Gemeente Diemen

GEMEENTEBLAD

Officiële uitgave van de gemeente Diemen

Nr. 459865

31 oktober

2024

Beveiligingskader Suwinet

Team Administratie Sociaal Domein – Team Sociale Zaken – Team Burgerzaken
2023-2024-2025

1. Inleiding

Verschillende instanties en overheidsinstellingen wisselen via Suwinet, een elektronische infrastructuur, persoonsgegevens met elkaar uit. Het betreft:

- Het Bureau Keteninformatisering werk en inkomen (BKWI),
- de stichting Inlichtingenbureau Gemeenten (IB),
- het Uitvoeringsinstituut Werknemersverzekeringen (UWV),
- de Sociale Verzekeringsbank (SVB),
- het Kadaster, RDW, Belastingsdienst, KvK
- de Dienst Uitvoering Onderwijs (DUO)
- Alle gemeenten

Met de faciliteit “Suwinet-Inkijk” worden persoonsgegevens voornamelijk op basis van het Burgerservicenummer (BSN) toegankelijk gemaakt voor bevoegde medewerkers. Via Suwinet (Suwinet-Inkijk en Suwinet-Inlezen) vragen ook overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar op. Dat is erg handig voor de dienstverlening omdat we daarmee voorkomen dat informatie dubbel uitgevraagd wordt aan klanten. De gemeente heeft die gegevens nodig om het recht op een uitkering vast te kunnen stellen en de juiste dienstverlening te kunnen leveren.

Dit betekent dat bevoegde gebruikers van Suwinet over nogal wat privacygevoelige informatie van burgers kunnen beschikken. Het gaat dan om gegevens over arbeidsverleden, werkgever, loon, uitkeringen/toeslagen, opleidingen, autobezit, eventueel woningbezit en bv toeslagen van burgers die in aanmerking (willen) komen voor een bijstandsuitkering. Toegang tot deze informatie over alle inwoners uit Nederland brengt de verantwoordelijkheid met zich mee om hier zorgvuldig en integer mee om te gaan. Bovendien zal naar verwachting het aantal bronnen waarvan Suwinet gebruik kan maken in de toekomst verder toenemen. De spelregels met betrekking tot het gebruik van Suwinet zijn in dit beveiligingskader vastgelegd. Aan dit kader is ook een checklist (bijlage 9) toegevoegd zodat wordt geborgd dat we deze spelregels ook naleven.

2. Kader voor Suwinet beveiliging

Suwinet moet veilig zijn: er gaat dagelijks heel veel en heel gevoelige informatie over de lijnen. Daarover zijn afspraken gemaakt tussen de SUWI-partijen. Dat zijn de gemeenten, de SVB en het UWV. De afspraken gaan over normenkaders en de verantwoording over de naleving daarvan. Deze afspraken worden gemaakt in het Ketenoverleg van Suwinet, dat wordt geadviseerd door de Domeingroep Privacy en Beveiliging.

Met ingang van 25 mei 2018 is de Europese Algemene verordening gegevensbescherming (AVG) in werking getreden. Organisaties zijn op grond van de AVG verplicht organisatorische en technische maatregelen te treffen om het gebruik van persoonsgegevens tot een minimum te beperken.

De verantwoording over informatieveiligheid met betrekking tot Suwinet is met ingang van 2017 ondergebracht in de bredere gemeentelijke verantwoording over informatieveiligheid in het kader van ENSIA (Eenduidige Normatiek Single Information Audit). Suwinet is één van de onderdelen waarover de gemeente zich horizontaal aan de gemeenteraad en verticaal aan de (landelijke) toezichthouders verantwoordt.

In dit beveiligingskader Suwinet zijn specifieke op het gebruik van Suwinet gerichte kaders verwerkt. Het gaat daarbij om:

- welke personen (functies) krijgen toegang tot welke gegevens,
- wat zijn de spelregels rondom autorisatie van Suwinet-Inkijk.
- hoe worden controles ten aanzien van Suwinet uitgevoerd,
- welke maatregelen worden genomen bij misbruik

3. Domeinen en normen

Met ingang van 1 april 2017 is het nieuwe "Specifiek Suwinet-normenkader Afnemers" van kracht geworden. Dit normenkader is integraal binnen ENSIA opgenomen. Waarbij de formulering van de vragen is afgestemd op de gehanteerde structuur en terminologie van de BIG.

