



EINDHOVEN

Beveiliging Suwinet 2017

gemeente Eindhoven
CTRL - Control, CCA - Concern Control en Advies
Definitief
april 2017

Colofon

Uitgave

Gemeente Eindhoven

CTRL - Control, CCA - Concern Control en Advies

Datum

april 2017

Inhoudsopgave

	Colofon	2
	Inhoudsopgave	3
1	Conclusies en aanbevelingen	4
1.1	Conclusie	4
1.2	Aanbevelingen	4
1.2.1	Essentiële aanbevelingen	4
1.2.2	Verbeteracties ter aanscherping huidige werkwijze	4
2	Inleiding	6
2.1	Regeling Suwi	6
2.2	Uitvoering en doelstelling audit	6
2.3	Afbakening onderzoek	7
2.4	Werkwijze	7
2.5	Normenkader en aanbevelingen	7
3	Bevindingen	9
3.1	Beveiligingsplan artikel 6.4 Regeling Suwi	9
3.2	Organisatorische aspecten	9
3.3	Logische toegangsbeveiliging	12
3.4	Autorisatiestructuur	14
3.5	Netwerk	16
3.6	Koppelingen	17
3.7	Verantwoording	17

1 Conclusies en aanbevelingen

1.1 Conclusie

Het afgelopen jaar is de beveiliging van Suwinet op hetzelfde niveau gehandhaafd. Dit betekent dat **de beveiliging van Suwinet binnen de gemeente Eindhoven voldoet aan de minimaal daar aan te stellen eisen.**

Hoewel wordt voldaan aan de minimale eisen is het wel goed belangrijk dat het gemeentelijk informatiebeveiligingsbeleid dit jaar wordt geactualiseerd en dat het Suwinet beveiligingsplan wordt geaccordeerd door het management. Ook zijn nog een aantal verbeteracties mogelijk om de beveiliging verder aan te scherpen. Deze acties staan hieronder beschreven. Het gemeentebrede proces om functiewijzigingen door te geven aan applicatiebeheerders is een punt dat al een aantal jaren terugkomt maar nog steeds niet is opgelost. Voor Suwinet zijn er nu andere maatregelen om dit te compenseren maar een permanente goed ingeregeld gemeente breed proces verdient heeft uiteraard de voorkeur.

1.2 Aanbevelingen

1.2.1 Essentiële aanbevelingen

Beveiligingsplan en organisatorische aspecten:

- I. Accordeer als Security Officer het concept gemeente brede informatiebeveiligingsbeleid en het informatiebeveiligingsplan Suwinet 2017.
- II. In 2017 wordt het werken met de zogeheten "White list"¹ ingevoerd binnen de gemeente Eindhoven. Het is belangrijk op korte termijn een project hiervoor te starten. Denk bij de invoering goed na over het beleggen van de verantwoordelijkheden in deze en de wijze waarop wordt omgegaan met het actueel houden van de white list en het gebruik maken en monitoren van de bijbehorende "escape"² functie.
- III. Per 1 april 2017 is het nieuwe Suwinet- normenkader van kracht. Dit normenkader is afgestemd op en houdt rekening met de Baseline Informatiebeveiliging Nederlandse Gemeente (BIG). Het is aan te bevelen om op het gebied van beleidsbepalingen aansluiting te zoeken bij het inrichten en ontwikkelen van de BIG.

1.2.2 Verbeteracties ter aanscherping huidige werkwijze

Beveiligingsplan en organisatorische aspecten:

- IV. Voorzie in een (korte) opleiding voor Suwinetgebruikers. Besteed hierbij extra aandacht aan vertrouwelijkheids- en beveiligingsaspecten. Neem hierbij ook medewerkers van Derden mee.

¹ De zogenaamde white list bevat de gegevens van Eindhovense burgers waar een klantrelatie mee is in het Sociaal Domein en waarvoor het dus is toegestaan om in Suwinet gegevens op te vragen.

² De escape functie is nodig om gegevens van klanten die (nog) niet in de white list staan op te vragen. Bijvoorbeeld bij nieuwe aanvragen.

- V. Besteed in de rapportages over het gebruik van Suwinet specifiek aandacht aan gebruik door Derden.

