Beveiligingsplan Suwinet 2019 e.v.

Datum: 26 november 2020

Marjan Schoenmakers

Kitty de Jonge

Versiebeheer Beveiligingsplan Suwinet V1, Addendum actualisatie november 2020

Oude waarde	**Nieuwe waarde**
4 d toegevoegd	Incidenten en **datalekken**
toegevoegd	Voorbeelden van **beveiligings**incidenten
toegevoegd	Het kwijtraken van een laptop, smartphone of tablet. Inbraak door een hacker, het klikken op een phising email. Voorbeelden van datalekken zijn:
toegvoegd	Zodra er persoonsgegevens op een plek terecht komen waar deze niet horen (of bij de verkeerde persoon) is er sprake van een datalek.
4 e laatste zin toegevoegd	Mocht dit wel gebeuren dan wordt dit gemeld als een datalek.
4 g toegevoegd	Er is een autorisatiematrix en een autorisatieprocedure. Deze worden beheerd door de security officer en de autorisaties worden goedgekeurd door de procesverantwoordelijke (of lijnmanager).
4 h toegevoegd	Er is training voor de medewerkers om bewust met suwinet te werken. Deze trainingen zijn gericht op het bewust worden van informatiebeveiliging en privacy gericht op suwinet. Voor nieuwe medewerkers wordt deze training binnen 3 maanden na indiensttreding afgerond. Het bewijs van de afgeronde training is zichtbaar voor de CISO en voor de security officer van suwinet. Verder wordt in team overleggen aandacht geschonken aan het veilig omgaan met Suwigegevens, het Beveiligingsplan en andere onderwerpen die hiermee te maken hebben.
9 Werkplekken *Om thuis te kunnen werken is er vooraf toestemming vereist*	Vanwege de coronapandemie is dringend verzocht thuis te werken in plaats van op kantoor.
10 BIG vervangen door toegevoegd	*BIO* Wachtwoorden worden encrypted (haching) en opgeslagen binnen een beveiligde omgeving.
11.3 toegevoegd	Dit wordt vastgelegd doormiddel van een bewustwordingstraining mbt suwinet. Deze training wordt afgerond binnen 3 maanden na indiensttreding.
12 toegevoegd	Een verzoek voor autorisatie gaat via TopDesk waarbij de Teamleider goedkeuring geeft.
15 Controle Toegevoegd	Een logregel bevat minimaal: a. de gebeurtenis; b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; c. het gebruikte apparaat; d. het resultaat van de handeling; e. een datum en tijdstip van de gebeurtenis.
Bijlage 1 2. toegevoegd	De rapportages gaan ook naar de CISO

INHOUD

I. Inleiding

De gemeente Rheden heeft als uitvoerder van diverse wetten en regelingen te maken met veel registraties. Om de efficiency en de effectiviteit te verbeteren worden de laatste jaren steeds meer van die registraties gekoppeld en is samenwerking binnen verschillende ketens noodzakelijk.

Als basis geldt o.a. de wet Structuur uitvoering werk en inkomen (Suwi). De Regeling Suwi verplicht elke gemeente te beschikken over een actueel informatieveiligheidsplan voor Suwinet. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevensbeveiliging noodzakelijk is. Voor alle ketenpartners is dit met beveiligingsvoorschriften uitgewerkt in artikel 6.4 en bijlage 1 van de Regeling Suwi.

Het beveiligingsplan Suwinet beschrijft de maatregelen ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van het gebruik van persoonsgegevens en informatiesystemen. Daarnaast beschrijft het welke mensen en middelen hiervoor beschikbaar zijn en hoe de naleving is geregeld. Het beveiligingsplan is geen statisch document; het is gebaseerd op diverse landelijke en sectorale uitgangspunten en documenten. De organisatie en de omgeving zijn voortdurend in ontwikkeling, onder andere door gewijzigde of vernieuwde inzichten en wetgeving of aanpassingen in de informatiesystemen. Dat betekent dat dit plan periodiek moet worden beoordeeld op actualiteit en dus mogelijk constante aanpassing nodig heeft.

Het Suwinet-beveiligingsplan staat niet op zichzelf. Binnen de gemeente zijn bepaalde zaken rondom informatieveiligheid geregeld in een voor de gehele organisatie geldend Informatiebeveiligingsbeleid 2019-2021. In het algemene Informatiebeveiligingsbeleid zijn zaken geregeld op het gebied van informatieveiligheid die voor alle organisatieonderdelen gelden ongeacht de betreffende systemen die daarbij gebruikt worden. Te denken valt aan bijvoorbeeld wachtwoordprocedures en een clear-desk policy. Deze regels zijn ook integraal van toepassing op het onderhavige beveiligingsplan Suwinet voor het gebruik van Suwinet-Inkijk.

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. ENSIA is gemeentebreed gebaseerd op de BIO. ENSIA heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren. Dit doet ENSIA door het toezicht te bundelen en aan te laten sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier beter op sturen.

1. Relatie met de gemeente Rozendaal

Het college van burgemeester en wethouders van Rozendaal heeft het college van burgemeester en wethouders van Rheden gemandateerd om de Participatiewet en aanverwante wet- en regelgeving uit te voeren. De uitvoering van deze wetgeving ligt vast in een Dienstverleningsovereenkomst. Medewerkers die belast zijn met de uitvoering van deze wet- en regelgeving voeren de werkzaamheden uit. Dit plan heeft ook betrekking op het werken met klantgegevens van inwoners van Rozendaal. De gemeente Rozendaal heeft geen eigen aansluiting op Suwinet. Per 1 februari 2019 is er 1 login voor Rheden/Rozendaal bij Suwinet Inkijk. Het beveiligingsplan Suwi geldt naast de gemeente Rheden ook voor de gemeente Rozendaal.

2. Suwinet, Suwinet-Inkijk en Wet Suwi

Suwinet is het netwerk waarover klantgegevens worden uitgewisseld voor het Digitaal Klant Dossier. Verschillende ketenpartners, waaronder de gemeente, wisselen via een elektronische infrastructuur persoonsgegevens met elkaar uit. Dit is het Suwinet.

Belangrijk aspect hierbij is de Wet eenmalige gegevensuitvraag (WEU 1-1-2008). Bij de start van de WEU is een aantal gegevens vastgelegd, dat in principe niet meerdere malen mag worden opgevraagd bij de klant. De klantgegevens die beschikbaar zijn via Suwinet moeten dus optimaal hergebruikt worden. Hiermee helpen we de burgers beter en we kunnen fraude en misbruik wat beter voorkomen.

Suwinet dient twee doelen:

1. Een dienstverlenend doel: Deze is wettelijk vastgelegd in De Wet eenmalige gegevensuitvraag (WEU). Hierin is een aantal gegevens vastgelegd, dat in principe niet meerdere malen mag worden opgevraagd bij de klant. De klantgegevens die beschikbaar zijn via Suwinet moeten dus optimaal hergebruikt worden.
2. Een controlerend doel: Rechtmatigheidscontrole en fraudebestrijding: gevallen opsporen waar de burger bij de ene overheidsinstantie andere informatie geeft dan bij de andere overheidsinstantie.

Suwinet-Inkijk is de applicatie die op Suwinet draait. Binnen deze applicatie zijn gegevens op basis van het burgerservicenummer (BSN) toegankelijk voor bevoegde medewerkers. De organisaties hebben de informatie over inkomen en vermogen nodig om de gegevensuitvraag aan de klant te beperken. Suwinet wordt gebruikt om informatie over inkomen en vermogen van een klant te verzamelen in het kader van uitkeringsverstrekking. Burgerzaken vraagt de gegevens daarnaast op voor 'adresonderzoeken', dat zijn die situaties waarin onduidelijkheid bestaat waar de burger woont.

Om de SUWI-keten (afspraken om samenwerking tussen ketenpartijen te stroomlijnen) effectief te laten functioneren moeten partijen er op kunnen vertrouwen dat de door hun instantie aangeleverde gegevens door de partners in de SUWI-keten op een zorgvuldige en controleerbare wijze worden behandeld en de privacy van die gegevens bij alle partners afdoende is gewaarborgd.

De Gezamenlijke elektronische Voorzieningen Suwi (GeVS) zijn voorzieningen waarin drie type partijen participeren: Bronhouders, Beheerders van de centrale (BKWI) en decentrale (Inlichtingenbureau) omgeving en Afnemers.

- *Bronhouders* – Bronhouders zijn de partijen die - ten behoeve van Afnemers - authentieke gegevens beschikbaar stellen aan de Beheerders via de centrale omgeving. De bronhouders vormen de zogeheten leveranciers van gegevens, zoals UWV, SVB en de Gemeenten, BRP, RDW, Kadaster, HR (KvK).
- *Beheerders* - Beheerder van de centrale omgeving (BKWI) is de partij die - conform de ketenafspraken en –standaarden zorgt voor het beschikbaar stellen van de centrale omgeving Suwi en voor de transformatie, autorisatie, transport en verdere routering van gegevens/berichten.
  Hiertoe stelt de Beheerder van de centrale omgeving instrumenten, zoals applicaties beschikbaar. De Beheerder van de centrale omgeving is BKWI. De Beheerder van de decentrale omgeving (IB) is de partij die voor de routering van 'berichten-op-maat' tussen de centrale omgeving en de gemeenten zorgt, gegevens van de gemeenten verzamelt en als Bron voor de uitwisseling van gegevens met de ketenpartijen fungeert. Hiertoe stelt de Beheerder van de decentrale omgeving instrumenten (voorzieningen en applicaties) beschikbaar. De Beheerder van de decentrale omgeving is het Inlichtingenbureau (IB).
- *Afnemers* - Afnemers zijn de partijen die via de GeVS - voor hun bedrijfsvoering en uitvoering van hun wettelijke taken - gegevens betrekken uit gegevensbronnen van de bronhouder.

