Gemeente Heerde

cittaslow

2016

Beveiligingsbeleid en beveiligingsplan Suwinet

www.heerde.nl

Inhoudsopgave

1. Inleiding informatiebeveiligingsbeleid Suwinet 2016

1.1 Suwinet

De gemeente Heerde gebruikt Suwinet-Inkijk om informatie over inkomen en vermogen van een klant te verzamelen. De gegevens komen onder andere van de Belastingdienst, de Dienst Uitvoering Onderwijs (studiefinanciering), het UWV Werkbedrijf, de Rijksdienst voor het wegverkeer en van de Basis Registratie Personen van de gemeenten.

De organisaties hebben deze informatie nodig om de gegevens uitvraag aan de klant te beperken. Sociale Zaken gebruikt Suwinet-Inkijk daarnaast om het recht op een uitkering vast te stellen. Burgerzaken vraagt de gegevens op voor 'adresonderzoeken', dat zijn die situaties waarin onduidelijkheid bestaat waar de burger woont.

Het gaat hierbij echter om privacygevoelige gegevens. Daarom moeten klanten er op kunnen vertrouwen dat "hun" gegevens op een zorgvuldige en controleerbare wijze worden behandeld. De wetgever heeft bij de start van Suwinet in 2002 aangegeven dat gegevens-beveiliging noodzakelijk is. Voor alle Suwinet-partijen is dit met beveiligingsvoorschriften uitgewerkt in bijlage XIV van de regeling Suwi.

1.2 Aanleiding aanpassing beveiligingsplan

Op 2 september 2014 heeft het College van B&W van de gemeente Heerde het Beveiligingsplan Suwinet 2014 vastgesteld[1]. In de inleiding van dit beveiligingsplan is aangegeven dat het plan geen statisch document is. De organisatie en de omgeving van de sociale zekerheid is voortdurend in ontwikkeling, onder andere door de wijziging in wetgeving of aanpassingen in de informatiesystemen. Dit betekent dat het plan periodiek op actualiteit moet worden beoordeeld.
De noodzaak tot evaluatie blijkt ook uit het onderzoek "Veilig gebruik Suwinet" door de Inspectie SZW. De inspectie SZW gaat in dit onderzoek uit van zeven essentiële normen voor het waarborgen van de vertrouwelijkheid, opgenomen in het Normenkader Gezamenlijke elektronische Voorzieningen SUWI (GeVS). Deze hebben betrekking op:

- De inrichting en het onderhoud van de beveiligingsfunctie en de beveiligings-organisatie van Suwinet (waaronder de aanstelling van een security officer);
- De logische toegangsbeveiliging, gericht op het voorkomen van ongeautoriseerde toegang tot en gebruik van persoonsgegevens;
- Het beveiligingsbeleid en het beveiligingsplan voor Suwinet.
  GeVS beschrijft in hoofdstuk "Organisatorische aspecten" onder de punten 1.1 t/m 1.5 de noodzaak tot tweedeling naar een informatiebeveiligingsbeleid en –plan. Deze werkwijze leidt tot een jaarlijks te evalueren beveiligingsplan terwijl het beveiligings-beleid minder frequent wijzigingen vraagt. De nu gekozen insteek is om de vereiste indeling onderdeel te laten worden van de in 2016 beoogde implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Vooruitlopend op de implementatie van bovengenoemde BIG is het document daarom gesplitst in een deel gericht op het beveiligingsbeleid en een deel dat het plan voor uitvoering beschrijft.

[1] Kenmerk: Verseon 266004

1.3 Leeswijzer

GeVS noemt de twee 'pijlers' informatiebeveiligingsbeleid en informatiebeveiligingsplan. Vanwege de leesbaarheid van dit document is ervoor gekozen om deze termen veelal te verkorten naar 'beveiligingsbeleid en –plan'.

Waar in deze notitie wordt gesproken over "Sociale Zaken" wordt hieronder in de Heerder situatie verstaan het onderdeel Inkomen van het Team Uitvoering Sociaal Domein. Dit team valt onder de afdeling Publiek.

In het beveiligingsbeleid is het kader voor het beveiligingsbeleid geschetst. Vervolgens is ingegaan op de bevoegdheden van gebruikers en aangegeven in welke situaties Suwinet gebruikt mag worden. Verder is een opsomming gegeven van de algemene gedragsregels ter beveiliging van persoonsgegevens waaraan medewerkers van de gemeente zich moeten houden.