Logische toegangsbeveiliging en autorisaties:

- VI. Sluit, indien de gemeentebrede procedure ten aanzien van het proces functiewijzigingen is gerealiseerd, hierbij aan. Ook voor de afdeling Burgerzaken moet aangesloten worden bij het gemeentebrede proces.
- VII. Richt daadwerkelijk een aparte gebruikerstabel in voor de gerechtsdeurwaarders (NB is reeds in ontwikkeling)

Controle en verantwoording:

- VIII. Maak bij de maandanalyses gebruik van de mogelijkheid om het gebruik binnen Eindhoven af te zetten tegen vergelijkbare gemeenten;
- IX. Beperk het gebruik van Suwinet in de thuiswerkomgeving tot een minimum. En monitor de gevallen waar dit toch gebeurt extra.
- X. Beleg de verantwoordingstaak richting Bureau Keten Informatisering Werk en Inkomen (BKWI) op de juiste plek in de organisatie.

2 Inleiding

2.1 Regeling Suwi

De regeling SUWI³ maakt onderdeel uit van de Wet SUWI, en is tot stand gekomen onder verantwoordelijkheid van de Minister van Sociale Zaken en Werkgelegenheid.

Het Suwinet is het netwerk dat toegankelijk is voor de partijen in de sector Werk en Inkomen gezamenlijk met het stelsel van technische en organisatorische voorzieningen daar bij behorend. Dit stelsel van voorzieningen stelt de ketenpartners in staat om gegevens van elkaar in te zien en uit te wisselen.

Suwinet vervult een essentiële functie bij de uitwisseling van gegevens door de partijen binnen het Suwidomein. Het niet of in onvoldoende mate functioneren van het Suwinet heeft grote invloed op het deel van de bedrijfsprocessen bij andere Suwi-partijen, die gebruik maken van bij een andere Suwipartij beschikbare informatie.

Op dit moment maken binnen de gemeente Eindhoven de sectoren Operations en Support, de afdeling Burgerzaken van de sector Publiekscontacten gebruik van Suwinet. Daarnaast voert de gemeente Eindhoven de Suwi-regeling uit voor de gemeente Waalre en wordt Suwinet in Eindhoven gebruikt door de Regionale Meld- en Coördinatiefuncties (RMC) en de gemeentelijke belasting deurwaarders (GBD) en ISD de Kempen. In de Regeling SUWI, 21 december 2001 en de bijbehorende bijlage XIV staan de afspraken en eisen die de Suwi-partijen moeten naleven om de beveiliging van Suwinet te verwezenlijken. Er is een richtlijn en normenkader opgesteld voor de inrichting van de beveiliging alsmede de jaarlijkse verantwoording naar het ministerie van Sociale Zaken en Werkgelegenheid, de Inspectie Werk & Inkomen en naar elkaar.

De Suwi-partijen hebben een eigen verantwoordelijkheid voor het beheer van de bedrijfsprocessen, de wijze waarop zij die beheersen en de wijze waarop zij daarover verantwoording afleggen. Opdracht voor het jaarlijks uitvoeren van een verplichte EDP-audit (ook wel IT-audit genoemd) is opgenomen in art. 5.22 en 6.4 van de regeling SUWI.

2.2 Uitvoering en doelstelling audit

Deze IT-audit is gebaseerd op het Suwinet-normenkader en heeft tot doel te beoordelen of opzet, bestaan en werking van het stelsel van procedures en maatregelen op de beveiliging van de betreffende gegevensuitwisseling voldoet aan de normen van de SUWI-wetgeving.

De doelstelling van de audit luidt als volgt:

Heeft de gemeente Eindhoven voldoende waarborgen gecreëerd ten aanzien van bescherming van vertrouwelijkheid en andere beveiligingsrisico's binnen het SUWI-domein?

Op verzoek van het Sociaal Domein wordt tijdens dit onderzoek extra aandacht besteed aan de inbedding in het proces van de gemeentelijke belasting deurwaarders (GBD) en de Regionale Meld en Coördinatie functies (RMC).

³ SUWI staat voor Structuur uitvoeringsorganisatie werk en inkomen

In 2015 is door Concerncontrol ook een audit uitgevoerd op Suwinet. Uit deze audit bleek dat een grote verbetering was gemaakt ten opzichte van 2014. Wel waren er nog wat kleinere verbeterpunten. Ook zijn audits uitgevoerd door het ministerie van SZW en het College Bescherming Persoonsgegevens (nb. de huidige Autoriteit Persoonsgegevens). Conclusie van de audits was dat Eindhoven voldeed aan de minimaal te stellen eisen. Tijdens deze audit kijken we ook of de verbeterpunten uit bovenstaande audits zijn gerealiseerd.

