Beveiligingsplan Suwinet 2016

Afdeling Werk en Inkomen, augustus 2015

Gemeente Helmond

GEMEENTE HELMOND

AFDELING WERK EN INKOMEN

BEVEILIGINGSPLAN SUWINET

Vastgesteld in het TMO

Van de Afdeling W&I

18 augustus 2015

Inhoudsopgave

1 Inleiding

De afdeling W&I stelt jaarlijks een informatiebeveiligingsplan Suwinet op en bij met daarin een opsomming van de beveiligingsactiviteiten van de afdeling W&I die noodzakelijk zijn om te voldoen aan het informatiebeveiligingsbeleid van de gemeente op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit informatiebeveiligingsplan vormt de basis voor de planning en bewaking en voortgang van de activiteiten op het gebied van Suwinet.

Dit informatiebeveiligingsplan Suwinet wordt jaarlijks geëvalueerd en aangevuld met nog in te voeren informatiebeveiligingsmaatregelen, die uit een lange termijn planning komen. Tevens wordt jaarlijks input verkregen uit activiteiten die een aanvulling vormen op de BIG planning die komen uit:

- Verbeteracties die volgen uit incidenten
- Verbeteracties die volgen uit audits
- Verbeteracties die volgen uit anderszins gesignaleerde risico's

Dit informatiebeveiligingsplan suwinet is o.a. aangevuld met acties die voortkomen uit de zelfevaluatie suwinet 2015.

2 Beleidskader

2.1 Definitie informatiebeveiliging

Het begrip 'informatiebeveiliging' heeft betrekking op:

- *beschikbaarheid* / *continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit* / *vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit* / *betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

(ZIE BIJLAGE 11 Classificatie van gegevens Suwinet processen)

2.2 Juridisch kader

In deze paragraaf wordt het juridische kader geschetst waar de afdeling W&I zich voor wat betreft informatiebeveiliging voor gegevensuitwisseling binnen de Wet SUWI aan dient te houden.

2.2.1 SUWI Wet- en regelgeving, de WPB en de Participatiewet, wettelijk kader

Op grond van de Wet SUWI en de Participatiewet wisselen UWV, SVB en gemeenten (de SUWI-partijen) persoonsgegeven uit in het kader van de uitvoering van hun wettelijke taken. Met het oog daarop dragen de SUWI-partijen zorg voor de instandhouding van de gemeenschappelijke elektronische voorzieningen SUWI (GeVS) voor de uitwisseling van die gegevens. Vanaf de inwerkingtreding van de Wet SUWI droeg deze voorziening de naam Suwinet. Het Besluit SUWI en de Regeling SUWI bevatten nadere regelgeving ten aanzien van de GeVS. Met name wordt genoemd artikel 6.4, tweede lid, van de Regeling SUWI, dat onder andere gemeenten verplicht in een beveiligingsplan aan te geven hoe zij zorgdragen voor de beveiliging van de gegevensuitwisseling via de GeVS, overeenkomstig hetgeen over de voor het stelsel van maatregelen en procedures te hanteren normen wordt bepaald in bijlage I bij de Regeling SUWI (Stelselontwerp & Beveiliging Gezamenlijke elektronische Voorzieningen SUWI). Naast de Wet SUWI en de daarop berustende regelgeving is de Wet bescherming persoonsgegevens (WBP) van toepassing als algemene wet op de gebieden die niet geregeld zijn.

2.2.2 Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens (WBP) stelt dat persoonsgegevens alleen voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verkregen. Ingevolge de WBP moeten persoonsgegevens in overeenstemming met de WBP en op behoorlijke en zorgvuldige wijze worden verwerkt. Op hoofdlijnen betekent dit:

- persoonsgegevens mogen slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld;
- voor de verwerking dient een van de in de WBP genoemde rechtvaardigingsgronden te bestaan;
- slechts onder bepaalde voorwaarden mogen persoonsgegevens voor andere doeleinden worden gebruikt dan waarvoor ze zijn verzameld;
- persoonsgegevens mogen slechts worden verwerkt voorzover zij voor het doel toereikend, ter zake dienend en niet bovenmatig zijn;
- de organisatie treft de nodige maatregelen zodat de persoonsgegevens, gelet op het doel waarvoor ze worden verwerkt, juist en nauwkeurig zijn;
- de organisatie legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking; de verantwoordelijke dient er tevens voor te zorgen dat ook de bewerker voldoende waarborgen biedt met betrekking tot technische en organisatorische beveiliging;
- de organisatie informeert de betrokkene over de verwerking van zijn persoonsgegevens en zij biedt de betrokkene de gelegenheid tot inzage in zijn persoonsgegevens; indien de gegevens feitelijk onjuist blijken te zijn of voor het doeleinde onvolledig, niet ter zake dienend of anderszins in strijd met de wet worden verwerkt, komt betrokkene het recht op correctie toe; in enkele gevallen kan betrokkene tevens gebruik maken van het recht van verzet.

Volgens de WBP dient iedere geautomatiseerde gegevensverwerking “bestemd voor de verwezenlijking van een doeleinde” te worden gemeld bij het College bescherming persoonsgegevens (CBP).
Verder is de Participatiewet relevant. In de Participatiewet is een aparte paragraaf opgenomen over de regels die van toepassing zijn bij de uitwisseling van persoonsgegevens. Deze paragraaf kan als volgt op hoofdlijnen worden geschetst:

- werkgevers hebben een informatieplicht om inlichtingen te verstrekken omtrent de aanvrager van een uitkering of een uitkeringsgerechtigde betreffende omstandigheden die noodzakelijk zijn voor de uitvoering van de Participatiewet;
- diverse instanties, zoals UWV, overige gemeenten, College voor zorgverzekeringen, pensioenfondsen, etc. hebben een informatieplicht naar de Sociale dienst indien dit noodzakelijk is voor de uitvoering van de Participatiewet;
- medewerkers die met persoonsgegevens in aanraking komen hebben een geheimhoudingsplicht, tenzij het voor de uitvoering van de Participatiewet noodzakelijk is deze persoonsgegevens te verstrekken aan anderen.
- de gemeente heeft een inlichtingenverplichting binnen gestelde regels ten aanzien van diverse instellingen, zoals het UWV, Sociale Verzekeringsbank, Belastingdienst en overige gemeenten.

2.3 Relevantie informatiebeveiliging voor Werkplein

Samenwerking op het Werkplein
Vanaf 1 september 2009 maakt de afdeling W&I onderdeel uit van het Werkplein, samen met het UWV en overige partners. Doel van de samenwerking is om werkzoekenden te ondersteunen en stimuleren om zo snel mogelijk (weer) aan het werk te gaan. Om de wettelijke taken te kunnen uitvoeren beschikken de ketenpartijen ieder over eigen geautomatiseerde systemen.

Gebruik Suwinet voor uitvoering wettelijke taken
De centrale voorziening Suwinet Inkijk biedt de mogelijkheid persoonsgegevens in de systemen van ketenpartners te raadplegen. Met Suwinet-Inkijk worden gegevens op basis van burgerservicenummers (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Het gaat over privacygevoelige gegevens met betrekking tot arbeidsverleden, loon, uitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering. Deze gegevens zijn onder andere nodig om het recht op een uitkering vast te stellen en de juiste dienstverlening te kunnen leveren. Suwinet mag door gemeenten alleen worden gebruikt voor de uitvoering van de in Suwinet genoemde wetten (art 62.2, wet SUWI). Dat is voor de gemeente op dit moment; de Participatiewet (inclusief Bbz 2004), IOAW en IOAZ. Iedere gemeente moet overeenkomstig artikel 6.4, Regeling SUWI, in een beveiligingsplan aan geven op welke wijze zij invulling geeft aan de beveiliging van de

gegevensuitwisseling in het kader van SUWI. Zowel de afdeling W&I als het UWV heeft een aparte login- en beveiligingsstructuur voor Suwinet. Wanneer medewerkers binnen de kaders van de wet- en regelgeving met taken zijn belast die te maken hebben met de uitvoering van de Participatiewet, dienen zij toegang te krijgen tot de klantdossiers en geautomatiseerde systemen die ze daarvoor nodig hebben. (art.9 Wet Suwi,eerste lid; art.7 Participatiewet , tweede lid; art.62 Wet Suwi) Wettelijk is de toegang tot de gegevens dus geregeld.

Processen en informatiesystemen
De primaire en ondersteunende processen van de afdeling Werk en Inkomen (W&I) zijn in hoge mate afhankelijk van een adequate informatievoorziening en betrouwbare informatiesystemen.
Om een beheersbare en betrouwbare informatievoorziening te realiseren is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen. Als de vertrouwelijkheid van opgeslagen gegevens geschaad wordt, of als de gegevens niet beschikbaar zijn of niet correct zijn, dan kan dit grote gevolgen hebben voor de dienstverlening van de gemeente(n) (lees: afdeling W&I) en het vertrouwen dat burgers, instellingen en bedrijven in de afdeling W&I hebben, zoals b.v. het verstrekken van uitkeringen op basis van verkeerde gegevens in de informatiesystemen.

Analyse en beveiligingsmaatregelen
Bescherming van persoonsgegevens houdt onder meer in dat deze gegevens op een veilige manier worden verzameld, verwerkt en gedeeld. Een veilige manier van omgaan met persoonsgegevens wil zeggen dat er door de gemeente procedures en processen zijn ingericht die de vertrouwelijkheid, integriteit en continuïteit van de gebruikte systemen waarborgen. De invoering van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) biedt de gemeente Helmond de mogelijkheid om tegen een geaccepteerd kader te toetsen hoe het staat me de invoering van informatiebeveiligingsmaatregelen.

2.4 Doelstelling informatiebeveiligingsplan

Dit informatiebeveiligingsplan Suwinet is er op gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensuitwisseling binnen onze afdeling en de overige SUWI-partners te waarborgen. Helmond streeft er naar om ‘in control’ te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de Plan, Do, Check, Act cyclus (PDCA-cyclus).

Doelstelling van dit informatiebeveiligingsplan is om inzicht te geven in de status en de volledigheid van de te nemen informatiebeveiligingsmaatregelen voor de afdeling W&I door de genoemde actiehouders en daarmee de betrouwbaarheid voor de informatievoorziening van de afdeling W&I te garanderen. Dit wordt op de volgende wijze bereikt:

- Ten eerste geeft het informatiebeveiligingsplan een overzicht van de informatiebeveiligingsmaatregelen voor het verantwoordelijkheidsgebied bedrijfsvoering.
- Ten tweede geeft dit informatiebeveiligingsplan inzicht in de toewijzing van de informatiebeveiligingsmaatregelen aan een verantwoordelijke partij. Informatiebeveiligingsmaatregelen die niet zijn toegewezen zijn al geïmplementeerd binnen de afdeling W&I of de informatiebeveiligingsmaatregelen is niet toegewezen omdat het een geaccepteerd risico betreft.
- Ten derde geeft dit informatiebeveiligingsplan houvast op het monitoren van de implementatie van (ontbrekende) informatiebeveiligingsmaatregelen binnen de afdeling W&I.

3 Kwaliteits- en verbetercyclus

3.1 Goedkeuring

Door de afdeling Informatievoorziening en Automatisering is een Informatiebeveiligingsbeleid opgesteld dat in juni 2015 is goedgekeurd door B&W. Dit beleid fungeert als leidraad voor dit beveiligingsplan. Dit informatiebeveiligingsplan is de concrete invulling van het opgestelde beleid op het gebied van Suwinet. Het management van de afdeling W&I dient aantoonbaar te maken dat zij het belang van informatiebeveiliging ondersteunt en zal dit beveiligingsplan Suwinet vaststellen in hun Team management overleg (TMO) en voor kennisname en vaststelling doorgeleiden naar het kernteam Dienstverlening en digitalisering, het MT en het college van Burgemeester en wethouders.

