Gemeente Heerlen

GEMEENTEBLAD

Officiële uitgave van de gemeente Heerlen

Nr. 262370

12 oktober

2020

Gemeente Heerlen - Informatiebeveiligingsbeheer Suwinet gemeente Heerlen

Het college van burgemeester en wethouders van de gemeente Heerlen

OVERWEGING
gelet op het bepaalde in Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI);
mede gelet op de Algemene verordening gegevensbescherming (AVG);
mede gelet op de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG);
mede gelet op het bepaalde in de Regeling logging medewerkers gemeente Heerlen 2015;
mede gelet op het bepaalde in de BKWI-handleiding Toegangsrechten voor Suwinet-Inkijk;
mede gelet op het bepaalde in de BKWI Verantwoordingsrichtlijnen GeVS 2020;
mede gelet op het bepaalde in het Informatiebeveiligingsbeleid Suwinet gemeente Heerlen;
mede gelet op de instemming van de Ondernemingsraad;

BESLUIT
vast te stellen het navolgende: Informatiebeveiligingsbeheer Suwinet gemeente Heerlen

Beleidsinhoud
De gemeente deelt op basis van de Wet SUWI persoonlijke informatie van inwoners met een aantal organisaties. Het gaat om informatie over arbeidsverleden, loon, uitkeringen en opleiding. Het is natuurlijk heel belangrijk dat het delen van deze informatie zorgvuldig gebeurt. Daarvoor heeft de gemeente Heerlen het beveiligingsbeleid Suwinet vastgesteld, dit naast het informatiebeveiligingsplan Suwinet en het informatiebeveiligingsbeheer Suwinet.
Het informatiebeveiligingsbeleid Suwinet zegt wat over de interne organisatie, waaronder:

- Governance: relevante functies met hun taken en verantwoordelijkheden zoals bijvoorbeeld de beveiligingsfunctie
- Aansluitbeleid: de randvoorwaarden voor aansluiting op de Gemeenschappelijke elektronische Voorziening Suwi (GeVS, ook wel Suwinet genoemd). Het aansluitbeleid betreft het beleid aangaande de bescherming van de eigen informatiehuishouding in relatie tot de eigen delen van Suwinet en de via Suwinet beschikbaar gestelde gegevens.

Het informatiebeveiligingsplan Suwinet wordt jaarlijks of vaker, wanneer daar aanleiding toe is, geactualiseerd. Het informatiebeveiligingsplan bevat verbetervoorstellen op basis van evaluaties.
Het informatiebeveiligingsbeheer Suwinet behelst een ingerichte beheersorganisatie waarin beheerprocessen en evaluatieactiviteiten zijn vormgegeven. Bijvoorbeeld:

- Evaluatie van het aansluitbeleid
- Logging en rapportage
- Autorisatiebeleid.

Daarnaast is sanctiebeleid bij oneigenlijk gebruik van Suwinet opgesteld.

SUWI-Aansluitbeleid

Aanleiding

Volgens het bepaalde in de artikelen 5.22 en 6.4 van de Regeling Suwi moeten UWV, SVB, Colleges van B&W, het Inlichtingenbureau en de op de GeVS aangesloten Suwi en niet Suwi partijen maatregelen treffen gericht op het waarborgen van een exclusieve, integere, beschikbare en controleerbare gegevensverwerking en zich daarover verantwoorden.
Vanaf 1 januari 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO). De BIO vervangt onder meer de BIG en de BIR en voorziet in een uniform en uitgebreid normenkader informatiebeveiliging voor de gehele overheidssector. Organisaties die de BIO (moeten) implementeren werken daarmee aan het verzekeren van een adequaat niveau van informatiebeveiliging.

Verantwoording en ENSIA

Transparantie en verantwoording zijn instrumentele functies ten behoeve van de besturing. Transparantie is het bieden van informatie over sturing, implementatie en beheersingsaspecten van de gebruikte Suwinet services en/of Digitaal Klant Dossier (DKD).
Verantwoording is een middel om over de mate van “in control zijn” een verklaring af te geven. Met die verklaring verstrekt het College van B&W aan de Gemeenteraad het signaal greep te hebben op de sturing van de dienstverlening en de informatiebeveiliging.
Iedere afnemende partij verantwoordt zich in het eigen jaarverslag en levert voor 1 mei van het kalenderjaar volgend op het verantwoordingsjaar een Transparantierapportage aan BKWI.
Gemeenten verantwoorden zich vanaf 2017 over informatiebeveiliging volgens de ENSIAsystematiek, die betrekking heeft op de beveiliging van alle gemeentelijke verwerkingen waarbij gebruik wordt gemaakt van de Suwinet services en/of DKD. De opzet is zodanig dat de op deze wijze tot stand gekomen

verantwoording van het College van B&W aan de Gemeenteraad geschikt is om als basis te dienen voor de Transparantierapportage die bij BKWI moet worden ingediend. De transparantierapportage bestaat uit:

- Een in control verklaring van het College van Burgemeester en Wethouders
- Een getrouwheidsverklaring van een Register EDP-auditor.
- Indien van toepassing: een bijlage met een overzicht van de normen waaraan (m.b.t. Suwinet/DKD) niet wordt voldaan.

In de bijlage is beschreven aan welke normen (inclusief de bijbehorende subnormen) de interne beheersmaatregelen voor de GeVS worden getoetst en waarover gerapporteerd moet worden in de transparantierapportage. Interne beheersmaatregelen bij gemeenten dienen op de laatste dag van het jaar in opzet en bestaan aan de genoemde normen te voldoen, voor andere afnemers geldt dat voldaan moet worden aan opzet, bestaan en werking van de genoemde normen.

Inleiding

De Gezamenlijke elektronische Voorziening Suwi wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. Binnen de Suwiketen participeren drie type stakeholders: Bronhouders, Beheerders van de centrale en decentrale omgeving en Afnemers. De Bronhouders stellen (authentieke) gegevens beschikbaar aan Afnemers. De Afnemers hebben deze gegevens nodig voor de uitvoering van hun wettelijke taken.

De Beheerder van de centrale omgeving zorgt voor de transformatie, autorisatie, transport en routering van deze gegevens/berichten op basis van technische en communicatie faciliteiten en IT componenten conform wetgeving en geldige ketenafspraken.

De Beheerder van de decentrale omgeving verzorgt de ontsluiting van het centrale deel naar de gemeenten. Daarbij verzorgt zij de routering van de 'berichten-op-maat' en verzamelt de gegevens van gemeenten en fungeert als Bron voor de uitwisseling van gegevens met de ketenpartijen. Deze centrale en decentrale faciliteiten en IT componenten representeren de GeVS en zijn beschreven in de Suwi-Ketenarchitectuur (KArWel).