2.3 Afbakening onderzoek

De reikwijdte van het onderzoek is het beoordelen van opzet, bestaan en werking van het stelsel van procedures en maatregelen gericht op de beveiliging van de gegevensuitwisseling via Suwinet.

Er is een geautomatiseerde koppeling tussen Suwinet en GWS. Deze koppeling en de beveiliging van de GWS-server vallen buiten de scope van dit onderzoek.

Tevens worden niet tot de scope van de IT-audit Beveiliging Suwinet gerekend:

- de kwaliteit van de gegevens;
- de tijdigheid en kwaliteit van de gegevensverstrekkingen;
- de gegevensverwerking binnen de gemeente Eindhoven⁴.

Ten tijde van het onderzoek was het nieuwe Suwinet- normenkader nog niet van kracht. Om deze reden is de audit nog uitgevoerd o.b.v. het Normenkader GeVS 2011 en is er niet inhoudelijk gekeken naar de nieuwe normen.

2.4 Werkwijze

Het onderzoek is uitgevoerd door middel van deskresearch en Interviews met de autorisatiebeheerder/functioneel beheerder t.a.v. Suwinet, de Security Officer Suwinet en de auditoren Sociaal Domein.

2.5 Normenkader en aanbevelingen

Onder de verantwoordelijkheid van de Domeingroep Privacy & Beveiliging (hierna te noemen: DPB) is een verantwoordingsrichtlijn (hierna te noemen: Verantwoordingsrichtlijn EDP-audit Suwinet) opgesteld. Deze richtlijn gaat in op de wijze waarop de verplichte EDP-audit van de beveiliging van Suwinet vorm en inhoud moet worden gegeven. Naast een eenduidig inzicht maakt de in de richtlijn voorgeschreven rapportagevorm het tevens mogelijk om op evenwichtige wijze over de beveiliging van het Suwinet te rapporteren. De relevante onderdelen van de verantwoordingsrichtlijn EDP-audit Suwinet hebben als het uitgangspunt voor de IT-audit gefungeerd.

⁴ Gegevensverwerking omvat zowel de gegevens die zijn verkregen via het Suwinet als uit andere omgevingen. In dit gebied vallen ook de ondersteunende bedrijfsprocessen en systemen die gegevens verwerken die niet onder de wet SUWI vallen (bijv. financiële processen, beheer van personeel)

Aanbevelingen zijn geprioriteerd. Aanbevelingen met twee uitroeptekens **!!** moeten opgevolgd worden om te kunnen (blijven) voldoen aan essentiële normen. Aanbevelingen met één uitroepteken **!** zijn aanscherpingen van de huidige werkwijze.

Per 1 april 2017 is het nieuwe Suwinet- normenkader van kracht, hiermee komt het Normenkader 2011 GeVS te vervallen. Bij het opstellen van het nieuwe normenkader is rekening gehouden met de punten uit de Baseline Informatiebeveiliging Nederlandse Gemeente (BIG). Waar voorheen het normenkader normen bevatte voor zowel afnemers, bronhouders en beheerders, wordt er vanaf nu een splitsing gemaakt tussen deze partijen.

Verantwoording over het voldoen aan de nieuwe normen vindt plaats in het kader van ENSIA aan de hand van een vragenlijst die per 1 juli 2017 beschikbaar wordt gesteld.

3 Bevindingen

3.1 Beveiligingsplan artikel 6.4 Regeling Suwi

! *Gemeentebreed informatiebeveiligingsbeleid*
De gemeente Eindhoven beschikt over een informatiebeveiligingsbeleid dat in juli 2014 is goedgekeurd door het daartoe bevoegde management. Het beleid wordt ten tijde van dit onderzoek geactualiseerd. Er is inmiddels een concept versie beschikbaar.

! *Beveiligingsplan Suwinet*
In 2014 is een beveiligingsplan opgesteld voor Suwinet. Dit plan is vervolgens ieder jaar en ook in 2017 geëvalueerd en geactualiseerd (in maart 2017) deze laatste versie is nog niet geaccordeerd door het MT Sociaal Domein.
Het concept beveiligingsplan Suwinet voldoet aan de daar aan te stellen eisen.