In het Suwinet normenkader zijn 26 normen ondergebracht binnen een drietal domeinen:

Beleidsdomein – Dit domein bevat uitgangspunten voor het gebruik van Suwinet services binnen de Afnemers organisatie.

Uitvoeringsdomein – Dit domein bevat de implementatie van componenten die voor het veilig gebruik van gegevens noodzakelijk zijn, zoals toegangsvoorziening, koppelingen met voorzieningen zoals applicaties, eventuele servers waarop de decentrale applicatie actief op zijn.

Controldomein – Dit domein bevat evaluatie-, meet- en beheersingsaspecten op basis waarvan beheerst en bijgestuurd kan worden.

Hieronder wordt per norm aangegeven hoe aan de norm voldaan wordt.

3.1 Beleidsdomein

De doelstelling van het "Beleidsdomein" is om aan te geven welke uitgangpunten en sturingsmiddelen er gelden voor het veilig gebruik Suwinet diensten.

B.01 Suwinet-aansluitbeleid

De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.

Duo+ (uitvoeringsorganisatie voor gemeenten Diemen, Uithoorn en Ouder-Amstel) heeft een strategisch- en tactisch informatiebeveiligingsbeleid opgesteld (bijlage 11 en 12).

Daarnaast is het onderhavige beveiligingskader vastgesteld door de gemeente Diemen, specifiek voor de aansluiting op Suwinet. Hierin zijn de taken en verantwoordelijkheden belegd en toegewezen aan daartoe bevoegde medewerkers.

Deze maatregelen zijn passend binnen BBN2 (BasisBeveiligingsNiveau).

B.02 Naleving en compliance aansluitbeleid

De Afnemer bewerkstelligt dat het aansluitingsbeleid correct wordt uitgevoerd en dat de vereisten hieruit worden nageleefd

Het aspect compliance richt zich op het naleven van de verplichtingen die voortkomen uit (a) wet- en regelgeving en (b) door de organisatie overeengekomen beleid, richtlijnen, standaarden, en architectuur.

Met de vaststelling van dit beveiligingskader zorgen we voor een kader waarmee we een correcte uitvoering en naleving van de beveiligingseisen die passen bij Suwinet borgen.

De uiteindelijke verantwoording wordt afgelegd via ENSIA.

B.03 Externe partijen

De organisatie stelt als Afnemer met externe partijen in een overeenkomst, waarvan een bewerkersovereenkomst onderdeel uitmaakt, minimaal vast dat de aan haar gestelde beveiligingseisen voor Suwinet onverkort van toepassing zijn op de dienstverlening die door deze externe partijen worden geleverd.

Duo+
ICT diensten zijn ondergebracht bij de uitvoeringsorganisatie Duo+. Duo+ heeft samen met gemeente Diemen een strategisch- en tactisch informatiebeveiligingsbeleid opgesteld. Ook is er een verwerkingsovereenkomst tussen gemeente Diemen en Duo+.

Sociale Recherche
Sociale Recherche Gooi- en Vechtstreek is gemachtigd tot het raadplegen van Suwinet. Om het zorgvuldig gebruik van gegevens te waarborgen is een Verwerkersovereenkomst getekend in het kader van de AVG.

Gemeente Diemen

B.04 Beveiligingsfunctie suwinet

De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.

Er is een Security Officer Suwinet aangesteld en aangemeld bij het BKWI conform de procedure van het BKWI. Het aanmeldformulier is te vinden op "I:\Diemen\Teams\TASD\TASDTSZ\Suwinet Beveiligingsdocumenten\Security Officer". De Security Officer is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document.

De taakomschrijving van de Security officer Suwinet is als bijlage 13 in dit plan opgenomen.

B.05 Taken, verantwoordelijkheden en functiescheiding

De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.

Niet iedere medewerker heeft voor de uitoefening van zijn functie toegang nodig tot alle binnen het Suwinet beschikbare gegevens. De verschillende toegangsniveaus zijn omschreven in de zogenaamde Autorisatierollen. De gebruikersbeheerder Suwinet kent, in opdracht van de teamleider, op basis de autorisatiematrix de autorisatierollen toe. Deze matrix en toelichting op de rollen en autorisaties zijn uitgewerkt in het document "Toegangsrechten voor Suwinet" en toegevoegd aan dit kader (bijlagen 3 en 4).

