Beveiligingsplan Suwinet

Versie: 10-08-2022

Inhoudsopgave

1. Inleiding

Het Bureau Keteninformatisering Werk en Inkomen (BKWI), het Werkbedrijf Regio Nijmegen (WBRN), de Stichting Inlichtingenbureau Gemeenten (IB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Belastingdienst, Dienst Uitvoering Onderwijs (DUO), de RDW (Rijksdienst voor het wegverkeer) en gemeenten wisselen persoonsgegevens met elkaar uit via Suwinet, een elektronische infrastructuur. In Suwinet zijn gegevens van inwoners te zien voor medewerkers die dat voor hun werk nodig hebben. Het gaat om privacygevoelige gegevens over adressen, arbeidsverleden, loon, uitkeringen en opleiding van inwoners. De organisaties hebben deze gegevens nodig om goede dienstverlening te kunnen leveren.

In dit Beveiligingsplan staat als eerste, het kader voor het Beveiligingsplan Suwinet. Hierna de bevoegdheden van gebruikers en in welke situaties zij Suwinet mogen gebuiken. Als afsluiting ‘Tien gouden tips’ voor medewerkers.

2. Kader Suwinet Beveiligingsplan

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) en de Vereniging voor Nederlandse Gemeenten (VNG) ondersteunen gemeenten. Als onderdeel van de Baseline Informatiebeveiliging Overheid (BIO) is het informatiebeveiligingsbeleid voor onze gemeente vastgesteld. Hierin zijn voor de gemeente regels opgenomen voor de beveiliging van gegevens. Dit informatiebeveiligingsbeleid vormt het vertrekpunt voor het Beveiligingsplan Suwinet.

Om Suwinet goed te laten functioneren moeten partijen erop kunnen vertrouwen dat “hun” gegevens op een zorgvuldige en controleerbare wijze worden gebruikt. Toetsing vindt, sinds 2017, plaats binnen de Eenduidige Normatiek Single Information Audit (ENSIA). Met deze methode leggen we elk jaar verantwoording af aan het college, de gemeenteraad, landelijke toezichthouders en inwoners.

3.1 Gebruikers van Suwinet

De volgende functies mogen Suwinet gebruiken:

- applicatiebeheerders Suwinet
- consulenten inkomen/ Bbz
- consulenten inkomen/Bbz uitgebreid
- consulent fraude en handhaving
- consulenten participatie
- medewerkers terugvordering, verhaal en boete
- medewerkers terugvordering, verhaal en boete uitgebreid
- administratief medewerkers uitkeringsadministratie
- administratief medewerkers uitkeringsadministratie met onderhoud werkvoorraad
- medewerker burgerzaken B/toezichthouder BRP
- medewerker schuldhulpverlening
- security-officer Suwinet

In de autorisatiematrix Suwinet staan de rollen van de functies en welke medewerkers Suwinet gebruiken.

3.2 Autorisatieprocedure, controle autorisaties en “Werkinstructie: Weet hoe het zit met Suwinet”

Autorisatieprocedure Suwinet :
- Het IRVN maakt in Topdesk de taak uitleg Suwinet aan voor de security officer Suwinet als er een personeelsmutatie is.
- Als de medewerker Suwinet nodig heeft voor het uitvoeren van de werkzaamheden voert de security officer Suwinet een kennismakingsgesprek Suwinet met de medewerker en geeft in de topdeskmelding aan voor welke functie in Suwinet de medewerker geautoriseerd moet worden.
- Tijdens het kennismakingsgesprek bespreekt de security officer Suwinet het Beveiligingsplan Suwinet, de werkinstructie “Weet hoe het zit met Suwinet” (zie bijlage 1), vraagt de medewerker de zorgvuldigheidsverklaring Suwinet te ondertekenen (zie bijlage 2) en deel te nemen aan de VNG E-learning “Veilig gebruik Suwinet”.
- Na het kennismakingsgesprek sluit de security officer Suwinet de taak in Topdesk en start de taak opvoeren gebruiker Suwinet in Topdesk voor de gebruikersbeheerder Suwinet.
- De gebruikersbeheerder Suwinet verzorgt de autorisatie in Suwinet.
- De gebruikersbeheerder Suwinet stuurt de medewerker een mail (cc security officer Suwinet) met inloggegevens, een linkje naar de informatie “Snel aan de slag met Suwinet” van het BKWI en vraagt de medewerker zich aan te melden voor de “Suwinetnieuwsbrief”.

