gemeente BORSELE

# GEMEENTEBLAD

Officiële uitgave van de gemeente Borsele

Nr. 504324

15 november 2022

## Beveiligingsplan Suwinet-inkijk Burgerzaken gemeente Borsele 2022

Het college van burgemeester en wethouders van de gemeente Borsele,

gelet op het bepaalde in de wet BRP, in de AVG en in het besluit Suwi;

Besluit:
1. Het beveiligingsplan SUWI–inkijk Burgerzaken 2022 gemeente Borsele vast te stellen.
2. Het Suwinet beleidsplan 2018 in te trekken.

### 1) Inleiding

Het beveiligingsplan Suwinet-inkijk beschrijft de maatregelen ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van het gebruik van persoonsgegevens en informatiesystemen met betrekking tot het behandelen van aanvragen omtrent inzage Suwinet-inkijk ten behoeve van de wet BRP, basisregistratie personen, juiste inschrijving op adressen en adresonderzoek. Daarnaast wordt aangegeven welke mensen en middelen hiervoor beschikbaar worden gesteld 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.

Binnen de gemeente zijn bepaalde zaken rondom informatieveiligheid geregeld in een voor de gehele organisatie geldend Strategisch Informatiebeveiligingsbeleid 2022 tot 2026.
In het Strategisch Informatiebeveiligingsbeleid zijn uitgangspunten geformuleerd die voor alle organisatieonderdelen en processen gelden ongeacht de betreffende systemen die daarbij gebruikt worden. Deze regels zijn dus ook integraal van toepassing op het onderhavige beveiligingsplan Suwinet-inkijk voor het gebruik van Suwinet-inkijk.
Jaarlijks dient het beveiligingsplan Suwinet-inkijk geëvalueerd te worden. Met onderhavig document wordt het vorige Suwinet-inkijk beleidsplan van de gemeente Borsele, inclusief de Autorisatiematrix, up-to-date gemaakt.

Suwinet-inkijk is het systeem van informatie-uitwisseling in de keten van werk en inkomen. Als basis geldt onder andere de wet Structuur uitvoering werk en inkomen (afgekort met 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.
Suwinet-Inkijk is de webapplicatie die draait op de beveiligde Suwinet-infrastructuur. Binnen deze applicatie worden gegevens, die bij diverse andere overheidsorganisaties of basisregistraties zijn opgeslagen, op basis van het burgerservicenummer (BSN) veilig toegankelijk gemaakt voor bevoegde medewerkers. De organisaties hebben de informatie over werk en inkomen nodig om de gegevensuitvraag aan de klant te beperken. Suwinet wordt gebruikt om informatie over werk en inkomen van een klant te verzamelen in het kader van onder meer uitkeringen, werk en re-integratie.
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, Handelregister (KvK).
- *Beheerders* - Beheerder van de centrale omgeving (BKWI) is de partij die - conform de ketenafspraken en –standaarden zorg draagt 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 is

de partij die voor de routering van 'berichten-op-maat' tussen de centrale omgeving en de gemeenten zorg draagt, 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 Inlichtingenbureau.
- *Afnemers* - Afnemers zijn de partijen die via de GeVS - voor hun bedrijfsvoering en uitvoering van hun wettelijke taken - gegevens betrekken uit gegevensbronnen van bronhouder.

## 2) Kader voor het Suwinet beveiligingsplan

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 VNG realisatie heeft VNG in de afgelopen jaren diverse handreikingen en ander ondersteuningsmateriaal ontworpen. Dit om gemeenten beter te helpen met de beveiliging van de informatievoorziening en Suwinet in het bijzonder. In dit kader kunnen worden genoemd:
- *BIO*: vanaf 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht als opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG). De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Gemeenten hebben de opdracht om dit gemeentebreed normenkader voor informatiebeveiliging te implementeren. De Informatiebeveiligingsdienst (IBD) ondersteunt en adviseert gemeenten daarbij.
- *ENSIA*: ENSIA staat voor Eenduidige Normatiek Single Information Audit. ENSIA is 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, PNIK, BAG, BRO en BGT eenvoudiger gemaakt. ENSIA is een interbestuurlijk traject waarbij departementen én gemeenten samenwerken om de verantwoordingslast (op termijn) te beperken.