3. Veilig werken met Persoonsgegevens

Informatieveiligheid is uitermate belangrijk voor het werk binnen een team waar heel veel met privacygevoelige informatie wordt gewerkt. Dit hoort dan ook bij de professionele en bekwame uitvoering van het werk. Cliënten vertrouwen op een zorgvuldige wijze van omgang en verwerken van hun gegevens. Reden waarom in het werken/of teamoverleg informatiebeveiliging en de omgang met persoonsgegevens altijd een terugkerend agendapunt is.

De correcte omgang met vertrouwelijke gegevens – waaronder persoonsgegevens – is erg belangrijk. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Daarom zijn er bij de gemeente speciale afgesloten containers. Hierin wordt het te vernietigen materiaal verzameld. De Connectie haalt de papierbakken op en neemt ze mee naar hun locatie in Arnhem waar zij de papieren versnipperen. Als zij een bak ophalen plaatsen ze direct een lege bak terug zodat medewerkers altijd papieren met gevoelige informatie in een afgesloten bak kunnen werpen.

Voor het werken met persoonsgegevens zijn vanuit de Europese Unie een aantal voorwaarden en verplichtingen opgesteld, die zijn opgenomen in de Algemene Verordening Gegevensbescherming (AVG). Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de gegevens, inclusief persoonsgegevens, niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is.

4. Maatregelen

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

b. Op de werkplekken mag geen publiek komen. Bezoekers worden aangekondigd en moeten zich bij binnenkomst in het gebouw eerst melden bij de receptie. De kans is daarom klein dat onbevoegden zonder opgemerkt te worden toegang krijgen tot de werkplek van de medewerkers. Het is echter nodig ook ten opzichte van collega's en dienstverleners zorgvuldig om te gaan met de privacy van cliënten.

c. Als een medewerker een voor hem/haar onbekende persoon in het gebouw tegenkomt waar officieel geen publiek zonder begeleiding mag komen, moet de medewerker deze persoon aan te spreken. Personen die niet bevoegd zijn om op deze plek te zijn worden hierdoor op deze overtreding gewezen. Het is de taak van de medewerker om hen beleefd maar duidelijk de weg naar het publieke gedeelte van het gebouw te wijzen en ze daar naartoe te begeleiden.

d. Het is belangrijk dat beveiligingsincidenten en datalekken worden gemeld bij de SO en CISO volgens de voorgeschreven procedure. Voorbeelden van beveiligingsincidenten zijn:

   Het kwijtraken van een laptop, smartphone of tablet. Inbraak door een hacker of het klikken op een phising email.

   Voorbeelden van datalekken zijn:

   Autorisatiemisbruik (bijvoorbeeld doorgeven van wachtwoorden aan anderen en mee laten kijken op het scherm door onbevoegden), doorgeven van gegevens aan onbevoegden (bijvoorbeeld doorspelen aan vrienden of bekenden), oneigenlijk gebruik (bijvoorbeeld informatie opvragen van personen die niet werk gerelateerd is). Zodra er persoonsgegevens op een plek terecht komen waar ze niet horen (of bij de verkeerde persoon is er sprake van een datalek.

e. Onbevoegden mogen niet de beschikking krijgen over vertrouwelijke informatie. Daarom mogen die gegevens niet onbeheerd op het bureau of het beeldscherm achterblijven (Clear desk policy). Voor zover nog niet gedigitaliseerd, worden dossiers bewaard in een kast die na werktijd op slot gaat.

f. Clear screen betekent dat het werkstation wordt vergrendeld met behulp van schermbeveiliging en met een wachtwoord weer ontgrendeld kan worden. De systemen zijn door systeembeheer zodanig ingesteld dat na een vaste periode de schermbeveiliging intreedt. Daarnaast kan de gebruiker zelf het scherm vergrendelen. Dit is te adviseren als de gebruiker langer dan één minuut zijn werkplek verlaat.

g. Er is een autorisatiematrix en een autorisatieprocedure. Deze worden beheerd door de security officer en de autorisaties worden goedgekeurd door de procesverantwoordelijke (of lijnmanager).

h. Er is training voor de medewerkers om bewust met suwinet te werken. Deze trainingen zijn gericht op het bewust worden van informatiebeveiliging en privacy gericht op suwinet. Voor nieuwe medewerkers wordt deze training binnen 3 maanden na indiensttreding afgerond. Het bewijs van de afgeronde training is zichtbaar voor de CISO en voor de security officer van suwinet.

   Verder wordt in team overleggen aandacht geschonken aan het veilig omgaan met Suwigegevens, het Beveiligingsplan en andere onderwerpen die hiermee te maken hebben.

II. Europees/Landelijk beleid

De VNG zet in op een generieke en proactieve gemeentelijke aanpak met betrekking tot informatiebeleid in het algemeen en informatiebeveiliging in het bijzonder. Samen met KING (Kwaliteitsinstituut Nederlandse Gemeenten) heeft de VNG in 2016 diverse handreikingen en ander ondersteuningsmateriaal ontworpen. Dit om gemeenten beter te helpen met de beveiliging van de informatievoorziening en specifiek, Suwi. In dit kader kunnen worden genoemd:

- *De BIO en de IBD*:) Baseline Informatiebeveiliging Overheid (BIO) en de totstandkoming en doorontwikkeling van de Informatiebeveiligingsdienst (IBD) zijn in het leven geroepen in de bijzondere ledenvergadering van najaar 2013. Toen nam de ALV van de VNG met een overgrote meerderheid een resolutie aan waarin gemeenten verklaren de BIO als gemeentebreed normenkader voor informatiebeveiliging te zullen implementeren. De IBD ondersteunt en adviseert gemeenten daarbij.
- *ENSIA*: ENSIA staat voor Eenduidige Normatiek en Single Information Audit. ENSIA wordt ontwikkeld om gemeenten in staat te stellen op transparante wijze aan de gemeenteraad verantwoording af te leggen over het gerealiseerde niveau van informatieveiligheid. Daarmee wordt de bestaande verantwoordingslast rond SUWI, DigiD, BRP etc. eenvoudiger gemaakt. ENSIA is een interbestuurlijk traject waarbij departementen én gemeenten samenwerken om de verantwoordingslast te beperken. De controle op de uitvoering van Suwi gebeurt inmiddels via de Ensia-audit.
- *Digitale Agenda 2020*: in juni jl. heeft de ALV ingestemd met een brede beweging van activiteiten gericht op de doorontwikkeling van gemeenten in de informatiesamenleving. Eén van de activiteiten onder deze noemer is de Bestuurlijke Visitatiecommissie Informatiebeveiliging. Deze commissie bestaande uit twee burgemeesters en een hoofd Publieke Dienstverlening bezoekt colleges van B&W en gaat met hen in gesprek over de lokale status van de informatiebeveiliging en hoe deze op niveau te brengen of houden.
- *Algemene Verordening Gegevensbescherming (AVG)*: Deze verordening harmoniseert privacyregelgeving in Europa en verbetert de privacybescherming van burgers. De AVG is per 25 mei 2018 in werking getreden. De organisatie heeft verschillende maatregelen getroffen om aan de vereisten van de AVG te voldoen.

5. Programma Borging veilige gegevensuitwisseling via Suwinet

Naar aanleiding van de resultaten van de uitgevoerde onderzoeken is het programma Borging Veilige Gegevensuitwisseling via Suwinet opgezet. Het doel is maatregelen te nemen om het zorgvuldig omgaan met gegevens die via Suwinet zijn verkregen te vergroten én de privacy van burgers beter te beschermen. Het programma 'Borging Veilige Gegevensuitwisseling via Suwinet' is opgezet door de Suwipartijen SVB, UWV en VNG om gemeenten te ondersteunen bij een zorgvuldige en veilige gegevensuitwisseling. De voorgestelde maatregelen dienen te worden genomen op het gebied van bewustwording, beleid betreffende misbruik, normenkader, telewerken, fijnmaziger autoriseren, beperking toekenning zoeksleutel, beperking toegang (whitelist) en verbetering logging en rapportages.

6. Nieuw normenkader

De Gezamenlijke elektronische Voorziening Suwinet (GeVS) wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. Binnen de Suwiketen participeren drie type stakeholders: Bronhouders, Beheerder van de centrale 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 routering van deze gegevens op basis van technische en communicatie faciliteiten en IT componenten. Deze faciliteiten en IT componenten representeren het zogeheten Suwinet.

De GeVS en de informatie die via GeVS wordt uitgewisseld moeten voldoen aan specifieke beveiligingseisen en aan de AVG. De beveiliging van GeVS kan in volle omvang alleen worden gerealiseerd wanneer de ketenpartijen gezamenlijk, ieder vanuit hun eigen verantwoordelijkheid, de juiste beveiligingsmaatregelen treffen.