2. Kader voor het Suwinet informatiebeveiligingsbeleid

2.1 Inleiding

Zowel het Bureau Keteninformatisering Werk & Inkomen (BKWI) als het Coördinatiepunt ICT ondersteunt de invoering bij gemeenten en stellen diverse voorbeelden via hun website beschikbaar. De gehanteerde plannen zijn veelal informatiebeveiligingsplannen die van toepassing zijn op de gehele organisatie. Onderwerpen zijn bijvoorbeeld:

- fysieke toegangsbeveiliging gebouwen;
- fysieke toegangsbeveiliging dossiers;
- fysieke toegangsbeveiliging tot computerapparatuur;
- beveiliging van digitaal opgeslagen gegevens;
- beveiliging van (digitale) communicatiekanalen;
- back-up van gegevens;
- integriteitbeleid gemeente;
- calamiteitenplan;
- waarborgen continuïteit (noodstroom en dergelijke);
- periodieke testen en evaluatie van bovengenoemde zaken.

De gemeente Heerde heeft voor de gehele gemeentelijke organisatie regels vastgesteld voor de beveiliging van gegevens.

2.2 Gebruikers van Suwinet-Inkijk

De volgende functies zijn geautoriseerd om gebruik te maken van Suwinet-Inkijk:

- security officer vraagt logging gegevens op;
- de teamcoördinator Sociale Zaken is verantwoordelijk voor en is betrokken bij de autorisatie van Suwinet-gebruikers.
- applicatiebeheer verzorgt de autorisatie voor Suwinet binnen het pakket;
- integrale kwaliteitsmedewerkers mogen raadplegen;
- medewerkers Sociale Zaken, die te maken hebben met rechtmatigheids- of fraudeonderzoeken, mogen raadplegen;
- medewerkers Burgerzaken belast met adresonderzoeken, mogen raadplegen;

Het afdelingshoofd Publiek is eindverantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk.

2.3 Gebruik van Suwinet-Inkijk

Hierboven is beschreven wie Suwinet-Inkijk mogen raadplegen. In deze paragraaf is aangegeven wanneer dat mag. Wordt Suwinet om andere redenen gebruikt dan zoals verwoord, dan is er in principe sprake van ongeoorloofd gebruik. Over het algemeen geldt dat slechts mag worden geraadpleegd, indien de stap binnen het werkproces van het klantvolgsysteem expliciet is beschreven.

- De security officer controleert handhaving van dit beveiligingsbeleid door rapportages bij het BKWI op te vragen en te analyseren. In uitzonderlijke gevallen krijgt de security officer toegang tot Suwinet Inkijk. Dit kan alleen incidenteel op verzoek van de teamcoördinator of manager. Daarnaast houdt de security officer de mutaties in het autorisatieoverzicht bij.
- De applicatiebeheerder ontvangt periodieke overzichten van het BKWI. Bij onregelmatigheden schakelt hij de teamcoördinator in. Deze bepaalt of nader onderzoek door de applicatiebeheerder gewenst is. In dat geval kan de applicatiebeheerder Suwinet-Inkijk raadplegen of BKWI om extra rapportages vragen. Daarnaast beheert de applicatiebeheerder de autorisaties en meldt hij mutaties (via mail) aan de security officer.
- Integrale kwaliteitsmedewerkers mogen raadplegen om besluiten te kunnen toetsen.
- Medewerkers Sociale Zaken mogen:
  - raadplegen bij het behandelen van aanvragen of bij een melding dat belanghebbende een uitkering of minimaregeling wil aanvragen, voor rechtmatigheidsonderzoeken en tussenonderzoeken voor zover het de Participatiewet, Ioaw, Ioaz, Bbz 2004 of een andere door het team uitgevoerde wet of regeling betreft. Het raadplegen van Suwinet-Inkijk moet met een afschrift in het dossier vastgelegd zijn. 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;
  - als uitvoerder terugvordering en verhaal raadplegen bij onderzoeken die samenhangen met vorderingen of met verhaal op onderhoudsplichtigen. Dit bijvoorbeeld ter vaststelling van de woonplaats, de draagkracht, het inkomen of de werkgever;
  - als administratief medewerkers raadplegen om standaard uitdraaien voor het onderzoek te maken.
- Medewerkers Burgerzaken mogen de gegevens raadplegen om adresonderzoeken te behandelen.

