Gemeente Zwijndrecht

GEMEENTEBLAD

Officiële uitgave van de gemeente Zwijndrecht

Nr. 422811

4 oktober

2023

INFORMATIEBEVEILIGINGSHANDBOEK SUWINET VOOR BURGERZAKEN ZWIJNDRECHT 2022

Burgemeester en wethouders van de gemeente Zwijndrecht,
Gelet op in artikel 3.8 Wet basisregistratie personen, de Wet bescherming persoonsgegevens en de Verordening Basisregistratie Personen van Zwijndrecht

Besluiten vast te stellen:
Het informatiebeveiligingshandboek SUWINET

I. Inleiding

1a. Aanleiding

De gemeente is verantwoordelijk voor een goede kwaliteit van gegevens in de Basisregistratie Personen (BRP). Een van de middelen om een goede kwaliteit adresgegevens te realiseren is het gebruik van Suwinet voor Burgerzaken. Via Suwinet-Inkijk vraagt de gemeente informatie over de – bij andere instanties - bekende adresgegevens en is daarmee onderdeel van de procedure Adresonderzoeken. Een inkijk als deze is handig voor het realiseren van een goede kwaliteit adresgegevens, maar brengt ook de verantwoordelijkheid met zich mee om hier zorgvuldig mee om te gaan. Want burgers vertrouwen erop dat hun privacy wordt beschermd en dat er alles aan wordt gedaan om misbruik te voorkomen.

Omdat medewerkers met persoonsgegevens werken, is zorgvuldig en integer gebruik van deze gegevens erg belangrijk. De medewerkers die geautoriseerd zijn voor Suwinet voor Burgerzaken, zijn gehouden aan de strenge regels rondom het zorgvuldig en integer gebruiken van de gegevens, welke gelden voor de BRP.

Onverkort gelden ook de regels vanuit de Algemene Verordening Gegevensbescherming (AVG) met betrekking tot handhaving vanaf 25 mei 2018.

1b. Reikwijdte

Vanuit het SUWI-normenkader is bepaald dat een gemeente dient te beschikken over een beveiligingsplan specifiek gericht op het gebruik van Suwinet of dat een op Suwinet specifieke passage is opgenomen in een algemene plan. In verband met de samenwerkingsverband van de Drechtsteden is gekozen voor een specifieke beveiligingsplan gericht op het gebruik van Suwinet. Dit betekent dat dit beveiligingsplan niet ingaat op onderwerpen zoals:

- Beveiliging van digitaal opgeslagen gegevens en communicatiekanalen;
- Back-ups van gegevens en een calamiteitenplan;
- Vernietiging van computers;
- Waarborging van de continuïteit;
- Periodiek testen en evaluatie van bovengenoemde zaken.

Immers, er is geen sprake van een systeem, maar van een beveiligde web-applicatie, welke beschikbaar wordt gesteld door het Bureau Keteninformatisering Werk en Inkomen (BKWI).
Aangezien Suwinet voor Burgerzaken voornamelijk bij de balies wordt gebruikt, zijn wel de geldende regels rondom toegang opgenomen. Verder is en blijft informatiebeveiliging met name mensenwerk. Zodanig is dit document ook geschreven op een wijze dat waarde biedt voor functionarissen op verschillende niveaus zoals het management, beheerders, gebruikers en controleurs.

1c. Samenhang met het informatiebeveiligingshandboek BRP en Waardedocumenten

De Inkijk Suwinet voor Burgerzaken wordt, zoals gezegd, uitsluitend gebruikt voor het inzien van adresgegevens in het kader van onderzoeken adres. Het behoeft geen nadere uitleg dat de adresgegevens onderdeel zijn van een Basisregistratie waar veel afnemers gebruik van maken en onjuiste (gedateerde) informatie van adressen kan leiden tot fraude door een ingezetene.

Omdat er sprake is van een uitsluitend gebruik van Suwinet voor Burgerzaken voor adresgegevens in het kader van onderzoeken adres, is het Handboek Beveiliging BRP en Waardedocumenten ook van toepassing op het gebruik deze inkijk en de gegevens die hieruit worden gebruikt. De procedure voor adresonderzoeken is een verantwoordelijkheid van het hoofd van de afdeling maatschappelijke ontwikkeling en dienstverlening. Dit beveiligingshandboek Suwinet voor Burgerzaken is derhalve door het College vastgesteld. Wijzigingen in dit Handboek, die afdeling-overstijgend zijn, worden door de concern manager meegenomen naar het Managementteam.