Voor een adequate werking en bescherming van GeVS zijn ketenafspraken noodzakelijk op het gebied van uitgangspunten en randvoorwaarden, wijze van implementatie, beheersen en het geven van wederzijds inzicht omtrent deze afspraken. De ketenafspraken staan dan ook in het teken van de beveiligingsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid. Het doel van deze afspraken is een passend beveiligingsniveau van de keten te garanderen.

III. Gemeentelijke informatisering- en automatiseringsstructuur

De infrastructuur en internetapplicaties vallen technisch, qua gebruik en beveiligingsaspecten onder verantwoordelijkheid van het team ICT van Bedrijfsvoeringsorganisatie De Connectie. De Suwi wetgeving eist een beveiligingsplan en stelt specifieke eisen aan (controle op) het gebruik door de functionele afdeling.

7. Internet

De gemeente Rheden maakt gebruik van het beveiligde netwerk voor Nederlandse gemeenten, KPN Lokale Overheid genaamd. Om de Suwinet-inkijk applicatie te gebruiken wordt eerst verbinding gemaakt met KPN Lokale Overheid waarna verbinding wordt gemaakt met Suwinet-inkijk. Er is een besloten gebruikersgroep die gebruik mag maken van KPN Lokale Overheid. KPN Lokale Overheid zorgt ervoor dat er geen onbevoegden kunnen binnenkomen in het netwerk Suwinet. Verder heeft de gemeente Rheden maatregelen getroffen voor een zo hoog mogelijk beveiligingsniveau:

1. de dataverbindingen met de buitenwereld voor Suwinet lopen via de firma KPN Lokale Overheid;
2. men kan veilig e-mailen, waarbij de ontvanger ook veilig op de mail kan antwoorden.
3. alle centrale computers en werkplekken zijn voorzien van actuele toegangs- en virussenbeveiligingsprogrammatuur.

De infrastructuur en internetapplicaties vallen technisch, qua gebruik en beveiligingsaspecten onder verantwoordelijkheid van team ICT van Bedrijfsvoeringsorganisatie De Connectie. Het gebruik van internet en het beveiligingsbeleid is centraal geregeld. De Suwi wetgeving eist een beveiligingsplan en stelt specifieke eisen aan (controle op) het gebruik door de Gebiedsteams Inkomen, Werk en re-integratie en Team Advies en Ondersteuning.

8. Backup

Door team ICT van de Bedrijfsvoeringsorganisatie De Connectie worden dagelijks back-ups van de systemen gemaakt. Als het nodig is kunnen deze teruggezet worden. De back-up media worden op een externe locatie bewaard, conform de BIO.

Er vind geen jaarlijkse uitwijktest plaats omdat De Connectie formeel geen uitwijkmogelijkheden heeft. Er is dus ook geen samenwerking met IBM. In plaats daarvan maakt De Connectie gebruik van een high availability oplossing met een tweede computer centrum van TDCA (Twin Data Center Arnhem) op het Akzo terrein.

9. Werkplekken

De werkplekken (inlog computers) zijn beveiligd door het gebruik maken van een 2-weg authenticatie. Zowel een wachtwoord van voldoende sterkte als iets wat iemand heeft: een token. Beiden zijn nodig om in te loggen. De Suwinet-inkijk applicatie heeft een eigen wachtwoord. Bij het gebruik van Suwinet is het niet toegestaan om de werkplek te verlaten. Bij het verlaten van de werkplek moet de applicatie worden afgesloten en moet men het bureaublad vergrendelen.

Binnen de gemeente Rheden zijn er interne richtlijnen opgesteld voor het thuiswerken. Hierin staat onder andere dat thuis de papieren werk-informatie goed wordt opgeborgen, c.q. niet zomaar rondslingert; Via de eigen internetverbinding thuis log je eerst in op het systeem van de gemeente Rheden. Dit gaat middels een inlogaccount met een wachtwoord en een token (een apparaatje met aanvullend gebruikersnummer). Printen op de eigen thuisprinter is niet direct mogelijk en is niet toegestaan.

Vanwege de coronapandemie is dringend verzocht thuis te werken in plaats van op kantoor.

10. Toegangsbeleid

Binnen De Connectie is het wachtwoordbeleid conform de BIO-richtlijnen, tenzij de applicatie dit niet kan afdwingen (denk hierbij aan legacy-systemen). Daarmee voldoen de aangesloten partijen (m.u.v. legacy systemen) eveneens aan de BIO-normen.

Ten aanzien van wachtwoorden geldt:

- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- Tijdelijke wachtwoorden of wachtwoorden die standaard in software of hardware worden meegegeven worden bij eerste gebruik vervangen door een persoonlijk wachtwoord.
- Gebruikers bevestigen de ontvangst van een wachtwoord.
- Wachtwoorden zijn alleen bij de gebruiker bekend.

- Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken.
- Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden.

Wachtwoorden worden encrypted (haching) en opgeslagen binnen een beveiligde omgeving.

Voor het beheer en het beheersen van beheerdersaccounts wordt gebruik gemaakt van wachtwoordkluis, met logging en auditing functionaliteit. Admin-accounts zijn aanvullend voorzien van tweefactorauthenticatie.

Toegang tot Suwinet is alleen mogelijk met behulp van een gebruikerscode en een wachtwoord. Deze twee sleutels worden aan de geautoriseerde medewerker ter beschikking gesteld en mogen door deze medewerker niet aan anderen bekend worden gemaakt. De toegang verloopt via een beveiligde internetverbinding. Bij gebruik van de digitale gemeentelijke werkplek komt die internetverbinding via het netwerk van de gemeente tot stand. Ook voor de toegang tot dit netwerk is een gebruikerscode en een wachtwoord vereist. Deze kunnen niet dezelfde zijn als de gebruikerscode en wachtwoord van Suwinet.

Suwinet vraagt, wanneer voor het eerst wordt ingelogd, het wachtwoord te wijzigen in een nieuw wachtwoord, dat moet voldoen aan een aantal eisen:

1. Het wachtwoord is 90 dagen geldig; Wanneer de gebruikersbeheerder een wachtwoord verstrekt aan een Suwinet-gebruiker moet deze gebruiker het door u verstrekte wachtwoord binnen 14 dagen wijzigen anders wordt het account geblokkeerd
2. Indien een gebruiker van Suwinet langer dan 90 dagen niet inlogt op Suwinet wordt het account automatisch geblokkeerd;
3. De gebruiker heeft het eigen beheer over het wachtwoord. Een wachtwoord is strikt persoonlijk en mag niet gedeeld worden met anderen.
4. Zodra een medewerker de gemeente verlaat, wordt het account verwijderd of ontoegankelijk gemaakt.

Om te voorkomen dat derden gebruik maken van ingelogde maar onbeheerde werkplekken (de medewerker is even weggeroepen), wordt de verbinding met het netwerk na korte tijd van niet gebruik geblokkeerd en moet opnieuw met wachtwoord en inlogcode worden ingelogd. Bij het gebruik van Suwinet is het niet toegestaan om de werkplek te verlaten. Bij het verlaten van de werkplek moet de applicatie worden afgesloten en moet men het bureaublad vergrendelen.

11. Medewerkers, taken en bevoegdheden

Medewerkers gaan op verantwoorde wijze om met de persoonsgegevens die zij raadplegen via Suwinet-inkijk. Alleen toegestaan is het raadplegen van persoonsgegevens van cliënten die een uitkering PW, IOAW en of IOAZ ontvangen, bij controle van de rechtmatigheid en doelmatigheid inzake de wettelijke voorschriften. Verder gelden de volgende richtlijnen:

1. Gegevens uit Suwinet-Inkijk mogen nooit gemaild worden, niet intern en niet extern. Het gebruik van Suwinet is toegestaan, bij voorkeur binnen kantoortijd op kantoor of elders. Het geprinte materiaal moet zorgvuldig worden afgeschermd om misbruik te voorkomen. Als men gegevens uitprint van Suwinet is het niet toegestaan deze op een andere printer dan die van de gemeente Rheden uit te printen. Dit moet gebeuren met de zogenaamde secureprinter. De gegevens dienen binnen de Gebiedsteams Inkomen, Werk en re-integratie het team Advies en Ondersteuning te blijven. De uitdraaien uit Suwinet worden in het persoonsdossier dan wel de mappen van de rechtmatigheidsformulieren bewaard.
2. De persoonsdossiers worden digitaal opgeslagen dan wel bewaard in een archiefkast die wordt afgesloten als de laatste medewerker de afdeling verlaat. Bij het verlaten van de werkplek moet men zich afmelden van de applicatie. Voor uitkeringsgerechtigden die hun gegevens willen inzien en eventueel wensen te corrigeren is een protocol vastgesteld, zie bijlage Terugmelding en correctieverzoeken DKD. Er zijn in het verleden nog geen (digitale) verzoeken binnengekomen.
3. Personeel dat in dienst is bij de gemeente valt onder het ambtenarenreglement. Bij benoeming hoeft niet apart een verklaring ondertekend te worden, dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit opgenomen. De desbetreffende medewerker wordt door de Security Officer (SO) voordat toegang tot de diverse applicaties wordt verleend, gewezen op de gebruikersafspraken en de regels over de vertrouwelijkheid. Hierbij wordt uiteraard gewezen op doelbinding en proportionaliteit van de gevoelige informatie.