Periodieke controle autorisaties Suwinet:
- De gebruikersbeheerder Suwinet stuurt het overzicht gebruikers naar de security officer Suwinet.
- De security officer Suwinet stuurt het overzicht gebruikers voor akkoord naar de Teamleiders waar Suwinet gebruikt wordt.
- De security officer Suwinet controleert het overzicht gebruikers met de gebruikers van de autorisatiematrix Suwinet en de mutaties op accounts via te downloaden specifieke rapportages.
- De security officer Suwinet controleert jaarlijks de rollen binnen de autorisatiematrix Suwinet met de rollen van de gebruikers in Suwinet.
- De security officer Suwinet maakt rapportages van deze controle.
- De rapportage gaat ter ondertekening naar de Teamleiders waar Suwinet gebruikt wordt en als de security-officer Suwinet het nodig vindt naar de directeur en verantwoordelijke wethouder.

3.3 Functie Suwinet-Inkijk:

Hieronder staat welke functie wat mag doen in Suwinet:

- Consulenten inkomen/Bbz gebruiken Suwinet bij het behandelen van aanvragen of een melding dat een inwoner een uitkering wil aanvragen, rechtmatigheidsonderzoeken en heronderzoeken voor zover het de Participatiewet, Ioaw, Ioaz, Bbz en Tozo betreft.
- Consulenten participatie gebruiken Suwinet bij de begeleiding van inwoners met een uitkering Participatiewet, Ioaw en Ioaz.
- Medewerkers terugvordering/verhaal/boete gebruiken Suwinet bij onderzoeken die samenhangen met boete, verhaal op onderhoudsplichtigen of vorderingen van de Participatiewet, Ioaw, Ioaz, Bbz en Tozo.
- Consulenten inkomen/Consulent Bbz uitgebreid en medewerkers terugvordering / verhaal / boete uitgebreid gebruiken de zwaardere rollen voor de poortwachters- en handhavings-werkzaamheden van de Participatiewet, Ioaw, Ioaz, Bbz en Tozo.

- Administratief medewerker uitkeringsadministratie met onderhoud werkvoorraad draait periodiek een bestand voor de whitelist.
- Administratief medewerker uitkeringsadministratie gebruiken Suwinet om signalen, rapportages en inkomsten- en wijzigingsformulieren te verwerken.
- Medewerker burgerzaken B/toezichthouder BRP gebruikt Suwinet voor adresonderzoeken.
- Medewerker schuldhulpverlening gebruikt Suwinet om de Wet Gemeentelijke Schuldhulpverlening uit te voeren.

3.4 Whitelist Suwinet (zie bijlage 3)

Vanaf juni 2017 werken we voor Suwinet binnen het Team Inkomen & Participatie met de whitelist/escapefunctie. Het kijken naar gegevens van inwoners waarmee we als gemeente nog geen dienstverleningsrelatie hebben, is door de whitelist/escapefunctie beter zichtbaar. Met medewerkers is afgesproken dat het gebruik van de escapefunctie navolgbaar moet zijn in onze vakapplicatie Civision Samenleving. Als dit niet mogelijk is, vullen zij het formulier “Afwijkende Raadpleging Suwinet” (bijlage 4) in. Ook voor het gebruik van de zwaardere rollen.

Bij een nieuw werkproces waarvoor Suwinet nodig is, vraagt de security-officer Suwinet aan de applicatiebeheerder Suwinet de whitelist uit te breiden met dit werkproces. Applicatiebeheer breidt de whitelist uit met het nieuwe werkproces en stuurt een nieuwe versie van de whitelist naar de security-officer Suwinet. De administratief medewerkers uitkeringsadministratie met onderhoud werkvoorraad draait periodiek een bestand voor de whitelist.

De medewerker burgerzaken B/toezichthouder BRP slaan de rapportages van de adresonder-zoeken op de vakapplicatie. Als dit niet mogelijk is, vullen zij het formulier “Afwijkende Raadpleging Suwinet” in.

De medewerker schuldhulpverlening slaat de rapportages van de onderzoeken gemeentelijke schuldhulpverlening op in de afdelingsmap/vakapplicatie . Als dit niet mogelijk is, vullen zij het formulier “Afwijkende Raadpleging Suwinet” in.