De volgende functionarissen binnen team Sociale Zaken, team Administratie en team Burgerzaken kunnen worden geautoriseerd om gebruik te maken van Suwinet-Inkijk of om gebruiksrechten te beheren:

- Casemanager inkomen en werk
- Consulent inburgering
- Toetser
- Medewerker uitkeringsadministratie
- Medewerker debiteuren administratie
- Beheerder
- Handhaver
- Medewerker burgerzaken
- Security Officer

Hieronder wordt op hoofdlijnen aangegeven wie wanneer Suwinet mag raadplegen. Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van onrechtmatig of doeloverschrijdend gebruik. In dat geval hoort de teamleider de betreffende medewerker en neemt zo nodig disciplinaire maatregelen met inachtneming van de CAR/UWO.

Functie	*Toegestaan gebruik*
Administratief / financieel medewerker (medewerker uitkeringsadministratie)	Bij controle van betaling lopende uitkeringen op grond van de Participatiewet, loaw of loaz.
Casemanager inkomen/werk (Participatiecoach)	Bij aanvragen/onderzoeken op grond van de Participatiewet, loaw of loaz.
Incasso/Terugvordering/Verhaal (medewerker debiteuren administratie)	Bij onderzoek in het kader van terugvordering en verhaal op grond van de Participatiewet, loaw of loaz.
Handhaving/SR	Bij aanvragen/onderzoeken op grond van de Participatiewet, loaw of loaz.en bij vermoedens van fraude binnen deze regelingen.
Toetser	Bij het toetsen van adviezen m.b.t. aanvragen/onder-zoeken op grond van de Participatiewet, loaw of loaz;
Consulent inburgering	Bij werkzaamheden in het kader van de Wet Inburgering.
Gebruikersbeheerder	Bij het toepassen van de correctieservice en het opvragen van gebruikersrapporten; Bij het aanbrengen van wijzigingen in het kader van gebruikersbeheer.
Medewerker burgerzaken	Bij controle van actuele adresgegevens
Security officer	Opvragen en controleren generieke en specifieke gebruiksrapportages

Autorisatiematrix
In de Autorisatiematrix is terug te zien welke gegevens bij welke functie kunnen worden geraadpleegd. Inzage in andere suwinet gegevens is voor de betreffende functie geblokkeerd. Zie bijlage 4.

Functiescheiding
De taken binnen het beheer worden verdeeld in verschillende groepen met verschillende functieprofielen. Deze profielen zijn bedoeld om enerzijds tot een effectief takenpakket te komen, anderzijds tot een adequate functiescheiding. Zo wordt ervoor gezorgd dat taken, bevoegdheden en verantwoordelijkheden niet bij één persoon komen te liggen, maar bij meerdere personen met tegengesteld belang. Zie bijlage 8.

Whitelist filter en escapefunctie
De whitelist is een bestand met BSN nummers waaraan getoetst wordt of de gegevens van de betreffende burger mogen worden bevraagd.
In de whitelist zijn de BSN nummers opgenomen van burgers die een (suwi) dienst-verleningsrelatie hebben, te weten:

a. burgers die een uitkering ontvangen op grond van de Participatiewet, Bbz, IOAW of IOAZ, of waarvan deze uitkering korter dan 3 maanden geleden is beëindigd;
b. burgers die een openstaande schuld hebben, voortvloeiende uit de onder a. genoemde wetten;
c. burgers die onderhoudsplichtig zijn t.o.v. onder a. genoemde personen.

Aan bepaalde gebruikers wordt via de escapefunctie autorisatie verleend om burgers te kunnen raadplegen die niet op de whitelist voorkomen, Dit is bijvoorbeeld nodig bij een nieuwe bijstandsaanvraag, een nog onbekende onderhoudsplichtige of een bijzonder onderzoek waarbij gegevens van derden nodig zijn. Deze gebruikers krijgen de mogelijkheid om via de escapefunctie het whitelist filter te passeren. Daarbij zijn zij verplicht om aan te geven wat de reden is om buiten de whitelist te raadplegen. Het gebruik van de escapefunctie wordt gelogd en via de gebruiksrapportages gecontroleerd. De whitelist escape reden Anders en zoeksleutels anders dan BSN moeten door de gebruiker bijgehouden worden op de lijst afwijkende raadplegingen Suwinet (I-schijf).

De whitelist wordt maandelijks digitaal aangeleverd bij BKWI door de beheerder.

B.06 Suwinet deel landschap afnemers (architectuur)
De Afnemer heeft de actuele documentatie van de technische infrastructuur, die bij het gebruik van Suwinet diensten een rol spelen, benoemd en vastgelegd in een ‘ Suwinet landschap’ document.