Om deze reden wordt ook verantwoording afgelegd aan de portefeuillehouder, verantwoordelijk voor de BRP (in het geval van de gemeente Zwijndrecht is dit de burgemeester). Wijzigingen in dit Handboek, die een grotere reikwijdte hebben dan de taken van de portefeuillehouder, worden door de portefeuillehouder meegenomen naar het College.

1d. Doelstelling
Dit document dient als het informatiebeveiligingsplan waarin staat beschreven wat de maatregelen zijn ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van het gebruik van persoonsgegevens via Suwinet voor Burgerzaken. Dit Handboek wordt met ingang van 2018 voortaan jaarlijks beoordeeld, zo nodig aangepast en aangescherpt en tevens jaarlijks vastgesteld. Dit wordt in gezamenlijkheid met de andere gemeenten in de regio Drechtsteden opgepakt en met de collega's van CIO-office Drechtsteden.

Door middel van het beveiligingsplan toont de gemeente Zwijndrecht aan op welke wijze het voldoet aan de 7 normen van de Inspectie SZW die gelijk staan aan het voldoen aan 'Veilig Suwinet'. Het voldoen aan deze normen draagt aanzienlijk bij het beperken van het risico op onrechtmatig gebruik binnen de organisatie. De normen omvatten het voldoen aan tenminste de volgende eisen:
- De organisatie beschikt over een formeel vastgesteld beveiligingsbeleid en –plan;
- De organisatie draagt op reguliere basis het beveiligingsbeleid en –plan uit;
- De organisatie evalueert tenminste eenmaal per jaar het beveiligingsbeleid en –plan;
- De organisatie heeft een duidelijk scheiding in taken, verantwoordelijkheden en bevoegdheden ten aanzien van het gebruik, de inrichting en het beheer van Suwinet;
- De organisatie autoriseert en registreert de toegang die gebruikers hebben tot de Suwinet applicaties op basis van een formele procedure.
- De organisatie controleert meerdere keren per jaar op verleende toegangsrechten en rechtmatig gebruik.
- De organisatie heeft een Security Officer toegewezen dat belast is met het bevorderen en adviseren over de beveiliging van Suwinet. Daarnaast controleert deze functionaris samen met leidinggevende of de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassingen van plannen op het gebied van de beveiliging van Suwinet.

Voor de overige normen geldt overigens nog steeds het vigerende algemene informatiebeveiligingsplan. De actualisatie daarvan zal meegenomen worden in het verder professionaliseren van de informatiebeveiliging in regionaal verband zoals dat nu door het CIO-office wordt opgezet. Daarbij komen dan ook de andere normen aan bod voor actualisatie. Informatiebeveiliging is iets waar voortdurend aan wordt gewerkt. Dit is derhalve geen statisch document, dat periodiek dient te worden beoordeeld op actualiteit en dus mogelijk regelmatig aanpassing behoeft.

1e. Kader gebruik Suwinet
Het gebruik van gegevens uit Suwinet is beperkt. In de factsheet is vermeldt wie waarvoor gegevens mag gebruiken. Als bijlage 1e. opgenomen.

1f. Aansluiting met Suwinet
Enkele documenten dienen onderdeel te zijn van dit Handboek. Dit zijn in dit geval de aanvraag om Suwinet te verkrijgen (als bijlage 1f.a. opgenomen), de informatie met betrekking tot geregistreerde personen conform de functies voor Suwinet (als bijlage 1f.b. opgenomen) en de geregistreerde gebruikers die Suwinet kunnen inkijken (als bijlage 1f.c. opgenomen).

II. Regionale en lokale maatregelen rondom Informatieveiligheid

De in dit Handboek opgenomen maatregelen staan niet los van reeds genomen maatregelen rondom Informatieveiligheid die regionaal en lokaal zijn genomen. Hieronder worden de belangrijkste maatregelen genoemd, die betrekking hebben op een veilig gebruik van de gegevens. Zo gelden de regels rondom wachtwoorden om eerst toegang te krijgen tot de beveiligde regionale werkomgeving en is het opvragen van informatie uit Suwinet niet toegestaan via een thuiswerkplek of buiten het netwerk van de Drechtsteden om.

Omdat gegevens uit Suwinet vooral bij de balies worden gebruikt zijn de volgende maatregelen voor toegangsbeheer van toepassing:
a. Wachtwoordbeleid Drechtsteden;
b. Regeling gebruik ICT-middelen Drechtsteden 2015;
c. Toegangsbeleid gemeentelijke gebouwen en ruimten;

d. Sleutel- en toegangsbeheer.