   Dit wordt vastgelegd doormiddel van een bewustwordingstraining mbt suwinet. Deze training wordt afgerond binnen 3 maanden na indiensttreding.

4. Voor extern of ingehuurd personeel dat dient te beschikken over de Suwinet-inkijk applicatie is in de meeste gevallen via de inleenovereenkomst van de uitzendbureaus of de daaraan gekoppelde algemene voorwaarden de geheimhouding van vertrouwelijke gegevens door het bureau en de medewerker gewaarborgd. Bij de inlening wordt door de Kwaliteitsmedewerker een ondertekende verklaring gevraagd over de omgang met vertrouwelijke gegevens waaronder Suwinet-inkijk autorisaties. Deze verklaring wordt in het persoonsdossier (bij Personeelszaken) geborgen.

12. Taken en rollen Suwinet-inkijk

In het kader van de beveiliging is het beheer voor het gebruik van Suwinet neergelegd bij de Security Officer, ondergebracht bij het team Advies en Ondersteuning. Deze is verantwoordelijk voor het beheren van accounts. Bij indiensttreding of bij functiewisseling krijgen medewerkers indien noodzakelijk dit Beveiligingsplan 'Suwinet-Inkijk' uitgereikt en tekenen zij de bijbehorende verklaring Suwinet (zie bijlage). Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. Een verzoek voor autorisatie gaat via TopDesk waarbij de Teamleider goedkeuring geeft.

13. College/Management

De verantwoordelijkheid voor het gebruik van Suwinet ligt te allen tijde bij het College van B&W en namens het college bij de managers. Het college is bestuurlijk eindverantwoordelijk voor een adequaat stelsel van procedures, afspraken en werkwijzen rondom het gebruik en beheer en de interne verantwoording daarover. Twee keer per jaar doet de Intern Controleur (IC)onderzoek naar het gebruik van Suwinet Inkijk. Daarvoor beschikt de IC over gebruikersrapportages die door het BKWI zijn klaargezet. Als er afwijkingen zijn in de trends of andere opvallende zaken, download de IC de Specifieke rapportage. In dat geval onderzoekt hij de interne systemen als C-Sam, Green Valley en of bevraagt de consulent. Dit alles om oneigenlijk of misbruik van privacygegevens te voorkomen.

Van dit onderzoek wordt een rapportage opgemaakt en ondertekend door de IC, manager en wethouder. Voor de ondertekening worden de rapportages besproken met de manager. De manager bespreekt het rapport met de wethouder. De verantwoordelijkheid om toegang te verlenen tot de gegevens behorend bij Suwinet-Inkijk berust functioneel gezien bij de verantwoordelijke teammanager en teamleider en wordt technisch uitgevoerd door de Applicatiebeheerder.

14. Security officer/applicatiebeheerder

Het gebruik van Suwinet vindt plaats onder toezicht van een Security Officer (SO). De SO beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De SO adviseert over en bevordert de beveiliging van Suwinet, verzorgt rapportages over de status met betrekking tot de beveiliging van Suwinet, zorgt dat de maatregelen worden nageleefd, evalueert de uitkomsten en adviseert en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De SO rapporteert en adviseert de teamleider Advies en Ondersteuning en schaalt bij een meningsverschil/incidentenprocedure zo nodig op naar een hoger echelon.

Jaarlijks wordt het beveiligingsplan Suwinet gecontroleerd op actualiteit en volledigheid. Wijzigingen worden in een addendum toegevoegd. Vanaf 2019 stellen we het Beveiligingsplan een maal per 3 jaar vast. Voor het eerst in 2021.

De Security Officer is verantwoordelijk voor het beheren van de accounts van zowel Suwinet inkijk als de applicatie Liaan, die wordt gebruikt voor DKD inlezen. Gebruikers krijgen een persoonlijk inlogaccount. Alvorens toegang tot Suwinet Inkijk mogelijk is, dient de gebruiker in te loggen in een beschikbaar systeem op basis van een inlogaccount met een wachtwoord, gecombineerd met een token. In de controle door de Security Officer wordt ook bekeken of een actualisering van het beveiligingsplan noodzakelijk is. Als dit het geval is, volgt een voorstel tot actualisering aan het managementteam en het college van B&W. De Security Officer onderzoekt per kwartaal of de toegangsverlening volgens proces verloopt. Daartoe spreekt zij met de betrokkenen, zoals deze in dit plan zijn vermeld. Tevens kan de Security Officer de volgende bronnen raadplegen:

1. De getekende verklaringen rechtmatig gebruik Suwinet
2. De bijgewerkte autorisatiematrix

Bovengenoemde taken behoren tot de genoemde functie en gaan over op de vervanger van de functionaris bij afwezigheid.

15. Intern Controleur

De (logging)-gegevens over het gebruik van Suwinet-Inkijk en Liaan worden uitgevraagd door de Intern controleur. Hij controleert periodiek gebruikersrapportages. Bij trendafwijking wordt een specifieke rapportage opgevraagd. De resultaten van deze controle worden teruggekoppeld aan de desbetreffende leidinggevende. De leidinggevende bespreekt de resultaten 4x per jaar met de portefeuillehouder.

Taken:

- Vier keer per jaar controle loggin gegevens. Doel: controleren of het gebruik van de gegevens binnen Suwinet-inkijk, Suwinet inlezen en DKD inlezen (Liaan) plaatsvindt binnen de wettelijke kaders en in overeenstemming met de doelen die de organisatie hiertoe heeft geformuleerd

Bovengenoemde taken behoren tot de genoemde functie en gaan over op de vervanger van de functionaris bij afwezigheid.

Een logregel bevat minimaal:

a. de gebeurtenis;

b. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon;

c. het gebruikte apparaat;

d. het resultaat van de handeling;

e. een datum en tijdstip van de gebeurtenis.

16. Teamleiders

De teamleiders van het team Inkomen, Werk en re-integratie en het Team Advies en Ondersteuning zijn samen verantwoordelijk voor het gebruik en de beveiliging van Suwinet-inkijk.

17. Gebruikersrollen en autorisaties

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie. Binnen Suwinet wordt voor de gemeente een aantal gegevens afgeschermd omdat deze voor de gemeente niet functioneel zijn. Afschermen van een gedeelte van de voor de gemeente beschikbare gegevens is technisch mogelijk, maar is niet functioneel.

Bij punt 20 en 21 volgt per functie wie in welke gevallen Suwinet-inkijk en Suwinet inlezen mag gebruiken. We spreken in die gevallen van geoorloofd gebruik. Wordt Suwinet om andere redenen gebruikt dan zoals hieronder verwoord, dan is er in principe sprake van ongeoorloofd gebruik.

18. Autorisaties toekennen

Bij het toekennen van autorisaties gelden vanuit het oogpunt van de taakstelling en privacy-bescherming de volgende uitgangspunten:

1. Alleen medewerkers die Suwinet-gegevens nodig hebben voor het uitvoeren van een wettelijke taak krijgen toegang tot Suwinet-Inkijk en Suwinet inlezen.
2. In de gemeentelijke organisatie zijn dat in ieder geval geen andere personen dan medewerkers van het Gebiedsteam Inkomen en Werk en re-integratie en een gering aantal van het team Advies en Ondersteuning.
3. Autorisaties worden toegekend op basis van 'need-to-know': alleen de informatie die nodig is om de functie uit te voeren mag opgevraagd worden.
4. Gemeenten zijn verplicht het Burgerservicenummer (BSN) in de administratie vast te leggen. Dit betekent dat van ieder persoon van wie informatie opgezocht moet worden het BSN bekend is. Informatie via Suwinet-inkijk is daarom alleen via het BSN te benaderen.
5. Autorisaties waarbij op andere of meer zoeksleutels dan alleen het BSN naar informatie gezocht kan worden, worden alleen toegekend aan preventie en SR (Sociale Recherche).
6. Bij vertrek van een medewerker of verandering van functie worden de toegekende autorisaties ingetrokken, dan wel aangepast aan de nieuwe functie door de Teamleider Inkomen, Werk en re-integratie of manager Team Advies en Ondersteuning. Verlopen autorisaties blijven staan zolang de medewerker in dienst is.

19. Medewerkers Sociale Recherche en de preventiemedewerkers

1. Afhandeling maandelijkse signalen Inlichtingen Bureau (IB);
2. Controle van tips zowel intern als extern;
3. Fraudesignalen en onderzoeken;
4. Bij preventieonderzoeken en thematische onderzoeken;
5. Suwinet inlezen en of DKD inlezen (Liaan)

Ad 1.

Liaan

De medewerkers SR (2 personen) gebruiken de Internetapplicatie Liaan voor frauderegistratie, herberekeningen en afhandeling van de signalen van het IB. Het zogenaamde Suwinet inlezen en DKD inlezen vindt met behulp van deze applicatie plaats.
Als afnemende en inlezende organisatie van Liaan heeft de gemeente gegevens van beveiliging geïmplementeerd. Maatregelen zijn genomen om doelbinding en beveiliging van DKD gegevens te waarborgen.