Periodieke controle whitelist Suwinet:
- De gebruikersbeheerder Suwinet stuurt de laatste versie van de whitelist en het script van de whitelist naar de security officer Suwinet.
- De security officer Suwinet controleert het script van de whitelist met de laatste versie van de whitelist.
- De security officer Suwinet maakt een rapportage van deze controle

3.5 Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen (BKWI) verzorgt rapportages over het gebruik van Suwinet. En legt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet vast.

Doel:
1. Voorkomen en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking;
2. Wetenschappelijke en/of statistische doelen.

De gebruikers van Suwinet weten dat het BKWI deze gegevens vastlegt.

3.6. Periodieke controle

Voor de jaarlijkse werkzaamheden Suwinet is er een PDCA-Cyclus Suwinet (zie bijlage 5). De security-officer Suwinet doet periodiek controles om te onderzoeken of we Suwinet goed gebruiken. De resultaten van deze controles bespreekt de security-officer Suwinet met de teamleiders van de teams waar Suwinet wordt gebruikt. Wanneer de security-officer Suwinet het nodig vindt krijgt de directeur en de verantwoordelijke wethouder ook de rapportages.

Afwijkende raadplegingen bespreekt de security-officer Suwinet met de medewerker. Zijn er signalen over oneigenlijk gebruik, dan vindt hierover een gesprek plaats met de betrokken teamleider, de security-officer Suwinet en de medewerker. De security-officer Suwinet maakt een verslag van het gesprek. Waar nodig schuift een medewerker van P&O aan.

3.7 Verdeling taken / verantwoording

De teamleiders, van de teams waar Suwinet wordt gebruikt, zijn eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet. Het beheer voor het gebruik van Suwinet ligt bij de applicatiebeheerders Suwinet van het Team Kwaliteit en Ondersteuning van het Sociaal Team. Deze medewerkers zijn verantwoordelijk voor:

- het beheren van accounts
- geven van wachtwoorden
- bijhouden van de autorisatiematrix
- uitdraaien van het gebruikersoverzicht
- bijhouden en uitbreiden van de whitelist

3.8 Functiebeschrijving security-officer Suwinet

De security officer Suwinet:

- is het aanspreekpunt voor Suwinet binnen de gemeente Berg en Dal;
- beheert en beheerst beveiligingsprocedures en – maatregelen van Suwinet, zodat de beveiliging van Suwinet overeenkomstig wettelijke eisen is ingevoerd;
- adviseert over de (informatie)beveiliging Suwinet;
- controleert of en in hoeverre we beveiligingsmaatregelen en -procedures nakomen en monitort de uitvoering van het opgestelde beleid;
- evalueert de uitkomsten en doet voorstellen voor implementatie en aanpassing van plannen op het gebied van de beveiliging Suwinet;
- heeft overleg met de CISO, de teamleiders van de teams waar Suwinet wordt gebruikt en de applicatiebeheerders Suwinet over informatiebeveiliging en -beheer Suwinet;
- rapporteert rechtstreeks aan de teamleiders van de teams waar Suwinet wordt gebruikt;
- Wanneer de security-officer Suwinet het nodig vindt rapporteert deze aan de directeur en de verantwoordelijke wethouder.

3.9 Informatiebewustzijn Suwinet

De security-officer Suwinet:

- Informeert de nieuwe medewerker over de VNG E-learning “Veilig gebruik Suwinet”.

- Vraagt de nieuwe medewerker binnen 3 maanden deel te nemen aan de VNG E-learning “Veilig gebruik Suwinet”.
- Vraagt de nieuwe medewerker het deelnamecertificaat van de VNG E-learning “Veilig gebruik Suwinet” te mailen naar de security-officer Suwinet.
- Slaat het deelnamecertificaat van de VNG E-learning “Veilig gebruik Suwinet” op.
- Verstuurt in het jaar diverse mails naar alle gebruikers over veilig gebruiken Suwinet.
- Organiseert jaarlijks een gebruikersbijeenkomst Suwinet.

3.10 Evaluatie en bijstelling Beveiligingsplan Suwinet

Na de jaarlijkse gebruikersbijeenkomst Suwinet/ENSIA informeren we, waar nodig, het Management Team over kleine wijzigingen. Voor 2024, waar nodig eerder, maken we een nieuw Beveiligingsplan Suwinet als bijlage bij het Informatiebeveiligingsbeleid.

4.Tien gouden tips bij beveiliging van persoonsgegevens

Voor het werken met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld.