Samenwerking Derden

In het beveiligingsplan is aandacht voor samenwerking met derden. Hieronder vallen de gemeente Waalre, Gemeentelijke Belasting Deurwaarders, ISD de Kempen en Regionale Meld- en Coördinatiefuncties. De beschrijving van de samenwerking en ieders verantwoordelijkheden is verbeterd ten opzichte van de vorige versie.

Uitdragen beveiliging Suwinet

Conform de richtlijnen moet het beveiligingsplan worden uitgedragen in de organisatie. Het plan moet daarvoor beschikbaar zijn op intranet en besproken worden tijdens afdelingsoverleggen. Dit is het afgelopen jaar voldoende gebeurd: er is twee maal een bericht op het gemeentelijk intranet geplaatst, er is een sociaal domein brede bijeenkomst over privacy gehouden..

Samenwerking Derden

In het informatiebeveiligingsplan 2017 is opgenomen dat awareness activiteiten verlopen via een contactpersoon bij de samenwerkingspartner als de gebruikers van deze samenwerkingspartners geen toegang hebben tot het intranet van de gemeente Eindhoven. Omdat alle samenwerkingsverbanden binnen de gemeente Eindhoven lopen gelden dezelfde awareness activiteiten.

3.2 Organisatorische aspecten

De taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting, het beheer en de beveiliging van Suwinetgegevens, applicaties en processen en infrastructuur zijn beschreven en goed belegd.

Het eigenaarschap Suwinet is belegd bij het Sectorhoofd Operations. De taken, verantwoordelijkheden en bevoegdheden van de eigenaar Suwinet zijn gedefinieerd in het informatiebeveiligingsplan.

De rol van Security Officer is sinds februari 2016 definitief ingevuld en gepositioneerd binnen de sector Operations. De taak van Security Officer wordt gecombineerd met de

rol van privacy functionaris binnen het Sociaal Domein. De taken, verantwoordelijkheden en bevoegdheden van de Security Officer zijn beschreven in het informatiebeveiligingsplan. Daarnaast is nog een uitgebreidere taakbeschrijving in een apart document met daarin ook beschreven op welke momenten in het jaar bepaalde taken worden uitgevoerd.

Hierdoor worden de beveiligingsprocedures en –maatregelen in het kader van Suwinet voldoende beheerd en beheerst.

De Security officer heeft in 2017 (september 2016 tot en met maart 2017):

- ◆ geadviseerd over de beveiliging van Suwinet een voorbeeld hiervan is het initiëren van het gebruik van de white list;
- ◆ gecontroleerd of de beveiligingsmaatregelen van Suwinet worden nageleefd;
- ◆ een evaluatie uitgevoerd van uitkomsten van controles;
- ◆ voorstellen gedaan tot implementatie of aanpassing van de beveiliging van Suwinet, met name op het gebied van de aanpassing in autorisaties; Eén maal gerapporteerd aan het hoogste management omtrent de beveiliging van Suwinet.

!!

BKWI heeft recentelijk het principe van de “white list” geïntroduceerd voor Suwinet.

Eindhoven heeft nog geen project opgestart om dit in 2017 te implementeren. Een whitelist is een positieve lijst waaraan wordt getoetst of bepaalde gegevens van burgers mogen worden opgevraagd in Suwinet. De lijst wordt toegepast op BSN- niveau. Hierdoor is het na invoering van de white list alleen nog mogelijk zijn om gegevens van personen op te zoeken waar de gemeente Eindhoven een dienstverleningsrelatie mee heeft. Hiermee wordt oneigenlijk gebruik van Suwinet tegen gegaan.

Als gebruikers van Suwinet toch gegevens op willen zoeken van burgers die niet op de whitelist staan (bijvoorbeeld bij een nieuwe aanvraag), kunnen ze gebruik maken van de escapefunctie. Dit is een specifieke autorisatie die alleen beschikbaar is voor medewerkers met specifieke taken. Deze rol brengt een groter risico op onzorgvuldig gebruik van gegevens met zich mee. Het verstrekken van deze autorisatie dient dan ook te worden beperkt tot een minimum, (bijvoorbeeld alleen toegankelijk voor een gebruiksbeheerder).

