Nota voor burgemeester en wethouders
Onderwerp
Suwinet jaarrapportage 2018

Team
DEV-BLD

1- Notagegevens	
Notanummer	2019-001480
Datum	02-08-2019
Programma:	
07 Inkomens-voorziening en arbeidsmarkt	
Portefeuillehouder Weth. De Geest	

2- Bestuursorgaan	
[X]B & W	10-09-2019
[ ]Raad	--
[ ]Burgemeester	--

College van B & W	
- Burgemeester	- Weth. Grijsen
- Weth. De Geest	- Weth. Verhaar
- Weth. Walder	- Weth. Rorink

Besluitenlijst	d.d.		d.d.		d.d.
[ ]Akkoordstukken	--	[X]Openbaar	10-09-2019	[ ]Besloten	--

Routing	d.d.
programmamanager	03-09-2019
wethouder	04-09-2019

	par.
[ ]adj.secr.	--
[X]gem.secr.	04-09-2019
BIS Openbaar	
Status	Definitief2019-09-11

Bijlagen

B & W d.d.: 10-09-2019

Besloten wordt:
1 De jaarrapportage Suwinet 2018 vast te stellen.
2 de raadsmededeling vast te stellen;
3 de stukken aan te bieden aan de raad;
4 de nota en het besluit openbaar te maken.

Financiële aspecten:

Financiële gevolgen voor de gemeente?	Nee
Begrotingswijziging	Nee

Voorstel openbaarmaking conform Wet Openbaarheid Bestuur (Wob)

[X] De nota en het besluit openbaar te maken
[ ] De nota en het besluit openbaar te maken vergezeld van bijgaand persbericht
[ ] De nota en het besluit openbaar te maken nadat

[ ] De nota en het besluit openbaar te maken, behalve…

[ ] Het besluit openbaar te maken, maar niet de nota, gelet op artikel:

[ ] De nota en het besluit niet openbaar te maken, gelet op artikel:

Kennisgeving/ Bekendmaking Awb

Kennisgeving (publicatie) conform Awb	Nee
Bekendmaking conform Awb	Nee

ADVIESRADEN:

Moet een van de adviesraden gehoord worden of op de hoogte gesteld? Nee

Toelichting

Inleiding

Suwinet biedt overheidsorganisaties de mogelijkheid om persoonsgegevens van burgers, die bij verschillende organisaties of basisregistraties zijn opgeslagen, te raadplegen in één webtoepassing. Suwinet wordt binnen de gemeenten gebruikt bij de uitvoering van de wettelijke taken o.a. op het gebied van de Participatiewet. Door de gegevens van een klant in Suwinet op te vragen, kan gecontroleerd worden welke inkomsten of vermogen deze klant heeft. Hiermee kan vastgesteld worden of iemand recht heeft op bijvoorbeeld een bijstandsuitkering. Suwinet bevat privacygevoelige informatie van bijna alle Nederlanders. Dit stelt hoge eisen aan de toegangsbeveiliging en vereist een zorgvuldig gebruik.

Met aanstellen van de Security Officer Suwinet in 2015 is in het takenpakket opgenomen dat er jaarlijks een rapportage wordt opgesteld met daarin een terugblik op de wijze waarop de informatiebeveiliging rondom Suwinet heeft gefunctioneerd. Als bijlage bij deze nota is de jaarrapportage Suwinet 2018 bijgevoegd. Daarin wordt teruggeblikt welke stappen de projectgroep binnen de gemeente Deventer in 2018 heeft gezet om de informatiebeveiliging van Suwinet op orde te houden. Daarin is de projectgroep geslaagd; binnen de ENSIA-verantwoording heeft de auditor geoordeeld dat de gemeente Deventer in 2018 voldeed aan de normen die gesteld worden aan de informatiebeveiliging van Suwinet.
In de rapportage wordt daarnaast aangegevenn de rapportage aangegeven welke aandachtspunten de gemeente Deventer voor 2019 ziet om de informatiebeveiliging op peil te houden.

Beoogd resultaat

Met het vaststellen van de jaarrapportage 2018 is het college (en tevens de raad) geinformeerd over de informatiebeveilging van Suwinet binnen de gemeente Deventer. De gemeente Deventer voldeed in 2018 aan de normen die gesteld worden aan de informatiebeveilging van Suwinet.

Kader

- Informatiebeveiligingsbeleid DOWR-i

- Informatiebeveiligingsplan gebruik Suwinet (juni 2016)

Argumenten voor en tegen

Voor: Het opstellen van een jaarlijkse rapportage omtrent de informatiebeveiliging Suwinet is een taak van de Security Officer Suwinet.