Deze hierboven genoemde documenten zijn reeds opgenomen in het informatiebeveiligingshandboek BRP en Waardedocumenten 2021.

III. Organisatie en verantwoordelijkheden

3a. Organisatie
De medewerkers van het team publiekscontacten zijn verantwoordelijk voor het uitvoeren van adresonderzoeken conform de BRP. Het team is onderdeel van de afdeling maatschappelijke ontwikkeling en dienstverlening.

De organisatie en verantwoordelijkheden rondom Suwinet kent taken die betrekking hebben op het gebruik, beheer en toezicht van het werken. Het is van groot belang dat de voorgenoemde taken duidelijk gescheiden van elkaar zijn belegd. De taken mogen dus in geen enkele geval worden gecombineerd. Dit ter voorkoming dat mensen hun directe collega's of zelfs zichzelf moeten controleren, wat de effectiviteit van de controle onderuit zou halen. Het gebruik is afhankelijk van de functie (Applicatiebeheerder en Medewerker Frontoffice Balie kunnen slechts in dit systeem). Rechten worden toegekend of verwijderd bij indiensttreding dan wel uitdiensttreding in genoemde functies.

3b. Verantwoordelijkheden
De volgende taken zijn belegd binnen het team / de afdeling.

Concern manager	verantwoordelijk voor de procedure adresonderzoeken BRP
De teamleider	verantwoordelijk voor de dagelijkse aansturing van de medewerkers en controles Suwinet
Applicatiebeheerder	verantwoordelijk voor het actueel houden van de autorisaties Suwinet
Gemandateerde	verantwoordelijk voor het opvragen van gebruiksrapportages Suwinet en het onderhouden van contacten met BKWI
Security Officer	verantwoordelijk voor controles Suwinet
Beveiligingsfunctionaris	verantwoordelijk voor de onafhankelijke controle op Informatiebeveiliging voor BRP, Suwinet Inkijk en Waardedocumenten
Med. Frontoffice balie	verantwoordelijk voor uitvoeren werkzaamheden adresonderzoeken

De functie "medewerker Frontoffice balie" is gelijk aan de gebruikte functienaam binnen het Handboek Beveiliging BRP. Slechts de applicatiebeheerders en de medewerkers Frontoffice balie hebben toegang tot Suwinet voor Burgerzaken.

Voor iedere medewerker die in dienst treedt voor het uitvoeren van werkzaamheden in het kader van de Wet Basisregistratie Personen (Wet BRP) geldt dat deze personen – ongeacht in vaste dienst of op basis van inhuur – een geheimhoudingverklaring ondertekenen, een VOG overleggen en de eed of belofte in handen van de burgemeester afleggen. Dit is reeds vastgelegd in het Informatiebeveiligingsplan BRP en Waardedocumenten 2022 (vastgesteld door het College op 1 november 2022)

Concern manager
De concern manager van de afdeling maatschappelijke ondersteuning en dienstverlening is procesverantwoordelijke voor de adresonderzoeken in het kader van het bijhouden van een goede BRP. Het hoofd van de afdeling zorgt er met de teamleider voor dat een goede en gedegen structuur is gerealiseerd waarbinnen de werkzaamheden in het kader van onder andere deze taak worden uitgevoerd.

Jaarlijks rapporteert het hoofd van de afdeling, of bij diens afwezigheid de teamleider, de portefeuillehouder over het gebruik van Suwinet voor Burgerzaken en over mogelijke verbeteringen in het kader van Informatieveiligheid. Oneigenlijk gebruik, zoals fraude, misbruik of dwang wordt direct gerapporteerd.

De teamleider
De teamleider zorgt met de concern manager voor een goede en gedegen structuur voor de uitvoering van werkzaamheden in het kader van onder andere de adresonderzoeken. De teamleider heeft geen toegang tot Suwinet voor Burgerzaken en is daarmee onafhankelijk van de uitvoering. Daarnaast zorgt

de teamleider voor controle op de werkzaamheden. De controlerende taken komen in twee mate voor. Enerzijds dient er een functionaris te zijn belast met het analyseren van de gebruiksrapportages (teamleider) om vervolgens zijn bevindingen te delen met de Security Officer. Deze laatste functionaris staat los van de lijnverantwoordelijkheid.