Gebruik van Suwinet-Inkijk in andere situaties motiveert de gebruiker in de rapportage in het klantvolgsysteem.

Wanneer een medewerker een BSN raadpleegt van een belanghebbende die niet voorkomt in het klantvolgsysteem, moet de medewerker dit BSN zelf registreren in een overzicht met de reden waarom de BSN is geraadpleegd. Hierbij kan men denken aan "mogelijke huisgenoot", "mogelijk kind", "mogelijke partner". Dit overzicht moet op verzoek aan de security officer, teamcoördinator of manager getoond worden. Bijlage 5 bevat een format hiervoor.

2.4 Logging rapportages

Het BKWI heeft rapportages ontwikkeld over het gebruik van Suwinet-Inkijk en logt iedere bevraging met BSN, datum/tijdstip en onderdeel van Suwinet. Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker van onder andere de gemeente kan worden nagegaan.

Het doel van deze logging is tweeledig:
1. Tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking;
2. Wetenschappelijke en/of statistische doeleinden.

De gebruikers van Suwinet-Inkijk weten dat over hen gegevens worden verzameld en vastgelegd. Met toegang tot Suwinet-Inkijk krijgen medewerkers de bijlagen van dit beveiligingsbeleid uitgereikt (bijlagen 1 tot en met 4) en tekenen zij de "verklaring rechtmatig gebruik Suwinet-Inkijk" (bijlage 1). Dit is een belangrijk onderdeel van de privacybescherming. De medewerkers zijn op de hoogte van de volgende informatie:

- Het bestaan van de logging-gegevens;
- De (aard van de) gegevens die binnen deze applicatie worden gelogd.

Doelen van de logging;

- Dat de gelogde gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- De wijze en het moment waarop en door wie een onrechtmatig of doel overschrijdend gebruik van het Suwinet-Inkijk is vast te stellen;
- Dat bij bovenstaande constatering de teamcoördinator dit bespreekt met de betreffende medewerker(s).

In het kader van de functiescheiding is het beheer voor het gebruik van Suwinet neergelegd bij het applicatiebeheer. Deze is uitvoerend verantwoordelijk voor het beheren van de accounts.

Het BKWI levert twee soorten rapportages. Een periodiek rapport gaat automatisch naar de applicatiebeheerder. Deze signaleert onvolkomenheden en overlegt met de teamcoördinator of er mogelijk sprake is van misbruik.
De (logging)-gegevens over het gebruik van Suwinet-Inkijk worden twee maal per jaar uitgevraagd door de security officer. De security officer analyseert twee keer per jaar de logging-gegevens om te bekijken of de gemeente aan de gemaakte afspraken voldoet. De resultaten van deze analyse worden gerapporteerd aan het afdelingshoofd Publiek.

3. Algemene gedragsregels ter beveiliging van persoonsgegevens

3.1 Inleiding

Voor het werken met en de omgang met persoonsgegevens is vanuit de overheid een aantal regels opgesteld, die zijn verwoord in verschillende wet- en regelgeving. Daaruit zijn gedragsregels afgeleid. Die gelden voor medewerkers van de gemeente Heerde in relatie tot al hun werkzaamheden, dus ook bij het gebruik van Suwinet.

3.2 Beheren van wachtwoorden

De applicatiebeheerder bepaalt hoe lang een wachtwoord geldig is. De gebruiker moet het toegekende wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord.
Bij een deel van de applicaties, waaronder Suwinet, vervalt het account automatisch als het een langere periode niet is gebruikt.

3.3 Einde dienstverband

Zodra een medewerker de gemeente verlaat, worden accounts verwijderd of ontoegankelijk gemaakt.

3.4 Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de applicatiebeheerder. Deze onderzoekt het incident, waar nodig met inschakeling van interne of externe deskundigheid (systeembeheer, Inlichtingenbureau).
Voorbeelden van incidenten zijn: een virusmelding op het systeem of een inbraak of poging tot inbraak.

3.5 Geheimhoudingsplicht

Gebruikers van Suwinet-Inkijk werken met persoonsgegevens. Voor het werken met persoonsgegevens zijn vanuit de overheid een aantal regels opgesteld, die zijn verwoord in de Wet bescherming persoonsgegevens.
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.

3.6 Gedragscode e-mail en internetgebruik

De gemeente Heerde hanteert een gedragscode voor gebruik van e-mail en internet. In deze gedragscode is aangegeven hoe de medewerkers behoren om te gaan met e-mail en internet op de werkplek. Tevens bevatten deze gedragscodes regels met betrekking tot de controle op het gebruik van e-mail en internet.