3.2 Verantwoording

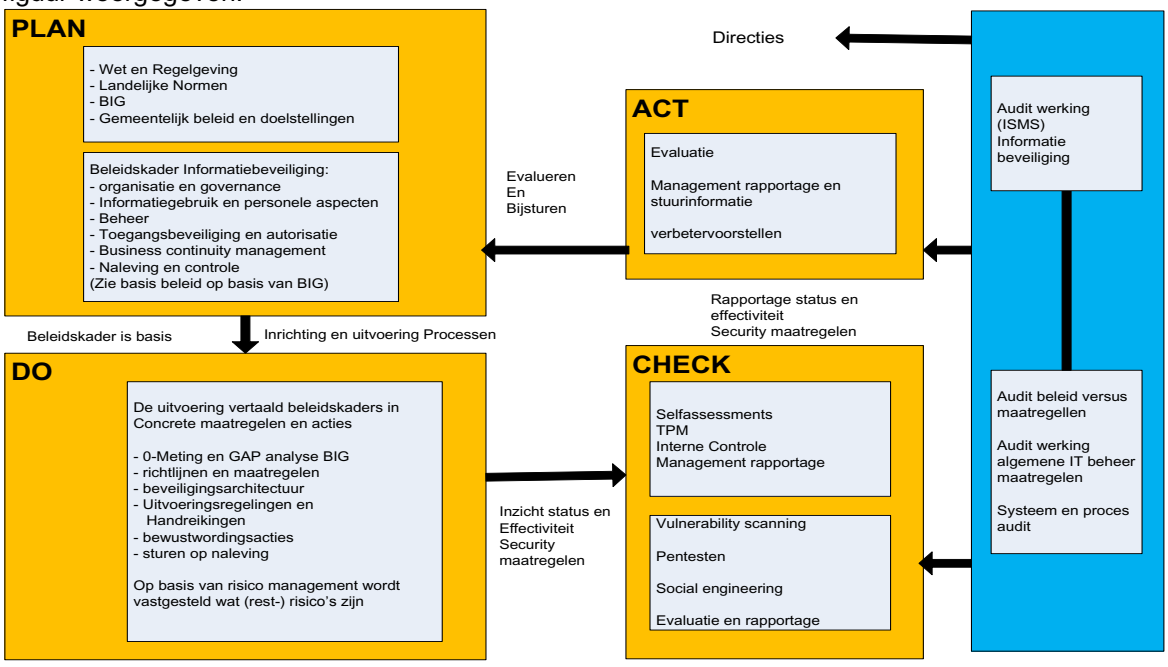
De resultaten van de uitgevoerde controles worden vermeld in een risicoparagraaf Suwinet in de Berap, en jaarrekening voor B&W en Raad. Tevens worden de samenwerkende gemeenten op de hoogte gesteld. De afdelingsmanager levert deze gegevens aan.

3.3 Periodieke audit en onderzoek

Ten behoeve van de kwaliteit van het Informatiebeveiligingsplan en ten behoeve van behoud van de kwaliteit van de wijzigingen wordt voorgesteld om de plannen jaarlijks te auditen.
Een interne audit wordt uitgevoerd door de interne auditer van de gemeente Helmond op inhoud, afstemming met het informatiebeveiligingsbeleid van de gemeente Helmond en door het hoofd ICT van de gemeente voor de ICT gerelateerde informatiebeveiligingsmaatregelen.

3.4 PDCA

Informatiebeveiliging is een continu verbeterproces. De zogenaamde PDCA-cyclus (Plan, do, check en act) vormt de basis voor dit evaluatie en verbeterproces. Deze kwaliteitscyclus is in de volgende figuur weergegeven:



Information Security Management System

Toelichting figuur:

- Plan: De cyclus start met het opstellen van informatiebeveiligingsbeleid. Dit beleid is gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en 'best practices' en betreft een uitwerking van regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning van activiteiten geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van het CIO/ICT jaarplan en uitgewerkt in het informatiebeveiligingsplan (IB-beleid) van de gemeente. Afdelingsspecifieke activiteiten worden gepland in het afdelings-IB plan of het afdelings- informatieplan (IM-functie).
- Do: Het beleidskader vormt de basis voor risicomanagement, uitvoering van (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering hiervan geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het proces.
- Check: Control is onderdeel van het proces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving.
  - Interne controle op het primaire proces;
  - Externe controle: betreft controle buiten het primaire proces door een auditor.[1] Dit heeft het karakter van een steekproef. Jaarlijks worden meerdere van dergelijke onderzoeken uitgevoerd, waarbij de CIO/ICT in principe opdrachtgever is. Bevindingen worden gerapporteerd aan de CIO en de directies.
- Act: De cyclus is rond met de uitvoering van verbeteracties o.b.v. check en externe controle. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de jaarplanning en beveiligingsplannen. De bevindingen worden in beginsel gerapporteerd aan de directie. Voor ingrijpende verbeteracties wordt een gevraagde beslissing voorgelegd. Deze actie zal binnen de afdeling W&I worden opgepakt.

3.5 Brede evaluatie

Binnen de gemeente Helmond is men op diverse onderdelen van het informatiebeveiligingsbeleid actief en wordt er ook onderkend dat er verbeteringen mogelijk zijn. Verbetermogelijkheden worden in beeld gebracht door evaluaties structureel en breed op te zetten en de resultaten van meerdere evaluatieactiviteiten in samenhang en met het voltallige management te bespreken. Daarbij wordt gebruik gemaakt van de resultaten uit de jaarlijkse zelfanalyse, interne audits en enquêtes die jaarlijks en breed uitgezet worden onder het personeel. Uit de enquête van 2015 blijkt duidelijk dat de mensen weten dat wat ze in Suwinet doen wordt vastgelegd / gelogd. Ze hebben bij indiensttreding op twee personen na een zorgvuldigheids/geheimhoudingsverklaring ingevuld en ze weten wat er in de verklaring staat. De betreffende twee hebben de verklaring op een later moment getekend.
Het vinden van het beveiligingsplan op intranet of in Schulinck is bij 40% van de ondervraagden niet helemaal duidelijk. De tien gouden regels (zie hoofdstuk10), over beveiliging, is bij 50% niet bekend. Conclusie is dat de vindplaats van het informatiebeveiligingsplan suwinet niet helder genoeg is.
De leidinggevende besteedt voldoende aandacht aan Suwinet; bijna 90% van de ondervraagden geeft dit aan. De maandelijkse nieuwsbrief, waarin ook onderwerpen over Suwinet staan, wordt door 85% van de medewerkers gelezen. De beveiliging van Suwinet leeft onder de medewerkers. De conclusies/bevindingen van het enquête onderzoek zijn teruggekoppeld in de organisatie middels een nieuwsbrief.

3.6 Jaarlijkse bijstelling

De organisatie en de omgeving van de sociale zekerheid is voortdurend in ontwikkeling, onder andere door wijziging in wetgeving of aanpassingen in de informatiesystemen. Dit betekent dat dit plan jaarlijks moet worden geëvalueerd en geactualiseerd. Dit informatiebeveiligingsplan is dan ook een dynamisch document en wordt telkens bijgesteld op basis van de lange termijn planning, zoals opgenomen in het informatiebeveiligingsbeleid:

- (nieuwe) Informatiebeveiligingsmaatregelen die voortkomen uit uitgevoerde risicoanalyses
- Verbeteracties die volgen uit incidenten
- Verbeteracties die voortkomen uit audits
- Verbeteracties die voortkomen uit anderszins gesignaleerde risico's
- Verbeteracties die voortkomen uit de evaluatie van het plan

Bovenstaande acties worden opgenomen in een overall planning (zie bijlage 10).

[1] Van onder meer de accountant, rijksoverheid (voor bijv. basisregistraties) en gemeentelijke auditors (intern).

4 Verdeling verantwoordelijkheden

Er is een aantal functies binnen de afdeling W&I die geautoriseerd zijn om gebruik te maken van Suwinet-Inkijk. Zij hebben daardoor een verantwoordelijkheid met betrekking tot het gebruik van Suwinet-Inkijk. In de onderstaande tabel volgen per functie de rechten met betrekking tot het gebruik van Suwinet-Inkijk en de verantwoordelijkheidsverdeling.
Het gaat om de volgende functies:

Functie	Taken/verantwoordelijkheden	Doel
Applicatiebeheerder Suwinet	Inrichten gebruikersrechten, opnemen gebruikers in het systeem (adm functie), opvragen gebruikersrapportage Suwinet	Zodanig toekennen van rechten dat de informatie betrouwbaar en vertrouwelijk is. autoriseren van gebruikers adh ondertekent door SO aanmeldingsformulier
Medewerker financiële administratie	Raadplegen van klantgegevens conform autorisatiematrix * t.b.v. gebruik Suwinet	Rechtmatig een uitkering kunnen verstrekken n.a.v. gegevens Inlichtingenbureau
Secretarieel administratief	Raadplegen van klantgegevens conform autorisatiematrix* t.b.v. gebruik Suwinet	Rechtmatig een uitkering kunnen verstrekken
SR Klantbegeleider	Raadplegen van klantgegevens conform autorisatiematrix* t.b.v. gebruik Suwinet	Rechtmatig een uitkering kunnen verstrekken en het verkrijgen van informatie t.a.v. het te volgen traject reïntegratie.
Kwaliteitscoaches	Raadplegen van klantgegevens conform autorisatiematrix* t.b.v. gebruik Suwinet	Rechtmatigheid beoordelen van de in behandelingsname en toekenning van een aanvraag/ toetsen van het werk van klantbegeleiders
Juridisch medewerker	Raadplegen van klantgegevens conform autorisatiematrix* t.b.v. gebruik Suwinet	Vaststellen terugvordering en verhaal van ten onrechte genoten uitkering
Security Officer	Opvragen specifieke gebruikersrapportages conform autorisatiematrix* t.b.v. gebruik Suwinet	Beheert en beheerst beveiligingsprocedures en –maatregelen in het kader van Suwinet.
Medewerker speciaal onderzoek opsporing en handhaving	Raadplegen van klantgegevens conform autorisatiematrix* t.b.v. gebruik Suwinet	Rechtmatigheid beoordelen van de aanvraag en toekenning van een uitkering

**Voor de autorisatiematrix zie bijlage1*

De afdelingsmanager W&I is eindverantwoordelijk voor het gebruik van Suwinet-Inkijk en de toepassing van de beveiligingsregels binnen de afdeling.

5 Procedure autorisatie tot Suwinet

De inhoud van deze procedure moet bekend zijn bij alle medewerkers die bij deze procedure betrokken zijn.

Het doel van deze procedure is het vastleggen van de verschillende stappen die noodzakelijk zijn voor het autoriseren van personen voor Suwinet. Hiermee wordt de logische toegangsbeveiliging afgedicht voor de Suwinet gegevens en de vertrouwelijkheid hiervan gewaarborgd.

Autorisatie:
Met een autorisatie wordt een door het bevoegd gezag gelegitimeerde toegang tot één of meerdere informatiesystemen van de gemeente bedoeld. De procedure bestaat uit drie afzonderlijke deelprocedures die gescheiden kunnen worden uitgevoerd:

- Autorisatie tot het netwerk;
- Autorisatie tot Suwinet;
- Periodieke controle autorisaties.

Om toegang te kunnen krijgen tot de gegevens is naast de specifieke autorisatie in de desbetreffende applicatie(s) tevens een bevoegdheid nodig op netwerk- en/of het systeemniveau. Deze bevoegdheden worden beheerd door de systeembeheerder. De bevoegdheden binnen Suwinet worden beheerd door de gebruiksbeheerder Suwinet van de afdeling Werk en Inkomen (W&I).