Anderzijds is er de teamleider die invulling geeft aan het beveiligingsbeleid en verantwoordelijk is voor de uitvoering conform de normen. Hieronder valt onder andere:
- het zorgdragen voor de organisatie rond Suwinet;
- het vaststellen van processen rond Suwinet;
- het beslissen over de bevoegdheden in Suwinet van functiegroepen en medewerkers;
- het bijsturen naar aanleiding van signaleren over (oneigenlijk) gebruik;
- het optreden na misbruik;
- het uitdragen van het belang van goed gebruik door hierover regelmatig tijdens werkoverleggen met de medewerkers in gesprek te zijn.

Vanuit het SUWI-normenkader is het vastgesteld dat er controle dient te plaatsvinden op verleende toegangsrechten en gebruik. BKWI stelt hiervoor rapportages ter beschikking. Op basis van deze rapportages is het de taak van de teamleider en de Security Officer om het gebruik te controleren op (vermoedelijk) misbruik en constateringen hiervan schriftelijk aan de concern manager te rapporteren. Indien er een vermoeden van misbruik bestaat, kan een specifieke rapportage worden opgevraagd. Deze controle vindt voortaan meerdere malen per jaar plaats. Zowel de teamleider (in de lijn) als de Security Officer melden gezamenlijk het gebruik en oneigenlijk gebruik aan de concern manager.

Jaarlijks rapporteert de concern manager van de afdeling, of bij diens afwezigheid de teamleider, de portefeuillehouder over het gebruik van Suwinet voor Burgerzaken en over mogelijke verbeteringen in het kader van Informatieveiligheid. Oneigenlijk gebruik, zoals fraude, misbruik of dwang wordt direct gerapporteerd.

De applicatiebeheerder
De applicatiebeheerder neemt kennis van dit Informatiebeveiligingsplan BRP en Waardedocumenten, derhalve ook van onderstaande en tekent voor gezien op de parafenlijst behorende bij dit Handboek.

De applicatiebeheerder oefent taken uit, betrekking hebben op werkzaamheden behorende tot de werkzaamheden BRP. De applicatiebeheerder heeft hiervoor een geheimhoudingsverklaring getekend en een integriteitsverklaring afgelegd. De applicatiebeheerder wordt geacht integer en zorgvuldig met de informatie uit Suwinet om te gaan en geen oneigenlijk gebruik van Suwinet te maken. Met oneigenlijk gebruik wordt bedoeld het opzoeken (en zo nodig verspreiden) van informatie uit Suwinet met een ander doel dat het gebruiken van Suwinet voor Burgerzaken ten behoeve van het uitvoeren van adresonderzoeken.

De gemandateerde
De gemandateerde is verantwoordelijk voor het opvragen van gebruiksrapportages Suwinet en het onderhouden van contacten met BKWI. De gemandateerde neemt in geval van calamiteiten contact op met de Suwidesk van BKWI via suwidesk@bkwi.nl of 0800-78943375. Bij afwezigheid van de gemandateerde neemt de Security Officer deze taak op zich.

De Security Officer
De controlerende taken komen in twee mate voor. Enerzijds dient er een functionaris te zijn belast met het analyseren van de gebruiksrapportages (teamleider) om vervolgens zijn bevindingen te delen met de Security Officer. Deze functionaris staat los van de lijnverantwoordelijkheid.

De gemandateerde neemt in geval van calamiteiten contact op met de Suwidesk van BKWI via suwidesk@bkwi.nl of 0800-78943375. Bij afwezigheid van de gemandateerde neemt de Security Officer deze taak op zich.

Vanuit het SUWI-normenkader is het vastgesteld dat er controle dient te plaatsvinden op verleende toegangsrechten en gebruik. BKWI stelt hiervoor rapportages ter beschikking. Op basis van deze rapportages is het de taak van de teamleider en de Security Officer om het gebruik te controleren op (vermoedelijk) misbruik en constateringen hiervan schriftelijk aan de concern manager te rapporteren. Indien er een vermoeden van misbruik bestaat, kan een specifieke rapportage worden opgevraagd. Deze controle vindt voortaan meerdere malen per jaar plaats. Teamleider en Security Officer melden het gebruik en oneigenlijk gebruik aan de concern manager.

Beveiligingsfunctionaris

De beveiligingsfunctionaris is verantwoordelijk voor de onafhankelijke controle op Informatiebeveiligingsplan voor BRP, Suwinet Inkijk en Waardedocumenten. In dit Handboek is deze functie verder beschreven.