3.7 Kennisnemen van het beveiligingsbeleid Suwinet

Dit beveiligingsbeleid Suwinet is van toepassing op alle gebruikers van Suwinet-Inkijk binnen de gemeente Heerde. Het beleid staat in de digitale map van de afdeling Publiek en is daarmee voor elke gebruiker van Suwinet toegankelijk. Alle gebruikers worden minimaal twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beleid.

Nieuwe medewerkers worden via de teamcoördinator op het beleid gewezen met de opdracht er kennis van te nemen. Hierdoor weten medewerkers welk gedrag de organisatie van hen verwacht én weten ze dat er gegevens worden bewaard waarmee het gedrag wordt gecontroleerd. Van dat laatste moeten ze zich bewust zijn in relatie tot hun eigen privacy. De organisatie kan de opgeslagen gegevens niet lukraak gebruiken: er moeten redelijke gronden zijn om de privacy van medewerkers te schenden.

3.8 Gegevensverstrekking aan derden via de telefoon

In principe wordt geen telefonische informatie over klanten verstrekt aan personen of instanties die beweren namens betrokkene te bellen. Het uitgangspunt is dat zeer terughoudend wordt omgegaan met verzoeken om telefonische informatie over klanten. Dit vanwege het risico dat de identiteit van de gesprekspartner verkeerd kan worden vastgesteld of dat persoonsgegevens worden verstrekt aan personen of instanties, die geen recht hebben op informatie. In voorkomende gevallen kan er een schriftelijk verzoek worden ingediend, voorzien van een machtiging.
Bij een verzoek om telefonische informatieverstrekking van een ketenpartner 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 er een vaste contactpersoon aan de lijn is.

3.9 Clear desk en clear screen policy

Onbevoegden mogen niet de beschikking krijgen over vertrouwelijke informatie. Daarom mogen die gegevens niet onbeheerd op het bureau of het beeldscherm achterblijven.
Voor zover nog niet gedigitaliseerd worden dossiers bewaard in een kast die na werktijd is gesloten. Clear screen betekent dat het werkstation moet worden vergrendeld met behulp van schermbeveiliging (met wachtwoord). De systemen zijn door systeembeheer zodanig ingesteld dat na een vaste periode de schermbeveiliging intreedt. Daarnaast kan de gebruiker ook zelf het scherm vergrendelen. Dit is te adviseren als de gebruiker langer dan een minuut zijn werkplek verlaat. Bezoekers moeten zich bij binnenkomst in het gebouw melden bij de receptie. De kans is daarom gering dat onbevoegden zonder te worden opgemerkt toegang krijgen tot de voor het publiek afgesloten werkplek van de medewerkers. Het is echter nodig ook ten opzichte van collega's en dienstverleners zorgvuldig om te gaan met de privacy van klanten.

3.10 Vertrouwelijke gegevens

Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Ook het vernietigen van deze gegevens moet op een veilige manier gebeuren. Daarom zijn er in het gemeentehuis van Heerde speciale containers geplaatst, waarin het te vernietigen materiaal wordt verzameld. Het vernietigingsbedrijf voert dit periodiek af.

3.11 Aanspreken van onbekende personen

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 aanspreken, zichzelf voorstellen en de persoon in kwestie 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 naartoe te begeleiden.

3.12 De dagelijkse werkzaamheden versus Informatiebeveiliging

Informatiebeveiliging is belangrijk voor het werk binnen een afdeling waar de medewerkers veelvuldig met privacygevoelige informatie werken en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Klanten vertrouwen op een zorgvuldige wijze van verwerken van hun gegevens. Reden waarom in het werkoverleg regelmatig aandacht voor dit onderwerp moet zijn.

3.13 Sancties

Als een medewerker de regels overtreedt, dan spreekt zijn teamcoördinator hem daarop aan. Er zijn rechtspositionele maatregelen mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen. Dit geldt voor alle werkzaamheden binnen de gemeente Heerde, niet alleen voor het gebruik van Suwinet.

4. Maatregelen naar aanleiding van inspectie 2015

Naar aanleiding van het inspectierapport in 2015 zijn in november 2015 onderstaande maatregelen genomen.