De gemeente Heerlen als bronhouder

Het Digitaal Klantdossier (DKD)

Het Digitaal Klantdossier (DKD) is een gemeenschappelijk, virtueel dossier. In het DKD wordt op het gebied van werk en inkomen informatie gedeeld door Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Sociale Verzekeringsbank (SVB) en gemeenten. Het DKD is ontwikkeld in het kader van de Wet eenmalige gegevensuitvraag (WEU), waarmee burgers voor de keten Werk en Inkomen maar eenmalig hun gegevens hoeven te verstrekken. De betrokken instanties moeten er verder voor zorgen dat die gegevens vervolgens digitaal voor iedere partij in de keten beschikbaar zijn.

Digitale aanlevering gegevensset gemeenten DKD

Om een volledig gevuld DKD voor burger en uitvoeringsorganisaties te kunnen garanderen, is digitale aanlevering van de gegevens door partijen wettelijk verplicht. Ook zijn gemeenten verplicht de afgesproken gegevensset binnen enkele seconden digitaal aan te leveren als hierom gevraagd wordt. Gemeenten leveren een vaste set gegevens aan het DKD. Er worden gegevens geleverd over:

- De klant; persoons- en adresgegevens;
- De aanvraag; voor welke wet, datum aanvraag en beslissing en de beslissing zelf;
- De uitkering; soort, begin- en eindedatum, normbedragen, inhoudingen en maatregelen;
- De vorderingen; datum en reden vordering, bedragen aanvang en saldo, status vordering;
- De bijzondere bijstand; soort kosten en datum betaalbaarstelling;
- De re-integratie en participatie; begin- en eindedatum re-integratie inzet met een omschrijving, loonkostensubsidie, participatieladder.

DKD en CBS

De gegevens die worden uitgewisseld in het DKD zijn veelal dezelfde gegevens die via het Centraal Bureau voor de Statistiek (CBS) landelijk worden uitgevraagd in de statistieken. Voor de aanlevering van deze gegevens in het meest actuele bericht verwijzen wij naar het document Richtlijnen gemeenten, selecties voor aanlevering.

De gemeente Heerlen als afnemer

De gemeente Heerlen gebruikt de volgende Suwinet-service:

- Suwinet-Inkijk
- Suwinet-Meldingen
- Suwinet-Mail.

De gemeente ontvangt voor de volgende Suwitaken gegevens:

- Suwinet-Inkijk voor GSD

De gemeente ontvangt voor de volgende niet-Suwitaken gegevens:
- Suwinet-Inkijk voor burgerzaken
- Suwinet-Inkijk voor het RMC

Suwinet-Inkijk
Voor deze functionaliteit wordt gebruik gemaakt van de landelijke Cloud-voorziening beschikbaar gesteld door BKWI. De beveiligingsmaatregelen in deze worden dan ook door BKWI bepaalt.
Binnen de gemeente Heerlen is toegang tot Suwinet-Inkijk afgeschermd en is inloggen alleen mogelijk vanuit onze eigen afgeschermde omgeving (tweefactor authenticatie om toegang te krijgen tot onze omgeving en daarna nogmaals een inlogcode en wachtwoord om in te loggen op Suwinet-Inkijk).

Suwinet-Meldingen
Voor deze functionaliteit wordt gebruik gemaakt van de landelijke Cloud-voorziening beschikbaar gesteld door BKWI. De beveiligingsmaatregelen in deze worden dan ook door BKWI bepaalt.
Suwi-meldingen tussen de gemeente Heerlen als Suwi-afnemer en Suwi-bronhouders worden verstuurt via de landelijke voorziening. Het gaat hierbij om meldingen die daadwerkelijk relevante gegevens bevatten; een gegeven of een situatie is gewijzigd. De bronhouder controleert en verwerkt vervolgens deze meldingen.

Suwinet-Mail
Suwinet-Mail is een door het BKWI geboden dienst die partijen uit het Suwidomein in staat stelt om e-mails te versturen via het besloten netwerk Suwinet. De e-mails gaan dan niet meer over publieke netwerken zoals internet. De voorziening Suwinet-Mail kan specifiek gebruikt worden voor het doen van navraag of een korte mededeling over een gezamenlijke klant waarbij privacygevoelige informatie uitgewisseld wordt en mondelinge communicatie niet lukt.
De verzender moet de extensie .suwi toe te voegen aan het email adres van de geadresseerde. Het email adres van gebruiker@domein.nl wordt gebruiker@domein.nl.suwi
Om foute adressering te voorkomen raadt BKWI aan om adressen van organisaties die ook van Suwinet-Mail gebruik maken in het adresboek te voorzien van de uitgang .suwi. Binnen de gemeente Heerlen is dit uiteraard dan ook gedaan. De aansluiting op Suwinet-Mail van de gemeente Heerlen is direct geregeld via het interne adressenboek en dit adressenboek wordt beheerd door de serverbeheer (Parkstad-IT).
Een lijst met organisaties die aangesloten zijn op Suwinet-Mail is te vinden op www.bkwi.nl onder Suwinet/ Suwinet-Mail: TabelSuwinetMailDomeinnamen

Gemnet
Gemnet is het landelijke besloten netwerk voor overheden, en dit wordt technisch beheert door KPN. Via dit netwerk wordt oa Suwinet-mail verzonden.
Met het Gemnet-netwerk heeft iedere lokale overheid de beschikking over een besloten digitaal netwerk met het allerhoogste veiligheidsniveau. Zo worden privacy- en securityproblemen met data-uitwisseling voorkomen. Het Gemnet-netwerk biedt daarnaast als koppelnetwerk dé toegang tot het besloten Digi-netwerk om gebruik te maken van landelijke voorzieningen en datacommunicatie met andere overheden. Tot slot is het Gemnet-netwerk onafhankelijk van het openbare internet en bovendien redundant uitgevoerd, waardoor het garant staat voor een zeer hoge beschikbaarheid.
De netwerkbeheerder (Parkstad-IT) beheert de aansluiting van de gemeente Heerlen op Gemnet.