De verantwoordelijkheid voor het beheren van de whitelist en beleggen van de escapefunctie ligt bij de gemeente zelf. Zo wordt intern o.a. bepaald welke BSN's op de lijst komen te staan en welke criteria gelden voor het opstellen. De keuzes die op dit gebied worden gemaakt zijn essentieel voor een goede beveiliging en moeten derhalve goed doordacht worden.

Samenwerking Derden

!

In het laatste beveiligingsplan wordt aangegeven dat vanaf 2016 specifiek zal worden ingezoomd op het gebruik van Suwinet door medewerkers van Derden. Dit hebben wij vast kunnen stellen voor RMC en GBS. Uit de rapportage is alleen voor buitenstaanders niet exact duidelijk welke deel gaat over derden en welk deel niet. Voor het specifieke gebruik voor de gemeente Waalre is het heel lastig om dit onderscheid te maken omdat hiervoor speciale queries moeten worden gerealiseerd. Daar komt bij dat na in gebruik name van de white list dit onderscheid niet meer gemaakt kan worden. De medewerkers die de verwerking voor Waalre uitvoeren maken wel deel uit van de reguliere controles waardoor gebruik van Suwinet ook voor Waalre wordt gemonitord. In het contract met Waalre is overeengekomen dat alleen wordt gerapporteerd in geval van bijzonderheden of calamiteiten.

Ook de taken, verantwoordelijkheden en bevoegdheden op het gebied van functioneel beheer/autorisatiebeheer zijn het afgelopen jaar vastgesteld. Het autorisatie beheer is belegd bij 2 personen binnen de sector I&B Functioneel beheer Sociaal Domein. Hiermee is vervanging bij afwezigheid is ook geregeld.

Samenwerking Derden

Er is geen speciale aandacht in de autorisatieprocedure voor medewerkers afkomstig van Derden. In de huidige situatie zijn alle medewerkers met Suwinet autorisatie werkzaam binnen de gemeente Eindhoven. Autorisatieaanvragen verlopen daarom altijd via Topdesk en de leidinggevende. Eventuele aanvragen van buiten de gemeente Eindhoven verlopen altijd via de security officer.

!

In de opleiding van nieuwe gebruikers wordt nauwelijks aandacht besteed aan (de beveiliging van) Suwinet. Wel worden gebruikers bij de aanmaak van hun userid schriftelijk gewezen op de vertrouwelijkheidsaspecten rondom het gebruik van Suwinet.

3.3 Logische toegangsbeveiliging

De laatste versie van de gebruikerstabel bevat 175 unieke gebruikers, gekoppeld aan personen, deze zijn verdeeld over verschillende rollen. Het aantal gebruikers is t.o.v. 2016 minimaal afgenomen (toen waren er 178 gebruikers).

Er is een formele en vastgestelde procedure ten aanzien van autorisatie en registratie van de gebruikers die toegang hebben tot de Suwinet applicaties.

Er vindt een periodieke (ic meerdere keren per jaar) controle plaats op verleende toegangsrechten op basis van de gegevens die de autorisatiebeheerder verkrijgt vanuit het centrale gebruikersmagazijn. De laatste controle is uitgevoerd in april 2016. De autorisatieoverzichten zijn aangepast. Deze controle wordt geregistreerd. Deze controle wordt conform de richtlijn in het beveiligingsplan Suwinet tweemaandelijks uitgevoerd.

Voor de afdeling Burgerzaken ontvangt functioneel beheer tot nu toe geen in- en uit dienstmeldingen en functiewijzigingen.

!

Interne functiewijzigingen worden niet actief gemeld en/of geregistreerd en bereiken de autorisatiebeheerder nog steeds slechts per toeval. Het risico hiervan is dat er gedurende het jaar medewerkers van functie veranderen en toch nog toegang hebben tot Suwinet (zie ook de bevinding onder de tabel hieronder).

Volgens de procedure informeert de functioneel beheerder één maal per jaar de afdelingshoofden welke medewerkers toegang hebben tot Suwinet. Dit is voor het laatst gebeurt in april 2016 en staat gepland voor de eerste week in april 2017. De afdelingshoofden controleren of dit nog correct is. Alle afdelingshoofden hebben een mailtje gehad met de overzichten van hun medewerkers. Alle afdelingshoofden hebben een reactie teruggestuurd. Gemeentebreed loopt een pilot om de autorisaties van medewerkers in geval van functiewijzigingen terug te brengen tot een "basis account" met alleen Intranet/Internet /Microsoft Office.