Tegen: Geen.

Extern draagvlak (partners)

De gemeente Deventer dient binnen de ENSIA (Eenduidige Normering Single Information Audit) - verantwoording te laten zien dat zij de informatiebeveiliging van Suwinet op orde heeft. De auditor heeft geconstateerd dat dit het geval was in 2018.

Financiële consequenties

Geen

Aanpak/uitvoering

De projectgroep die zich binnen de gemeente Deventer bezighoudt gaat ook in 2019 verder met de informatiebeveiliging van Suwinet. Voor 2019 geldt een nieuw beveiligingsplan, welke door uw college op 19 februari jl is vastgesteld.

Speerpunten voor de informatiebeveiliging van Suwinet in 2019 zullen qua uitvoering de volgende zijn:
- een diepgaander onderzoek naar de verstrekte autorisaties aan medewerkers (komt hetgeen waar zij op papier voor geautoriseerd zijn overeen met de autorisaties in de praktijk en kloppen de toegekende autorisaties bij de rollen/verantwoordelijkheden die men heeft);

- een diepgaander onderzoek naar gebruik van de whitelist (is een gefilterde lijst met bijv alleen mensen die in Deventer woonachtig zijn) en er antwoord komt op vragen zoals wanneer en waarom de escape-functie wordt ingezet, wijze van archiveren van persoonsgegevens zowel door medewerkers binnen de uitvoering alsmede het bewaren en verwijderen van opgevraagde (nadere) rapportages bij BKWI waarin persoonsgegevens van medewerkers en klanten staan opgenomen, opstellen onderliggende contracten voor uitvoering Suwinet binnen DOWR-verband.

RAADSMEDEDELING

Onderwerp	Suwinet jaarrapportage 2018		
Mededelingennr	2019-001480	**Portef.houder**	Weth. De Geest
Team	DEV-BLD	**BenW-besluit d.d.:**	10 september 2019

1. Inleiding: waarom deze mededeling

Suwinet biedt overheidsorganisaties de mogelijkheid om persoonsgegevens van burgers, die bij verschillende organisaties of basisregistraties zijn opgeslagen, te raadplegen in één webtoepassing. Suwinet wordt binnen de gemeenten gebruikt bij de uitvoering van de wettelijke taken o.a. op het gebied van de Participatiewet. Door de gegevens van een klant in Suwinet op te vragen, kan gecontroleerd worden welke inkomsten of vermogen deze klant heeft. Hiermee kan vastgesteld worden of iemand recht heeft op bijvoorbeeld een bijstandsuitkering. Suwinet bevat privacygevoelige informatie van bijna alle Nederlanders. Dit stelt hoge eisen aan de toegangsbeveiliging en vereist een zorgvuldig gebruik.

Met aanstellen van de Security Officer Suwinet in 2015 is in het takenpakket opgenomen dat er jaarlijks een rapportage wordt opgesteld met daarin een terugblik op de wijze waarop de informatiebeveiliging rondom Suwinet heeft gefunctioneerd. Als bijlage bij deze nota is de jaarrapportage Suwinet 2018 bijgevoegd. Daarin wordt teruggeblikt welke stappen de projectgroep binnen de gemeente Deventer in 2018 heeft gezet om de informatiebeveiliging van Suwinet op orde te houden. In de rapportage wordt daarnaast aangegeven welke aandachtspunten de gemeente Deventer voor 2019 ziet om de informatiebeveiliging op peil te houden.

2. Kader

- Informatiebeveiligingsbeleid DOWR-i
- Informatiebeveiligingsplan gebruik Suwinet (juni 2016)

3. Kern van de boodschap

Binnen de ENSIA-verantwoording heeft de auditor geoordeeld dat de gemeente Deventer in 2018 voldeed aan de normen die gesteld worden aan de informatiebeveiliging van Suwinet.

4. Nadere toelichting

De projectgroep die zich binnen de gemeente Deventer bezighoudt gaat ook in 2019 verder met de informatiebeveiliging van Suwinet. Voor 2019 geldt een nieuw beveiligingsplan, welke door het college op 19 februari jl is vastgesteld.

Speerpunten voor de informatiebeveiliging van Suwinet in 2019 zullen qua uitvoering de volgende zijn:

- een diepgaander onderzoek naar de verstrekte autorisaties aan medewerkers (komt hetgeen waar zij op papier voor geautoriseerd zijn overeen met de autorisaties in de praktijk en kloppen de toegekende autorisaties bij de rollen/verantwoordelijkheden die men heeft);
- een diepgaander onderzoek naar gebruik van de whitelist (wanneer en waarom wordt de escape-functie ingezet), wijze van archiveren van persoonsgegevens zowel door medewerkers binnen de uitvoering alsmede het bewaren en verwijderen van opgevraagde (nadere) rapportages bij BKWI waarin persoonsgegevens van medewerkers en klanten staan opgenomen, opstellen onderliggende contracten voor uitvoering Suwinet binnen DOWR-verband.