De proceseigenaar is de manager van de afdeling Werk en Inkomen .

De verantwoordelijkheid voor deze procedure ligt te allen tijde bij het college van B&W en namens deze bij de manager van de afdeling Werk en Inkomen.

De verantwoordelijkheid om toegang tot het netwerk te verlenen berust bij de afdeling Informatievoorziening en Automatisering.
De uitvoering hiervan ligt bij de systeembeheerder.

De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet berust bij manager van de afdeling Werk en Inkomen**,** dan wel zijn vervanger.
De uitvoering hiervan ligt bij de gebruiksbeheerder Suwinet van de afdeling Werk en Inkomen.

De manager van de afdeling Werk en Inkomen is verantwoordelijk voor het actueel houden van deze procedure.

De security officer:
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, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet.

(Voor de functiebeschrijving van de Security Officer zie bijlage 9).

Uitvoering

Autorisatie tot het netwerk

Voor de autorisatie voor het gebruik van het gemeentelijk netwerk wordt verwezen naar het algemeen integraal Informatiebeveiligingsbeleid van de gemeente Helmond. Hierin staat het beleid en het proces autorisatie tot het netwerk beschreven.

Autorisatie tot Suwinet

- De om autorisatie verzoekende medewerker dient met behulp van het daarvoor bestemde formulier (zorgvuldigheids- geheimhoudingsverklaring, zorgvuldigheidsverklaring) schriftelijk een autorisatieverzoek in voor een nieuwe of gewijzigde autorisatie voor Suwinet bij de teammanager Staf. De medewerker ondertekent de verklaring evenals de teammanager van de medewerker. Deze teammanager geeft op het formulier aan welke functie de medewerker gaat invullen.

- De teammanager Staf beoordeelt het autorisatieverzoek. Hierbij worden de raadpleegbare gegevens afgestemd op de taakinhoud van de aanvrager, zoals vastgelegd in de “autorisatiematrix ten behoeve van gebruik Suwinet”;

- Op de zorgvuldigheids- geheimhoudingsverklaring, zorgvuldigheidsverklaring is door de teammanager Staf aangegeven tot welke autorisatie de medewerker mag worden toegelaten (conform de autorisatiematrix ten behoeve van Suwinet). Hij geeft dit formulier aan de gebruiksbeheerder Suwinet. Daarnaast verstrekt hij het beveiligingsplan Suwinet aan de medewerker die de aanvraag heeft ingediend.

- De Gebruiksbeheerder Suwinet kan aan de hand van dit formulier de autorisatie in Suwinet regelen. De gebruiksbeheerder zorgt dat de autorisatie wordt verwerkt. Team Staf biedt de verklaring aan voor archivering bij het team documentaire informatievoorziening.

- De systemen zijn voor geautoriseerde gebruikers slechts toegankelijk met gebruik van persoonlijke toegangscodes. De wachtwoorden zijn maximaal 60 dagen geldig en bestaan uit minimaal 8 tekens die aan bepaalde eisen moet voldoen. Wanneer het account 60 dagen niet wordt gebruikt, vervalt het account automatisch. Na 5 maal foutief inloggen wordt het account geblokkeerd. De beheerder dient deze weer vrij te geven en eventueel een nieuw wachtwoord toe te kennen.

- De gebruiker krijgt van de gebruiksbeheerder Suwinet, die het autorisatieniveau heeft verwerkt, een terugmelding over het autorisatieverzoek. Tevens krijgt de gebruiker een korte instructie hoe hij zich aan kan melden en hoe om te gaan met Suwinet.

- Bij vertrek of wijziging van de functie van een medewerker geeft de leidinggevende van deze medewerker dit door aan de teammanager Staf. De laatstgenoemde geeft de mutatie schriftelijk door aan de gebruiksbeheerder Suwinet, waarna de gebruiksbeheerder de autorisatie intrekt of wijzigt;

Periodieke controle autorisaties

De gebruiksbeheerder Suwinet zorgt per maand voor een overzicht en een geprint verslag van de in het systeem toegekende autorisaties. De interne controleur toetst op basis van dit overzicht of:

- de geïmplementeerde autorisaties overeenkomen met de toegekende autorisaties;
- de geregistreerde gebruikers en de aan hen toegekende autorisaties correct zijn. Hierbij wordt het controleverslag vergeleken met de autorisatieformulieren en tevens vergeleken met wat is vastgelegd in het beveiligingsplan Suwinet (autorisatiematrix) van de gemeente;

Bij eventuele fouten meldt de interne controleur die aan de security officer en aan het hoofd W&I zodat deze fout kan worden hersteld.

De gebruikersbeheerder Suwinet vraagt maandelijks de gebruikersrapportage Suwinet op bij het BKWI. De medewerker interne controle van het team Staf analyseert en signaleert de afwijkende patronen in de autorisaties. De afwijkingen worden vastgelegd in het document “Controleoverzicht Gebruikersrapportage Suwinet afdeling W&I” (bijlage 3). De Security Officer rapporteert aan de afdelingsmanager van de afdeling W&I. De bevindingen uit de rapportages worden per kwartaal in het managementteam van de afdeling W&I teruggekoppeld/gedeeld. Als er wijzigingen/beëindigingen in de autorisaties moeten plaatsvinden dan zal aan de hand van het controleoverzicht een schriftelijke mutatie/beëindiging aan de gebruiksbeheerder Suwinet worden doorgegeven. De gebruiksbeheerder Suwinet past de autorisatie aan of beëindigt deze. De medewerker wordt van de mutatie/beëindiging op de hoogte gesteld door zijn/haar teammanager.

Maandelijks vind er ook een controle plaats door de interne controleur op wijzigingen in taak/functie en op beëindiging dienstverband (vast of tijdelijk personeel). De teammanager van de betreffende medewerker is verantwoordelijk voor het doorgeven van de wijzigingen/beëindigingen aan de Security Officer.

Zie bijlage 2 proces autoriseren tot Suwinet

Zie bijlage 3 Controle-overzicht gebruikersrapportage Suwinet Afdeling W&I Gemeente Helmond

Zie bijlage 4 Maandelijkse verantwoording autorisaties Suwinet

Zie bijlage 6 procesbeschrijving controle

6 Gebruik Suwinet-Inkijk

In de onderstaande tabel wordt per functie aangegeven in welke gevallen Suwinet-Inkijk gebruikt mag worden. We spreken in die gevallen van geoorloofd gebruik.
Wordt Suwinet om andere redenen gebruikt dan hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

Functie	Gebruik
• Secretarieel administratief • SR klantbegeleider	• Bij afhandeling aanvragen Participatiewet IOAW, IOAZ, BBZ uitkering • Bij heronderzoeken • In die gevallen ter beoordeling van de medewerker. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage van de medewerker.
• Medewerker financiële administratie	• Bij afhandeling maandelijkse signalen van het Inlichtingenbureau (IB)
• Juridisch medewerker	• Bij debiteuren(her)onderzoeken ter vaststelling van actuele woon- en/of verblijfplaats., dienstverband, werkgever, draagkracht, inkomen. • In die gevallen ter beoordeling van de medewerker. De reden van raadplegen van Suwinet-Inkijk wordt in die gevallen gemotiveerd in de rapportage van de medewerker.
• Kwaliteitscoach	• Bij toetsing van de rapportages/adviezen
• Medewerker speciaal onderzoek opsporing en handhaving (*)	• Bij afhandeling fraudesignalen

(*) Zware rol; een raadpleging, binnen Suwinet, op een zoeksleutel anders dan het burgerservicenummer (BSN) is een zwaar middel en moet een uitzondering zijn. Voor een raadpleging van klantgegvens zou het BSN als zoeksleutel het uitgangspunt moeten zijn. Raadplegen op andere zoeksleutels is voorbehouden aan medewerkers die verantwoordelijk zijn voor handhaving en fraudepreventie.

Maatregelen tegen ongeoorloofd gebruik
Om ongeoorloofd gebruik te voorkomen zijn afspraken met betrokkenen noodzakelijk. In de bijlagen zijn documenten opgenomen waarin de afspraken zijn vastgelegd en waarmee de betrokken medewerkers formeel verplicht worden zich aan de afspraken te houden.

In de bijlagen zijn de volgende documenten opgenomen:
- model geheimhoudings- en zorgvuldigheidsverklaring (voor externen) (bijlage 7)
- model zorgvuldigheidsverklaring (voor vaste medewerkers van de gemeente Helmond) (bijlage 8)

De teammanager van de betreffende medewerker zorgt ervoor dat de geheimhoudings- en zorgvuldigheidsverklaring of zorgvuldigheidsverklaring ondertekend wordt.
Medewerkers die niet als ambtenaar van de gemeente Helmond zijn aangesteld, zoals uitzendkrachten, consultants en extern adviseurs, welke toegang krijgen tot Suwinet-Inkijk, dienen de geheimhoudings- en zorgvuldigheidsverklaring te ondertekenen.
Vaste medewerkers, die onder de ambtenarenwet vallen, dienen de zorgvuldigheidsverklaring te ondertekenen.

Nieuwe medewerkers krijgen, na het invullen van bovenstaande verklaring, het beveiligingsplan Suwinet van team Staf overhandigd. Het beveiligingsplan staat ook op intranet en in het handboek van Schulinck.

7 Controle op gebruik Suwinet-Inkijk

7.1 BKWI registreert het gebruik van Suwinet-Inkijk

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft rapportages ontwikkeld omtrent de logging van het gebruik van Suwinet-Inkijk.
Het BKWI is verplicht om loggegevens, waarmee het gebruik van Suwinet-Inkijk per medewerker van o.a. de gemeente kan worden nagegaan te bewaren.

Het gaat daarbij om de volgende gegevens:
- het tijdstip van iedere login en logout en andere acties;
- de gebruikersnaam van degene die inlogt/uitlogt;
- elk BSN (of andere zoeksleutel) waarvan gegevens worden opgevraagd wordt als actie geregistreerd;
- elke actie, zoals de bekeken kolom- of overzichtspagina´s.

Het doel van deze logging is tweeledig:
- tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende verwerking;
- statistische doeleinden.

7.2 Suwinet-gebruiker moet weten dat zijn handelingen worden geregistreerd

In hoofdstuk 6 staat al vermeld voor welke functies en in welke situaties het gebruik van Suwinet-Inkijk is geoorloofd. Het inachtnemen van deze regels is in eerste instantie een verantwoordelijkheid van de medewerker zelf. Daarnaast hebben de teammanagers hierin een controlerende en sturende rol. Vanuit beveiligingsoogpunt behoudt het management zich het recht voor om zo nodig controles uit te voeren op bijvoorbeeld autorisaties, inkijkacties teneinde te bepalen of de gebruiker zich houdt aan de gedragsregels m.b.t. het gebruik van Suwinet-Inkijk.

Met het oog hierop moeten de medewerkers die (gaan) werken met Suwinet-Inkijk op de hoogte zijn van de navolgende informatie:
- het bestaan van de logging-applicatie;
- het doel van de logging (tegengaan en controleren van onrechtmatige of doeloverschrijdende verwerking);
- de aard van de gegevens die binnen deze applicatie worden gelogd;
- het feit dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- het feit dat onrechtmatig of doeloverschrijdend gebruik van het Suwinet-Inkijk kan worden gecontroleerd;
- Indien de individuele medewerkers hun zoekgedrag niet kunnen verantwoorden en er aanwijzingen zijn voor normoverschrijdend gedrag heeft dit tot gevolg dat er disciplinaire maatregelen worden getroffen.