Beleidskaders Informatiebeveiliging Suwinet
In onderstaande tabel is minimale evaluatiecyclus van deze drie documenten uitgewerkt:

Document	Minimale cyclus	Eerst komende jaar van uitvoering	Opmerkingen
IBbeleid Suwinet	3 jaarlijks	2020	
IBbeveiligingsplan Suwinet	Jaarlijks	2020	
IBbeheer Suwinet	Jaarlijks	2020	

Dataclassificatie en beheersmaatregelen Suwinet (BBN-2)

Informatiebeveiliging is het geheel van maatregelen en procedures om informatie te beschermen. Het doel is: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en de informatievoorziening en het minimaliseren van de kans op beveiligingsincidenten en de impact hiervan in relatie tot het bedrijfsbelang en de bedrijfsprocessen.
Het beschermingsniveau van data wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van informatie:

- Beschikbaarheid: hoeveel en wanneer data toegankelijk is en gebruikt kan worden. De onderscheiden niveaus zijn: niet nodig; noodzakelijk; belangrijk en essentieel.
- Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid). De onderscheiden niveaus zijn: niet zeker; beschermd; hoog en absoluut.
- Vertrouwelijkheid: de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.

De onderscheiden niveaus zijn: openbaar; bedrijfsvertrouwelijk, vertrouwelijk en geheim.
Het toekennen van classificatieniveaus aan data is van groot belang, omdat daarmee het (vereiste) beschermingsniveau kenbaar gemaakt wordt.
De gegevens van Suwinet vallen in de categorie vertrouwelijk (BBN-2). De vanuit de BIO opgelegde beheersmaatregelen voor dit niveau zijn dan ook van toepassing. Middels de ENSIA wordt getoetst of is voldaan aan deze beheersmaatregelen.

Periodieke DPIA Suwinet

Conform het Informatiebeveiligingsbeleid Suwinet gemeente Heerlen moet voor de gegevensverwerking Suwinet een Data Protection Impact Assessment (DPIA) worden uitgevoerd. Omdat de gegevensverwerkingen risicovol zijn, zal de DPIA driejaarlijks moeten worden uitgevoerd, voor het eerst in 2020.

Logging en rapportage

Voor de uitvoering van veel (gemeentelijke) taken op grond van de bijvoorbeeld de Participatiewet en de IOAW/Z, is het kunnen raadplegen van persoonsgegevens van burgers via Suwinet-Inkijk essentieel. Persoonsgegevens zijn per definitie privacygevoelig en dienen met de hoogst mogelijke zorgvuldigheid te worden gebruikt en behandeld.
Om die zorgvuldigheid te bewerkstelligen zijn er meerdere maatregelen te nemen. Vooral door:

a. een zorgvuldig, adequaat en up-to-date autorisatiebeleid;
b. het beperken van de toegang tot gegevens van alleen relevante personen;
c. en het afstemmen van de gegevensset op de te verrichten wettelijke taken kan een gemeente de privacy van burgers beter waarborgen.

Als aan deze voorwaarden is voldaan blijft de toegang tot gegevens in Suwinet-Inkijk voorbehouden aan geautoriseerde medewerkers. En als de gemeente werkt met whitelisting wordt ook bereikt dat die geautoriseerde medewerkers niet zondermeer gegevens kunnen opvragen van burgers waar geen dienstverleningsrelatie mee is of is geweest.
Deze maatregelen zijn te beschouwen als maatregelen aan de ‘voorkant’ van het proces en minimaliseren het risico op oneigenlijk gebruik of zelfs misbruik van gegevens. Toch blijft het ook noodzakelijk om aan de ‘achterkant’ van het proces het gebruik van Suwinet-Inkijk te monitoren en te controleren. Daarvoor maken wij als gemeente gebruik van de gebruikersrapportages Suwinet-Inkijk. BKWI heeft twee soorten rapportages: generieke en specifieke rapportages.

Het analyseproces gebruikersrapportages

a. Opvragen van de gebruikersrapportage: De daartoe geautoriseerde medewerker haalt de gebruikersrapportage op uit Suwinet. Analyse vindt plaats zoals binnen de organisatie omschreven en vastgelegd. Een exemplaar is voor de gebruikersbeheerder met het oog op de tabellen over het accountbeheer.
b. Analyse van de gebruikersrapportage en trekken van conclusies: De analyse van tabellen leidt tot conclusies over het algemeen gebruik van Suwinet, de zorgvuldigheid, het veilig gebruiken de actualiteit en proportionaliteit van het accountbeheer. De bevindingen worden kort gerapporteerd, de Privacy Officer is hiervoor verantwoordelijk.
c. Bij twijfel over een juist gebruik - vervolgstappen: Zijn er op basis van de rapportages twijfels over het zorgvuldig gebruik, dan zijn er verschillende vervolgstappen mogelijk. Allereerst kan de rapportage worden besproken met een teamleider of het team (het team weet dat er controles plaatsvinden) om meer inzicht te krijgen in de achtergrond van bijvoorbeeld een afwijkend patroon. Zijn er onvoldoende verklaringen, dan kan een specifiek rapportage worden opgevraagd bij BKWI, waarin het raadpleeggedrag op persoonsniveau wordt getoond. Het opvragen van een specifieke rapportage kan alleen door een daartoe gemandateerde functionaris.
d. Geen directe aanleiding wel nader onderzoek als vast onderdeel: Gemeenten kunnen ook, als onderdeel van het interne controle plan, een bepaald aantal keren per jaar specifieke rapportages opvragen om bijvoorbeeld steekproeven te doen.
e. Analyse specifieke rapportage: vervolgstappen: De specifieke rapportages worden geanalyseerd door een daartoe gemandateerd persoon, binnen de gemeente Heerlen de Privacy Officer. Blijkt er een afwijkend patroon bij een medewerker, dan gaat de Privacy Officer een gesprek aan met de leidinggevende om naar de achtergronden daarvan te vragen. Bij aanwijzingen voor norm

overschrijdend gedrag wordt de zaak overgedragen aan het organisatie onderdeel dat het integriteitsbeleid uitvoert. De Privacy Officer legt de bevindingen van de analyse van de specifieke rapportage vast.

f. Overdracht: zie verder Sanctiebeleid bij oneigenlijk gebruik van Suwinet gemeente Heerlen

Generieke rapportages

BKWI verstrekt de aangesloten organisaties op reguliere basis generieke rapportages over het gebruik van Suwinet. Deze geanonimiseerde rapportages zijn bedoeld om het management te ondersteunen bij het beoordelen van het gebruik van Suwinet. De tabellen in de rapportage zijn gebaseerd op automatische logging van alle raadplegingen op Suwinet-Inkijk.
Daarbij worden de volgende handelingen gelogd (inclusief datum en tijdstip):

- Iedere inlog van een medewerker op Suwinet-Inkijk met zijn inlogcode en wachtwoord,
- Iedere keer dat met een BSN persoonsgegevens worden gezocht,
- Iedere keer dat met andere zoeksleutel dan BSN persoonsgegevens worden opgezocht,
- Iedere raadpleging van een pagina met persoonsgegevens of zonder persoonsgegevens (algemene gegevens).