Jaarrapportage Suwinet 2018

Aanleiding
In 2015 is een projectgroep voortvarend aan de slag gegaan om de informatiebeveiliging van Suwinet op niveau te krijgen. Er is in die periode ook een Security Officer Suwinet aangesteld, die belast is met de uitvoering van een aantal taken, welke beschreven zijn in de 'Procedure veilig gebruik en beheer Suwinet'. Eén van die taken is om een jaarlijks een rapportage tbv de directie op te stellen waarin de volgende zaken aan de orde komen:
 de uitkomsten of verrichtingen van de uit te voeren/uitgevoerde onderzoeken en toetsingen
 aanwezigheid van onverenigbare rollen;
 frauduleus gedrag van medewerkers of niet volgen van procedures;
 geconstateerde tekortkomingen in de beveiligingsvoorzieningen ;
 wijziging van procedures / afspraken / opvolgingspatroon;
 het handelen in afwijking met de vastgelegde functiescheiding;
 afwijkingen of wijzigingen op volgens de toegestane rol toegekende autorisaties.

Bovenstaande punten zijn verwerkt in de terugblik 2018 die hieronder opgenomen is. Daarnaast zijn deze punten ook als zodanig meegenomen in de ENSIA-verantwoording waar wij als Deventer goed op hebben gescoord. Zie hiervoor bijlage 1.

Aandachtspunten voor 2018
In de jaarrapportage Suwinet over 2017 hebben wij aangegeven welke aandachtspunten wij voor 2018 zagen. Dit waren de volgende punten:

- Herziening van het informatiebeveiligingsplan, waarbij een DOWR-breed plan diende te worden opgesteld; en
- Uitvoeren van een onderzoek naar het gebruik van de escapefunctie binnen de whitelist.

Terugblik 2018
Maandelijks[1] komt onze projectgroep Suwinet bijeen om de BKWI[2]-rapportage van de voorgaande maand te bespreken en te analyseren. Dit doen we aan de hand van door onszelf vastgestelde normen. Komen we boven die normen, dan zullen wij een nadere rapportage opvragen. Deze nadere rapportage wordt vervolgens weer besproken binnen de projectgroep. De agenda's, verslagen en BKWI-rapportages worden op sharepoint op een besloten omgeving opgeslagen.

Domeinen
Suwinet kent verschillende domeinen waarbinnen gegevens kunnen worden geraadpleegd. In Deventer hebben wij toegang binnen de volgende domeinen:

- Burgerzaken
- Belastingdeurwaarder
- Werk en Inkomen
- RMC

Van deze domeinen wordt maandelijks een generieke rapportage opgevraagd en – als die rapportage daar aanleiding voor geeft – wordt er extra onderzoek gedaan. Nader onderzoek houdt in dat we nadere rapportages bij het BKWI opvragen en analyseren. Binnen de domeinen Burgerzaken, Belastingdeurwaarder en RMC hebben slechts enkele medewerkers toegang tot Suwinet en is het aantal te raadplegen gegevens niet erg uitgebreid. Binnen het domein Werk en Inkomen ligt het zwaartepunt van onze controles.

Nadere rapportages
In 2018 zijn binnen het domein Werk en Inkomen verscheidene nadere rapportages opgevraagd. Dit was bijvoorbeeld het geval toen de projectgroep meer informatie nodig had over het aantal geblokkeerde accounts, zoeksleutel anders dan bsn en een overzicht van medewerkers die buitenproprtioneel veel raadplegingen hebben gedaan. Vaak betreft het overigens nieuwe medewerkers die onvoldoende scherp hebben dat iedere klik binnen Suwinet wordt geregistreerd. De nadere rapportages hebben geen aanleiding gegeven om enige vorm van misbruik te veronderstellen.

[1] Een enkele keer lukt het niet om bijeen te komen vanwege vakanties, of wanneer de generieke rapportage nog niet beschikbaar is.
[2] Bureau Keteninformatisering Werk en Inkomen

Bewustwording
In september 2018 is een presentatie gegeven over het gebruik van Suwinet aan de:
- Sociale Recherche
- inkomensconsulenten
- uitkeringsdaministratie
- frontoffice publiekszaken
- jongerenloket
- terugvordering en verhaal.

