integriteitsbeleid / Maatregelen en sancties personeel				
Document waaruit blijkt dat medewerkers worden ge/bijschoold in Suwinet [bv. inwerkplan, opleidingsplan]				
Overig, namelijk…				
Overig, namelijk…				
Overig, namelijk…				

2 Overzicht autorisaties Suwinet

In beheer bij: .....

Verantwoordelijk afdeling hoofd: .....

Laatst uitgevoerde integrale controle: .....

Getekend: .....

Account	Autorisatie-rollen Suwinet	Medewerker, naam	Afd./team	Functie(groep)	Laatste mutatie	Status account • Actueel • Beeindigd dd… • In onderzoek

3 Controleoverzicht Gebruikrapportage Suwinet Sociale Zaken gemeente…

Maand: .....

Controle uitgevoerd door: .....

Controle uitgevoerd dd.: .....

Bijzonderheden geconstateerd bij de gebruiksrapportage: .....

	Nee	Ja	Toelichting
Tabel 1			
Tabel 2			
Tabel 3			
Tabel 4			
Tabel 5			
Tabel 6			
Tabel 7			
Tabel 8			
Tabel 9			
Tabel 10			
Tabel 11			
Tabel 12			

Advies Specifieke rapportage:

De beoordeling van de rapportage geeft geen aanleiding tot het opvragen van een specifieke gebruikersrapportage.

De beoordeling van de rapportage geeft aanleiding tot het opvragen van een specifieke gebruikersrapportage, namelijk: .....

Advies maatregelen:

De beoordeling van de rapportage heeft geen aanleiding gegeven tot het nemen van maatregelen.

De beoordeling van de rapportage heeft aanleiding tot het nemen van de volgende maatregelen, namelijk: .....
Af te handelen door:.....

4 Het proces Autoriseren Suwinet

De gemeente moet in een procesbeschrijving vastleggen hoe dit proces loopt en wie daarbij betrokken zijn. Er ligt een relatie naar het gemeentelijk Informatiebeveiligingsbeleid en het P&O-beleid (bv. bij het uit dienst treden van medewerkers).

Wat	Wie: functie, medewerker	Document	Opmerking	Conclusies
1. Vaststellen schema functiegroepen uitvoering WWB en bijbehorende autorisatierollen Suwinet			Dit is een taak van de proceseigenaar/lijnmanagement. Het schema legt vast welke functiegroepen tot welke autorisatierollen in Suwinet toegang kan krijgen. De beheerder kan de aanvragen voor autorisatie hieraan toetsen. Het is voor hem een extra handvat om geen aanvragen toe te laten die niet te maken hebben met de uitvoering van de WWB. Het biedt inzicht hoe de gemeente de rollen heeft toegedeeld naar functiegroep, uitgaande van doelbinding en proportionaliteit.	
2. Aanvraag autorisatie			Een medewerker voor de uitoefening van zijn taken toegang wil krijgen tot Suwinet vraagt via een formulier toegang aan. Hij tekent dit formulier. In dit formulier kan bv. ook een passage staan over de vertrouwelijkheid van Suwinet.	
3. Besluiten over de aanvraag autorisatie			Het nemen van een besluit op aanvraag voor toegang tot Suwinet is een taak van het lijnmanagement. Deze toetst of de aanvraag past op de functiegroep/taken van de medewerker en de gevraagde autorisatierol(len). Hij geeft akkoord door het Aanvraagformulier te tekenen.	
4. Autorisatie toekennen, medewerker opvoeren in Suwinet als gebruiker			Dit is de taak van de autorisatiebeheerder Suwinet. Hij autoriseert alleen een getekende aanvraag die tevens past bij het vastgestelde schema functiegroepen en rollen.	
5. Intrekken autorisatie: besluiten			Verantwoordelijk lijnmanager geeft opdracht om een autorisatie in te trekken. Aandachtspunt: de relatie naar P&O, er moeten afspraken zijn wie accounts gemeentebreed afsluit van vertrokken medewerkers.	
6. Intrekken: realiseren			Beheerder voert uit op grond van een schriftelijk verzoek tot intrekken van de lijnmanager.	
7. Opschonen en actualiseren autorisaties; periodiek			Dit is een taak van de autorisatiebeheerder. Volgens een draaiboek /procedurebeschrijving toetst hij periodiek op: uit dienst, mutatie functie, niet-gebruikte accounts. Hij rapporteert over zijn bevindingen aan de lijnmanager. Deze bepaalt of er accounts stopgezet moeten worden en/of autorisatierollen moeten worden ingetrokken of uitgebreid.	

5 Het proces controleren gebruik Suwinet

De gemeente moet in een procesbeschrijving vastleggen hoe dit proces verloopt, de periodiciteit en wie daarbij betrokken zijn, aan wie gerapporteerd wordt. Er ligt een relatie naar het gemeentelijk Informatiebeveiligingsbeleid en het Integriteitsbeleid (P&O). De resultaten van de controles zijn input voor bijscholing/bewustwording van de medewerkers.

Wat	Wie: functie, medewerker	Document	Opmerking	Conclusies
1. Het opvragen van Gebruiks-rapportages			Degene die geautoriseerd is voor het ophalen van Gebruiksrapportages Suwinet is de proceseigenaar/ lijnmanager. Hij kan dit opdragen aan een medewerker informatiebeveiliging, die op basis van functiescheiding niet de autorisatiebeheerder en ook niet een medewerker met een gebruiksautorisatie kan zijn.	
2. Het uitvoeren van controles op de Gebruiksrapportages en het rapporteren over de uitgevoerde controle			Zie hierboven. De rapportages maken onderdeel uit van de maraps en bestuursrapportages voor het MT.	
3. Opvragen individuele gebruiksrapportages			Zijn er signalen over oneigenlijk gebruik, dan kan een daartoe aangewezen functionaris op naam rapportages opvragen. Dit hoort de taak van de lijnmanager te zijn.	
4. Het informeren van een daarvoor aangewezen functionaris over de resultaten en adviseren over vervolgstappen n.a.v. controles van individuele medewerkers			Indien individuele medewerkers hun zoekgedrag niet kunnen verantwoorden en er aanwijzingen zijn voor normoverschrijdend gedrag moet er worden opgeschaald naar Integriteitsbeleid (bepaald door P&O, HRM). Dit beleid moet zijn beschreven.	
5. Periodieke rapportage over controles, resultaten en maatregelen aan bestuur (besturen)			De resultaten van de uitgevoerde controles kunnen worden door de lijnmanager vermeld in een paragraaf Suwinet in de bestuursrapportages en jaarrekening voor B&W/Raad en ingeval van een RSD/ ISD het DB/AB.	