1. Beheren van wachtwoorden

De gebruiker moet het door de applicatiebeheerder Suwinet uitgegeven wachtwoord wijzigen zodra de eerste inlog plaats vindt. Na 45 dagen vervalt dat wachtwoord. De gebruiker beheert dus het wachtwoord.

2. Melden van beveiligingsincidenten

Gebruikers melden beveiligingsincidenten via Topdesk. De Chief Information Security-Officer (CISO) / Adviseur Gegevensbescherming ondernemen actie om het incident te onderzoeken. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

Hoe we met persoonsgegevens omgaan staat in de Algemene Verordening Gegevensbescherming (AVG). In de wet SUWI en in de CAO zijn geheimhoudingsbepalingen opgenomen, waarin staat dat we persoonsgegevens alleen gebruiken voor het uitvoeren van de functie.

4. Omgang met persoonsgegevens

We gaan vertrouwelijk en veilig om met persoonsgegevens die we verwerken. Hoe we dit doen, staat in het Privacybeleid Berg en Dal. In een ambtseed of integriteitsverklaring verklaren onze medewerkers integer en vertrouwelijk hun werk te doen.

5. Kennisnemen van het Beveiligingsplan Suwinet

Het Beveiligingsplan Suwinet geldt voor alle gebruikers van Suwinet. Alle gebruikers zijn op de hoogte. De security-officer Suwinet informeert nieuwe gebruikers. Gebruikers van Suwinet weten dat gebruikersgegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers.

6. Geven van informatie aan derden via de telefoon

Het uitgangspunt is dat we terughoudendheid zijn om telefonisch informatie over inwoners en bedrijven te geven. Het voeren van telefoongesprekken brengt namelijk de risico’s met zich mee dat we persoonsgegevens geven aan personen die geen recht op deze informatie hebben. In principe geven we dan ook geen telefonische informatie over inwoners aan personen of instanties die beweren namens betrokkene te bellen. In die gevallen kan de beller een schriftelijk verzoek doen, met een machtiging. Bij een verzoek om telefonische informatie van een ketenpartner (UWV / GSD / Inlichtingenbureau / SVB) bellen we deze beller via het algemene nummer van de (vestiging van de) ketenpartner terug. Dit geldt niet als een vaste contactpersoon belt.

7. Clean desk en clear screen policy

Vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zo is ingericht, dat onbevoegden niet bij deze informatie kunnen. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Dossiers bewaren we na werktijd in een gesloten

kast. Bezoekers moeten zich bij binnenkomst in het gemeentehuis eerst melden bij de receptie. De kans is daarom klein dat onbevoegden toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat we het werkstation vergrendelen met de schermbeveiliging (met wachtwoord) als we weggaan van de werkplek.

8.Vertrouwelijke gegevens in de papierbak
Zorgvuldige omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Binnen de gemeente is geregeld hoe we vertrouwelijke stukken verzamelen en vernietigen. Iedereen is daarvan op de hoogte. Vertrouwelijke gegevens moeten in de bak komen die bestemd is voor oud papier. De verzamelde vertrouwelijke gegevens leveren we regelmatig aan bij het vernietigingsbedrijf.

9. Aanspreken van onbekende personen
Als je een onbekende persoon in de gang tegenkomt spreek je deze persoon aan. Je vraagt de persoon zichzelf voor te stellen en vraagt wat hij/zij hier doet. Inwoners die niet bevoegd zijn, begeleiden we beleefd maar duidelijk naar de receptie.

10. De dagelijkse omgang met persoonsgegevens
Omdat we dagelijks omgaan met persoonsgegevens is informatiebeveiliging ontzettend belangrijk. Inwoners vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Dit is de reden waarom we op diverse manieren aandacht geven aan dit onderwerp.

Bijlage 1: Werkinstructie: “Weet hoe het zit met Suwinet”

Waar vind je de belangrijke documenten over Suwinet?
De belangrijke documenten Suwinet zijn te vinden op Bedsi: werkwijzer / ict / informatieveiligheid.

Naar wie kan je toe voor een nieuw wachtwoord?
Jouw wachtwoord is persoonlijk en alleen bedoeld om zelf in te loggen in Suwinet.
Het wachtwoord Suwinet is 45 dagen geldig. Op het eerste scherm van Suwinet kan je het wachtwoord Suwinet zelf wijzigen. Maak in jouw agenda een herinnering voor jezelf aan om het wachtwoord binnen de 45 dagen te wijzigen. Als jouw wachtwoord toch verlopen is kan je voor een nieuw wachtwoord mailen naar:

ApplicatiebeheerCSAM@bergendal.nl

Clean desk en clear screen
Vertrouwelijke gegevens mogen niet onbeheerd op jouw bureau achterblijven. Bewaar dossiers na werktijd in een gesloten kast. Clear screen betekent dat je het werkstation vergrendelt met behulp van schermbeveiliging (met wachtwoord) als je de werkplek verlaat.