Aan de hand van de in de tabellen opgenomen cijfers voor onze gemeente, de vergelijkingen met andere gemeenten en onze kennis van de eigen werkprocessen, kunnen wij de cijfers interpreteren. Daarbij wordt gebruik gemaakt van de informatie in bijlage 4.
Deze rapportage biedt inzicht in het gebruik van Suwinet Services door medewerkers van onze organisatie. De gegevens in deze rapportage zijn niet herleidbaar tot de individuele medewerkers, maar herleidbare gegevens kunnen wel opgevraagd worden, dit via de zogenaamde specifieke rapportages. In de rapportage worden aantallen en percentages weergegeven. Om houvast te geven bij deze cijfers, wordt in sommige tabellen een vergelijking van het gebruik van onze organisatie gemaakt met het gemiddelde van de gemeentelijke afnemers.
Tevens beschikken wij hiermee over de mogelijkheid om toezicht te houden op het gebruik van klantgegevens en hierop te sturen. Dit is nodig, omdat het gebruik van Suwinet aan regels is gebonden. Suwinet-Inkijk mag alleen gebruikt worden voor de uitvoering van taken:

- Die in de Wet SUWI en de Participatiewet zijn vermeld of;
- Die zijn genoemd in de gegevensleveringsovereenkomst(en), conform het Aansluitprotocol (bijlage bij de Regeling SUWI).

Deze rapportage bevat vier onderdelen die achtereenvolgens het totale gebruik, het zorgvuldig gebruik, het accountbeheer en het doelmatig gebruik van Suwinet-Inkijk behandelen. Omdat onze organisatie gebruik maakt van Suwinet-Mail, zijn hiervoor twee aparte tabellen opgenomen in het hoofdstuk over doelmatig gebruik.
Deze rapportage verschijnt iedere maand en rapporteert over de voorgaande zes maanden. Hiervoor is de rol 'opvragen gebruiksrapportages (R347)' nodig. De privacy officers tbv Suwinet beoordelen deze rapportage maandelijks. Hierbij wordt gelet op afwijkingen ten opzichte van voorgaande perioden, en afwijkingen ten opzichte van vergelijkbare gemeenten.
De rapportage en de beoordeling voor de privacy officer wordt maandelijks beschikbaar gesteld aan de betreffende teamleiders. De teamleider kan op basis van de gebruikersrapportage bezien of er zorgvuldig en efficiënt wordt gemaakt van Suwinet-Inkijk of dat er nader onderzoek nodig is. Hij/zij is ook degene die zich in de lijn verantwoordt over het gebruik van Suwinet.
Op basis van de dataclassificatie Suwinet (BBN-2) worden de rapportages twee jaar bewaart.

Specifieke rapportages

Naast deze generieke rapportages kunnen aangesloten organisaties specifieke rapportages opvragen, bijvoorbeeld ter ondersteuning van het interne controleproces. Deze rapportages worden niet op reguliere basis verstrekt. Ze bevatten gegevens over de handelingen van geautoriseerde gebruikers, ofwel persoonsgegevens. Daarom is op deze rapportages de Algemene Verordening Gegevensbescherming van toepassing.
Het BKWI kan voor iedere tabel uit de generieke rapportage een specifieke rapportage aanleveren.
De privacy officers tbv Suwinet bepaalt of een specifieke rapportage gemaakt wordt. Hierbij wordt op detailniveau gekeken naar het daadwerkelijke gebruik van de Suwinet-Inkijk.
Op basis van de dataclassificatie Suwinet (BBN-2) worden de rapportages twee jaar bewaart.

Verslag aan portefeuillehouder en college

Ieder kwartaal wordt de beoordeling van de generieke rapportage gezonden aan de portefeuillehouder Informatiebeheer. Ook wordt daarbij melding gemaakt van eventueel opgevraagde specifieke rapportages en de beoordeling daarvan.
Minimaal een keer per jaar wordt de beoordeling van de generieke rapportage over de afgelopen twaalf maanden gezonden aan het college. Ook wordt daarbij melding gemaakt van eventueel opgevraagde specifieke rapportages en de beoordeling daarvan.

Autorisatiebeleid

Aanvraag

Informatiesystemen mogen alleen door medewerkers worden gebruikt als die vanuit de bedrijfsfunctie noodzakelijk zijn. Autorisaties mogen dus alleen verleend worden aan personen op basis van zakelijke noodzaak. De proceseigenaar (lees teamleider) van het door het informatiesysteem ondersteunde proces is eindverantwoordelijk voor het verlenen van autorisaties. Indien personen toegang tot een applicatie nodig hebben, wordt dit door zijn of haar teamleider, aangevraagd. Nieuwe autorisatieaanvragen (alsook wijzigingen) volgen het change management-proces. Dit geldt zowel voor permanente toegang tot de systemen als voor tijdelijke toegang. De aanvraag wordt gedaan middels het invullen en versturen van een (web)formulier. Dit gebeurt ook voor het aanvragen van een wijziging.
De volgende situaties kunnen zich voordoen:

1. aanvraag voor een nieuwe medewerker;
2. verandering van functie binnen de organisatie;
3. uitdiensttreding van de medewerker;
4. verdenking van oneigenlijk gebruik.

Generieke personeelsmutaties en functiewijzigingen worden direct door het team OPC vanaf het moment van wijziging doorgegeven aan de verantwoordelijken van de verschillende applicaties.
Verdenkingen van oneigenlijk gebruik worden door de verantwoordelijke in overleg met de Security Officer Suwinet doorgegeven. De betreffende applicatiebeheerder verwerkt de autorisatiewijziging(en) in de betreffende applicaties in nauw overleg met de functioneel beheerder.

Autorisatiematrix Suwinet-Inkijk GSD gemeente Heerlen

Op basis van de functieprofielen van de gemeente Heerlen is in onderstaande fijnmazige autorisatiestructuur in een matrix uitgewerkt. Afwijking hiervan is alleen toegestaan na akkoord van de Security officer.
Binnen Suwinet-Inkijk worden de gegevens uit de verschillende bronnen separaat of gecombineerd getoond op Inkijkpagina's. Een pagina die gegevens uit één bron toont, noemen we een bronpagina. Een pagina die gegevens uit meerdere bronnen toont, noemen we een overzichtspagina.
Toegang verstrekken tot deze pagina's doen wij als gemeente zelf en kan op twee manieren, door:

- de pagina aan een eigen rol (aangemaakt door u zelf) toevoegen. Alle accounts met deze rol krijgen dan toegang tot de pagina.
- de pagina als een vaste rol (aangemaakt door BKWI) met dezelfde naam aan een account toekennen.