Om toegang te verkrijgen tot Suwinet maakt de geautoriseerde medewerker gebruik van de gemeentelijke werkplek of beveiligde thuiswerkomgeving. Vanaf deze werkplek wordt verbinding gemaakt met het Internet. Het internetverkeer vindt beveiligd plaats, volgens gangbare technieken.

3.2 Uitvoeringsdomein
De doelstelling van het uitvoeringsdomein is om vast te stellen of wij als Afnemer de afgesproken Suwinet diensten gebruiken conform de uitgangspunten en de aansluitvoorwaarden.

U.01 TPM externe partijen
De externe partij, de provider aan wie de Afnemer de ICT diensten heeft uitbesteed in het kader Suwi , verstrekt jaarlijks een assurance verklaring in de vorm van een Third Party Memorandum (TPM) aan de Afnemer. De afnemer verwerkt dit in zijn ICV.

Gemeente Diemen heeft het beheer van de algemene werkplek ondergebracht bij een bedrijfsvoeringsorganisatie (Duo+). Over opzet, bestaan en werking van beveiligingsmaatregelen wordt aan de gemeente Diemen regulier verantwoording afgelegd. Vooralsnog gebeurt dit niet in de vorm van een TPM.

U.02 Autorisatie beheerproces
De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.

U.03 Toegangsmechanisme: gebruikersidentificatie- en authenticatie (IA)
Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.

In het document “Procedure autorisatie tot Suwinet” staat beschreven hoe autorisaties worden toegekend en beheerd. Dit document is als bijlage 2 toegevoegd aan dit kader.

U.04 Toegangsmechanisme: autorisatie

Toegang tot Suwinet diensten door gebruikers en beheerders behoort te worden beperkt overeenkomstig het vastgestelde (Suwinet) toegangsbeleid gebaseerd op de AVG.

Niet iedere medewerker heeft voor de uitoefening van zijn functie toegang nodig tot alle binnen het Suwinet beschikbare gegevens. De verschillende toegangsniveaus zijn omschreven in de zogenaamde Autorisatierollen. De gebruikersbeheerder Suwinet kent, in opdracht van de teamleider, op basis de autorisatiematrix de autorisatierollen toe. Deze matrix en toelichting op de rollen en autorisaties zijn uitgewerkt in het document "Toegangsrechten voor Suwinet" en toegevoegd aan dit kader (bijlagen 3 en 4). Zie ook de toelichting onder norm B.05.

U.05 Suwinet-informatie

De Afnemer heeft alle Suwinet -informatie (bij transport) binnen en buiten de eigen locaties en apparatuur waarmee Suwinet -informatie toegankelijk wordt gemaakt, beveiligd volgens de geldende standaarden

Raadplegen bij thuiswerken

Het is vanaf maart 2020 toegestaan om Suwinet te raadplegen in de beveiligde thuiswerkomgeving van de gemeente Diemen tijdens kantoortijden. Indien noodzakelijk is raadplegen buiten kantoortijden ook mogelijk.Richtlijnen met betrekking tot veilig gebruik Suwinet worden periodiek gedeeld met desbetreffende medewerkers.

Opslag van informatie

Informatie die uit Suwinet is opgehaald kan worden gebruikt in schriftelijke rapportages die nodig zijn voor de uitvoering van de Participatiewet, loaw of loaz. Deze rapportages worden opgeslagen in het back-office systeem en in het 'digitale dossier' in het zaaksysteem

U.06 Classificatie van informatie

De organisatie van de Afnemer classificeert de informatie, in relatie tot de via Suwinet uitgewisselde gegevens, op basis van een classificatie voorschrift die gerelateerd is aan de classificatie-indicatie van de bronhouders.

De risicoklasse is door middel van een zelfscan vastgesteld op BBN2 (BasisBeveiligingsNiveau).
De rapportage van de zelfscan is te vinden op I:\Diemen\Teams\TASD\TASDTSZ\Suwinet beveiligingsdocumenten\Classificatie Beveiligingsniveau.

U.07 Suwinet- inlezen en dkd inlezen (inleesfunctionaliteit)

De aangesloten partijen wisselen onderling gestructureerde gegevens uit via de service Suwinet -Inlezen die direct worden ingelezen in een applicatie (inlees applicatie).

Suwinet-inlezen en dkd inlezen worden niet gebruikt door gemeente Diemen.