- Sociale Zaken gebruikt het 'Autorisatie-aanvraagformulier Suwinet gebruik'.
- Heerde werkt volgens de essentiële procesbeschrijvingen:
  a. Autoriseren, het proces Autoriseren Suwinet;
  b. Gebruiksrapportages, het proces controleren gebruik Suwinet.
- Alle gebruikers van Suwinet-Inkijk hebben in november 2015 de gebruiksverklaring (bijlage 1) en de vernieuwde autorisatieaanvraag ondertekend.
- De gebruikers van Suwinet-Inkijk hebben toegang tot het actuele informatiebeveiligings-beleid en –plan Suwinet.
- Alle gebruikers van Suwinet-Inkijk worden twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beveiligingsbeleid en -plan. De teamcoördinator Sociale Zaken bespreekt twee keer per jaar de risico's van het gebruik van Suwinet.

Toepassing en naleving van de bovenstaande maatregelen is onderwerp van de periodieke controle door de security-officer.

5. Inleiding informatiebeveiligingsbeveiligingsplan Suwinet 2016

Vooruitlopend op de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is de vorige versie van het document gesplitst in een deel gericht op het beveiligingsbeleid en een deel dat het plan van uitvoering voor het komende jaar beschrijft. De reden van deze splitsing is dat beleid gedurende langere tijd van toepassing is terwijl het plan jaarlijks de uitvoering van het vastgestelde beleid evalueert en op basis daarvan acties agendeert.

Onderstaand de acties die vóór de procesevaluatie van 2016[2] uitgevoerd moeten zijn.

[2] De evaluatie is gepland in oktober 2016.

5.1 Geplande acties

Nr.	Omschrijving, actie	Verantwoordelijk	Periode
1	De applicatiebeheerder kan geen gebruik maken van Suwinet-inkijk.	Teamcoördinator Sociale Zaken	Oktober 2015
2	Periodieke overzichten gebruik Suwinet-Inkijk opvragen.	Security Officer Suwinet	1 x per maand
3	Risico analyse, aanzet en ontwikkeling op basis van: • 7-normen • GeVS • BIG	Security Officer Suwinet	Januari 2016
4	Opvragen en beoordelen specifieke rapportage + Controle accounts (inactief, vertrokken medewerkers). Controle op gebruik van Suwinet. Rapporteren over de toepassing van afspraken binnen Sociale Zaken: • Sociale Zaken gebruikt het 'Autorisatie-aanvraagformulier Suwinet gebruik'. • Heerde werkt volgens de essentiële procesbeschrijvingen: - Autoriseren, het proces Autoriseren Suwinet; - Gebruiksrapportages, het proces controleren gebruik Suwinet. • Alle gebruikers van Suwinet-Inkijk hebben in november 2015 de gebruiksverklaring (bijlage 1) en de vernieuwde autorisatieaanvraag ondertekend. • De gebruikers van Suwinet-Inkijk hebben toegang tot het actuele informatiebeveiligings-beleid en –plan Suwinet. • Alle gebruikers van Suwinet-Inkijk worden twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beveiligingsbeleid en -plan. De teamcoördinator Sociale Zaken bespreekt twee keer per jaar de risico's van het gebruik van Suwinet. • Controle op gebruik van Suwinet. Rapporteren over: • Kwaliteitszorg en borging van rechtmatig gebruik. • Controleren van Clear desk en clear screen policy.	Security Officer Suwinet	Januari 2016

Nr.	Omschrijving, actie	Verantwoordelijk	Periode
	• Controleren: Het omgaan met vertrouwelijke gegevens. Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Ook het vernietigen van deze gegevens moet op een veilige manier gebeuren. Daarom zijn in het gemeentehuis van Heerde speciale containers geplaatst, waarin het te vernietigen materiaal is verzameld. Het vernietigingsbedrijf voert dit periodiek af.		
5	Alle gebruikers worden minimaal twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beveiligingsbeleid en Beveiligingsplan Suwinet 2014 SUWI en afspraken.	Teamcoördinator Sociale Zaken	April 2016
6	Opvragen en beoordelen specifieke rapportage + Controle accounts (inactief, vertrokken medewerkers). Controle op gebruik van Suwinet. Rapporteren over de toepassing van afspraken binnen Sociale Zaken: • Sociale Zaken gebruikt het 'Autorisatie-aanvraagformulier Suwinet gebruik'. • Heerde werkt volgens de essentiële procesbeschrijvingen: a. Autoriseren, het proces Autoriseren Suwinet; b. Gebruiksrapportages, het proces controleren gebruik Suwinet. • Alle gebruikers van Suwinet-Inkijk hebben in november 2015 de gebruiksverklaring (bijlage 1) en de vernieuwde autorisatieaanvraag ondertekend. • De gebruikers van Suwinet-Inkijk hebben toegang tot het actuele informatiebeveiligings-beleid en –plan Suwinet. • Alle gebruikers van Suwinet-Inkijk worden twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beveiligingsbeleid en -plan. De teamcoördinator Sociale Zaken bespreekt twee keer per jaar de risico's van het gebruik van Suwinet. • Controle op gebruik van Suwinet. Rapporteren over: • Kwaliteitszorg en borging van rechtmatig gebruik. • Controleren van Clear desk en clear screen policy. • Controleren: Het omgaan met vertrouwelijke gegevens. Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens, waaronder persoonsgegevens. Ook het vernietigen van deze gegevens moet op een veilige manier gebeuren.	Security Officer Suwinet	Juli 2016