Voor de duidelijkheid sluiten de eigen rollen in Suwinet-Inkijk altijd aan op de binnen de organisatie gebruikte functieprofielen.

Wettelijke grondslag GSD

In onderstaande tabel is per functieprofiel aangeven welke wettelijke grondslag van toepassing is:

	Wettelijke grondslag						
HR21 functieprofiel	Wet SUWI / Besluit SUWI / Regeling SUWI	Participatie wet	Wet Inkomensvoorziening oudere en gedeeltelijke arbeidsongeschikte werkloze werknemer IOAW	Wet Inkomensvoorziening oudere en gedeeltelijke arbeidsongeschikte werkloze gewezen zelfstandige IOAZ	Wet gemeentelijke schuldhulpverlening	Wet BRP	Wet Inburgering
Consulent Inkomen	X						
Consulent re-integratie	X						X
Klantmedewerker Bijz Voorz. WS							
Consulent Handhaving en Debiteuren							
Medewerker sociale recherche							
Consulent zelfstandigenloket	X			X			
Medewerker Uitkeringsadministratie							
Juridisch stafadviseur							

Overzichtspagina's

	Eigen rol (= functieprofiel)

Vaste Suwinet rol	Consulent Inkomen	Consulent reintegratie	Klantmedewerker Bijz Voorz. WS	Consulent Handhaving en Debiteuren	Medewerker sociale recherche	Consulent zelfstandigenloket	Medewerker Uitkeringsadministratie	Juridisch stafadviseur
Handhaving					X			
Kostendelerstoets	X		X		X		X	X
Landelijk doelgroepregister								
Rechtmatigheid+	X	X	X			X	X	X
Re-integratie		X						X
Terugvordering en Verhaal				X				

Bronpagina's

	Eigen rol (= functieprofiel)							
Vaste Suwinet rol	Consulent Inkomen	Consulent reintegratie	Klantmedewerker Bijz Voorz. WS	Consulent Handhaving en Debiteuren	Medewerker sociale recherche	Consulent zelfstandigenloket	Medewerker Uitkeringsadministratie	Juridisch stafadviseur
Bedrijvenregister		X			X			
Belastingdienst	X		X	X	X	X	X	X
Bijstandsregelingen	X	X	X	X	X	X	X	X
DUO gegevens	X	X	X	X	X	X	X	X
Fraude vorderingen				X	X			
GBA	X	X	X	X	X	X	X	X
GBA-volledig								
Inkomstenverhoudingen								
Kadaster	X		X	X	X	X		X
RDW		X		X				
RDW+					X			
RDW Peildata	X		X		X	X		X
SVB gegevens	X		X	X	X	X	X	X
UWV uitkeringen	X		X		X	X	X	X
UWVWb	X	X	X		X	X		X

Zoekpagina's

	Eigen rol (= functieprofiel)							
Vaste Suwinet rol	Consulent Inkomen	Consulent reintegratie	Klantmedewerker Bijz Voorz. WS	Consulent Handhaving en Debiteuren	Medewerker sociale recherche	Consulent zelfstandigenloket	Medewerker Uitkeringsadministratie	Juridisch stafadviseur
Zoek in GBA				X				
Zoek+ in GBA					X			
Zoek in Kadaster				X	X			
Zoek in PIVA								
Zoek in RDW				X				
Zoek in RDW+					X			

Overig

	Eigen rol (= functieprofiel)							
Vaste Suwinet rol	Consulent Inkomen	Consulent reintegratie	Klantmedewerker Bijz Voorz. WS	Consulent Handhaving en Debiteuren	Medewerker sociale recherche	Consulent zelfstandigenloket	Medewerker Uitkeringsadministratie	Juridisch stafadviseur
Fraude scorekaart	X		X		X	X		
SBR Query (SuwiBedrijvenregister)		X						

Onderhouden status wijzigingsverzoeken *volgt*								
Correctieservice	X	X	X	X	X	X	X	X
Portaal Inburgering (diverse rollen) *volgt*								

Bijzondere taken

			Eigen rol (= functieprofiel)		
Vaste Suwinet rol	Suggestie voor taken	Toelichting / bijzonderheden	Gebruikersbeheerder	Gemandateerde	Securitty Officer
Beheer: ww & blokkeren	Alleen de 'lichte' taken rondom gebruikersbeheer Suwi	Met deze rol kan de gebruikersbeheerder wachtwoorden (ww) resetten en accounts (de)blokkeren. Het is een beperkte rol van de gebruikersbeheerder.	X		
Gebruikersadministratie	Alle taken rondom gebruikersbeheer Suwi	Met deze uitgebreide rol kan de gebruikersbeheerder Suwi-accounts en autorisaties aanmaken en beheren (blokkeren, deblokkeren, muteren, wachtwoorden resetten, rollen bepalen, toekennen en intrekken).	X		
Onderhouden correctieservice	Specifieke taken in gebruikersbeheer Suwi	Suwinet biedt bronhouders de mogelijkheid de kwaliteit van gegevens te verbeteren door deze open te stellen voor correctie (burger) of terugmelding (professional). Op deze pagina kunnen de instellingen van de correctieservice worden beheerd.	X		
Opvragen generieke gebruiksrapportages	Taken rondom het gebruikersbeheer Suwi en interne controle	Via deze link kan de geanonimiseerde gebruiksrapportage worden opgehaald. Deze maandelijkse rapportage geeft inzicht in het gebruik van Suwinet door uw gemeente over de afgelopen 6 maanden. De rapportage leent zich voor bespreking met het management en Security Officer en kan aanleiding zijn om nadere, meer specifieke rapportage op te vragen door de bij het BKWI geregistreerde gemandateerde.		X	
Opvragen specifieke gebruiksrapportages	Taken rondom de interne controle	Het opvragen van specifieke gebruikersrapportage kan alleen plaatsvinden door een daarvoor door de GSD gemandateerde en bij BKWI geregistreerde medewerker. Specifieke rapportages zijn alleen op aanvraag beschikbaar en lenen zich voor interne onderzoeken bij de GSD.		X	

Autorisatiematrix Suwinet-Inkijk RMC gemeente Heerlen

Wettelijke grondslag RMC

In onderstaande tabel is per functieprofiel aangeven welke wettelijke grondslag van toepassing is:

	Wettelijke grondslag	
HR21 functieprofiel	Wet SUWI / Besluit SUWI / Regeling SUWI	Wet educatie en beroepsonderwijs inzake regionale samenwerking voortijdig schoolverlaten en jongeren in een kwetsbare positie
RMC medewerker	X	X

RMC-Inkijk module

	Eigen rol (= functieprofiel)					
Vaste Suwinet rol	Consulent met RMC-taken	Cosnulent kwetsbare jongeren	Medewerker bedrijfsvoering	Functioneel beheer	Privacy-officer	CIO
RMC medewerker	X	X				

Gebruikersbeheerder	X	X		
Opvragen generieke rapportages	X	X	X	X
Opvragen specifieke rapportages			X	X

Betreft uitsluitend door het BKWI vastgestelde rollen en bevoegdheden, geen afwijkingen binnen een rol mogelijk.