In Liaan is een faciliteit beschikbaar om doelbinding en beveiliging van de DKD gegevens te toetsen. Het inlezen en voorinvullen van DKD-gegevens is ten behoeve van SUWI-taken. De tool maakt het mogelijk per gebruiker een overzicht samen te stellen van de door de gebruiker geraadpleegde gegevens.
Iedere bevraging wordt gelogd. Bij het loggen worden de volgende gegevens opgeslagen: Datum, Tijd, Partij Suwi (gemeente), Gebruiker, Applicatie, Doelbinding, Bericht, BSN, Kenteken. Hierdoor kan inzage worden verkregen welke BSN-nummers en kentekens bevraagd zijn. Wij schatten in dat het risico op oneigenlijk dan wel misbruik gering is, gelet op het zeer beperkte aantal gebruikers. Per kwartaal toetst de Intern Controleur de raadplegingen van de gebruikers. Hierbij wordt gekeken of de gebruiker de BSN ’s en of kentekens heeft geraadpleegd die nodig zijn voor onderzoek binnen haar vakgebied.
De functioneel beheerder is applicatiebeheerder en gebruikersbeheerder om de rechten te beheren. De Intern Controleur doet de logincontroles zoals deze ook voor Suwi-Inkijk worden gedaan.

20. Consulent, financieel en administratief mdw, kwaliteits- en juridische mdw

1. Aanvragen ogv de PW, Ioaw, Ioaz, Bbz uitkering, verhaal en beslag;
2. Heronderzoeken (zowel rechtmatigheids- als doelmatigheidsonderzoeken);
3. Debiteuren(her)onderzoeken ter vaststelling van actuele woonplaats, draagkracht, hoogte inkomen, werkgever etc.;
4. Verwerking, controle van de maandelijkse mutatieformulieren en in die gevallen ter beoordeling van de consulent/medewerker.

21. Rollen binnen gebiedsteams

De functies binnen de gemeente die geautoriseerd zijn om gebruik te maken van Suwinet-Inkijk liggen vast in rollen per gebiedsteam.

Zo zijn onderstaande gebruikersrollen voor Inkomen, Werk en re-integratie en Advies en Ondersteuning:

1. Consulenten uitkeringsadministratie, medewerkers financiële administratie;
2. Consulenten werk en inkomen;
3. Kwaliteitsmedewerkers en intern controleur;
4. Medewerkers sociale recherche en de preventiemedewerkers. (‘zware rollen’)
5. Inburgering

Schema functies en toegang tot gebruikersrollen voor Suwinet-Inkijk

Medewerker/functie	Gebruikersrol	(Gebieds)team
Consulent werk	Consulent werk	Werk en re-integratie
Consulent inkomen	Consulent inkomen	Inkomen
Kwaliteitsmedewerker	Consulent inkomen	Team Advies en Ondersteuning
Medewerkers financiële administratie	Consulent inkomen	Team Advies en Ondersteuning
Administratieve medewerker uitkeringenadministratie	Consulent inkomen	Inkomen
Sociale Rechercheur, preventiemedewerkers en adm.medewerker SR	Consulent fraude	Team Advies en Ondersteuning
Functioneel beheerder Werk en Inkomen en Intern controleur	Gebruiksbeheerder	Team Advies en Ondersteuning

22. Instructie medewerkers

Medewerkers worden om verschillende redenen geautoriseerd voor het gebruik van deze gegevens. In de aan hun te geven instructie (zie bijlage) zal duidelijk moeten worden gemaakt dat zowel dienstverlening als controle te ver kunnen doorschieten: Gegevens inzien kan en moet, maar alleen voor zover het nodig is voor het uitvoeren van de opgedragen taak.

Voor het werken en omgaan met persoonsgegevens is vanuit de Europese Unie een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Daaruit zijn gedragsregels afgeleid die gelden voor medewerkers van de gemeente (Gebiedsteams Inkomen, Werk en re-integratie en Team Advies en Ondersteuning) in relatie tot hun werkzaamheden, in het bijzonder bij het gebruik van Suwinet-Inkijk en DKD inlezen.

23. Functiescheiding

Er zijn verschillende functies waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van cliëntgegevens/informatie. De taken en verantwoordelijkheidsgebieden zijn gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Hiervoor zijn onderstaande taken bij verschillende personen belegd:

1. Uitvoering van taken (het gebruik van Suwinet);
2. Het beheer van autorisaties (toegang verlenen tot Suwinet);
3. Kwaliteitszorg en borging van rechtmatig gebruik (controle op gebruik van Suwinet);
4. Management (beslissen over bevoegdheden van functiegroepen, en/of individuele medewerkers, uitdragen belang goed gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet);
5. Opvragen rapportages.

In het toekennen van autorisaties is de functiescheiding als volgt verwerkt:

1. Verlenen toegang (betreffende teamleider of teammanager in combinatie met Applicatiebeheerder) gescheiden van gebruik (alle overige gebruikers van Suwinet-Inkijk en DKD inlezen).
2. Beveiligingsmaatregelen alsook advisering over gebruik en beveiliging Suwinet zijn beide belegd bij de Security Officer. Echter ook de medewerker Interne Controle heeft een eigen rol in de controle op de beveiliging en processen rondom Suwinet. Deze IC-medewerker rapporteert zelfstandig onder andere aan het MT en B&W. Hiermee is deze scheiding van taken ondervangen.
3. De autorisaties worden met inachtneming van deze uitgangspunten op verzoek van de betreffende teamleider of teammanager toegekend door de Applicatiebeheerder. In het verzoek wordt gemotiveerd aangegeven waarom aan een (groep) gebruiker(s) een bepaalde autorisatie moet worden toegekend.
4. Raadplegen van Suwinet-Inkijk in andere situaties wordt via de whitelist vastgelegd. In de applicatie Liaan bestaat geen whitelist. Een BSN raadplegen van een cliënt die onbekend is in het cliëntvolgsysteem in verband met een rechtmatigheids- en/of fraudeonderzoek wordt door de medewerker zelf geregistreerd om dit indien nodig achteraf te kunnen verantwoorden aan de medewerker Interne Controle.

Er is geen capaciteit om tot verdere functiescheiding te komen. De taken met betrekking tot Suwi vormen geen dagtaak. Ze zijn van een zodanig geringe omvang dat iemand dit naast zijn reguliere werk doet. Daarom zijn de taken bij de meest logische functionaris belegd.

24. Proces toekennen autorisaties

1. De medewerker die in dienst komt (of tijdelijk wordt ingehuurd) en voor de uitoefening van zijn taak het gebruik van Suwinet nodig heeft, wordt op verzoek van de Teamleider Inkomen en Werk en re-integratie geautoriseerd door de Suwinetbeheerder. Dit verzoek wordt neergelegd in het "meldingsformulier in dienst nieuwe medewerkers" waarin alle organisatiebreed te doorlopen stappen bij het in dienst komen van een medewerker zijn vastgelegd. In het "meldingsformulier in dienst nieuwe medewerkers" wordt vastgelegd dat de medewerker geautoriseerd moet worden voor Suwinet en welk gebruikersprofiel (rol) aan hem wordt toegekend.
2. Wanneer Suwinet om andere redenen wordt gebruikt, dan is er in principe sprake van ongeoorloofd gebruik. Over het algemeen geldt dat slechts mag worden geraadpleegd, indien die stap binnen het werkproces expliciet is beschreven.
3. Consulenten mogen raadplegen bij het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, Ioaw, Ioaz, Bbz of een andere door de teams uitgevoerde regeling betreft. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen.
4. Medewerkers die verantwoordelijk zijn voor terugvordering en verhaal mogen raadplegen bij onderzoeken die samenhangen met verhaal op onderhoudsplichtigen of vorderingen. Dit bijvoorbeeld ter vaststelling van woonplaats, draagkracht, inkomen of werkgever.
5. De administratief medewerker mag raadplegen om standaard uitdraaien voor het onderzoek van de consulent Werk en Inkomen te maken.
6. De medewerker uitkeringsadministratie mag gegevens uit Suwinet-Inkijk raadplegen. Dit ten behoeve van de berekening en uitbetaling van de uitkering.
7. Kwaliteitsmedewerkers mogen raadplegen om besluiten te kunnen toetsen.
8. De medewerkers van team Burgerzaken mogen de gegevens uit Suwinet-Inkijk raadplegen om adresonderzoeken te behandelen.
9. Handhaving (Sociaal Rechercheur en Preventie) mag raadplegen bij het behandelen van aanvragen of melding dat belanghebbende een uitkering wil aanvragen, rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, Ioaw, Ioaz, Bbz of een andere door de teams uitgevoerde regeling betreft.

   Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur van Suwinet dat de medewerker de voor hem/haar van belang zijnde gegevens kan raadplegen. Bij de onderzoeken wordt telkens de afweging gemaakt over noodzaak, subsidiariteit en proportionaliteit van het instrument wat wordt ingezet. Aan deze medewerkers zijn de zgn 'zware rollen' toegekend.
10. Voor de medewerkers van SR is er een internetapplicatie Liaan beschikbaar. Hierin zitten modules Herberekenen, Inlichtingenbureau en Frauderegistratie. Tevens gebruiken we dit voor DKD-inlezen.