7.3 Rapportages over het gebruik van Suwinet-Inkijk

BKWI verstrekt maandelijks een rapportage over het gebruik van Suwinet-services. Hierin zitten geen gegevens die op personen herleidbaar zijn. De rapportages geven een algemeen beeld en zijn slechts beperkt bruikbaar voor het signaleren van misbruik. Een opvallende afwijking ten opzichte van voorgaande rapporten kan een indicatie zijn dat nader onderzoek wenselijk is.
Op verzoek van de Security Officer kan BKWI een gedetailleerde rapportage leveren, waarmee het gebruik kan worden geanalyseerd. De rapportage wordt dan met de extensie *.suwi* verstuurd (Suwimail). De mail gaat dan over een besloten overheidsnetwerk.

7.4 Controles op rapportages BKWI

Binnen team Staf wordt de gebruikrapportage Suwinet van het BKWI door de interne controleur nader bekeken. De raadplegingen binnen de afdeling W&I worden vergeleken met het gemiddelde van de gemeentelijke afnemers van gelijke grootte (gemeentegrootteklassen) met onze arbeidsmarktregio en de raadplegingen van heel Nederland.
Indien in de vergelijkingen grote afwijkingen zitten wordt er een specifieke rapportage opgevraagd bij het BKWI door de Security officer.
Ook het gebruik van Suwinet door de medewerkers kan nader worden geanalyseerd.
De bevindingen worden in het document 'Controle overzicht gebruikersrapportage Suwinet afdeling W&I' vastgelegd. Indien uit de specifieke rapportages blijkt dat er aanvullende maatregelen moeten worden genomen dan wordt dit ook opgenomen in dit document.
De bevindingen in het rapport worden voorgelegd aan de security officer. De security officer legt deze bevindingen vervolgens voorn aan het management van de afdeling W&I. De managers zullen de beveiliging van Suwinet ieder kwartaal bespreken in hun team-overleggen.

Zie bijlage 3 controle-overzicht Gebruikersrapportage Suwinet.
Zie bijlage 5 Criteria Controle/overzicht Gebruikersrapportage Suwinet afdeling WI
Zie bijlage 6 Procesbeschrijving controle

8 Protocol inzage in Suwinet-Inkijk door cliënt en / of gemachtigde

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, in de hieronder beschreven gevallen, is gegevensinzage door derden mogelijk. De via Suwinet-Inkijk opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op usb stick). Er mag wel een afdruk worden gemaakt voor de cliënt of zijn gemachtigde.
Hieronder volgt een instructie voor een aantal situaties waar de gebruiker van Suwinet-Inkijk mee te maken kan krijgen.

8.1 De cliënt verzoekt om inzage in zijn gegevens, schriftelijk of mondeling

Het is mogelijk dat een cliënt telefonisch vraagt om een uitdraai van zijn / haar gegevens. Telefonisch wordt geen info verstrekt en de cliënt dient zich persoonlijk te melden bij de afdeling W&I. Indien dit niet mogelijk is moet hij/zij een schriftelijk verzoek indienen, dat binnen de wettelijk verplichte termijn dient te worden beantwoord.

Handel het verzoek als volgt af.

- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs.
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm.
- Vernietig het uitgedraaide exemplaar als de cliënt het niet meeneemt.
- Beëindig inkijksessie.

Als de cliënt inzage wil in gegevens die bij een ketenpartner zijn geregistreerd (maar die niet op Suwinet staan), dient de cliënt te worden verwezen naar de betreffende ketenpartner.

8.2 Gemachtigde verzoekt schriftelijk om inzage in cliëntgegevens

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven.
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs.
- Stel de identiteit en het BSN van de cliënt vast aan de hand Gws4all of anders van een geldig legitimatiebewijs.
- Maak een uitdraai van de geraadpleegde gegevens of laat gemachtigde meekijken op het scherm.
- Vernietig het uitgedraaide exemplaar als de gemachtigde het niet meeneemt.
- Beëindig inkijksessie.

8.3 Een derde verzoekt om inzage in cliëntgegevens

(Met derde wordt **niet** bedoeld een cliënt of een samenwerkende partij).
Dit is niet mogelijk.

9 Protocol correctieverzoek Suwinet-Inkijk door cliënt en / of gemachtigde

9.1 De cliënt verzoekt om correctie

- Informeer de cliënt dat hij/zij een officieel verzoek voor correctie moet indienen.
- Stel de identiteit en het BSN van de cliënt vast aan de hand van een geldig legitimatiebewijs.
- Als de klant een mondeling verzoek doet terwijl hij/zij bij je is:
    - Maak een verzoekschrift en laat het ondertekenen.
    - Maak een kopie van het verzoek.
    - Verstrek een kopie aan de cliënt.
- Gebruik het origineel om het verzoek af te handelen en archiveer het in het cliëntdossier.
- Informeer de klant over de doorgevoerde wijziging.

9.2 Gemachtigde verzoekt om correctie

- Informeer zo nodig de gemachtigde dat hij/zij een officieel schriftelijk verzoek moet indienen.
- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven.
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs.
- Stel de identiteit en het BSN van de cliënt vast aan de hand Gws4all of anders van een geldig legitimatiebewijs.
- Handel het verzoek af en archiveer het in het cliëntdossier.
- Informeer de gemachtigde over de doorgevoerde wijziging.

9.3 Een derde verzoekt om correctie

Dit is niet mogelijk

10 Gouden gedragsregels waar medewerkers op worden geattendeerd.

Voor het werken met en de omgang met persoonsgegevens is vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Daaruit zijn gedragsregels afgeleid, die gelden voor medewerkers van de afdeling W&I in relatie tot al hun werkzaamheden, dus ook bij het gebruik van Suwinet. Afhankelijk van de functie heeft een medewerker toegang tot diverse informatiesystemen binnen de afdeling W&I. Het management van de afdeling W&I wil medewerkers erop attenderen dat het gebruik van deze systemen verbonden is aan een aantal verplichtingen.

Hieronder wordt een opsomming gegeven van de 10 belangrijkste gedragsregels die binnen het Werkplein regelmatig actief worden uitgedragen tijdens teamoverleggen, afdelingsoverleggen, op intranet, in kalenders en in maandelijkse nieuwsbrieven:

1. Wachtwoorden zijn strikt persoonlijk

Wachtwoorden zijn strikt persoonlijk en dienen uitsluitend door medewerkers zelf gebruikt te worden om toegang te krijgen tot de betreffende systemen. Wachtwoorden mogen dus niet aan derden of een collega worden gegeven en moeten worden bewaard op een veilige plek. Medewerkers moeten het door de gebruikersbeheerder uitgegeven wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Het wachtwoord moet minimaal uit 8 karakters bestaan waarvan 1 hoofdletter, 1 cijfer en 1 vreemd teken. Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 5 keer worden herhaald.
Als medewerkers de gemeente verlaten, wordt het account verwijderd. Wanneer een account 60 dagen niet wordt gebruikt, vervalt het account automatisch. Na 5 maal foutief inloggen wordt het account geblokkeerd. De gebruikersbeheerder dient deze weer vrij te geven en eventueel een nieuw wachtwoord toe te kennen.

2. Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten door medewerkers worden gemeld bij hun teammanager en de gebruikersbeheerder. Deze onderzoeken het incident, waar nodig met inschakeling van interne of externe deskundigheid (systeembeheer, Inlichtingenbureau).
Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak. De betreffende teammanager beoordeelt welke verdere actie noodzakelijk is.

3. Geheimhoudingsplicht

Er wordt met persoonsgegevens gewerkt. Voor het werken met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens (WBP). Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de gegevens, inclusief persoonsgegevens, niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is. Medewerkers dienen kennis te nemen van deze plicht en de van toepassing zijnde geheimhoudings- en zorgvuldigheidsverklaring te ondertekenen.

4. Gedragscode e-mail en internetgebruik

De gemeente hanteert een protocol voor gebruik van e-mail en internet. In dit protocol is aangegeven hoe medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop gebruik van externe e-mail en internet wordt geobserveerd. Het protocol is voor alle medewerkers van de gemeente te raadplegen op het gemeentelijk Intranet. IB beleid te vinden op interactieve pdf, informatiebeveiliging
http://intranet.helmond.nl/hi/informatieveiligheid .

5. Kennisnemen van het beveiligingsplan Suwinet

Dit beveiligingsplan Suwinet is van toepassing op iedereen die gebruik maakt van Suwinet-Inkijk binnen de afdeling W&I. Het plan is opgenomen in het handboek Schulinck. Alle gebruikers worden erop geattendeerd dat ze kennis moeten nemen van het plan. De nieuwe medewerkers krijgen bij toekenning van de autorisatie van Suwinet het beveiligingsplan toegestuurd met het verzoek/opdracht het plan door te nemen. Hierdoor weten medewerkers welk gedrag de organisatie van hen verwacht én weten ze dat er gegevens worden bewaard waarmee hun gedrag kan worden gecontroleerd. Van dat laatste moeten medewerkers bewust zijn in relatie tot hun eigen privacy. De organisatie kan de opgeslagen gegevens niet lukraak gebruiken.

6. Gegevensverstrekking aan derden via de telefoon

Er wordt geen telefonische informatie over cliënten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. Dit vanwege het risico dat de identiteit van de gesprekspartner verkeerd kan worden vastgesteld of dat persoonsgegevens worden verstrekt aan personen of instanties, die geen recht hebben op informatie. In voorkomende gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner[2] wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven als een medewerker een vaste contactpersoon aan de lijn heeft.

7. Clear desk en clear screen policy

Onbevoegden mogen niet de beschikking krijgen over vertrouwelijke informatie. Daarom mogen die gegevens niet onbeheerd op het bureau of het beeldscherm achterblijven. Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De systemen zijn door afdeling I&A zodanig ingesteld dat na een vaste periode de schermbeveiliging intreedt. Daarnaast kunnen medewerkers als gebruikers zelf het scherm vergrendelen door de toetscombinatie “Windowsvlaggetje-L” gelijktijdig aan te slaan (L staat voor "lock"). Dit is te adviseren als medewerkers langer dan een minuut hun werkplek verlaten. Bezoekers dienen zich bij binnenkomst in het gebouw eerst te melden bij de receptie. Bij de receptie moet een inschrijfformulier worden ingevuld door de receptiemedewerkers en bezoekersbadges worden uitgereikt aan de bezoekers. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Het is echter nodig ook ten opzichte van collega's en dienstverleners zorgvuldig om te gaan met de privacy van klanten.

8. Vertrouwelijke gegevens

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden.
Daarom zijn er op iedere kamer binnen de afdeling W&I speciale papierbakken geplaatst, waarin het te vernietigen materiaal verzameld wordt. De verzamelde vertrouwelijke gegevens worden regelmatig aangeleverd bij het vernietigingsbedrijf. Vertrouwelijke gegevens dienen niet terecht te komen in een gewone prullenbak.

9. Aanspreken van onbekende personen

In het geval dat een medewerker een voor hem of haar onbekende persoon in het gebouw tegenkomt waar officieel geen publiek zonder begeleiding mag komen, dient de medewerker deze persoon aan te spreken, zichzelf voor te stellen en de persoon in kwestie te vragen wat hij/zij hier doet.
Personen die niet bevoegd zijn om zich op deze plek te bevinden worden hierdoor op deze overtreding gewezen. Het is de taak van alle medewerker om hen beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naartoe te begeleiden.

10. Sancties

Als medewerkers de regels binnen onze organisatie onvoldoende naleven kunnen zij daarop worden aangesproken en kunnen rechtspositionele maatregelen getroffen worden. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen. Dit geldt voor alle werkzaamheden binnen de afdeling W&I. Voor dit beveiligingsplan zijn geen nadere regels nodig.