Goedkeuring en verwerking

Nieuwe autorisatieaanvragen volgen het Change Management-proces, en worden dus aangevraagd bij de Helpdesk. Autorisaties worden geregistreerd middels het gebruik van de autorisatiematrix. Aan de hand van de opgestelde autorisatiematrix autoriseert de verantwoordelijke al dan niet de autorisatieaanvraag.

Autorisaties dienen daarbij vooraf te worden getoetst aan het functieprofiel van de te autoriseren persoon ter voorkoming van het toekennen van nodeloos veel rechten waar eventueel misbruik van gemaakt kan worden. Bij de aanvragen voor toegang wordt onderscheid gemaakt tussen aanvragen zonder verdere privileges op het systeem (eindgebruikers) en aanvragen met privileges op het systeem (beheerders). De toegekende autorisaties worden in de autorisatiematrix bijgehouden door de functioneel beheerder van de desbetreffende applicatie.

Na goedkeuring van de verantwoordelijke wordt de autorisatie op het netwerk en in het desbetreffende systeem geïmplementeerd door de desbetreffende technisch beheerder. De functioneel beheerder implementeert de autorisaties binnen de applicaties.

Verantwoordelijkheden

Taken en verantwoordelijkheidsgebieden t.a.v. autorisatiebeheer worden gescheiden en separaat belegd om mogelijkheden tot ongeautoriseerde of onbedoelde wijziging of misbruik te beperken.

We onderscheiden de volgende rollen:

- Teamleider/Domeinmanager: beslissingsbevoegdheid t.a.v. de aanvraag voor toegang tot een systeem
- Security Officer: is binnen de organisatie het aanspreekpunt en de verantwoordelijke voor alle activiteiten, op het gebied van informatiebeveiliging rondom Suwinet en rapporteert direct aan B&W.
- Applicatiebeheerder: is binnen de organisatie het aanspreekpunt en de verantwoordelijke voor het beheer van de applicatie Suwinet.
- Gemandateerde: is binnen de organisatie gemachtigd tot het aanvragen en ontvangen van specifieke rapportages aangaande het gebruik van Suwinet; dit is de Privacy Officer tbv Suwinet.
- Gebruikersbeheerders: dat zijn gemandateerde medewerkers die bevoegd zijn om medewerkers van de eigen organisatie toegang te geven tot Suwinet-Inkijk.
- Functioneel beheerder: aanvragen/ toewijzen en controleren van autorisatieaanvragen autoriseren van de aanvragen voor toegang voor de medewerkers.
- Applicatiebeheerder: technische realisatie van de aanvragen binnen de desbetreffende informatiesystemen (in de gebruikersadministratie).
- Technisch beheerder: technische realisatie van de aanvragen binnen de ICT-infrastructuur (Netwerk-, server-, dba-beheer).
- Gebruiker: de medewerker die gebruik maakt van Suwinet.
- Bewijzer: in de zin van audit, de persoon/specialist die namens de organisatie verklaart in hoeverre de organisatie voldoet aan de gestelde eisen en regels. Dit is vaak een functioneel beheer, applicatiebeheerder, gebruikersbeheerder, technisch beheerder, maar kan ook een andere functionaris zijn.
- Beoordelaar: in de zin van audit, de leidinggevende die de verklaringen van bewijzers beoordeeld en indien van toepassing vrijgeeft voor gebruik binnen de audit. Binnen onze organisatie dus de teamleider of domeinmanager.

Toetsing & evaluatie

Verleende autorisaties dienen regelmatig te worden geëvalueerd, getoetst en indien nodig te worden herzien. De beheerders stellen daarvoor regelmatig overzichten op met de uitstaande bevoegdheden. Deze overzichten worden door de verantwoordelijken beoordeeld op actualiteit en zo nodig worden de autorisaties aangepast. Dit gebeurd voor eindgebruikers één maal per halfjaar en voor beheerders één maal per kwartaal.

Ook het team OPC verstrekt op regelmatige basis een overzicht met de personeelsmutaties uit de afgelopen periode aan de technisch- en applicatiebeheerder zodat een controle tussen de werkelijke en de geïmplementeerde situatie kan plaatsvinden.

Op centraal niveau dient er een overkoepelend overzicht te zijn van verleende autorisaties voor de verschillende applicaties. Zoals beschreven worden verleende autorisaties gedocumenteerd in een autorisatiematrix. Een digitale kopie van deze matrix dient te worden aangeleverd aan de Security Officer die het centrale overzicht bewaakt.

Soort Gebruiker	Minimale cylcus	U itvoering in periode	Opmerkingen

Eindgebruiker	Één maal per halfjaar	Maart 2020 Oktober 2020
Beheerders	Één maal per kwartaal	Januari 2020 April 2020 Juli 2020 Oktober 2020

Inwerkingtreding

Dit informatiebeveiligingsbeheer Suwinet treedt in werking na publicatie. Dit kader wordt minimaal één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, geëvalueerd, beoordeeld en zo nodig bijgesteld en vastgesteld. Aanpassingen van dit kader worden bekendgemaakt. De meest actuele versie van dit kader is te vinden op www.overheid.nl.

Aldus besloten in de vergadering van het college der gemeente Heerlen op 6 oktober 2020.
de burgemeester,
drs. R. Wever
de secretarisa.i.,
L. Schouterden

Bijlage 1: Scope van de verantwoording: normenkader GeVS vanaf 2020

Deze bijlage beschrijft aan welke normen (inclusief de bijbehorende subnormen) de interne beheersmaatregelen voor de GeVS worden getoetst en waarover gerapporteerd moet worden in de transparantierapportage. Interne beheersmaatregelen bij gemeenten dienen op de laatste dag van het jaar in opzet en bestaan aan de genoemde normen te voldoen, voor andere afnemers geldt dat voldaan moet worden aan opzet, bestaan en werking van de genoemde normen.