U.08 Suwinet-mail

Het beschermen van de uitwisseling van informatie via Suwinet -Mail wordt uitgevoerd conform formeel beleid- en procedures en beheersmaatregelen.

Suwinet-mail wordt niet gebruikt door gemeente Diemen.

U.09 Scheiding van faciliteiten (productieomgeving)

De Afnemer behoort de via Suwinet geleverde gegevens alleen via de productieomgeving beschikbaar te stellen.

Er kan gebruik gemaakt worden van de zogeheten OTAP-omgevingen (Ontwikkel-, Test-, Acceptatie- en Productieomgeving). Binnen deze omgevingen worden specifieke activiteiten verricht. Hierbij behoren verschillende verantwoordelijkheden. Deze OTAP-omgevingen kunnen in beheer zijn bij externe providers. In het kader van het gebruik van Suwinet gegevens is het een vereiste dat de Suwinet gegevens slechts via de productie omgeving beschikbaar gesteld moet worden.

U.10 Server

De Suwinet Servers worden gehardend volgens een vastgestelde configuratiebaseline.

Er is geen Suwinetserver in ons eigen netwerk.

U.11 Netwerkverbindingen

De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet .

Alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld zijn beveiligd tegen ongeautoriseerde toegang. Dit is vastgelegd in het Duo+ encryptiebeleid.

U.12 Telewerken

Afnemer heeft beleid, operationele richtlijnen en procedures voor telewerken ontwikkeld en geïmplementeerd.

Het is alleen toegestaan om Suwinet te raadplegen op een reguliere werkplek in het gemeentehuis of in de beveiligde thuiswerkomgeving van de gemeente Diemen tijdens kantoortijden. . Indien noodzakelijk is raadplegen buiten kantoortijden ook mogelijk.

3.3 Controldomein

De doelstelling van de laag control (beheersing) is erop gericht te zorgen en/of vast te stellen dat:

- de Afnemer haar omgeving zodanig heeft ingericht dat kwetsbaarheden binnen haar infrastructurele omgeving niet doorwerken in overige delen van Suwinet,
- de Afnemer het juiste beveiligingsniveau van technische componenten ten aanzien van toegangsvoorziening, applicatie, koppelingen, platformen en servers en netwerken heeft geïmplementeerd,
- de Afnemer evaluatieactiviteiten verricht om blijvend aan de overeengekomen condities en randvoorwaarden te kunnen voldoen,
- de Afnemer aantoonbaar de via Suwinet verkregen gegevens slechts rechtmatig gebruikt

C.01 Evaluatie van aansluitbeleid

(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologiën .

Het Beveilingskader Suwinet wordt jaarlijks geëvalueerd en indien nodig aangepast aan wijzigingen in beleid, wet- en regelgeving, ICT of risicoklasse van de via Suwinet beschikbaar gestelde gegevens.

C.02 Risicomanagement

Bij de beoordeling van de te treffen maatregelen ofwel risicomanagement houdt de Afnemer rekening met de risicoklasse van de berichten die worden uitgewisseld.

Gezien onze eigen inschatting van de risicoklasse treffen we beveiligingsmaatregelen die passen bij de BBN2.
Bij de inkoop van applicaties en systemen hanteert Duo+ een aantal inkoopvoorwaarden. Hierbij wordt rekening gehouden met de op dat moment geldende beveiligingseisen. Deze inkoopvoorwaarden zijn te vinden op Intercomm (https://intranet.duoplus.nl/umbraco/wegwijzer/juridische-zaken-en-inkoop/inkoop-en-aanbestedingen).
Het incidentmanagementproces en responsbeleid is te vinden op Intercomm (https://intranet.duoplus.nl/umbraco/wegwijzer/informatieveiligheid-en-privacy/).

C.03 Wijzigingenbeheer

Afnemer heeft wijzigingenbeheer procesmatig en procedureel zodanig ingericht dat wijzigingen in relatie tot Suwinet tijdig, geautoriseerd en getest worden doorgevoerd

Dit is geregeld binnen het Change Management van Duo+.

C.04 Beoordeling van toegangsrechten

Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).

De toekenningen, wijzigingen en gebruik van toegangsrechten tot Suwinet worden periodiek gecontroleerd. Dit is vastgelegd in de “Procedure autorisatie tot Suwinet” (bijlage 2) en de “Procedure controle gebruik Suwinet” (bijlage 3).