BIJLAGE 1: Autorisatiematrix t.b.v. gebruik Suwinet

AUTORISATIESMATRIX TEN BEHOEVE VAN GEBRUIK SUWINET Versie 23 februari 2015

	Functies binnen afdeling W & I	GBA 005	GBA-V RXXX	Zoek in GBA 018	VIS 025	B&O 002	Bedrijvenregister 024	Correctieservice 031	CWI 003	Fraude scorekaart 004	GSD 019	Kadaster R678	Belastingdienst 1043	Klant algemeen 042	Klant algemeen+ 043	Klantbeeld 029	RDW 020	RDW peildata R454	Zoek in RDW RXXX	SBR Query SBQR	Opvragen gebruiksrapportages R347	Langdurigheidstoeslag 034	Handhaving RXXXX	Terugvordering RXXXX	Fraudevordering R1272	Kostendelersnorm R 2769	Inburgeringsportaal SCI06	WIS module applicatie
1. administratief (financieel) medewerker	procesondersteuners financiële medew	✓	✓	x	x	✓	✓	✓	✓	✓	✓	✓	x	✓	✓	✓	x	x	x	x	x	x	✓	x	x	x	x	x
2. Medewerker rechtmatigheid	KB Inkomen KB BBZ KB bijzondere bijstand medew terugvord/verhaal	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	x	✓	✓	x	x	✓	x	x
3. Medewekers reintegratie	KB Werk KB inburgering	✓	x	x	✓	✓	✓	✓	✓	✓	✓	x	x	✓	✓	x	✓	x	x	✓	x	x	x	x	x	x	x	x
4. Terugvordering/verhaal	Boete-ambtenaar, medew terugvord/verhaal	✓	x	x	x	x	x	✓	x	x	✓	x	x	✓	✓	x	x	x	x	x	x	x	✓	✓	✓	x	x	x
5. Medew Handhaving/ Sociale re	Handhaving /SR Medewerker preventie	✓	✓	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	x	x	✓	x	✓	x	x	x
6. opvragen gebruikersrapportage	Security officer	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x
7. Gebruikersbeheer	Appl beheerder /coord	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x	x
8. combi 2 + 3	KB tel intake, Integrale KB (TAZ) Kwaliteitscoaches	✓	✓	x	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	x	✓	x	✓	✓	x	x	✓	x	x
9.langdurigheidstoeslag	Sr Klantbegeleider	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x	x	x	x	x	x
10. Inburgering	KB Inburgering	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓	x
11. Wis-module	Medewerkers team Poort Administratief medew KB tel intake kwaliteitscoach	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	✓

KB= Klantbegeleider

BIJLAGE 2: Proces autoriseren Suwinet

	Wat	Wie: functie medewerker	Document	Opmerking	Conclusies
1.	Vaststellen schema functies (groepen) uitvoering WWB en bijbehorende autorisatierollen Suwinet	Afdelingsmanager W&I	Autorisatiematrix en Schema functies (groepen) en rollen	Schema legt vast welke functiegroepen tot welke autorisatierollen in Suwinet toegang kunnen krijgen. Het biedt inzicht hoe de gemeente Helmond de rollen heeft toegedeeld naar functiegroep, uitgaande van doelbinding en proportionaliteit.	Toekennen autorisatie te toetsen aan vastgestelde documenten.
2.	Aanvraag autorisatie	Teammanager afdeling W&I	Formulier aanmelden nieuwe medewerker, Zorgvuldigheidsverklaring of geheimhoudings- en zorgvuldigheidsverklaring	Een medewerker voor de uitoefening van zijn taken toegang wil krijgen tot Suwinet vraagt via een formulier toegang aan. Hij tekent dit formulier.	Teammanager beoordeeld of een medewerker aanvraag Suwinet mag indienen en zorgt voor het beschikbaar stellen van de verklaringen. Geeft op dit formulier aan de functie van de medewerker en paraaf.
3.	Besluiten over de aanvraag autorisatie	Teammanager team Staf	Formulier aanmelden nieuwe medewerker, Zorgvuldigheidsverklaring of geheimhoudings- en zorgvuldigheidsverklaring	Het nemen van een besluit op aanvraag voor toegang tot Suwinet is een taak van teammanager Staf. Deze toetst of de aanvraag past op de functiegroep/taken van de medewerker en de gevraagde autorisatierol(len) Hij geeft akkoord door de zorgvuldigheidsverklaring, geheimhoudings-en zorgvuldigheidsverklaring te tekenen.	Teammanager van de afdeling W&I dient de aanvraag in en de teammanager Staf neem een besluit.
4.	Autorisatie toekennen, medewerker opvoeren in Suwinet als gebruiker	Teammanager Staf beheerder Suwinet	Zorgvuldigheidsverklaring of geheimhoudings- en zorgvuldigheidsverklaring	Dit is de taak van de autorisatiebeheerder Suwinet. Hij autoriseert alleen een medewerker als hij een getekende aanvraag, door de teammanager Staf heeft ontvangen.	Teammanager Staf kent de autorisatie toe en de beheerder Suwinet voert de gegevens in op Suwinet
5.	Intrekken/wijzigen autorisatie	Teammanager afdeling W&I	formulier voor het afmelden van een medewerker of formulier waarop kan worden aangegeven dat de medewerker een andere functie(taken) heeft gekregen	teammanager geeft aan het secretariaat door dat een medewerker uit dienst is gegaan of dat de medewerker een een andere functie heeft geaccepteerd waarbij of te wel de rol wijzigt of de medewerker geen toegang meer mag hebben tot Suwinet.	Secretariaat zorgt dat de mutatie wordt doorgegeven aan de teamleider Staf
6	Ondertekenen van de beeindiging/wijziging	Teammanager Staf	formulier voor het afmelden van een medewerker of formulier waarop kan worden aangegeven dat de medewerker een andere functie(taken) heeft gekregen	Verantwoordelijkheid teammanager Staf geeft opdracht om een autorisatie in te trekken of te wijzigen door het formulier voor akkoord te tekenen.	Het formulier gaat naar de gebruikersbeheerder
6.	Intrekken/wijzigen autorisatie in Suwinet	Gebruikersbeheerder	Afmeldformulier	Beheerder voert uit op grond van een schriftelijk verzoek tot intrekken/wijzigen van de teammanager Staf	Getekend formulier door de teammanager en de teammanager Staf
7.	Opschonen en actualiseren autorisaties; periodiek	Beheerder Suwinet	Lijst uit het systeem	De interne controleur vraagt maandelijks aan de gebruikersbeheerder een overzicht van de gebruikers in Suwinet. In dit overzicht staan de gebruikers en de rollen die zijn toegekend binnen Suwinet.	ter controle aan de interne controleur
8.	Periodiek controle op autorisaties	Interne controle	mutatieformulier	De medewerker Interne controle binnen W&I voert de controle uit op de toegekende autorisaties en hoe deze zijn opgenomen in Suwinet. Tevens worden de niet actieve gebruikers gescreend. De bevindingen worden gerapporteerd aan de afdelingsmanager W&I en aan de security officer.	Up to date houden van de toegekende autorisaties in Suwinet.

BIJLAGE 3: Controleoverzicht gebruikrapportage Suwinet afd. W&I

Controle-overzicht Gebruikrapportage Suwinet afdeling W&I.

Maand: …… Controle uitgevoerd d.d: ……..……

Controle uitgevoerd door:
…….

Bijzonderheden geconstateerd bij de gebruikersrapportage:

	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:
……..

Integriteit: De beoordeling van de rapportage geeft aan dat er normoverschrijdend gedrag heeft plaatsgevonden en er wordt opgeschaald naar Integriteitsbeleid en het gedrag heeft vergaande consequenties.

Af te handelen door:
……...

BIJLAGE 4: Maandelijkse verantwoording autorisaties Suwinet

Maandelijkse verantwoording autorisaties Suwinet

Maand:

In opdracht van Security officer d.d.:

Akkoord Afdelingsmanager W&I

Datum:

Akkoord / niet akkoord

	Naam medewerker	Afdeling /team	Reden mutatie autorisatie, wijziging functie, uit dienst of anders	Huidige autorisatie Suwinet 1 -11	Mutatie in autorisatie 1 t/m 11	Niet meer ingelogd vanaf datum	Uit dienst: datum	Blokkering akkoord Ja/nee	Account beëindigen Ja/nee
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
21									
22									
23									

BIJLAGE 5 Criteria Controleoverzicht Gebruikrapportage Suwinet afdeling W&I

De rapportage verschijnt iedere maand en rapporteert over het gebruik van Suwinet bij de gemeente Helmond over die betreffende maand en de voorgaande vijf maanden.
De rapportage geeft inzicht in het gebruik van Suwinet door de medewerkers van de afdeling WI. Met behulp van deze rapportage kunnen we toezicht houden op het gebruik van deze applicatie en eventueel kunnen we bijsturen.
De rapportage bevat 4 onderdelen:

- Het totale gebruik (tabel 1.1)
- Het zorgvuldig gebruik (tabel 2.1 - 2.5)
- Het accountbeheer (tabel 3.1 – 3.4)
- Het doelmatig gebruik (tabel 4.1 – 4.3)

In de rapportage worden aantallen en percentages weergegeven. Om houvast te geven bij de cijfers wordt in sommige tabellen een vergelijking van het gebruik van de gemeente Helmond gemaakt met het gemiddelde van de gemeentelijke afnemers:

- Van gelijke grootteklasse op basis van het aantal inwoners
- Van gelijke grootteklasse op basis van het aantal actieve gebruikers
- Van heel Nederland

Tabel	Toelichting / signaal	Mogelijke vervolgactie
1.1 Totaal Gebruik Deze tabel bevat het absoluut aantal raadplegingen (ge-raadpleegde pagina's) over de afgelopen zes maanden.	De trend is hier belangrijk. Een plotselinge stijging kan wijzen op: • extra uitgevoerde controles, • wetswijzigingen en herbeoordelingen, • plotselinge sterke stijging van aanvragen. Een plotselinge daling kan wijzen op: • vakantieperiode, • ziekte onder medewerkers, • wijziging in processen, bijvoorbeeld door invoering geautomatiseerde controles of afschaffen toetsing. Er is een trend vastgesteld van rond de 600 raadplegingen per dag. Het totaal verbruik / door het aantal werkdagen. Nagaan of de trend afwijkt.	Indien er niet onmiddellijk een verklaring voor een afwijking in het patroon is, dan kan een teamleider worden geraadpleegd. Als ook afwijkende patronen in andere overige tabellen worden gevonden, dan kan een specifieke rapportage op medewerkersniveau worden opgevraagd bij het BKWI. Dat kan van alle accounts of van specifieke rollen.
2.1 Raadplegingen op zoeksleutel anders dan BSN De norm is om op te vragen via de BSN (= zoeksleutel). Specifieke functionarissen zijn geautoriseerd met een zogenaamde "zware rol". Zij kunnen ook buiten het BSN persoonsgegevens raadplegen, zoals op naam en geboortedatum, op kenteken.	Bij een plotselinge stijging is de vraag: • zijn er meer medewerkers geautoriseerd met deze zware rol, • zijn er specifieke handhavingscontroles uitgevoerd waarbij het BSN niet gebruikt kon worden. Bij een hoger percentage in vergelijking met andere gemeenten is de vraag: • zijn er niet teveel medewerkers geautoriseerd voor deze zware rol.	De vraag naar bijzondere handhavingsacties kan beantwoord worden door de betreffende teamleider. De vraag over de juiste toewijzing van deze zware rollen kan aan de gebruikersbeheerder worden gesteld. Uit de autorisatiematrix kan worden geconcludeerd of de rollen juist zijn toegewezen. Valt daaruit geen verklaring af te leiden, dan bij het BKWI een specifieke rapportage opvragen voor de medewerkers die geautoriseerd zijn voor deze rollen.