Daarnaast is de e-learningsmodule van de VNG bij medewerkers onder de aandacht gebracht. Een aantal medewerkers heeft deze e-learningmodule gevolgd. Tot slot weten medewerkers de leden van de projectgroep goed te vinden als zij twijfels of vragen hebben bij het mogen raadplegen van Suwinet.

Onderzoek naar escapefunctie whitelist
Binnen de projectgroep is een onderzoek gedaan naar het gebruik van de escapefunctie binnen de whitelist. Een whitelist is een lijst die de BSN's bevat van alleen die inwoners waar de gemeente/organisatie een dienstverleningsrelatie mee heeft of mee heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens van die burger. Als de raadpleging toch nodig is i.v.m. de uitvoering van wettelijke taken, dan kan de (geautoriseerde) medewerker het filter passeren door middel van een zogenaamde 'escapefunctie'. De inzet van dit filtermechanisme bevordert een veilig en proportioneel gegevensgebruik door medewerkers en draagt bij aan het beschermen van de privacy van burgers. Sinds 2017 wordt in Deventer met de whitelist gewerkt. In de generieke rapportage over 'gebruik escapefunctie' is te zien hoe vaak de escapefunctie is gebruikt, hoeveel pagina's daarvoor zijn geraadpleegd en met welke reden. In deze rapportages staan geen herleidbare gegevens naar BSN's of accounts, daarvoor moet een specifieke rapportage worden opgevraagd.
De specifieke rapportage bevat wel tot personen herleidbare gegevens. In het geval van de escapefunctie, is te zien welke medewerker op welk moment een BSN heeft benaderd via de escapefunctie, dat niet in de whitelist staat. Ook is te zien welke pagina's zijn bezocht en wat de reden was.

In 2018 is geconstateerd dat een aantal opvragingen binnen de whitelist zijn gedaan die niet terug te leiden zijn naar GWS (het systeem waarin bijstandsaanvragen worden afgehandeld) of naar de Basis Registratie Personen (BRP). Het gaat dan dus om mensen die niet in Deventer wonen en die geen bijstandsuitkering hebben. Het gaat om 133 raadplegingen door zowel consulenten als sociaal rechercheurs. Er is met de teammanager van deze medewerkers een gesprek gevoerd, waarbij afgesproken is dat hij met de betreffende medewerkers in gesprek zou gaan en zou achterhalen waarom deze personen zijn geraadpleegd binnen Suwinet. De raadplegingen bleken om de volgende redenen te zijn gedaan:

- Onderzoek onderhoudsplicht ouders bij aanvraag bijzondere bijstand van jongeren onder de 21 jr
- Onderzoek onderhoudsplicht ouders
- Aanvragen waarbij niet rechthebbende partners zijn betrokken
- Verhuizingen/woningruil
- Mogelijke samenwoning/kamer bewoning
- Signalen van het Inlichtingenbureau met betrekking tot de kostendelersnorm
- Onderzoek alimentatieplichtig naar kinderen of ex partners.

In gesprek met de teammanager is aangegeven dat - hoewel dit taken zijn die inkomensconsulenten/medewerkers Sociale Recherche uitvoeren in het kader van de Participatiewet - Suwinet voor een aantal van deze redenen toch niet mag worden gebruikt omdat gegevens van andere personen (niet zijnde de klanten met een bijstandsuitkering) worden gecheckt. Evenmin mag Suwinet worden gebruikt voor interne controle. De teammanager heeft deze boodschap vervolgens binnen het team verspreid.

IDU
Maandelijks wordt de in-uit-en-doorstroomlijst opgesteld en afgetekend door de verantwoordelijk teammanager. Op die manier wordt bijgehouden of er nieuwe autorisaties moeten worden toegekend aan nieuwe medewerkers, of dat verstrekte autorisatie bijgesteld moeten worden als gevolg van het

doorstromen van een medewerker naar een andere functie of dat bepaalde autorisaties moeten worden beëindigd in verband met het vertrek van een medewerker.
Op deze manier houden we grip op het aantal geblokkeerde accounts en zorgen we ervoor dat een medewerker niet langer in Suwinet kan als hij dit ook niet meer voor de uitoefening van zijn werkzaamheden nodig heeft. Daarmee wordt misbruik voorkomen.