De medewerker Frontoffice balie
Omwille van de continuïteit zijn er minimaal 2 personen aangewezen als medewerker Frontoffice balie, zoals bedoeld voor de inkijk Suwinet voor Burgerzaken.

De medewerker Frontoffice balie neemt kennis van dit Informatiebeveiligingsplan BRP en Waardedocumenten, derhalve ook van onderstaande en tekent voor gezien op de parafenlijst behorende bij dit Handboek.

De medewerker Frontoffice balie oefent taken uit, betrekking hebben op werkzaamheden behorende tot de werkzaamheden BRP. De medewerker Frontoffice balie heeft hiervoor een geheimhoudingsverklaring getekend en een integriteitsverklaring afgelegd. De medewerker Frontoffice balie wordt geacht integer en zorgvuldig met de informatie uit Suwinet om te gaan en geen oneigenlijk gebruik van Suwinet te maken. Met oneigenlijk gebruik wordt bedoeld het opzoeken (en zo nodig verspreiden) van informatie uit Suwinet met een ander doel dat het gebruiken van Suwinet voor Burgerzaken ten behoeve van het uitvoeren van adresonderzoeken.

Het behoort tot de vaste taken van de medewerker Frontoffice Balie (BRP) om adresonderzoeken uit te voeren. De applicatiebeheerder autoriseert en verwijdert autorisaties al naar gelang de medewerker als medewerker Frontoffice balie in dienst of uit dienst treedt.

3c. Logging
Rapportagegegevens BKWI ontwikkelt rapportages omtrent het gebruik van Suwinet. BKWI is wettelijk verplicht om gegevens te registreren waarmee het gebruik per medewerker kan worden nagegaan. Hierbij worden de volgende gegevens geregistreerd:

Gebruikers (applicatiebeheerders en medewerkers Frontoffice balie) moeten weten dat vanuit het beveiligingsoogpunt gegevens over hen worden verzameld en vastgelegd. Medewerkers die (gaan) werken met Suwinet moeten op de hoogte zijn van:
- Het bestaan van de registraties;
- De (aard van de) gegevens die worden geregistreerd;
- De doelen van de registraties;
- Dat de geregistreerde 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 wordt geconstateerd;
- Dat bij bovenstaande constatering dit wordt gecommuniceerd met de desbetreffende medewerker(s) en mogelijk sancties voorvloeien bij oneigenlijk gebruik.

Gegevens die bij het inloggen en gebruik van Suwinet voor Burgerzaken worden geregistreerd door BKWI zijn:
- Het tijdstip van iedere inlog en uitlog en andere actie;
- De gebruikersnaam van degene die inlogt/uitlogt;
- Elk BSN (of andere zoeksleutel) waarvan gegevens worden opgevraagd wordt als actie geregistreerd;
- Elke actie, zoals de bekeken kolom- of overzichtspagina´s.

Het doel van deze registratie is tweeledig:
- Het tegengaan en controleren van onrechtmatige, onregelmatige of doel overschrijdende verwerking;
- Voor wetenschappelijke en/of statistische doeleinden.

Gebruik voor andere doeleinden is dus absoluut niet toegestaan. Dat geldt ook voor het doorleveren van gegevens. Fraude en misbruik, alsmede het verstrekken van informatie onder dwang door de autorisatie-verantwoordelijke blijkt uit de rapportages van het BKWI. Afhankelijk van het soort oneigenlijk gebruik worden passende maatregelen genomen conform de bepalingen in artikel 16 van de CAR-UWO. Dit ter beoordeling van de teamleider en de concern manager.
Het behoort tot de vaste taken van de medewerker Frontoffice Balie (BRP) om adresonderzoeken uit te voeren. De applicatiebeheerder autoriseert en verwijdert autorisaties al naar gelang de medewerker als medewerker Frontoffice balie in dienst of uit dienst treedt. De applicatiebeheerder autoriseert binnen

een week na indiensttreding van de medewerker en binnen een week na uitdiensttreding van de medewerker. De teamleider of de concern manager informeert de applicatiebeheerder uiterlijk een week voor aanvang over indiensttreding en uitdiensttreding van de medewerker.

Jaarlijks controleert de applicatiebeheerder de actualiteit van de registratie en rapporteert hierover schriftelijk aan de teamleider.