2.2 Percentage raadplegingen buiten kantoortijd dat wil zeggen tussen 19.00 uur en 06.00 uur.	Gegevens in deze tabel zijn absolute getallen Bij de gemeente Helmond mag men thuiswerken en wordt er bij het team IO s' avonds telefonisch contact gezocht met burgers voor de invordering. Een afwijkende trend kan wijzen op overwerk- en inhaalacties of een tijdelijke avondopenstelling. Voor raadplegingen buiten kantoortijden moet in alle gevallen naar een verklaring worden gezocht.	Teamleiders kunnen uitsluitsel geven over overwerk in de avonduren. Is de verklaring niet afdoende, dan kan een specifieke rapportage worden opgevraagd bij het BKWI.
2.3 Meest geraadpleegde BSN De tabel bevat de top-5 meest geraadpleegde BSN's en het aantal raadplegingen dat daarop is gedaan (ook in %) door het aantal actieve gebruikers.	De trend is dat een BSN door gemiddeld 4-5 actieve gebruikers wordt geraadpleegd (gezien het proces bij de gemeente Helmond) Wanneer het aantal raadplegingen op de top 5 per maand sterk verschilt en/of sterk ver- schilt in %, dan moet worden gezocht naar een verklaring. Allereerst moeten worden onderzocht of het een klant betreft. Volgens kan worden nagegaan of de klant bewerkelijk is: bijvoorbeeld er moet nader onderzoek worden gedaan, veel mensen zijn met de klant bezig. Aan de andere kant kan dit een sterke aanwijzing zijn dat een persoon die om de een of andere reden in de belangstelling staat, niet op rechtmatige gronden wordt geraadpleegd.	Wanneer er niet een verklaring te vinden is, een specifiek rapportage opvragen over het BSN en de medewerkers die op dat BSN raadplegingen hebben gedaan. Medewerker kan worden aangesproken op het gebruik.
2.4 **Hoogst aantal actieve gebruikers dat hetzelfde BSN heeft geraadpleegd.** De vorige tabel bevatte het aantal meest geraadpleegde BSN's, ongeacht of dat door een of meerdere personen is geraadpleegd. In deze tabel gaat het om het BSN dat door de meeste gebruikers is geraadpleegd.	Gezien het proces bij de gemeente Helmond zijn er 4-5 gebruikers per BSN bezig. Intake, Klantbegeleider inkomen, klantbegeleider werk, medewerker preventie, kwaliteitscoach. Wanneer het aantal personen dat eenzelfde BSN raadpleegt per maand sterk verschilt en/ of sterk verschilt van het gemiddelde, dan moet worden gezocht naar een verklaring. Een afwijkend patroon kan een indicatie zijn voor misbruik. Verschillen tussen gemeen- ten kunnen (ook) wijzen op verschillende werkprocessen.	Vraag een specifieke rapportage op medewerkersniveau op bij BKWI. Vervolgens kan ook door koppeling van het BSN met het cliënten- bestand worden vastgesteld of deze BSN's wel tot het cliëntenbestand horen.
2.5 Hoogst aantal raadplegingen per actieve gebruiker Dit is de top 5 van Suwinet gebruikers.	Grote afwijkingen van het gemiddelde of afwijkingen in de tijd kunnen worden verklaard door bv. opdracht aan een medewerker om specifiek bepaalde controles uit te voeren (in bulkwerk). De telefonische intakers hebben de	Wanneer geen verklaring kan worden gevonden in taaktoedeling/procesgang dan een specifieke rapportage opvragen om deze top-gebruikers te identificeren. Foutief gebruik van Suwinet kan zo

	hoogste scores in deze tabel. Zijn er andere gebruikers dan wordt er onderzocht hoe het komt dat deze mensen zoveel raadplegingen doen in Suwinet.	boven water komen.
3.1 Percentage geblokkeerde accounts op de eerste dag van de maand Accounts worden automatisch geblokkeerd bij BKWI na 5 mislukte pogingen om in te loggen. Gemeente Helmond wordt een account (automatisch) geblokkeerd na 50 dagen niet-gebruik.	In deze tabel het aantal geblokkeerde accounts als percentage van het totaal aantal accounts en in absolute getallen. Alle afwijkingen van 0 zijn aanleiding voor nader onderzoek. De interne controleur kan daarvoor een lijst uit de gebruikersadministratie raadplegen. Hij / zij kan onderzoeken: • is de medewerker nog wel in dienst (bij uit dienst had zijn account direct afgesloten moeten worden), • heeft de betreffende medewerker Suwinet wel nodig voor zijn werk • waarom gebruikt de medewerker Suwinet niet.	Er is een actief beheer op de autorisaties en er is in beeld hoeveel accounts er zijn geblokkeerd. Vervolgacties kunnen zijn: • account afsluiten, • wijzen op afspraken over het gebruik van Suwinet in de processen. • procedures met betrekking aan- en afsluiten van accounts aanscherpen of beter naleven
3.2 Ongebruikte accounts Deze tabel geeft aan hoeveel accounts de afgelopen 90 dagen niet gebruikt zijn.	De gebruikersbeheerder kan in zijn gebruikersadministratie per account achterhalen wat de laatste datum van gebruik was. Hij kan deze verifiëren bij BKWI. In alle gevallen zijn niet-gebruikte accounts reden voor nadere actie door de interne controleur. Er is een actief beheer op de autorisaties en er is in beeld hoeveel accounts er ongebruikt zijn.	Vervolgstap kan zijn: • navraag doen bij de teammanager van de betreffende medewerker naar de reden niet-gebruik, • afsluiten van accounts van mensen die uit dienst zijn, • afsluiten accounts van mensen die Suwinet niet nodig hebben voor hun werk. • autorisatie aanpassen • autorisatiebeleid aanpassen of beter naleven. In het beveiligingsplan Suwinet is opgenomen dat wanneer een account 50 dagen niet wordt gebruikt, vervalt het account automatisch. De Security officer gaat dan over tot het beëindigen van de autorisatie.
3.3 Aangemaakte accounts, verwijderde accounts en wijzigingsacties op accounts	Hier worden de mutaties geregistreerd door de beheerder van Suwinet, zijnde de applicatiebheerders van de gemeente Helmond. Zij mogen alleen muteren als de security officer hier opdracht voor geeft. Aanmelding, beëindiging of wijziging krijgen zij met behulp van een formulier door.	De ondergetekende formulieren door de security officer in een bepaald maand moeten aansluiten met de cijfers die in deze tabel worden gepresenteerd. Is dat niet het geval dan een specifieke rapportage opvragen waarin de accounts worden benoemd (naam).

3.4 Verdeling van de rollen De tabel geeft een overzicht van de beschikbare rollen (die gekoppeld zijn aan specifieke pagina's in Suwinet Inkijk) en het aantal medewerkers dat een autorisatie voor die rol heeft. Het kan zijn dat een medewerker voor meerdere rollen is geautoriseerd. Dat is af te lezen uit de autorisatiematrix	Speciale aandacht moet besteed worden aan het aantal 'zware' rollen: zijn daar logisch te verklaren wijzigingen in, zijn ze nog proportioneel in verhouding tot het aantal medewerkers dat met die controle- en opsporingstaken is belast. Meer in het algemeen biedt deze tabel de mogelijkheid om de toedeling van rollen te toetsen aan de functie van medewerkers: zijn rollen te ruim, te krap en wel juist toebedeeld. De gebruikersbeheerder kan in zijn administratie achterhalen wie welke autorisatie heeft. Afwijkingen in de aantallen moeten logisch verklaard kunnen worden, bijvoorbeeld door een wijziging in de inrichting van een proces.	Het is aan te bevelen dat er periodiek een toets plaats vind of de autorisaties van de medewerkers nog passen bij (proportioneel zijn voor) hun functie. Met name de zware rollen.
4.1 Verdeling van de raadplegingen over de pagina's In de tabel staan alle beschikbare pagina's van Suwinet In-kijk en het aantal keren dat die pagina is geraadpleegd. In de autorisatiematrix van de is aangegeven welke medewerker voor welke rollen is geautoriseerd.	Afwijkingen in het patroon kunnen mogelijk worden verklaard door specifieke controles, een nieuwe pagina of een vervallen pagina. Speciale aandacht moet worden besteed naar de pagina's met de speciale zoeksleutels: • GSD Zoek in BRP, • GSD Zoek in de BRP uitgebreid, • GSD Zoek in de RDW. • GSD Zoek in de RDW plus Steeds moet de vraag worden gesteld of het aantal raadplegingen op deze zoeksleutels rechtmatig (en proportioneel) is. Pieken in het gebruik van deze pagina's moeten worden onderzocht op misbruik.	Een vervolgactie kan zijn een nader onderzoek naar de roltoedeling op basis van de autorisatiematrix. Indien er mogelijk misbruik wordt vermoed,wordt er een specifieke rapportage op gevraagd.
4.2 verzonden Suwimail Suwi-mail is beveiligde mail. Ketenpartijen worden geacht deze beveiligde Suwi-mail te gebruiken.	Een dalend gebruik, vermoedelijk laag gebruik of niet-gebruik kan erop wijzen dat de onbeveiligde mail wordt gebruikt.	In de volgende tabel 4.3 ontvangen mail zou bijna hetzelfde aantal moeten staan als in deze tabel. Wijken deze getallen af dan de medewerkers erop attenderen dat e-mail via het beveiligde netwerk verzonden moet worden.
4.3 Ontvangen Suwimail Suwi-mail is beveiligde mail. Ketenpartijen worden geacht deze beveiligde Suwi-mail te gebruiken.	Een dalend gebruik, vermoedelijk laag gebruik of niet-gebruik kan erop wijzen dat de onbeveiligde mail wordt gebruikt. Als organisatie hebben we weinig invloed op de getallen in deze tabel omdat het over ontvangen mail gaat.	Breng Suwi-mail onder de aandacht van de medewerkers. Zie verder wat er bij tabel 4.2 is gemeld.

BIJLAGE 6 procesbeschrijving controle

	Wat	Wie: functie medewerker	Document	Opmerking	Conclusies
1	Het opvragen van gebruikersrapportages bij BKWI	Security officer	Via suwi mail	Security Officer vraagt rechtstreeks op bij BKWI.	
2.	Het uitvoeren van controles op de gebruikersrapportages en het rapporteren over de uitgevoerde controle.	Medewerker interne controle van het team Staf	Controle overzicht gebruiksrapportage Suwinet	Rapportages maken onderdeel uit van de Bestuursrapportages (Beraps voor het MT).	De controles, resultaten en maatregelen kunnen worden meegenomen in de Bestuursrapportages (Beraps).
3.	Opvragen individuele gebruiksrapportage	Security officer	Controle overzicht gebruiksrapportage Suwinet	Zijn er signalen over ongeoorloofd/oneigenlijk gebruik dan kan er op naam rapportages worden opgevraagd.	Bij de gemeente Helmond vraagt de security officer deze rapporten op bij de BKWI
4.	Het informeren door de security officer aan het afdelingsmanagement over de resultaten en adviseren over de vervolgstappen n.a.v. controles van individuele medewerkers	Security officer	Controle overzicht gebruiksrapportage Suwinet	Indien individuele medewerkers hun zoekgedrag niet kunnen verantwoorden en er aanwijzigingen zijn voor normoverschrijdend gedrag heeft dit vergaande consequenties (ontslag)	De teammanager zal in eerste instantie de medewerker aanspreken in de HRM cyclus, functionerings-beoordelingsgesprek.
5.	Periodieke rapportage over controles, resultaten en maatregelen aan bestuur.	Afdelingsmanager W&I	Bestuursrapportage (Berap)		De resultaten van de uitgevoerde controles kunnen worden vermeld in een paragraaf Suwinet in de Berap, en jaarrekening voor B&W/Raad. Tevens worden de samenwerkende gemeenten op de hoogte gesteld.