Nr.	Omschrijving, actie	Verantwoordelijk	Periode
	Daarom zijn in het gemeentehuis van Heerde speciale containers geplaatst, waarin het te vernietigen materiaal is verzameld. Het vernietigingsbedrijf voert dit periodiek af.		
7	Minimaal 1x per jaar evaluatie van beveiligingsbeleid en beveiligingsplan SUWI, aantoonbaar te maken m.b.v. agenda, verslaglegging, opvolging, mailwisseling.	Integrale kwaliteitsmedewerker /Beleidsmedewerker Sociale Zaken	Oktober 2016
8	Alle gebruikers worden minimaal twee keer per jaar in een periodiek overleg geattendeerd op de inhoud van het beveiligingsbeleid en Beveiligingsplan Suwinet 2014 SUWI en afspraken.	Teamcoördinator Sociale Zaken	Oktober 2016

Bijlage 1. Verklaring rechtmatig gebruik Suwinet

Door aansluiting op Suwinet is het mogelijk om gegevens uit te wisselen met onder andere de Belastingdienst, de Informatiebeheergroep, de Rijksdienst voor het wegverkeer, het Uitvoeringsorgaan Werknemersverzekeringen en andere gemeenten (zijnde de bronnen).
Als gevolg daarvan zijn deze instanties te beschouwen als "verantwoordelijke" in de zin van de wet Bescherming Persoonsgegevens en daarom allemaal gebonden aan de bepalingen in deze wet. In de toekomst wordt het aantal bronnen uitgebreid. Deze verklaring geldt ook voor bronnen die in de toekomst aangesloten worden.

De gemeente Heerde is op grond van voornoemde bepalingen gehouden om interne maatregelen te nemen ter voorkoming van een (mogelijk) onrechtmatig, onregelmatig of doel overschrijdend gebruik van de beschikbare (persoons-)gegevens. Dit betekent dat de manager Dienstverlening en Bedrijfsvoering de verplichting heeft om regelmatig (met behulp van zogeheten audit logging-gegevens) te laten controleren of het gebruik van de gegevens uit Suwinet niet onwettig geschiedt of verder gaat dan is toegestaan.

Ondergetekende,……

Verklaar (aanstrepen wat van toepassing is):

- Als medewerker Sociale Zaken het raadplegen van de gegevens in Suwinet te beperken tot de gegevens van klanten die blijkens de volgens de gemeentelijke applicatie bij haar of hem in behandeling zijn en deze gegevens enkel aan te wenden voor rechtmatigheids- en -fraudeonderzoeken;
- Als medewerker Burgerzaken het raadplegen van de gegevens uit Suwinet te beperken tot de gegevens die noodzakelijk zijn om de adresonderzoeken te behandelen;
- Op de hoogte te zijn van de controle die de security-officer regelmatig dient in te stellen.

Datum:……

Handtekening:……...

Bijlage 2. Protocol gebruik gegevens Suwinet-Inkijk

Ter ondersteuning van de uitvoering van de Participatiewet, de Leerplichtwet en het beheer van de Gemeentelijke Basis Administratie is de gemeente Heerde aangesloten op de Suwinet-Inkijk. Hiermee is het mogelijk om gegevens uit te wisselen met onder andere de Belastingdienst, IBG, UWV, RDW en andere gemeenten. In de toekomst worden nog andere bronnen toegevoegd.