Hoofdstuk	Nummer	Normen
5. Informatiebeveiligingsbeleid	5.1.1	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
	5.1.2	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
6. Organiseren van informatiebeveiliging	6.1.1	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
	6.1.2	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
7. Veilig personeel	7.2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
9. Toegangsbeveiliging	9.2.1	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
	9.2.2	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
	9.2.5	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
	9.2.6.	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
10. Cryptografie	10.1.1	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
12. Beveiliging	12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben
	12.4.1	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
	12.4.2.	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang
18. Naleving	18.1.4	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving

Bijlage 2 – Verklaring zorgvuldig gebruik Suwinet

Door aansluiting op Suwinet is het mogelijk om gegevens uit te wisselen met o.a. de Belastingdienst, de Informatiebeheergroep, het Uitvoeringsorgaan Werknemersverzekeringen, het Werkbedrijf, de RDW en gemeenten (zijnde de bronnen). Als gevolg daarvan zijn genoemde instanties te beschouwen als "verantwoordelijke" in de zin van de Algemene Verordening Gegevensbescherming (AVG) en daarom allemaal gebonden aan de bepalingen in deze wet. In de toekomst zal het aantal bronnen uitgebreid worden. Deze verklaring geldt ook voor bronnen die in de toekomst aangesloten gaan worden.
De gemeente is op grond van voornoemde bepalingen gehouden om interne maatregelen te nemen ter voorkoming van een (mogelijk) onrechtmatig, onregelmatig of doeloverschrijdend gebruik van de beschikbare (persoons-) gegevens. Dit betekent dat de gemeente Heerlen de verplichting heeft om regelmatig (met behulp van zogeheten auditlogginggegevens) te laten controleren of het gebruik van de gegevens uit Suwinet niet onwettig geschiedt of verder gaat dan is toegestaan.

Ondergetekende: .....
Team: .....

verklaart:

- het raadplegen van de gegevens in Suwinet te beperken tot de gegevens van inwoners die bij haar of hem in behandeling zijn voor zover het de Participatiewet, loaw, loaz, Bbz betreft;
- deze gegevens enkel aan te wenden voor het behandelen van de desbetreffende uitkeringsaangelegenheid voor zover het de Participatiewet, loaw, loaz, Bbz betreft;
- er voor te zorgen dat het gebruik van de escapefunctie navolgbaar is in de vakapplicatie en/of Suwinet-Inkijk. Als dit niet mogelijk is, de raadpleging bij te houden op het formulier "Afwijkende Raadpleging Suwinet".
- op de hoogte te zijn van de controle die de security- en privacy-officers regelmatig dienen in te stellen;
- kennis genomen te hebben van de informatie inzake veilig telewerken;
- op de hoogte te zijn dat er onderzoek plaats zal vinden / maatregelen genomen zullen worden als er sprake lijkt van onjuist gebruik van de gegevens van Suwinet-Inkijk en/of andere Suwinet services.

Datum: .....
Handtekening: .....

Bijlage 3 – Verantwoording afwijkende Suwinet raadplegingen
Onderstaande tabel geldt voor Suwinet raadpleging waarbij gebruik wordt gemaakt van de escape-functionaliteit, met reden anders.
Deze tabel dient afgeschermd te worden opgeslagen op een niet toegankelijke plek.

Naam: .....
Team: .....

BSN	NAW	Datum	Reden raadpleging

Bijlage 4 – Toelichting tabellen generieke gebruiksrapportage Suwinet-Inkijk

Tabel	Signaal	(mogelijke) Vervolgactie
Hoofdstuk 1 – algemeen beeld gebruik Suwinet-Inkijk		
1.1: totaal gebruik Deze tabel bevat het absoluut aantal raadplegingen 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.	Als er niet onmiddellijk een verklaring is voor een afwijking in het patroon, dan is het raadzaam dat een teamleider wordt geïnformeerd. Als er ook afwijkingen in andere tabellen worden gevonden, dan is het raadzaam een specifieke rapportage op medewerkersniveau op te vragen bij het BKWI. Dat kan van alle accounts of van specifieke rollen.
Hoofdstuk 2 – Zorgvuldig en veilig gebruik		
2.1 Percentage raadplegingen op zoeksleutel anders dan BSN. De norm is om op te vragen via het BSN. Alleen specifieke functionarissen zijn geautoriseerd voor andere zoeksleutels (zgn. 'zware rol'). Zij kunnen ook buiten het BSN persoonsgegevens raadplegen, zoals op naam en geboortedatum.	Bij een plotselinge stijging is de vraag: • zijn er meer medewerkers geautoriseerd voor 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 te veel medewerkers geautoriseerd voor deze zware rol?	Of er sprake is geweest van bijzondere handhavingsacties kan de betreffende teamleider beantwoorden. Of deze zware rollen juist zijn toegewezen kan geconcludeerd worden aan de hand van de eigen autorisatiematrix. Valt daaruit geen verklaring af te leiden, vraag dan bij BKWI een specifieke rapportage op over 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.	Een afwijkende trend kan wijzen op overwerk- en inhaalacties of een tijdelijke avondopenstelling. Voor raadplegingen buiten kantoortijden is het advies in alle gevallen naar een verklaring te zoeken.	Teamleiders kunnen uitsluitsel geven over overwerk in de avonduren. Is de verklaring niet afdoende, vraag dan een specifieke rapportage op 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 %).	Wanneer het (percentuele en/of absolute) aantal raadplegingen op de top 5 per maand sterk verschilt dan moet worden gezocht naar een verklaring. Betreft het BSN een klant? Vervolgens is de vraag of de klant 'bewerkelijk' is: bijvoorbeeld: er moet nader onderzoek worden gedaan, veel mensen zijn met de klant bezig etc. Aan de andere kant kan dit een sterke aanwijzing zijn dat een persoon die om de een of andere reden in de belangstelling staat, onrechtmatig wordt geraadpleegd.	Wanneer er geen verklaring te vinden is, vraag dan een specifieke rapportage op over het BSN en de medewerkers die op dat BSN raadplegingen hebben gedaan.
2.4 Hoogst aantal gebruikers dat hetzelfde BSN heeft geraadpleegd. De vorige tabel bevatte het aantal meest geraadpleegde BSN's, ongeacht of dat door één of meerdere personen is geraadpleegd. In deze tabel gaat het om het BSN dat door de meeste gebruikers is geraadpleegd.	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 oneigenlijk gebruik. Verschillen tussen gemeenten kunnen (ook) wijzen op verschillende werkprocessen.	Vraag bij BKWI om een specifieke rapportage met de medewerkers die het specifieke BSN hebben geraadpleegd. Vervolgens kan ook door koppeling van het BSN met het klantenbestand worden vastgesteld of deze BSN's wel tot het klantenbestand horen. Hebt u de whitelist geactiveerd, dan kunt u specifieke rapportages opvragen waarin alle BSN´s staan die zijn opgevraagd waarvoor de escapefunctie is gebruikt. Zie verder bij 4 Gebruik escapefunctie.
2.5 Hoogst aantal raadplegingen per gebruiker. Dit is de top 5 van Suwinet gebruikers.	Grote afwijkingen van het gemiddelde of afwijkingen in de tijd kunnen worden verklaard door bijv. de opdracht aan een medewerker om specifiek bepaalde controles uit te voeren (in bulkwerk).	Wanneer geen verklaring kan worden gevonden in taaktoedeling of procesgang vraag dan een specifieke rapportage aan om deze topgebruikers te identificeren.
Hoofdstuk 3 - Accountbeheer		
3.1 Percentage geblokkeerde accounts. Accounts worden automatisch geblokkeerd bij BKWI na 5 mislukte pogingen om in te loggen. Gemeenten kunnen zelf instellen wanneer een account (automatisch) geblokkeerd moet worden, bijvoorbeeld na een x aantal dagen niet-gebruik.	Alle afwijkingen kunnen aanleiding zijn voor nader onderzoek. De gebruikersbeheerder kan daarvoor zijn gebruikersadministratie raadplegen. Hij/zij kan onderzoeken: of de medewerker nog in dienst is (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.	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.
3.3 Aangemaakte accounts, verwijderde accounts en wijzigingen op accounts Deze tabel laat de activiteiten van de gebruikersbeheerder zien.	Accounts die binnen korte tijd zijn aangemaakt en weer verwijderd, of zijn gewijzigd en weer teruggezet.	Navraag doen bij de gebruikersbeheerder, specifieke rapportage opvragen bij BKWI
3.4 Verdeling van de rollen en het aantal autorisaties. 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	Het is raadzaam speciale aandacht te geven aan het aantal 'zware' rollen: • -zijn daar logisch te verklaren wijzigingen in?	Het is aan te bevelen periodiek te toetsen of de autorisaties van de medewerkers nog passen bij (proportioneel zijn voor) hun functie. Dit geldt vooral voor de zware rollen.