BIJLAGE 7: Geheimhoudings- en zorgvuldigheidsverklaring

Gemeente Helmond

Geheimhoudings- en zorgvuldigheidsverklaring (voor externen)

Ondergetekende,

Naam:	Geboortedatum:
Bedrijfsnaam:	
Werkzaam bij het team:	Functie: (in te vullen door teammanager en
akkoord) Plaats:	
Datum:	Aanvraag: 0 GWS 0 Suwinet 0 Overig

- er van op de hoogte is dat de privacywet- en regelgeving een zorgvuldige omgang met persoonsgegevens beoogt te beschermen en dat deze wet- en regelgeving het gebruik van persoonsgegevens in de ruimste zin van het woord verbindt aan regels.

- zorgvuldig zal omgaan met de (persoons)gegevens en de inhoud van de documenten die hij/zij bij de uitvoering van de werkzaamheden mag inzien en zich daarbij houdt aan de werkinstructies zoals opgenomen in de functionele beschrijvingen. Concreet betekent dit onder meer dat hij/zij:
  - niet meer (persoons)gegevens inkijkt dan strikt noodzakelijk is;
  - zorgvuldig archiveert;
  - (persoons)gegevens niet aan onbevoegden verstrekt;
  - het wachtwoord zorgvuldig hanteert.

- kennis heeft genomen van de regels die gelden voor het zorgvuldig omgaan met persoonsgegevens.

- gedurende de duur van zijn/haar inzet voor de gemeente Helmond enkel die (persoons)gegevens gebruikt, die van belang zijn voor het uitvoeren van de dagelijkse werkzaamheden.

- alle medewerking zal geven aan het naleven van de privacywet- en regelgeving van toepassing op en/of opgesteld binnen de dienst Samenleving en Economie van de gemeente Helmond.

- Verplicht zich tegenover de Gemeente Helmond tot geheimhouding van verkregen kennis van zaken Gemeente Helmond betreffende, ten aanzien waarvan hem/haar geheimhouding is opgelegd of waarvan hij/zij het vertrouwelijke karakter moet begrijpen, zowel gedurende de periode waarin hij/zij bij de Gemeente Helmond werkzaam is als daarna.
  In dit kader is het ondermeer niet toegestaan enige informatie aan derden te verstrekken omtrent persoonsgegevens van burgers welke met behulp van geautomatiseerde systemen van de Gemeente Helmond worden uitgewisseld of welke in deze systemen zijn opgeslagen.

- Gebruik Suwinet:
  U als toekomstige gebruiker van Suwinet-Inkijk moet weten dat uw gebruik wordt geregistreerd. Uw handelingen binnen Suwinet worden verzameld en vastgelegd middels een logging applicatie. Hierbij wordt gekeken of uw gebruik van de persoonsgegevens van uitkeringsgerechtigden en/of werkzoekenden niet op een onrechtmatige of onregelmatige wijze is geschiedt;
  - Het doel van de logging; (tegengaan en controleren van onrechtmatige of doeloverschrijdende verwerking);
  - de (aard van de) gegevens die binnen deze applicatie worden gelogd;

- dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- U wordt in Suwinet geautoriseerd alleen voor de gegevens die van belang zijn voor het uitvoeren van uw taken. Het is niet de bedoeling dat u via een andere omweg meer informatie uit Suwinet haalt dan voor uw taken nodig is;
- Indien een (mogelijk) onrechtmatig, onregelmatig of doeloverschrijdend gebruik van (de persoonsgegevens binnen) Suwinet-inkijk wordt geconstateerd wordt dit met u kortgesloten.
- Indien de individuele medewerkers hun zoekgedrag niet kunnen verantwoorden en er aanwijzingen zijn voor normoverschrijdend gedrag heeft dit vergaande consequenties.
- de bewaartermijn van de gelogde gegevens is 18 maanden.

Ondergetekende realiseert zich dat handelen in strijd met deze verklaring grond kan zijn voor strafrechtelijke, civielrechtelijke en/of arbeidsrechtelijke maatregelen, waaronder onmiddellijke beëindiging van het dienstverband of onmiddellijke beëindiging van een dienstverleningsovereenkomst.

Handtekening:

Autorisatie toekennen cfm autorisatiematrix:

Omcirkel 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 - 10 - 11 **(Zie hieronder)**

Teammanager Staf T. Tromp

Na ondertekening inleveren bij SE.WI.STAF.

1. administratief (financieel) medewerker	procesondersteuners financiële medew
2. Medewerker rechtmatigheid	KB Inkomen KB BBZ KB bijzondere bijstand medew terugvord/verhaal
3. Medewekers reintegratie	KB Werk
4. Terugvordering/verhaal	Boete-ambtenaar, medew terugvord/verhaal
5. Medew Handhaving/ Sociale recherche	Handhaving /SR Medewerker preventie
6. opvragen gebruikersrapportage	Security officer
7. Gebruikersbeheer	Appl beheerder /coord
8. combi 2 + 3	KB tel intake, Integrale KB (TAZ) Kwaliteitscoaches
9. langdurigheidstoeslag	Sr Klantbegeleider
10. Inburgering	KB inburgering
11. Wis Module	Medewerkers team Poort Administratief medew KB tel intake kwaliteitscoach

BIJLAGE 8: Zorgvuldigheidsverklaring

Zorgvuldigheidsverklaring Gemeente Helmond

Ondergetekende,

Naam:

Functie:
(in te vullen door teammanager en akkoord)
Organisatie-onderdeel: Aanvraag: 0 GWS
0 Suwinet
Plaats: 0 Overig

Datum:

Zegt toe dat hij/zij:

- er van op de hoogte is dat de privacywet- en regelgeving een zorgvuldige omgang met persoonsgegevens beoogt te beschermen en dat deze wet- en regelgeving het gebruik van persoonsgegevens in de ruimste zin van het woord verbindt aan regels.

- zorgvuldig zal omgaan met de (persoons)gegevens en de inhoud van de documenten die hij/zij bij de uitvoering van de werkzaamheden mag inzien en zich daarbij houdt aan de werkinstructies zoals opgenomen in de functionele beschrijvingen. Concreet betekent dit onder meer dat hij/zij:
- niet meer (persoons)gegevens inkijkt dan strikt noodzakelijk is;
- zorgvuldig archiveert;
- (persoons)gegevens niet aan onbevoegden verstrekt;
- het wachtwoord zorgvuldig hanteert.

- kennis heeft genomen van de regels die gelden voor het zorgvuldig omgaan met persoonsgegevens.

- gedurende de duur van zijn/haar inzet voor de gemeente Helmond enkel die (persoons)gegevens gebruikt, die van belang zijn voor het uitvoeren van de dagelijkse werkzaamheden.

- alle medewerking zal geven aan het naleven van de privacywet- en regelgeving van toepassing op en/of opgesteld binnen de dienst Samenleving en Economie van de gemeente Helmond.

- Gebruik Suwinet:

U als toekomstige gebruiker van Suwinet-Inkijk moet weten dat uw gebruik wordt geregistreerd. Uw handelingen binnen Suwinet worden verzameld en vastgelegd middels een logging applicatie. Hierbij wordt gekeken of uw gebruik van de persoonsgegevens van uitkeringsgerechtigden en/of werkzoekenden niet op een onrechtmatige of onregelmatige wijze is geschiedt;

- Het doel van de logging; (tegengaan en controleren van onrechtmatige of doeloverschrijdende verwerking)
- de (aard van de) gegevens die binnen deze applicatie worden gelogd;
- dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- U wordt in Suwinet geautoriseerd alleen voor de gegevens die van belang zijn voor het uitvoeren van uw taken. Het is niet de bedoeling dat u via een andere omweg meer informatie uit Suwinet haalt dan voor uw taken nodig is;
- Indien een (mogelijk) onrechtmatig, onregelmatig of doeloverschrijdend gebruik van (de persoonsgegevens binnen) Suwinet-inkijk wordt geconstateerd wordt dit met u kortgesloten.
- Indien de individuele medewerkers hun zoekgedrag niet kunnen verantwoorden en er aanwijzingen zijn voor normoverschrijdend gedrag heeft dit vergaande consequenties, disciplinaire maatregelen.

- de bewaartermijn van de gelogde gegevens is 18 maanden;

- Gedurende de duur van zijn/haar inzet voor de werkzaamheden voor de gemeente Helmond en na beëindiging van deze werkzaamheden, tegenover derden geheimhouding zal betrachten met betrekking tot alle (persoons)gegevens waarvan hij/zij bij de uitvoering van de voornoemde werkzaamheden kennis neemt.

- Er van op de hoogte is dat ten aanzien van de geheimhouding de ambtenarenwet van toepassing is.

Handtekening medewerker:

Autorisatie toekennen cfm autorisatiematrix:
Omcirkel 1 – 2 – 3 – 4 – 5 – 6 – 7 – 8 – 9 -10 - 11 **(Zie hieronder)** **Teammanager Staf T. Tromp**

Na ondertekening inleveren bij SE.WI.STAF.

1. administratief (financieel) medewerker	procesondersteuners financiële medew
2. Medewerker rechtmatigheid	KB Inkomen KB BBZ KB bijzondere bijstand medew terugvord/verhaal
3. Medewekers reintegratie	KB Werk
4. Terugvordering/verhaal	Boete-ambtenaar, medew terugvord/verhaal
5. Medew Handhaving/ Sociale recherche	Handhaving /SR Medewerker preventie
6. opvragen gebruikersrapportage	Security officer
7. Gebruikersbeheer	Appl beheerder /coord
8. combi 2 + 3	KB tel intake, Integrale KB (TAZ) Kwaliteitscoaches
9. langdurigheidstoeslag	Sr Klantbegeleider
10. Inburgering	KB inburgering
11. Wis Module	Medewerkers team Poort Administratief medew KB tel intake kwaliteitscoach

BIJLAGE 9 Functiebeschrijving security officer

De Security Officer (SO) legt verantwoording af aan de afdelingsmanager van de afdeling W&I. De Security officer heeft, indien de situatie daarom vraagt, de verantwoordelijkheid om rechtstreeks bij het college van B&W zaken bespreekbaar te maken.

Vanuit de afdeling W&I is de SO verantwoordelijk voor het opzetten en onderhouden van beleid en processen gericht op:

- Het veilige gebruik en de continuïteit van de bedrijfsprocessen;
- Het voldoen aan interne en externe eisen op het gebied van Informatiebeveiliging;
- Het beschermen van de reputatie van de organisatie.

De Security Officer ontleent toegevoegde waarde aan kennis van de organisatie en de vertaalslag die moet worden gemaakt van de algemene IB-normen naar de specifieke bedrijfssituatie. Die algemene IB-normen ten behoeve van Suwinet hebben vooral betrekking op personeel en organisatie, communicatie (ten behoeve van bewustwording), gebouwen en ruimten (ten behoeve van fysieke beveiliging), informatiebeveiligingsincidenten en de invulling van business continuity management in de organisatie.