Op de gegevens van Suwinet-Inkijk zijn de bepalingen van de Wet bescherming persoonsgegevens van toepassing. In verband hiermee zijn aan het raadplegen van Suwinet-Inkijk regels verbonden.

Voor de gemeente Heerde luiden die regels als hieronder.

1. De teamcoördinator Sociale Zaken wijst een medewerker functioneel beheer aan als applicatiebeheerder voor het gebruik van Suwinet-Inkijk, alsmede medewerkers die worden geautoriseerd om gegevens uit dit systeem te raadplegen.
2. De medewerkers van het team Sociale Zaken die geautoriseerd zijn voor het raadplegen van de gegevens uit Suwinet-Inkijk, worden beperkt tot het inwinnen van informatie in verband met rechtmatigheids- of fraudeonderzoeken. Dit blijkt uit de werkprocessen in gemeentelijke applicaties.
3. De medewerkers van Burgerzaken die geautoriseerd zijn voor het raadplegen van de gegevens uit Suwinet-Inkijk, worden beperkt tot het inwinnen van informatie in verband met de behandeling van adresonderzoeken.
4. De geautoriseerde medewerker heeft toegang tot Suwinet-Inkijk door middel van een toegangscode. Deze is strikt persoonlijk.
5. Controle op gebruik van de gegevens van Suwinet-Inkijk vindt plaats met behulp van een audit-logging systeem.
6. Van de personen die niet voorkomen in het klantvolgsysteem en waarvoor Suwinet-Inkijk is geraadpleegd, houdt de medewerker afzonderlijk een eigen registratie in een Word- of Excelbestand bij. In dit overzicht is minimaal de BSN, naam en datum en reden opvraag vermeld.

Doel: verantwoording bij controle.

- Het management benoemd een security-officer die de taak heeft te bevorderen en controleren dat de beveiliging van het Suwinet op orde is. Dit doet de security officer door rapportages uit het audit logging systeem te analyseren.
- De security-officer controleert twee maal per jaar het gebruik van de gegevens van het Suwinet-Inkijk en rapporteert zijn bevindingen aan de manager Dienstverlening en Bedrijfsvoering.
- Indien sprake is van een kennelijk onjuist gebruik van de gegevens van Suwinet-Inkijk hoort de teamcoördinator of manager de betreffende medewerker en neemt zo nodig maatregelen.

Bijlage 3. Protocol inzage in Suwinet-Inkijk door klant en/of gemachtigde

Om de privacy van de klant te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, hieronder beschreven gevallen, is gegevensinzage door derden mogelijk.
De via Suwinet-Inkijk opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op USB-stick). Er mag wel een print worden gemaakt voor de klant of zijn gemachtigde.

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

De klant verzoekt om inzage in zijn gegevens, schriftelijk of mondeling

Het is mogelijk dat een klant telefonisch vraagt om een uitdraai van zijn/haar gegevens. In dat geval dient de klant verwezen te worden naar het KCC van de gemeente Heerde. Is dit niet mogelijk, dan moet hij/zij een schriftelijk verzoek indienen dat binnen de wettelijk verplichte termijn dient te worden beantwoord.
Handel het verzoek als volgt af:

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

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

Gemachtigde verzoekt schriftelijk om inzage in klantgegevens

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

Een derde verzoekt om inzage in klantgegevens

Dit is niet mogelijk.

Bijlage 4. Protocol correctieverzoek Suwinet-Inkijk door klant en/of gemachtigde

De klant verzoekt telefonisch om correctie

- Informeer de klant dat hij/zij een officieel verzoek voor correctie moet indienen;
- Stel de identiteit en het BSN van de klant vast aan de hand van een geldig legitimatiebewijs.

De klant verzoekt mondeling om correctie, terwijl hij/zij op het gemeentehuis is

- Maak een verzoekschrift en laat het ondertekenen;
- Maak een kopie van het verzoek;
- Verstrek een kopie aan de klant;
- Gebruik het origineel om het verzoek af te handelen en archiveer het in het klantdossier;
- Informeer de klant over de doorgevoerde wijziging.

Gemachtigde verzoekt om correctie

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

Een derde verzoekt om correctie

Dit is niet mogelijk.

Bijlage 5. Format overzicht Suwinet geraadpleegde BSN van buiten Civision WIZ bekende personen

Datum:	*BSN*:	*Behandelaar*:	*Aanleiding*:
DD-MM-JJJJ	…	…	…