11. De gegevensbeheerder en de daarbij aangesloten medewerkers mogen raadplegen om onderzoek in te stellen naar aanleiding van de logging gegevens.

25. Wijzigen autorisatie

- De werkzaamheden van medewerkers kunnen veranderen. Dit kan een uitbreiding of beperking van de toegekende Suwinet rollen betekenen. Wijzigingen als gevolg van veranderende taken doorlopen dezelfde stappen als bij een eerste autorisatie-verlening.
- De Security Officer besteedt in deze gevallen in het bijzonder aandacht aan het voorkomen van een onbedoelde stapeling van bevoegdheden. Hiermee wordt bedoeld dat niet meer benodigde autorisatie-rollen ook daadwekelijk worden ingetrokken bij de toekenning van nieuwe rollen die vanwege het nieuwe takenpakket rechtmatig noodzakelijk zijn en dat de verleende autorisatie afgestemd doelmatig blijft.

26. Whitelist

Persoonsgegevens zijn per definitie privacygevoelig en dienen met de hoogst mogelijke zorgvuldigheid te worden gebruikt en behandeld.
Voor het gebruik van Suwinet-Inkijk dienen medewerkers te zijn geautoriseerd. Daarmee is de toegang tot gegevens beperkt tot personen die uitvoering geven aan deze genoemde wettelijke taak. Op dit moment kan een geautoriseerde medewerker in principe gegevens opvragen van iedere in Nederland woonachtige persoon. Dit betreft dan ook personen waar geen dienstverleningsrelatie mee is op basis van de gemeentelijke wettelijke taken. De gegevensraadpleging is dus niet begrensd tot de 'eigen' burgers. Het zou kunnen leiden tot raadplegingen van gegevens van burgers waarmee geen dienstverleningsrelatie mee is. Dit is onwenselijk.
Om dit tegen te gaan gebruiken we nu binnen Suwinet-Inkijk een filtermechanisme, de zogenaamde 'whitelist'. Deze whitelist bevat alleen BSN's van personen waarmee de gemeente een dienstverleningsrelatie heeft of heeft gehad. Is die relatie er niet (geweest), dan krijgt de medewerker in principe geen toegang tot de gegevens.
Indien de raadpleging toch noodzakelijk is kan de medewerker gebruik maken een zogenaamde escape-functie. Dit filtermechanisme zorgt voor een veilig en proportioneel gegevensgebruik door de medewerker en draagt bij aan de privacy van de burger.

Wie staan er op de whitelist

- Alle klanten en hun eventuele partners die een uitkering levensonderhoud of bijzondere bijstand ontvangen of in de **afgelopen maanden** hebben ontvangen, een openstaande schuld aan de organisatie hebben of onderhoudsplichtig zijn.
- Deze klanten blijven op de whitelist staan tot een half jaar na het beëindigen van de regeling.

Wie mag er gebruik maken van de escape-functie

Gekozen is om iedere consulent de toegang tot de escape-functie te geven. Indien een medewerker persoonsgegevens opvraagt van een BSN dat niet op de whitelist staat, verschijnt een melding op zijn scherm. Alleen een medewerker met een autorisatie voor de escapefunctie kan toch doorgaan. Er zal moeten worden aangegeven waarom de escapefunctie wordt gebruikt.
Er is geëvalueerd of de escapefunctie voor iedere consulent noodzakelijk is. Dit blijkt handiger te zijn omdat geen consulent in dienst is die zich alleen met 'nuggers' (niet-uitkeringsgerechtigden) bezighoudt.

Hoe vaak wordt de whitelist geactualiseerd

Wekelijks wordt er een actuele lijst geüpload bij het BKWI om een zo actueel mogelijk bestand te verkrijgen, waardoor het gebruik van de escapefunctie zo veel mogelijk wordt voorkomen. Deze taak zal worden uitgevoerd door de Security Officer. Indien deze persoon niet aanwezig is zal dit door de intern controleur worden uitgevoerd.

27. Misbruik en beveiligingsincidenten

Bij controle van het gebruik kan er sprake zijn van constateringen die afwijken van het normale gebruiksbeeld. In dit geval wordt er een specifieke rapportage opgevraagd. Indien deze rapportage daar aanleiding toe geeft stelt de Security Officer een onderzoek in en betrekt daarbij altijd de volgende personen;

1. Intern controleur
2. Teamleider Inkomen en Werk en re-integratie/ Teammanager Advies en Ondersteuning.

Onderzocht wordt of er sprake was van doelmatig en rechtmatig gebruik van de Suwinet inkijk voorziening. Het kan nodig zijn met betrokken medewerker te spreken om dit uiteindelijk vast te stellen.

Indien er geen misbruik is geconstateerd is hiermee het onderzoek ten einde. De gegevens kunnen geanonimiseerd in de rapportage verwerkt worden.

Bij geconstateerd misbruik zal de SO een rapportage opstellen waarin de zwaarte van het misbruik omschreven wordt en deze aan de leidinggevende richten. Zo nodig wordt er opgeschaald. Er kan sprake zijn van de situatie dat misbruik geconstateerd is en dat de medewerker die hier verantwoordelijk voor is niet meer bij de gemeente werkzaam is. In deze situatie wordt beoordeeld welke stappen ondernomen worden. Hiertoe behoort ook het eventueel inlichten van een nieuwe werkgever.

Als er beveiligingsincidenten (waaronder datalekken) optreden worden gemeentelijke procedures gevolgd voor het melden en afhandelen van beveiligingsincidenten (zie ook paragraaf 4.d). Indien deze incidenten gevolgen hebben voor de beschikbaarheid, integriteit of vertrouwelijkheid van SUWInet of Liaan zal de gemeentelijke CISO worden betrokken bij de afhandeling van deze incidenten.

28. Misbruik en sancties

Er wordt onderscheid gemaakt tussen vermoedelijk misbruik en geconstateerd misbruik. Een sanctie wordt alleen toegepast bij misbruik. Opzettelijk onjuist gebruik wordt aangemerkt als misbruik. Indien er sprake is van misbruik door een medewerker, informeert de Security Officer Suwinet de verantwoordelijke teamleider of teammanager. Deze heeft een informerend gesprek met de medewerker. Dit gesprek wordt gerapporteerd richting de Security Officer Informatieveiligheid, MT en college van Burgemeester & wethouders (B&W) omdat hier sprake is van een ernstig veiligheidsincident. Als het om een Rozendaalse klant gaat, wordt de Ciso van Rozendaal betrokken.

Onder ernstig misbruik wordt in ieder geval verstaan het beschikbaar stellen van gegevens van burgers aan derden voor commerciële doeleinden. De Security Officer meldt gebleken misbruik aan de Teamleider of verantwoordelijke manager met een advies over de ernst van dit misbruik. De sanctie wordt afgestemd op de ernst van het misbruik en de omstandigheden. Ernstig misbruik kan leiden tot strafontslag of bij ingeleend personeel tot het onmiddellijk beëindigen van de inleenverhouding en melding aan de uitlener.

Conform de Ambtenarenwet en de CAR/UWO zijn rechtspositionele maatregelen mogelijk. De zwaarte van de sanctie is ter beoordeling aan de werkgever. Op basis van hetgeen in de CAR-UWO is beschreven aan disciplinaire maatregelen (van berisping tot ontslag op staande voet) bepaalt de werkgever de zwaarte van de disciplinaire maatregel. De medewerker wordt hiervan schriftelijk in kennis gesteld. Tegen deze beslissing is bezwaar en beroep mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen.

Onjuist gebruik leidt tot een nadere instructie, waarschuwing of sanctie bij de betrokken medewerker. Onjuist gebruik is:

1. Elk gebruik dat niet ten dienste staat van de uitkeringsverlening;
2. Het opvragen van gegevens ten behoeve van derden;
3. Het verstrekken van die gegevens aan derden.

Incidentele fouten zoals het ingeven van een verkeerd BSN–nummer wordt niet gezien als onjuist gebruik.

IV. Communicatie

De medewerker is altijd zelf bij zijn of haar werkzaamheden verantwoordelijk voor het voorkomen van oneigenlijk gebruik van informatie door derden. In bijlage 1 'Regels bij beveiliging van persoonsgegevens' is de lijst opgenomen met 'gouden tips' en aandachtspunten.

Het beveiligingsplan Suwinet is van toepassing op iedereen die gebruik maakt van Suwinet-Inkijk binnen de gemeente. Het plan wordt beschikbaar gesteld op het intranet en in het Handboek Schulinck. Van deze publicatie worden de betreffende medewerkers per mail op de hoogte gesteld.

Het binnen de gemeente geldende informatieveiligheidsbeleid (inclusief instructies en protocollen) is op iedereen van toepassing die gebruik maakt van Suwinet-Inkijk. Bestaande gebruikers zijn op de hoogte; nieuwe gebruikers worden op de hoogte gesteld.

Het plan wordt na vaststelling actief gecommuniceerd met de medewerkers. Het beveiligingsplan moet actief binnen de eigen organisatie worden uitgedragen en om te borgen dat haar medewerkers op de hoogte zijn van de inhoud en betekenis.