rol heeft. Het kan zijn dat een medewerker voor meerdere rollen is geautoriseerd. Dat is af te lezen uit de autorisatietabel van de gemeente.	• -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 niet te ruim, te krap en wel juist toebedeeld? De gebruikersbeheerder kan in zijn administratie achterhalen wie welke autorisatie heeft. En dat vergelijken met de vastgestelde autorisatiematrix. Afwijkingen in de aantallen moeten logisch verklaard kunnen worden, bijvoorbeeld door een wijziging in de inrichting van een proces.	
Hoofdstuk 4- Doelmatig gebruik		
4.1 Aantal raadplegingen per pagina. In de tabel staan alle beschikbare pagina's van Suwinet -Inkijk en het aantal keren dat die pagina is geraadpleegd. In de autorisatiematrix van de gemeente is aangegeven welke medewerker voor welke rollen/pagina's is geautoriseerd.	Afwijkingen in het patroon kunnen mogelijk worden verklaard door specifieke controles, een nieuwe pagina of een vervallen pagina. Speciale aandacht voor de pagina's met de speciale zoeksleutels: • • Zoek in BRP (uitgebreid) • • Zoek in Kadaster, • • Zoek in de RDW (+). Iedere keer kunt u de vraag stellen of het aantal raadplegingen op deze zoeksleutels rechtmatig (en proportioneel) is. Pieken in het gebruik van deze pagina's moeten worden onderzocht op misbruik en oneigenlijk gebruik.	Een vervolgactie kan zijn een nader onderzoek naar de roltoedeling op basis van de autorisatiematrix van de gemeente. Indien er sprake is van mogelijk misbruik of oneigenlijk gebruik, vraag dan een specifieke rapportage op bij BKWI.
4.2 Gebruik escapefunctie bij whitelisting. Deze tabel geeft aan hoe vaak en met welke reden een BSN is opgevraagd die niet op de whitelist van de gemeente stond. Dus eigenlijk niet-klanten. Uw organisatie draagt zorg voor het vullen van de whitelist met alle BSN waarmee uw organisatie een dienstverleningsrelatie heeft.	Een hoog gebruik van de escapefunctie kan wijzen op: • • -een te krappe of slecht onderhouden whitelist • • -onnodige opvragingen, oneigenlijk gebruik	Als er sprake is van een te krappe of slecht onderhouden whitelist dan kan de gemeente de whitelist aanpassen. Voor het gebruik van de escapefunctie kan aparte specifieke rapportage opgevraagd worden. Daarin staat welk BSN is opgevraagd, door wie met welke reden en welke pagina's bekeken zijn. Deze rapportage geeft u zicht op het opvragen van niet-klanten. Zie verder de 'Handreiking whitelist en escape' en de 'Handreiking omgaan met de escape'.
4.2a Onderhouden werkvoorraad Deze tabel laat zien hoe vaak per maand de whitelist door de gemeente ververst of aangevuld door upload van een bestand of handmatige toevoeging.	Als de frequentie van bijwerken van de whitelist laag is dan zal er veel vaker gebruik gemaakt moeten worden van een escape door het (nog) ontbreken van de BSN. Als de whitelist wel regelmatig wordt bijgewerkt maar vaker door handmatige toevoeging dan door een upload van het hele bestand, dan kan dat meer capaciteit vragen.	Bekijk het interne proces van het onderhouden van de whitelist. Zijn er vaste tijden? Zijn die regelmatig genoeg? Waarom is er gekozen voor handmatige toevoeging ipv het gehele bestand steeds te verversen?
4.3 en 4.4 Suwimail verkeer. Suwimail is beveiligde mail. Ketenpartijen worden geacht, op het moment dat zij persoons-informatie uitwisselen of informatie uitwisselen die tot personen herleidbaar is, Suwimail te gebruiken	Een dalend gebruik, vermoedelijk laag gebruik of niet-gebruik kan erop wijzen dat de onbeveiligde mail wordt gebruikt.	Breng Suwimail onder de aandacht van de medewerkers.