Normenkader
De Gezamenlijke elektronische Voorziening Suwinet wordt binnen de keten van Werk en Inkomen gebruikt bij het uitwisselen van gegevens. De GeVS en de informatie die via GeVS wordt uitgewisseld dienen te voldoen aan specifieke beveiligingseisen en aan de Europese privacy verordening 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 over 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.
Vanaf 1 april 2017 is het oude normenkader GeVS 2011 vervangen door het nieuwe specifieke normenkader Suwinet Afnemers. In de basis dekt dit dezelfde risico's af, het is alleen opgesplitst naar doelgroep (afnemers, beheerder en bronhouders), waardoor niet op de doelgroep van toepassing zijnde normen konden worden weggelaten.

### 2.1 Aansluiting Suwinet
Het Bureau Keteninformatisering Werk en Inkomen (BKWI) is verantwoordelijk voor de digitale gegevenslevering en keteninformatisering waar het de gegevensuitwisseling over burgers en bedrijven betreft. BKWI levert de gegevens voor Suwi-inkijk via een beveiligde verbinding via Diginetwerk. De infrastructuur en internetapplicaties vallen technisch, qua gebruik en beveiligingsaspecten onder verantwoordelijkheid van GR De Bevelanden, ICT.
Het gebruik van internet en het beveiligingsbeleid is organisatiebreed geregeld. De Suwi wetgeving eist een beveiligingsplan en stelt specifieke eisen aan (controle op) het gebruik door team Burgerzaken (aansluiting Burgerzaken).

De gegevens die voor Burgerzaken via Suwinet-Inkijk beschikbaar zijn betreffen de adresgegevens van iedereen die werkt of een uitkering ontvangt. Deze komen uit de loonaangifte die werkgevers en uitkeringsinstanties periodiek doen naar de Belastingdienst. De adresgegevens vanuit UWV mogen alleen gebruikt worden voor controle op de juistheid van adresgegevens in de BRP en het uitvoeren van adresonderzoek door de toezichthouder BRP.

gemeente BORSELE

## 3) Toegang Suwinet-Inkijk

De ICT-faciliteiten van de gemeente Borsele zijn beveiligd door een gebruikersnaam en wachtwoord. Van buiten het gemeentehuis kan een medewerker alleen met behulp van een zogenaamde tweestaps-verificatie via een VPN verbinding op het interne netwerk inloggen. Naast gebruikersnaam en wachtwoord, is dan ook een veilig gegenereerde tokencode vereist om op het netwerk te komen. De Suwinet-Inkijk toepassing heeft een eigen gebruikersnaam en 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 het scherm worden vergrendeld.
Indien een medewerker thuis werkt moet dat papierarm gebeuren. Het is af te raden om dossiers of documenten daaruit mee naar huis te nemen. Zijn er toch stukken met persoonsgegevens nodig dan dienen die goed te worden opgeborgen en uit het zicht van derden te blijven.

In het kader van de functiescheiding is de rol van Autorisatiebeheerder Suwinet-inkijk belegd bij de applicatiebeheerder Burgerzaken (niet zijnde toezichthouder BRP). De Autorisatiebeheerder beheert de Suwinet gebruikersadministratie en is uitvoerend verantwoordelijk voor het beheren van alle Suwinet-Inkijk accounts en het up-to-date houden van de autorisatiematrix (zie bijlage 4). Het up-to-date houden van de autorisatieprocedure is de verantwoordelijkheid van de domeinmanager Dienstverlening.
Zodra een medewerker de gemeentelijke organisatie verlaat, wordt het account tezelfdertijd verwijderd of ontoegankelijk gemaakt. Deze procedure wordt gestart in TOPdesk.

De medewerkers raadplegen Suwinet-Inkijk alleen via VDI.
Gebleken is dat Suwi-inkijk raadpleegbaar is buiten om de VDI-omgeving. Er is een onderzoek gestart om a. te zorgen dat er via een tweestapsverificatie geraadpleegd wordt of b. dat het niet buitenom VDI te raadplegen is. Dit om te zorgen dat Suwi-inkijk voldoet aan het wachtwoordbeleid van de gemeente Borsele.