Hierdoor weten medewerkers welk gedrag de organisatie van hen verwacht én weten ze dat er gegevens worden bewaard waarmee het gedrag kan worden gecontroleerd. Van dat laatste moeten ze zich bewust zijn in relatie tot hun eigen privacy en dat van de klant. De organisatie kan de opgeslagen gegevens niet lukraak gebruiken: er moeten redelijke gronden zijn om de privacy van medewerkers binnen te treden.

Jaarlijks wordt dit onderwerp geagendeerd voor de overleggen. Alle gebruikers worden er minimaal twee keer per jaar in een periodiek overleg op geattendeerd dat ze kennis moeten nemen van het plan. Nieuwe medewerkers worden via de kwaliteitsmedewerker op het plan gewezen met de opdracht er kennis van te nemen.

Uitgangspunten:

- Minimaal twee keer per jaar vindt in het werkoverleg van het Team Inkomen, Werk en re-integratie en bij de gebruikers van Team Advies en Ondersteuning een bespreking plaats over het onderwerp. Alle gebruikers worden er dan op geattendeerd dat ze kennis moeten nemen van het plan. De Security Officer en kwaliteitsmedewerker zijn hierbij aanwezig en van dit werkoverleg wordt een verslag gemaakt.

- Nieuwe medewerkers worden door de Security Officer en kwaliteitsmedewerker op het plan en de daarin opgenomen Suwinet "handreiking voor gebruik" gewezen met de opdracht er kennis van te nemen.

- De nieuwe medewerker wordt er op gewezen dat van zijn of haar raadplegingen op Suwinet logging gegevens worden vastgelegd. Hierdoor vernemen medewerkers welk gedrag de organisatie van hen verwacht én weten ze dat er gegevens worden bewaard waarmee het gedrag kan worden gecontroleerd .

- Van dat laatste moeten ze zich bewust zijn in relatie tot hun eigen privacy en die van de klant. De organisatie kan de opgeslagen gegevens echter niet lukraak gebruiken, er moeten redelijke gronden zijn om de privacy van medewerkers binnen te treden.

- Zij krijgen ter ondertekening de "Verklaring rechtmatig gebruik Suwinet" (zie bijlage) aangeboden. Het ondertekenen van de verklaring is een belangrijk onderdeel van de bewustwording van de medewerker.

29. Evaluatie

Betrokkenen houden jaarlijks een evaluatiebijeenkomst. Het beveiligingsplan Suwinet wordt jaarlijks geëvalueerd en een maal per 3 jaar vastgesteld.
Bij de evaluatie maken we zo nodig een addendum.

Bijlage 1 Regels bij beveiliging van persoonsgegevens

Regels bij beveiliging van persoonsgegevens in relatie tot verkregen Suwi gegevens

Voor het werken met en de omgang met persoonsgegevens zijn vanuit de Europese Unie een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Concreet kunnen deze regels in relatie tot de SUWI wetgeving als volgt worden vertaald:

1. Beheren van wachtwoorden

De werkplekken (inlog computers) zijn beveiligd door middel van wachtwoorden met een aanvullend gebruikersnummer (token). De werknemer moet zijn wachtwoord invoeren alvorens de pc gebruikt kan worden. De Suwinet-inkijk applicatie heeft een eigen wachtwoord. Bij het gebruik van Suwinet is het niet toegestaan om de werkplek te verlaten. Bij het verlaten van de werkplek moet de applicatie worden afgesloten en moet men zich op de computer afmelden.

2. Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de applicatiebeheerder van Suwinet en of bij de Servicedesk. Door de Servicedesk worden alle incidenten vastgelegd in Topdesk en bewaakt door de teammanager of teamleider. De rapportages hiervan gaan ook naar de CISO. Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3. Geheimhoudingsplicht

Binnen de Gebiedsteams Inkomen, Werk en re-integratie en Team Advies en Ondersteuning wordt met persoonsgegevens gewerkt. Voor het werken met en de omgang met persoonsgegevens zijn vanuit de Europede Unie een aantal regels opgesteld, die zijn verwoord in de Algemene Verordening Gegevensbescherming (AVG). In de wet SUWI en in het ambtenarenrecht zijn geheimhoudingsbepalingen opgenomen, waarin wordt aangegeven dat de persoonsgegevens niet verder bekend mogen worden gemaakt dan voor de uitoefening van de functie noodzakelijk is. Van extern personeel wordt hetzij via de inleenovereenkomst met de uitzendorganisatie, hetzij via een ondertekende verklaring de geheimhouding gevraagd.

4. Gedragscode internet- en e-mailgebruik

De gemeente hanteert een protocol voor gebruik van email en internet. In dit protocol is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevat dit protocol regels voor de manier waarop het gebruik van externe e-mail en internet wordt geobserveerd. Het protocol is voor alle medewerkers van de gemeente te raadplegen op het gemeentelijke Intranet.

5. Kennisnemen van het informatiebeveiligingsbeleid

Het binnen de gemeente geldende informatiebeveiligingsbeleid, incl. het Beveiligingsplan Suwi met instructies en protocollen is op iedereen binnen de Gebiedsteams Inkomen, Werk en re-integratie en TAO van toepassing die gebruik maakt van Suwinet-inkijk. Alle gebruikers hebben een exemplaar van het beveiligingsplan ontvangen en alle nieuwe medewerkers/gebruikers (ook gedetacheerde medewerkers) ontvangen via de SO of kwaliteitsmedewerker een exemplaar.

Gebruikers van Suwinet-inkijk moeten weten dat over hen gegevens worden vastgelegd en verzameld. Dit is een belangrijk onderdeel van de privacybescherming ten opzichte van deze medewerkers. In het beveiligingsplan is hier uitgebreid aandacht aan besteed.

Een aantal keren per jaar en bij de evaluatie van het beveiligingsplan wordt dit onderwerp geagendeerd voor het werkoverleg.

6. Gegevensverstrekking aan derden via de telefoon

Het uitgangspunt is dat er met terughoudendheid aan verzoeken om telefonische informatie over betrokkenen wordt tegemoetgekomen. Het voeren van telefoongesprekken brengt namelijk de risico’s met zich mee dat de identiteit van de gesprekspartner verkeerd wordt vastgesteld of dat persoonsgegevens worden verstrekt aan personen die geen recht op informatie hebben. In principe wordt er dan ook geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen.

In die gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging. Bij een verzoek om telefonische informatieverstrekking van een ketenpartner wordt de verzoeker teruggebeld via het algemene nummer van de (vestiging van de) ketenpartner met het verzoek te worden doorverbonden. Dit terugbellen kan achterwege blijven indien verzoek afkomstig is van een vaste contactpersoon.

7. Clear desk en clear screen policy

De vertrouwelijke omgang met persoonsgegevens houdt onder andere in dat elke werkplek zodanig is ingericht, dat onbevoegden niet de beschikking kunnen krijgen over deze informatie. Vertrouwelijke gegevens mogen niet onbeheerd op het bureau achterblijven. Dossiers worden bewaard in een kast die na werktijd wordt gesloten. Bezoekers dienen zich bij binnenkomst in het gemeentehuis eerst te melden bij de receptie. De werkplekken bevinden zich achter beveiligde deuren. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de werkplek van de medewerkers. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De screensaver is zodanig ingesteld dat na een x-aantal minuten de schermbeveiliging intreedt. Dit is door de afdeling Systeembeheer voor iedere medewerker standaard ingesteld.

8. Geen vertrouwelijke gegevens in de prullenbak

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

9. Aanspreken van onbekende personen

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

10. De dagelijkse werkzaamheden tegenover informatiebeveiliging

Informatieveiligheid is uitermate belangrijk voor het werk binnen de Gebiedsteams Inkomen, Werk en re-integratie en TAO waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Ook cliënten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom middels het werkoverleg geregeld aandacht aan dit onderwerp besteed dient te worden.

11. Thuiswerken

Binnen de betreffende teams is het van essentieel belang om op een correcte wijze om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Tevens is dit een belangrijk aandachtspunt voor het thuiswerken. Specifiek voor het thuiswerken zijn er interne richtlijnen. Hierin staat onder andere dat thuis de papieren werk-informatie goed wordt opgeborgen, c.q. niet zomaar rondslingert. Via de eigen internetverbinding thuis log je eerst in op het systeem van de gemeente Rheden. Dit gaat middels een inlogaccount met een wachtwoord en een token (een apparaatje met aanvullend gebruikersnummer). Printen op de eigen thuisprinter is niet toegestaan en niet direct mogelijk.

Vanwege de coronapandemie is thuiswerken de regel geworden in plaats van uitzondering.

Bijlage 2 Protocol inzage in Suwinet door cliënt en/of gemachtigde

Protocol inzage in Suwinet door cliënt en/of gemachtigde

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, in de hieronder beschreven gevallen, is gegevensinzage door derden mogelijk.

De via Suwinet-inkijk opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op diskette).

Hieronder volgt een handleiding voor een aantal situaties waar de Suwi-gebruiker mee te maken kan krijgen.

Protocol AVG: https://www.rheden.nl/Footer/Privacy/AVG_verzoek_indienen

INZAGE

1. De cliënt verzoekt om inzage, hetzij schriftelijk, hetzij mondeling, in diens gegevens

- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (rijbewijs, paspoort, etc.);
- Vraag om het burgerservicenummer (BSN) van de cliënt;
- Stel vast dat het BSN is ontleend aan een officieel document (ID-bewijs, paspoort etc.)
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
- Berg (mogelijk tweede) uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel uitgedraaid exemplaar;
- Beëindig inkijksessie.