De autorisatiematrix (bijlage 4) en wordt minimaal 1 keer per jaar geëvalueerd en waar nodig aangepast en opnieuw vastgesteld.

C.05 Logging
Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.

C.06 Monitoring en rapportage
De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen).

Het BKWI heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet. Hiermee kan het gebruik van Suwinet-Inkijk per medewerker worden nagegaan.

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd. Bij indiensttreding krijgen zij het "Protocol suwinet" (bijlage 1) uitgereikt en tekenen zij de "Zorgvuldigheidsverklaring gebruik Suwinet" (bijlage 5). Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers.

De procedure met betrekking tot het controleren van het gebruik is vastgelegd in de bijlage "Proces controle gebruik Suwinet" (bijlage 7).

Generieke gebruiksrapportage
BKWI verstrekt maandelijks generieke gebruiksrapportages over het gebruik van Suwinet. Deze geanonimiseerde rapportages zijn bedoeld om het management te ondersteunen bij het beoordelen van het gebruik van Suwinet. Deze geven een globaal beeld van het gebruik en bevatten geen persoonsinformatie.
De generieke gebruiksrapportages worden maandelijks opgevraagd door de Security officier Deze rapportages worden maandelijks besproken in het afstemmingsoverleg TSZ/TASD. De gebruikersrapportage van het Team Burgerzaken wordt ook besproken in dit overleg. De Security officer maakt hier een verslag van.

Specifieke gebruiksrapportage
Wanneer afwijkingen worden geconstateerd in de generieke rapportage wordt een specifieke rapportage aangevraagd over de maanden waarin de afwijkingen zijn geconstateerd. Deze specifieke gebruiksrapportages bevatten gegevens over de handelingen van geautoriseerde gebruikers, onder andere persoonsgegevens van zowel gebruikers (gebruikersnamen) als geraadpleegde personen (burgerservicenummers).
BKWI heeft in lijn met de Algemene Verordening Gegevensbescherming een zorgvuldig proces ingericht voor het opvragen van specifieke gebruiksrapportages door aangesloten organisaties.

De Security officer onderzoekt de specifieke rapportage en doet hiervan verslag aan de teamleiders. Indien uit het onderzoek blijkt dat er sprake is van onrechtmatig of verkeerd gebruik van Suwinet spreekt de teamleider dit met de betreffende medewerker en treft deze de nodige maatregelen. De teamleider brengt verslag uit aan de Security officer bij incidenten.

C.07 Evaluatie van IAA rapportages (organisatorisch en technisch)
De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.

De procedure voor het inrichten en beheersen van identificatie, authenticatie en autorisatie (IAA) voor gebruik van Suwinet is vastgelegd in de "Procedure autorisatie tot Suwinet" (bijlage 2) . Deze procedure is onderdeel van dit beveiligingskader en wordt jaarlijks, samen met het beveiligingskader, geëvalueerd en zo nodig aangepast.

C.08 Transparantie rapportage
Het management van de Afnemer (in geval van gemeenten is dit het college van B&W) publiceert en/of levert aan de Beheerder jaarlijks een transparantierapportage conform een afgesproken format.

Als gemeente hebben wij onze verantwoording ingericht volgens de ENSIA lijn. En daarmee is de transparantie ingevuld. De beheerder (BKWI) kan van de ENSIA-verantwoording/controleverklaring gebruikmaken.

4. Overzicht bijlagen

Onderstaande bijlage behoren bij het Beveiligingskader Suwinet

Gemeente Diemen

Bijlage 1: Protocol suwinet
Bijlage 2: Procedure autorisatie tot Suwinet
Bijlage 3: Toegangsrechten voor Suwinet
Bijlage 4: Autorisatiematrix Suwinet
Bijlage 5: Zorgvuldigheidsverklaring gebruik Suwinet
Bijlage 6: Formulier autorisatie suwinet gebruiker (aanvraag/intrekking/wijziging)
Bijlage 7: Proces controle gebruik Suwinet
Bijlage 8: Functiescheiding Suwinet
Bijlage 9: Checklist suwinet
Bijlage 10: Werkwijze bij verzoek tot inzage of correctie
Bijlage 11: Strategisch Informatieveiligheidsbeleid Duo+
Bijlage 12: Tactisch Informatieveiligheidsbeleid Duo+
Bijlage 13: Taakomschrijving Security Officer
Bijlage 14: Tien tips voor beveiliging van persoonsgegevens