Waarvoor mag je Suwinet gebruiken?
Suwinet mag je gebruiken voor het uitvoeren van de Participatiewet / IOAW / IOAZ / BBZ / TOZO / Adresonderzoeken Burgerzaken en onderzoeken Gemeentelijke Schuldhulpverlening.

Waarvoor mag je Suwinet niet gebruiken?
Suwinet mag je niet gebruiken voor alle andere regelingen die we binnen de gemeente uitvoeren. Denk hierbij bijvoorbeeld aan:
Doe Mee! Regeling
SMI
Wet op de Lijkbezorging
Voedselbank
WMO
Jeugdwet

Mag je Suwinetschermen uitprinten/archiveren?
Nee dat mag niet. Als informatie uit Suwinet belangrijk is voor een besluit, kopieer dan de informatie uit Suwinet en plak deze informatie in jouw rapportage.

Hoe zorg je voor navolgbaarheid van het gebruik van Suwinet?
Een raadpleging in Suwinet is navolgbaar als:
-er rond de raadpleegdatum een rapportage (contactregistratie Csam) aangemaakt is
-de raadpleging met datum op het formulier afwijkende raadpleging Suwinet staat

Sla het formulier afwijkende raadpleging Suwinet digitaal op in de map die de security-officer Suwinet heeft aangegeven.

Moet je nog wat doen als je in Suwinet gaat zoeken op geboortedatum / adres / kenteken?
Als je een inwoner in Suwinet opzoekt doe je dat normaal gesproken met het BSN. Soms hebben we geen BSN van een inwoner en kan er een speciale reden zijn om via geboortedatum / postcode en huisnummer / kenteken te zoeken. Dit zijn de zogenaamde “zware rollen”. Diverse medewerkers zijn geautoriseerd voor deze “zware rollen”. Ook deze raadplegingen moet je bijhouden op het formulier afwijkende raadpleging Suwinet.

Wat doe je bij een beveiligingsincident Suwinet?
Een beveiligingsincident meld je via Topdesk. De Chief Information Security-Officer (CISO) / Adviseur Gegevensbescherming ondernemen actie om het incident te onderzoeken. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

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. Deze instanties zijn “verantwoordelijke” in de zin van de Algemene Verordening Gegevensbescherming (AVG) en daarom allemaal gebonden aan de bepalingen in deze wet.

De gemeente heeft maatregelen genomen ter voorkoming van onrechtmatige en doeloverschrijdend gebruik van de beschikbare (persoons-) gegevens. De teamleiders van de teams waar Suwinet wordt gebruikt, laten het gebruik van de gegevens uit Suwinet regelmatig controleren.

Ondergetekende: ……

Team : ……..

verklaart:

- Het Beveiligingsplan Suwinet met bijlagen gelezen te hebben;
- Alleen gegevens van inwoners in Suwinet te bekijken voor het uitvoeren van de Participatiewet, Ioaw, Ioaz, Bbz, Tozo, Adresonderzoeken Burgerzaken of Wet gemeentelijke Schuldhulpverlening;
- Deze gegevens alleen te gebruiken voor het uitvoeren van de Participatiewet, Ioaw, Ioaz, Bbz, Tozo, Adresonderzoeken Burgerzaken of Wet gemeentelijke Schuldhulpverlening;
- Ervoor te zorgen dat het gebruik van Suwinet navolgbaar is in een rapportage (contactregistratie Csam). Als dit niet mogelijk is, de raadplegingen bij te houden op het formulier “Afwijkende Raadpleging Suwinet”;
- Op de hoogte te zijn van de controles die de security-officer Suwinet regelmatig doet;
- Binnen 1 maand de VNG E-Learning: “Veilig gebruik Suwinet” te doen;
- Op de hoogte te zijn dat er onderzoek plaats vindt / maatregelen volgen als er sprake is van onjuist gebruik van de gegevens van Suwinet.

Datum: ……

Handtekening: …….....