Functie-inhoud

- Opstellen en beheren van beleid, standaarden en procedures op het gebied van informatiebeveiliging, inclusief het volgen en signaleren van externe ontwikkelingen en interne ontwikkelingen gericht op Suwinet;
- Zorgdragen voor het opstellen en naleven van informatiebeveiliging ten behoeve van Suwinet;
- Adviseren en actief uitdragen van beleid op het gebied van informatiebeveiliging van Suwinet in de organisatie;
- Uitvoeren van risicoanalyses met betrekking tot informatiebeveiliging Suwinet binnen de organisatie;
- Opstellen van een jaarplanning met betrekking tot informatiebeveiliging Suwinet;
- Coördineren van activiteiten met betrekking tot informatiebeveiliging Suwinet;
- Adviseren van het hoogste management met betrekking tot informatiebeveiliging Suwinet;
- Uitvoeren van interne controles en coördineren van audits van ten behoeve van Suwinet;
- Rapporteren aan het hoogste management, onder andere over naleving van het informatiebeveiligingsbeleid, de voortgang van de implementatie van informatiebeveiligingsmaatregelen en over de uitkomsten van zelf te initiëren interne onderzoeken van Suwinet;
- Onderhouden van interne en externe contacten op het terrein van informatiebeveiliging Suwinet;
- Signaleren van afwijkingen op het informatiebeveiligingsbeleid aangaande Suwinet;

BIJLAGE 10 PLANNING

Uitvoeringsacties beveiliging Suwinet in 2014 – 2015
Dit plan inclusief het stelsel van procedures en maatregelen voor de dagelijkse praktijk wordt jaarlijks op relevantie en actualiteit geëvalueerd en beoordeeld en bij noodzaak daartoe bijgesteld.

De beveiligingsbeheerder, de proceseigenaar en de IT auditor beoordelen jaarlijks de daarbij behorende procedures en bijlagen op actualiteit en op naleving van de beleidsuitgangspunten.

Hieronder volgt een overall planning:

1. Regelen

Wat	Wie	Wanneer	Gerealiseerd
Vaststellen Beveiligingsplan Suwinet	Teammanagement W&I	26 augustus 2014	26 augustus 2014
Bijpraten portefeuillehouder, brief VNG 12-11-2013 erbij betrekken	Afdelingshoofd W&I	Augustus 2014	September 2014
Vaststellen Beveiligingsplan Suwinet door college van B&W	Afdelingshoofd W&I	September 2014	25 november 2014
Voorleggen aan de Raad afstemmen met portefeuilehouder	portefeuillehouder	Eind 2014	Raadvergadering van 31 maart 2015 is de brief van 6 maart van het Ministerie van Sociale Zaken en Werkgelegenheid, Inspectie SZW. Onderzoek Veilig gebruik Suwinet 2014 ter kennisname voorgelegd
Zelfevaluatie Suwinet 2015 vaststellen in TMO	Team Staf	Augustus 2015	
Evaluatie van de enquete/vragenlijst aangaande beveiligingsplan delen in het TMO	Security officer	Augustus 2015	
Vaststellen Beveiligingsplan door heet TMO Suwinet 2016	Team Staf	Augustus 2015	
Rapportage evaluatie beveiligingsplan Suwinet ter kennisname in het MT			
Zelfevaluatie Suwinet gezien door het college	Team Staf	01 September 2015	
Vaststellen Beveiligingsplan Suwinet door het college	Team Staf	01 September 2015	
Beveiligingsplan Suwinet delen met omliggende gemeenten	Team Staf	September 2015	
Vaststellen vragenlijst onderzoek veilig gebruik Suwinet 2015 door het college	Team Staf	15 of 22 september 2015	

2. Uitvoeren

Wat	Wie	Wanneer	Gerealiseerd
Niet geoorloofde autorisaties suwinet beëindigen	Gebruikersbeheerder	20 augustus 2014	20 augustus 2014
Nieuwe autorisatiematrix invoeren	Gebruikersbeheerder	Week 33-34	22 augustus 2014
Zorgvuldigheids- en geheimhoudingsverklaringen Suwinet laten invullen en ondertekenen	Team Staf	Week 33	Op 31 oktober waren de verklaringen allemaal binnen
Autorisaties die zijn toegekend , verwerken	Gebruikersbeheerder	Week 33-34	22 augustus 2014

Suwinet gebruik uitdragen in de organisatie via de teamoverleggen	Team Staf	In augustus – september 2014.	TAZ 19-08-2014 WE 26-08-2014 PO 16-10-2014 IO 04-11-2014 Z&O 04-11-2014
Beschikbaar stellen beveiligingsplan Suwinet 2014 aan medewerkers	Team Staf	Via managementmail	27 augustus 2014
Plan opnemen in Handboek GWS	Team Staf		27 augustus 2014
Plan opnemen in Grip Schulinck	Team Staf	April 2015	23 juni 2015
Voorbereiden zelfevaluatie Suwinet inclusief onderbouwen van vragen	Team Staf, beveiigingsbeheerder	Juni-juli 2015	31 juli 2015
Rapportage bevindingen Zelfevaluatie Suwinet 2015 definitief maken	Afdeling FC IT auditor en afdeling W&I team staf , beveiligingsbeheerder	Juli 2015	31 juli 2015
Actiepunten zelfevaluatie afwerken en verwerken in beveiligingsplan	Team Staf, beveiligingsbeheerder	Augustus 2015	
Input voor de 2e Berap, paragraaf Suwinet	Security officer	Augustus 2015	
Enquête/vragenlijst opstellen voor de gebruikers Suwinet	Security officer	Juli 2015	4 augustus 2015
Evaluatie van de enquête en bevindingen terugkoppelen in TMO	Security officer	Augustus 2015	
Afronden evaluatie beveiligingsplan Suwinet	Security officer	Augustus 2015	
Plan opnemen op intercom	Team Staf, beveiligingsbeheerder	Juli 2015	24 juli 2015
Naar aanleiding van vastgesteld gemeente breed beveiligingsbeleid risico –analyse opstellen	IT auditor, beveiligingsbeheerder, Ciso	Oktober 2015	
Input voor het jaarwerk paragraaf Suwinet	Security officer	Januari jaarlijks	
Input voor de 1e Berap, paragraaf Suwinet	Security officer	Maart jaarlijks	
Nieuwe medewerkers introduceren in gebruik Suwinet	Team Staf, beveiligingsbeheerder	Continue	Bij aanmelding
Inplannen dat Suwinet periodiek onderwerp is van de teamoverleggen, bijv, n.a.v. uitgevoerde controles	Team Staf, security officer	continue	Wanneer er aandachtspunten zijn die teruggekoppeld moeten worden in de teamoverleggen
Veilig Suwinet als onderdeel van de BIG	Team Staf	September/oktober	
In de Nieuwsbrief W&I maandelijks kijken of er een item over Suwinet kan worden opgenomen	Team Staf, beveiligingsbeheerder	continue	

3. Rapporteren

Wat	**Wie**	**Wanneer**	**Gerealiseerd**
Rapportages BKWI dec 2013-mei 2014 beoordelen	Team Staf	Augustus 2014	23 oktober 2014
Bevindingen en eventuele maatregelen vaststellen	Teammanagersoverleg	September 2014	Oktober 2014
Rapportage BKWI juni- aug 2014 beoordelen	Team Staf	30 oktober 2014	30 oktober 2014
Bevindingen en eventuele maatregelen vaststellen	Teammanagersoverleg	30 oktober 2014	30 oktober 2014
Rapportage BKWI vanaf september 2014 maandelijks	Team Staf	continue	
Bevindingen en eventuele maatregelen vaststellen	Teammanagersoverleg	continue	

4. Handhaven en bijstellen

Wat	Wie	Wanneer	Gerealiseerd
P. Knoops coord Hit-team, autorisatie suwinet beëindigt. In oktober evalueren of hij de aansluiting mist.	Team Staf	oktober 2014	19 oktober 2014 P. Knoops is akkoord met de beëindiging
Bevindingen en maatregelen die voortvloeien uit de maandelijkse rapportage gebruik Suwinet	Afdelingshoofd W&I	Continue	
Gemeenten Peel 6.1 op de hoogte stellen van beveiligingsplan Suwinet	Team staf	Periodiek	
Evalueren en actualiseren beveiligingsplan Suwinet	Team Staf	Jaarlijks	

BIJLAGE 11 Classificatie van gegevens Suwinet processen

Versie	Datum	Status	Korte omschrijving wijziging	Besproken met:	Vastgesteld door
1.0	18 augustus 2015	Definitief	Bepalen classificatie n.a.v. vastgesteld IB beleid	M v.d. Ven-Pleite	M v.d. Ven-Pleite afdelingshoofd WI / informatie eigenaar

Algemeen
Om te kunnen bepalen welke beveiligingsmaatregelen minimaal dienen te worden getroffen t.a.v. de processen en informatiesystemen worden classificaties gebruikt. In het gemeentebreed IB beleid staat een classificatie op drie betrouwbaarheidsaspecten van informatie opgenomen, namelijk:

- beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatiesystemen;
- integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden.

De gegevens uit de Suwinet processen zijn in 2015 voor het eerst volgens dit gemeentebreed IB beleid geclassificeerd en door de informatie eigenaar in augustus 2015 vastgesteld. Daarnaast zijn in het IB beleid-plan Suwinet aanvullende normen vastgesteld. De gemeente moet op grond van de aan zeven essentiële normen uit het Normenkader 'Gezamenlijke elektronische Voorzieningen Suwinet beveiligingsmaatregelen nemen. Hierop wordt jaarlijks getoetst.

Classificatie van gegevens
De classificatie vanuit het gemeentebreed IB beleid is als volgt.

- beschikbaarheid : zonder gevolgen
- integriteit : kritisch
- vertrouwelijkheid : vertrouwelijk

Classificatie op basis van beschikbaarheid

Norm voor beschikbaarheid volgens gemeentebreed IB beleid

Klasse	Beschikbaarheid	Norm beschikbaarheid	Maatregelen
Zonder gevolgen (1/2)	Gegevens kunnen zonder gevolgen 5 werkdagen niet beschikbaar zijn.	Niet verplicht.	Geen verplichte maatregelen

Norm voor integriteit volgens gemeentebreed IB beleid

Integriteit	Classificatie criteria	Maatregelen
Kritisch	Het kwaliteitsniveau van de informatie/gegevens heeft een ernstige impact op een proces. - kan ernstige gevolgen hebben voor de betrokkene; - kan leiden tot ernstige schade voor de bedrijfsvoering van de gemeente of haar relaties; - kan ernstige consequenties voor de openbare orde en veiligheid hebben.	De volgende minimale beheer aspecten zijn doorgevoerd: - mutatie (CRUD) alleen mogelijk met juiste autorisatie - wijzigingen alleen op bron - periodieke foutcontrole verplicht - versie beheer verplicht - ondertekening door geautoriseerd persoon verplicht - functiescheiding verplicht - logging van CRUD en/of uitgifte verplicht - bron verificatie verplicht - input validatie verplicht - bewijslast verplicht (audit)

Norm voor vertrouwelijkheid volgens gemeentebreed IB beleid

Klasse	Vertrouwelijkheid	Classificatie criteria	Maatregelen
Vertrouwelijk (2)	Informatie waarvan de toegang is beperkt tot medewerkers, bestuursleden en hiertoe geautoriseerde afnemers en derden, voor de uitvoering van hun taak/functie. (bv: persoonsgegevens, medische gegevens, financiële gegevens)	Persoonsgegevens die direct of indirect informatie geven over de persoonlijke of economische situatie van een betrokkene, waarvan ongeautoriseerde blootstelling negatieve gevolgen heeft voor de betrokkene. Financiële en/of technische bedrijfsgegevens waaruit informatie kan worden afgeleid over de bedrijfsvoering of het productieproces van een betrokkene. Gegevens waarvan ongeautoriseerde blootstelling: ernstige gevolgen kan hebben voor de betrokkene; kan leiden tot ernstige schade voor de bedrijfsvoering van de gemeente of haar relaties; ernstige consequenties kan hebben voor de openbare orde en veiligheid.	Informatie met deze classificatie wordt technisch/organisatorisch tegen oneigenlijke inzage afgeschermd. Controleerbaarheid ten aanzien van wie inzage heeft gehad is verplicht.

Voor Akkoord:
Helmond, 18 augustus 2015

_____
M. v.d. Ven - Pleite
Informatie-eigenaar Suwinet