### 3.1 Persoonsgegevens

Medewerkers gaan op verantwoorde wijze om met de persoonsgegevens die zij raadplegen via Suwinet-inkijk. Er mag alleen geraadpleegd worden als daar een wettelijke grondslag voor is en het nodig is voor de taakuitoefening van de functie. De volgende richtlijnen gelden:

- 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. Printen van Suwinet-Inkijk gegevens is niet toegestaan. Dit laatste uit het oogpunt van privacybescherming én dat te allen tijde alleen de online gegevens actueel zijn.
- De persoonsdossiers worden digitaal opgeslagen dan wel bewaard in een archiefkast welke wordt afgesloten wanneer de laatste medewerker de kamer verlaat. Bij het verlaten van de werkplek dient men zich af te melden van Suwinet-Inkijk. Voor cliënten die hun gegevens willen inzien is een protocol vastgesteld, zie bijlage 3. Mocht een cliënt een verzoek tot correctie van gegevens wensen, dan wordt hij of zij door de dienstdoende medewerker doorgeleide gedaan naar de juiste collega of ketenpartner die deze gegevens onderhoud.
- Personeel dat in dienst is bij de gemeente valt onder het ambtenarenreglement. Bij het aanvaarden van het dienstverband ondertekent de medewerker een eed of belofte, over o.a. het op verantwoorde wijze omgaan met (privacygevoelige) informatie. De desbetreffende medewerker wordt voordat toegang tot de diverse applicaties wordt verleend, door de Autorisatiebeheerder Suwinet gewezen op de gebruikersafspraken en de regels over de vertrouwelijkheid en ondertekent de “Verklaring rechtmatig gebruik Suwinet” (zie bijlage 1). Pas daarna wordt toegang tot Suwinet verleend. Hierbij wordt uiteraard gewezen op doelbinding (wettelijke basis) en proportionaliteit (niet meer gegevens dan noodzakelijk) voor het legitiem raadplegen van persoonsgegevens.
- Voor extern of ingehuurd personeel dat dient te beschikken over de Suwinet-Inkijk applicatie behoort via de inleenovereenkomst van het uitzendbureau of de daaraan gekoppelde algemene voorwaarden de geheimhouding van vertrouwelijke gegevens door het bureau en de medewerker gewaarborgd te zijn.

- Door de Autorisatiebeheerder Suwinet-inkijk wordt het Suwinet autorisatieformulier digitaal opgeslagen (via JOIN). De digitale versie van de Verklaring rechtmatig gebruik Suwinet wordt door de Security Officer opgenomen in het zaaksysteem.
- Onnodige verwerking van persoonsgegevens is niet toegestaan (dataminimalisatie). Zo mag het technisch nummer van een klantdossier, waarmee veelvuldig met derden wordt gecommuniceerd, niet gelijk zijn aan het BSN (beginselen van proportionaliteit en subsidiariteit).

Informatieveiligheid is belangrijk voor het werk binnen een team waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk.

Inwoners vertrouwen op een zorgvuldige omgang en verwerking van hun gegevens. Reden waarom in het werk- en of teamoverleg informatiebeveiliging altijd een terugkerend agendapunt moet zijn.

**3.2 Gebruikersrollen**
Er zijn verschillende taakgebieden waarin Suwinet-inkijk gebruikt wordt voor het raadplegen van klant/persoonsgegevens. Binnen Suwinet wordt voor de gemeente een aantal gegevens afgeschermd omdat deze voor de gemeente niet functioneel zijn.
Autorisaties voor Suwinet-Inkijk worden per gebruikersrol toegekend. Deze gebruikersrollen moeten overeenkomen met de autorisatiematrix. Zoveel als technisch mogelijk zijn pagina's ondergebracht in zelf voor gedefinieerde rollen binnen Suwinet Inkijk.
In dit document worden de gebruikersrollen beperkt tot de werkzaamheden door team Burgerzaken.

### 3.2.1 Gebruikersrollen

*Autorisatiebeheer*
Draagt zorg voor autorisatiebeheerproces, dus het zorgvuldig en veilig aanmaken/wijzigen/intrekken van Suwinet accounts op basis van de autorisatiematrix.

*Security Officer*
Is bevoegd om de maandelijkse generieke en specifieke rapportages op te vragen.

*Medewerker team Burgerzaken*
Enkele medewerkers van team Burgerzaken (toezichthouders BRP) mogen gebruik maken van Suwinet-Inkijk ten behoeve van juiste inschrijvingen in de BRP, het uitvoeren van adresonderzoeken.