Bijlage 3: Inhoud whitelist Team Inkomen & Participatie (versie 13)

Ten behoeve van de White-list genereert Civision Samenlevingszaken (CSAM) een bestand op basis van een script.

In dit script worden de BSN-nummers verzameld van de volgende personen:
1. Klanten én eventuele partners met een uitkering Participatiewet, IOAW, IOAZ, BBZ, of Bijzondere Bijstand
 met een lopende uitkering op de dag waarop het bestand wordt gemaakt of
 met een beëindigde uitkering waarvan de einddatum maximaal één jaar vóór de aanmaakdatum van het bestand ligt.

2. Klanten met een incidentele uitkering Bijzondere bijstand (inclusief Individuele Inkomenstoeslag en Individuele Studietoeslag) waarvan de datum van registratie in CSAM maximaal één jaar voor de aanmaakdatum van het bestand ligt.

3. Klanten én eventuele partners met een vordering waarvan de hoogte van de schuld op de aanmaak datum van het bestand hoger is dan € 0,00

4. Klanten met een onderhoudsplicht waarvan de hoogte van de schuld (onderhoudsplicht) op de aanmaak datum van het bestand hoger is dan € 0,00

5. Personen waarvan één van de volgende werkprocessen is opgevoerd in CSAM en de werkprocessen op de aanmaakdatum van het bestand niet zijn afgesloten:

 HA115 Aanvraag Participatiewet
 HA215 Aanvraag IOAW
 HA315 Aanvraag IOAZ
 HA415 Aanvraag BBZ
 HA416 Aanvraag BBZ TOZO
 HA417 Aanvraag BBZ TOZO 2
 HA418 Aanvraag BBZ TOZO 3
 HA419 Aanvraag BBZ TOZO 4
 HA420 Aanvraag BBZ TOZO 5
 HA615 Aanvraag Bijzondere bijstand

(inclusief Individuele Inkomenstoeslag en Individuele Studietoeslag)
 HA616 Aanvraag TONK
 HA620 Aanvraag Energietoeslag 2022
 HD115 Vastleggen debiteur
 HD215 Onderzoek debiteur
 HD220 Eerste aanschrijving onderzoek Onderhoudsplicht
 HD315 Voorschotverstrekking
 HM915 Melding aanvraag levensonderhoud

Bijlage 4: Formulier afwijkende raadpleging Suwinet

Naam medewerker:

Hoe heb je gezocht? -Bsn -Geboortedatum -Postcode/huisnr. -Kenteken	Bsn	Achternaam inwoner	Datum	Reden raadpleging	Team Inkomen & Participatie: Bsn uitkeringsdossier

Bijlage 5: PDCA-cyclus Suwinet gemeente Berg en Dal 2022

Actie	Datum	Door wie	Check	Act
Evaluatie Beveiligingsplan Suwinet met alle gebruikers	November	Kwaliteitsmedewerker Team Inkomen & Participatie		
Waar nodig bijstelling Beveiligingsplan Suwinet naar MT en medewerkers	Juli	“		
Opdracht aanpassing Whitelist Suwinet	Waar nodig bij nieuw werkproces	“		
Aanpassing werkinstructie: “Weet hoe het zit met Suwinet”	Waar nodig	“		
Controle raadplegingen escapefunctie en raadplegingen Burgerzaken en Gemeentelijke Schuldhulpverlening	Maart/Juni/ September/ December	“		
Uitvoeren zelftest Ensia/Suwinet	Augustus	Ciso / Kwaliteitsmedewerker Team Inkomen & Participatie		
Gebruikersbijeenkomst	November	Kwaliteitsmedewerker Team Inkomen & Participatie		
Opstellen PDCA-cyclus 2023	November	“		
Informatiebewustzijn Deelnemerscertificaat VNG E-learning “Veilig gebruik Suwinet opvragen bij nieuwe medewerkers Diverse mails	Binnen 3 maanden na indiensttreding Jaarlijks	“ “		
Check voortgang PDCA-cyclus Suwinet	Elk kwartaal	“		
Gebruikersoverzicht downloaden/ analyseren / rapporteren en bespreken / laten tekenen en uitzetten vervolgacties	Elk kwartaal	“		
Uitdraai Suwigebruikers opvragen/controleren /laten tekenen en vervolgacties	Elk kwartaal	“		
Controle autorisatiematrix en mutaties op accounts	Elk kwartaal	“		
Controle rollen autorisatiematrix met rollen gebruikers Suwinet.	Jaarlijks	“		