De status van de gebruikers in de gebruikerstabel is als volgt:

Status	Aantal
Account geblokkeerd	3
Account verlopen	12
Foutieve inlogpoging	2
Tijdelijk wachtwoord	4
Tijdelijk wachtwoord verlopen	1
Wachtwoord verlopen	1
Actief	152
TOTAAL	175

Ongeautoriseerde toegangspogingen en essentiële activiteiten worden gedetecteerd. 7,4% van de accounts betreft een verlopen account of account met een verlopen wachtwoord. Ten opzichte van vorig jaar is het aantal gebruikers met een verlopen account hoger, waar dit er eerst slechts 3 waren, zijn het er nu 12. Verklaring hiervoor is dat de jaarlijkse controle vlak na deze audit staat gepland.

Uit de analyse op de gebruikersadministratie blijkt het volgende; de autorisatietabel bevat één gebruiker die niet meer in dienst is bij gemeente Eindhoven en één gebruiker die inmiddels een andere functie heeft, maar wel nog de rol 'Specialist Inkomen'.

Aanvullend op de tweemaandelijks controle heeft er eind 2016 een eenmalige opschoning van de gebruiksadministratie plaatsgevonden. Hier zijn de Suwinet gebruikers vergeleken met het Gebruikers Magazijn Eindhoven (GME). Gebruikers die niet in het gebruikers magazijn staan mogen geen toegang hebben en zijn gedurende de opschoning geblokkeerd.

Er is interne controle op het gebruik van Suwinet door de auditoren van het Sociaal Domein. De van het BKWI verkregen informatie over het gebruik van Suwinet wordt maandelijks geanalyseerd op basis van richtlijnen voor de maandanalyses. Als er uit deze analyse opvallende bevindingen naar voren komen vraagt de auditor meer informatie op bij het BKWI en indien nodig bespreekt de auditor deze met het betrokken afdelingshoofd.

!

In de maandanalyses die Eindhoven ontvangt van het BKWI staan voor een aantal indicatoren vergelijkingen met gemeenten van vergelijkbare omvang. Dit kan een indicatie zijn voor de omvang van het gebruik van Suwinet door Eindhoven. Van deze mogelijkheid wordt tot op heden nog geen gebruik gemaakt.

In de richtlijnen staan aandachtspunten en "normen" voor de maandelijks analyses. Het is belangrijk deze richtlijnen jaarlijks te evalueren, dit is in maart 2017 gebeurd.

Communicatie naar het management vindt twee maal per jaar plaats in januari en in juli.

De laatste keer heeft plaatsgevonden in januari 2017. De auditoren vragen hiernaast twee maal per jaar de volledige logging op van het gebruik van Suwinet en vergelijkt deze op basis van zogeheten queries met de inhoud van de applicatie GWS@ALL. Wat dit laatste betreft is het wel belangrijk dat de controles in dit verband voldoen aan de wettelijke eisen. Bepaalde controles mogen bijvoorbeeld alleen worden uitgevoerd indien sprake is van een gerichte verdenking. Deze activiteiten worden op korte termijn vervangen door gebruik te gaan maken van de eerder genoemde white list.

Uitgangspunten voor deze controles zijn er nog steeds niet maar met de invoering van de white list zijn ze ook overbodig.

Afdelingshoofden ontvangen een overzicht van de belangrijkste gebruikers binnen hun afdeling. De Security officer meldt opvallende zaken en bespreekt deze met het afdelingshoofd.

Samenwerking Derden

!

Er zijn twee aparte gebruikerstabellen voor de RMC-werkzaamheden en voor de gebruikers van Burgerzaken. Dit werkt heel overzichtelijk. Er is een aparte gebruikerstabel voor de gerechtsdeurwaarderstaak in ontwikkeling. Onderstaande tabel geeft kort weer wat de stand van zaken is ten aanzien van deze gebruikers.

Rol	Aantal	Status	Aantal
RMC			
RMC medewerker	3	Actief	2
Opvragen gebruiksrapportages	2	Tijdelijk wachtwoord verlopen	1
		Tijdelijk wachtwoord	2
TOTAAL	5		5

<i>Rol</i>	<i>Aantal</i>	<i>Status</i>	<i>Aantal</i>
Burgerzaken			
<i>Actuele adresgegevens</i>	4	Actief	5
<i>Opvragen generieke gebruiksrapportages</i>	2	Tijdelijk wachtwoord verlopen	1
TOTAAL	6		6
TOTAAL 11			

De auditoren ontvangen vanaf 2016 ook aparte maandrappportages van BKWI voor het gebruik door RMC en Burgerzaken. Vanaf dat moment vinden de analyses dan ook per onderdeel plaats.