Het is mogelijk dat een cliënt telefonisch vraagt om een uitdraai van zijn/haar gegevens. In dat geval dient de cliënt verwezen te worden naar zijn/haar consulent of moet een schriftelijk verzoek indienen, dat binnen de wettelijk verplichte termijn dient te worden afgehandeld.
Indien de cliënt inzage wil in al zijn/haar gegevens die bij een ketenpartner zijn geregistreerd, dient de klant te worden verwezen naar de betreffende ketenpartner.

2. Gemachtigde verzoekt schriftelijk om inzage in cliëntgegevens

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (ID-bewijs, paspoort, etc.);
- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (ID-bewijs, paspoort, etc.);
- Vraag om het BSN van de cliënt;
- Stel vast dat het BSN is ontleend aan een officieel document (ID-bewijs, paspoort etc.)
- Maak een uitdraai van de geraadpleegde gegevens of laat de gemachtigde meekijken op het scherm;
- Berg (mogelijk tweede) uitdraai onmiddellijk op in het cliëntendossier of vernietig eventueel uitgedraaid exemplaar;
- Beëindig inkijksessie.

3. Een derde verzoekt om inzage, hetzij schriftelijk, hetzij mondeling in cliëntgegevens

- Dit is niet mogelijk

CORRECTIE

1. De cliënt verzoekt om correctie

- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (ID-bewijs, paspoort, etc.);
- Vraag om het BSN van de cliënt;
- Stel vast dat het BSN is ontleend aan een officieel document (ID-bewijs, paspoort etc.);
- Informeer de cliënt dat hij/zij een officieel verzoek moet indienen via een standaardformulier;
- Maak twee kopieën van het verzoek;
- Verstrek een kopie aan de cliënt, archiveer de andere kopie.

2. Gemachtigde verzoekt om correctie

- Stel vast dat de machtiging schriftelijk is gegeven en nauwkeurig omschreven;
- Stel de identiteit van de gemachtigde vast aan de hand van een geldig legitimatiebewijs (ID-bewijs, paspoort, etc.);
- Stel de identiteit van de cliënt vast aan de hand van een geldig legitimatiebewijs (ID-bewijs, paspoort, etc.);
- Vraag om het BSN van de cliënt;
- Stel vast dat het BSN is ontleend aan een officieel document (ID-bewijs, paspoort etc.)
- Informeer de gemachtigde dat hij/zij een officieel verzoek moet indienen via een standaardformulier;
- Maak twee kopieën van het verzoek;
- Verstrek een kopie aan de gemachtigde, archiveer de andere kopie

3. Een derde verzoekt om correctie

- Dit is niet mogelijk

Digitaal verzoek

Het is ook mogelijk om digitaal een AVG verzoek in te dienen.

https://www.rheden.nl/Footer/Privacy/AVG_verzoek_indienen

Bijlage 3 Geheimhoudingsverklaring

Verklaring omtrent geheimhouding van vertrouwelijke gegevens en het gebruik van Suwinet-inkijk.
(deze verklaring is noodzakelijk voor medewerkers waarbij de geheimhouding niet via het ambtenarenreglement of de inleenovereenkomst is geregeld)

De ondergetekende verklaart dat:

Geheimhouding algemeen
Hij/zij verplicht is tot geheimhouding van alle vertrouwelijke informatie die hij/zij vanwege de overeenkomst met de gemeente Rheden heeft verkregen tenzij op hem een wettelijke plicht tot bekendmaking rust. Informatie geldt als vertrouwelijk als dit door de gemeente is meegedeeld of als dit voortvloeit uit de aard van de informatie. De geheimhouding geldt tijdens de uitvoering maar ook na voltooiing van de werkzaamheden.

Gebruik Suwinet-inkijk
Hij/zij kennis heeft genomen van het beveiligingsplan Suwinet en de bijlagen over het gebruik van de Suwinet-inkijk applicatie en de wijze waarop het gebruik van deze applicatie wordt vastgelegd en gecontroleerd.

Rheden, d.d._____

naam: *voornaam:* *functie/rol Suwinet-inkijk*:

Handtekening,

_____

Bijlage 4 Procedure terugmeldingen en correctieverzoeken DKD

Deze procedure maakt deel uit van het beveiligingsplan Suwinet. De procedure voorziet in de handelingen, die verricht moeten worden, indien van een burger of één van de ketenpartners een melding wordt ontvangen van een geconstateerd verschil in de gegevens, die vanwege gemeente Rheden in het DKD zijn aangebracht.

Er is een mailadres beschikbaar voor correctieverzoeken en meldingen: correctieservice@rheden.nl. De Security Officer Suwinet heeft toegang tot dit mailadres.

Taken en bevoegdheden

- De daartoe aangewezen medewerker van gemeente Rheden heeft de taak een adequaat onderzoek te laten doen naar aanleiding van een correctieverzoek van een burger of een terugmelding door een ketenpartner, het gegeven zo nodig aan te passen, aan te vullen of te verwijderen. Indien een gegeven wordt aangepast, gewijzigd of verwijderd wordt de melder (burger)hiervan op de hoogte gebracht. Ook indien het betreffende correctieverzoek wordt afgewezen wordt de melder (burger) hiervan in kennis gebracht.
- De betreffende ketenpartner, welke een terugmelding heeft gedaan, wordt na een aanpassing van het gegeven in de applicatie van de bronhouder van de verwerking hiervan middels de betreffende autorisatie op DKD geïnformeerd.

Uitvoering

1. Een burger dient een correctieverzoek in voor de gegevens over hem/haar opgenomen in het DKD of een ketenpartner doet mededeling over een geconstateerde afwijking tussen één of meerdere gegevens opgenomen in DKD en de gegevens waarvan men kennis heeft of kennis heeft gekregen.
2. De terugmelding of het correctieverzoek worden ontvangen door de daartoe aangewezen medewerker.
3. Naar aanleiding van een correctieverzoek of terugmelding wordt overgegaan tot een onderzoek. De daartoe aangewezen medewerker is verantwoordelijk voor de afhandeling van de terugmelding.
4. De burger, die een correctieverzoek heeft ingediend, of de ketenpartner, die een terugmelding heeft gedaan, wordt zo spoedig mogelijk doch binnen 7 werkdagen na de ontvangst hiervan in kennis gesteld of naar aanleiding van het verzoek of de terugmelding gegevens in DKD zijn verbeterd, aangevuld of verwijderd. Ook bij een afwijzing van zijn/haar correctieverzoek wordt dit binnen 7 dagen aan de burger medegedeeld.
5. Blijkt uit het onderzoek dat het gegeven of de gegevens verbeterd, aangevuld of verwijderd moeten worden, dan zorgt de daartoe aangewezen medewerker dat hieraan uitvoering wordt gegeven.

Controle

- Eenmaal per jaar wordt door de Security Officer aan de hand van een aantal willekeurig gekozen terugmeldingen getoetst of conform het voorschrift wordt gewerkt.
- De Security Officer rapporteert schriftelijk over de toetsing aan de verantwoordelijke manager
- In deze rapportage zijn de volgende elementen standaard opgenomen:
    - Wanneer is de toetsing uitgevoerd?
    - Waaruit bestond de toetsing?
    - Wat is er geleerd van de toetsing?
    - Wat zijn de voorgestelde vervolgacties aan het management?

Rapportage controle terugmeldingen en correctieverzoeken DKD

Aan: de teammanager TAO
Van: De Security Officer Suwinet

Betreft: rapportage controle Terugmeldingen en Correctieverzoeken DKD
Datum:

Inleiding

Op …….. is gecontroleerd of er onregelmatigheden zijn met betrekking tot het uitvoeren van de Procedure Terugmeldingen en Correctieverzoeken DKD en de daarin vastgelegde werkwijze voor het verwerken van inhoudelijke terugmeldingen van ketenpartners en correctieverzoeken van burgers.

Beschrijving controle
Het volgende is gecontroleerd:

Wie heeft gecontroleerd?
De volgende medewerker(s) heeft/hebben gecontroleerd:
-De Security Officer

Resultaten van de controle

Aanbevelingen
De volgende aanbevelingen worden gedaan:

Gemeente Rheden, …….

Security Officer Suwinet

……

Voor gezien: Teammanager TAO

Bijlage 5 Rapportage autorisatiecontrole

Rapportage autorisaties Suwinet, kwartaal .., jaar …

Aan: de teammanager TAO
Van: De Security Officer Suwinet

Betreft: rapportage gebruikersautorisaties Suwinet Inkijk
Datum:

Inleiding

Op …….. is een controle op de gebruikers van suwinet gedaan. In deze rapportage vindt u de aantallen mutaties die hebben plaatsgevonden in de gebruikers t.b.v. Suwinet Inkijk.

Beschrijving controle
Het volgende is gecontroleerd:

Wie heeft gecontroleerd?
De volgende medewerker(s) heeft/hebben gecontroleerd:
-De Security Officer

Resultaten van de controle

Aanbevelingen
De volgende aanbevelingen worden gedaan:

Gemeente Rheden, …….

Security Officer Suwinet

……

Voor gezien: Teammanager TAO

……