Geheimhoudingsverklaringen
Iedere nieuwe medewerker (ingehuurd of in dienst van de gemeente) die een autorisatie krijgt om persoonsgegevens te raadplegen in Suwinet, krijgt bij de start in de nieuwe functie uitleg over het gebruik van Suwinet en de informatiebeveiliging daaromtrent. Daartoe wordt een geheimhoudingsverklaring ondertekend en legt het projectgroeplid - dat vanuit de uitvoering aan het projectgroepoverleg Suwinet is afgevaardigd – aan de nieuwe medewerker uit wat de spelregels zijn. De spelregels worden tevens op schrift overhandigd aan de nieuwe medewerker. Ook wordt aan de nieuwe medewerker gevraagd om de e-learning module van de VNG te volgen.

Beveiligingsplan
In 2018 is gestart met het herzien van het informatiebeveiligingsplan. Het vorige plan dateerde uit 2016. Het beveiligingsplan is in samenwerking met de gemeenten Olst-Wijhe en Raalte tot stand gekomen, omdat op dit thema al veel wordt samengewerkt en het wenselijk was om in gezamenlijkheid tot een nieuw beveiligingsplan te komen.
Zowel de directie als het college van de gemeente Deventer hebben het informatiebeveiligingsplan vastgesteld[3].

Autorisaties
De autorisaties zijn vastgelegd in onze autorisatiematrix. Deze is in december 2018 herzien en opnieuw vastgesteld. De autorisatiematrix is terug te vinden op het besloten gedeelte van sharepoint. Zodra er wijzigingen in de accounts/autorisaties doorgevoerd moeten worden, dan wordt met het opstellen van de nieuwe IDU-lijst een verzoek naar Functioneel Beheer verstuurd om de wijziging door te voeren. We krijgen dan per mail een bevestiging als de wijziging is doorgevoerd. Voorbeelden van mails zijn op de besloten sharepoint site te vinden.

Logboek
Er is een logboek ontwikkeld dat inzicht moet bieden aan de mogelijke incidenten die zich in de organisatie voordoen. In 2018 hebben zich geen incidenten voorgedaan, waardoor het logboek nog niet gevuld is. Daarnaast is er een aparte gemeentebrede meldknop aangemaakt voor het melden van incidenten op het gebied van informatiebeveiliging, waaronder voor Suwinet.

Speerpunten 2019
Speerpunten voor de informatiebeveiliging van Suwinet in 2019 zullen qua uitvoering de volgende zijn:

- een diepgaander onderzoek naar de verstrekte autorisaties aan medewerkers (komt hetgeen waar zij op papier voor geautoriseerd zijn overeen met de autorisaties in de praktijk en kloppen de toegekende autorisaties bij de rollen/verantwoordelijkheden die men heeft);
- een diepgaander onderzoek naar gebruik van de whitelist (wanneer en waarom wordt de escape-functie ingezet), wijze van archiveren van persoonsgegevens zowel door medewerkers binnen de uitvoering alsmede het bewaren en verwijderen van opgevraagde (nadere) rapportages bij BKWI waarin persoonsgegevens van medewerkers en klanten staan opgenomen, opstellen onderliggende contracten voor uitvoering Suwinet binnen DOWR-verband.

Conclusie
Er is over de periode januari 2018 tot 31 december 2018 (voor zover na te gaan) geen onrechtmatig gebruik gemaakt van Suwinet inkijk. Dit wordt ook bevestigd in de ENSIA-verantwoording 2018. De auditor heeft geoordeeld dat de gemeente Deventer voldoet aan de normen die aan de informatiebeveiliging van Suwinet gesteld worden.

[3] Het college heeft het plan op 19 februari 2019 vastgesteld. Dit betekent dat voor 2018 nog het oude informatiebeveilgingsplan uit 2016 van toepassing was.

Bijlage 1: Normenoverzicht Suwinet tbv ENSIA 2018

Norm	Beschrijving norm	Toelichting norm	Externe audit oordeel
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet.	VOLDOET
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	Het voorkomen dat risico's optreden als gevolg van het ontbreken van coördinatie op het gebied van activiteiten aangaande de bescherming van de eigen delen van Suwinet.	VOLDOET
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat.	VOLDOET
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken.	VOLDOET
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten.	VOLDOET
U.11	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	Het voorkomen van ongeautoriseerde toegang tot netwerkdiensten.	VOLDOET
C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau	VOLDOET
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	Het vaststellen of: de autorisaties en veranderingen hierin juist en tijdig zijn aangebracht, de juiste functiescheiding zijn toegepast en voldaan wordt aan de principes van doelbinding en proportionaliteit, oneigenlijk autorisatie-toekenningen hebben plaatsgevonden.	VOLDOET
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).	Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie.	VOLDOET
AP	Bewerkstelligen dat alle medewerkers bewust zijn van beveiligingsrisico's ten aanzien van het werken met (privacy) gevoelige data/	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	VOLDOET