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

*** en

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

3.4 Autorisatiestructuur

Er zijn richtlijnen voor de autorisatiebeheerder ten aanzien van de noodzaak voor medewerkers om toegang te krijgen en indien nodig tot welke informatie zij toegang moeten krijgen (rekening houdend met wettelijke kaders, doelbinding en proportionaliteit). Deze richtlijnen zijn in 2016 verder aangescherpt. Uit de registratie in Topdesk blijkt dat nieuwe aanvragen worden getoetst aan dit kader. De Security officer stemt in geval van twijfel af met BKWI over rechtmatigheid van bepaalde autorisaties. De autorisatiestructuur Suwinet ziet er als volgt uit:

Het aantal rollen ten opzichte van 2016 is toegenomen met 1 rol. De rol voor het opvragen van gebruiksrapportages is binnen de gemeente opgesplitst in twee nieuwe rollen, te benoemen; 'Opvragen generieke gebruiksrapportages' en 'Opvragen specifieke gebruiksrapportages'. De laatste rol brengt een verhoogde kans op onzorgvuldig gebruik met zich mee, en is (tweemaal) toebedeeld aan de auditors van het Sociaal Domein. *RMC* en *Burgerzaken*, die ook de mogelijkheid hebben om gebruiksrapportages op te vragen, behouden de originele rol hiervoor. En hebben niet de mogelijkheid om specifieke rapportages op te vragen.

Voor een rol die toebehoort tot gebruiksbeheer is een extra tabblad aangemaakt, deze rol is ook nieuw t.o.v. vorig jaar. Het betreft hier de rol *Filteronderhoud*, die is ingericht voor het onderhouden van de werkvoorraad. Dit is een rol die toebehoort aan de gemeentelijke deurwaarders, waarvoor de gebruikerstabel nog gemaakt moet worden. Er zijn 2 rollen (in totaal 26 medewerkers) medewerker handhaving en terugvordering en verhaal die een grotere kans op onzorgvuldig gebruik met zich meebrengen

De rollen 'Medewerker Frontoffice A' en 'Medewerker Frontoffice B' zijn opgeheven (voorheen 14 gebruikers). Het grootste gedeelte van deze gebruikersgroep heeft geen nieuwe autorisatie binnen Suwinet gekregen.

Nieuwe rol	Aantal
Geen nieuwe autorisatie	9
Medewerker MDT A/B	3
Specialist Participatie	1
Terugvordering en Verhaal	1

3.5 Netwerk

Medewerkers van de gemeente Eindhoven hebben de mogelijkheid tot telewerken. Middels Virtual Desktop Infrastructure (VDI) logt een medewerker in op het gemeentelijk netwerk. Vervolgens beschikt de medewerker over dezelfde applicaties en rechten, waar men ook over beschikt indien de medewerker fysiek inlogt op een werkplek binnen de gemeente.

Via VDI is het niet mogelijk om 'informatie' op de eigen, niet zijnde netwerk Eindhoven, schijf op te slaan. Wel is het mogelijk om 'zaken' te printen op een lokaal aangesloten printer of om schermprints/foto's te maken.

In een thuiswerkomgeving is sociale controle afwezig en neemt het risico op oneigenlijk gebruik van de vertrouwelijke gegevens toe.

*** en

3.6 Koppelingen

Eindhoven maakt geen gebruik van de Suwinet-Inlezen functionaliteit.

De geautomatiseerde koppeling tussen Suwinet en GWS en de beveiliging van de GWS-server vallen zoals beschreven in paragraaf 2.4 buiten de scope van dit onderzoek.

3.7 Verantwoording

!

De organisaties die Suwinet gebruiken zijn verplicht zich te houden aan de eisen voor privacy en beveiliging. Jaarlijks moet over het gebruik van Suwinet verantwoording worden afgelegd aan het BKWI. Eindhoven voldoet niet aan deze verantwoordingseis. Overigens heeft dit tot op heden vanuit BKWI geen consequenties gehad.