3d. Monitoring
Onder monitoren wordt verstaan: signaleren, analyseren en rapporteren. In het kader van Suwinet is het begrip bijsturen hieraan toegevoegd.
Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot Suwinet diensten en ongeautoriseerd gebruik van deze diensten tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris.
Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd en te worden gerapporteerd. Een deel van de logging (Suwinet inkijkfunctie) is in het bezit van de centrale beheerder (BKWI) en dient voor controle doeleinden periodiek te worden opgevraagd.
Bureau Keteninformatisering Werk en Inkomen (BKWI) heeft gebruikersrapportages ontwikkeld over het gebruik van Suwinet-Inkijk. Via deze rapportages monitort en controleert de Security Officer Suwinet het gebruik van Suwinet-Inkijk. De gebruikersrapportage bevat vier onderdelen: het totale gebruik, het zorgvuldig gebruik, het accountbeheer en het doelmatig gebruik van Suwinet-Inkijk. Deze rapportage bevat geen persoonsgegevens over de medewerker en over de geraadpleegde personen.
De (logging-)gegevens over het gebruik van Suwinet-Inkijk worden periodiek opgevraagd door de Security Officer Suwinet.
De Security Officer Suwinet houdt periodiek een steekproef of bevragingen Suwinet aan de gemaakte afspraken voldoen. De activiteiten zijn vastgelegd in de Procedure Controle Gebruik.
Bij vermoedens van ongeoorloofd gebruik, vraagt de Security Officer Suwinet bij het BKWI een specifieke rapportage op en controleert deze.
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 Security Officer Suwinet een rapportage opstellen waarin de zwaarte van het misbruik omschreven wordt. Er wordt onderscheid gemaakt tussen vermoedelijk misbruik en geconstateerd misbruik. Een sanctie wordt alleen toegepast bij geconstateerd misbruik. Opzettelijk onjuist gebruik wordt aangemerkt als misbruik. Indien er sprake is van misbruik door een medewerker, informeert de Security Officer Suwinet de gemeentesecretaris.
Onder ernstig misbruik wordt in ieder geval verstaan het beschikbaar stellen van gegevens van burgers aan derden voor commerciële doeleinden.
Afhankelijk van het soort oneigenlijk gebruik worden passende maatregelen genomen conform de bepalingen in de CAR-UWO.
Onjuist gebruik is:
1. Het opvragen van gegevens ten behoeve van derden;
2. Het verstrekken van die gegevens aan derden.

4. Procedures
4a Procedure autorisatie Suwinet (korte instructie)
Deze procedure is als bijlage 4a. opgenomen.

4b. Procedure autorisatie Suwinet Inkijk (Handleiding Suwinet-Inkijk Gebruikersadministratie)
Deze procedure is als bijlage 4b. opgenomen.

4c. Procedure Autorisatie Suwinet-Inkijk.pdf
Deze procedure is als bijlage 4c. opgenomen.

4d. Procedure gebruik, opslag en archivering informatie Suwinet
Deze procedure is als bijlage 4d. opgenomen.

De informatie uit Suwinet Inkijk wordt geprint en opgeslagen in het adresonderzoekdossier. Deze dossiers worden gedurende het onderzoek en de administratieve afhandeling ervan sinds 4 november 2018

telkens na het afronden van het dossier opgeslagen ons digitale archiveringssysteem Inproces. De Archiefwet is van toepassing op archivering van deze onderzoekdossiers BRP.

4e. Controleprocedure
Deze procedure is als bijlage 4d. opgenomen.

Controle vindt steekproefsgewijs plaats om te controleren of uitsluiten die gegevens worden geraadpleegd, welke voor het doel (adresonderzoeken BRP gerechtvaardigd zijn.

4f. Procedure bij het verstrekken van informatie onder dwang
Deze procedure is als bijlage 4f. opgenomen.

4g. Procedure bij vermoeden van fraude en misbruik door de gebruiker
Deze procedure is als bijlage 4g. opgenomen.

4h. Procedure Periodieke controles autorisaties.pdf
Deze procedure is als bijlage 4h. opgenomen.

4i. Procedure autorisatie Matrix voor Suwi-inkijk Burgerzaken.pdf
Deze procedure is als bijlage 4i. opgenomen.

4j. Procedure Periodieke evaluatie en controle.pdf
Deze procedure is als bijlage 4j. opgenomen.

Dit Handboek Beveiliging Suwinet voor Burgerzaken en alle hiertoe behorende bijlagen is op 9 november 2022 vastgesteld namens het college van Burgemeester en Wethouders van de gemeente Zwijndrecht.
De heer W.H.J.M. van der Loo/ mevrouw P.W. Croonenberg-Borst
De burgemeester/ de secretaris