**3.3 Functiescheiding**
Er zijn verschillende functies in relatie tot het gebruik van Suwinet-inkijk.
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:

- Uitvoering van taken (het gebruik van Suwinet);
- Het beheer van autorisaties (toegang verlenen tot Suwinet, onderhouden autorisatiematrix);
- Kwaliteitszorg en borging van rechtmatig gebruik;
- Management (beslissen over bevoegdheden van rollen, en/of individuele medewerkers, uitdragen belang zorgvuldig gebruik, bijsturen na oneigenlijk gebruik, optreden na misbruik Suwinet);
- Beleid voorstellen, opvragen rapportages en doen van controles op gebruik van Suwinet.

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

1. Verlenen en ontnemen toegang is gescheiden van het gebruik van Suwinet-Inkijk.
2. Beveiligingsmaatregelen alsook advisering over gebruik en beveiliging Suwinet zijn belegd bij de Security Officer Suwinet.
3. De autorisaties worden met inachtneming van punt 1 en 2 aan de hand van een ondertekend autorisatieformulier in opdracht van de domeinmanager Dienstverlening toegekend dan wel ingetrokken of gewijzigd. De Autorisatiebeheerder Suwinet is verantwoordelijk voor uitvoering van deze opdrachten en archiveert autorisatieformulier in het digitaal archief. In de opdracht wordt gemotiveerd aangegeven waarom aan een (groep) gebruiker(s) een bepaalde autorisatie moet worden toegekend of ontnomen.
4. Raadplegen van Suwinet-Inkijk in andere situaties wordt gemotiveerd in de rapportage. Een BSN raadplegen van een persoon die onbekend is in de basisregistratie personen wordt door de medewerker zelf geregistreerd in een dossier adresonderzoek in iBurgerzaken om dit achteraf te kunnen verantwoorden.

**3.4 Uitgangspunten autorisaties**
Medewerkers mogen Suwinet-Inkijk raadplegen bij het behandelen van aanvragen met betrekking tot:

- medewerkers bij team Burgerzaken (toezichthouders BRP) ten behoeve van juiste inschrijvingen in de BRP en adresonderzoek;
- Autorisaties worden toegekend op basis van 'need-to-know': alleen de informatie die nodig is voor de opgedragen taakuitoefening mag opgevraagd worden.
- Autorisaties worden toegekend aan de hand van de voorgedefinieerde rollen uit de autorisatiematrix.
- Gemeenten zijn verplicht het Burgerservicenummer (BSN) in de administratie vast te leggen. Dit betekent dat van ieder persoon van wie informatie in Suwinet-Inkijk moet worden opgezocht, dat aan de hand van het BSN moet gebeuren. Informatie via Suwinet-inkijk is daarom in beginsel alleen via het BSN te benaderen.

- Bij vertrek van een medewerker of verandering van taakstelling worden de toegekende autorisaties in opdracht van de domeinmanager Dienstverlening ingetrokken, dan wel aangepast aan de nieuwe rol.
- Alleen de domeinmanager Dienstverlening is bevoegd om autorisatieformulieren te ondertekenen. Bij afwezigheid wordt de mandaatregeling gemeente Borsele toegepast.

**3.5 Security Officer Suwinet**
Het gebruik van Suwinet vindt plaats onder toezicht van de Security Officer (SO) Suwinet. Hij is in zijn rol onafhankelijk. De SO beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet in overeenstemming met 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, 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 aan de domeinmanager Dienstverlening.
Jaarlijks controleert de SO of actualisering van het beveiligingsplan noodzakelijk is. Een geactualiseerd beveiligingsplan wordt ter vaststelling aan het college van B&W voorgelegd. De SO onderzoekt met regelmaat (minimaal twee keer per jaar) of de toegangsverlening en toegangsintrekking tot Suwinet-Inkijk correct verloopt. Daartoe kan hij spreken met de betrokkenen, zoals deze in dit plan zijn vermeld. Tevens kan de SO de volgende bronnen raadplegen:

- Het logboek van de accounts van de autorisatiebeheerder
- De gearchiveerde autorisatie aanvragen/intrekkingen
- De getekende verklaringen rechtmatig gebruik Suwinet
- De bijgewerkte autorisatiematrix

**3.6 Autorisatiebeheerder**
De rol van Autorisatiebeheer Suwinet-Inkijk is belegd bij Applicatiebeheer Burgerzaken. Deze applicatiebeheer is geen toezichthouder BRP. Het uitvoeren van het aanmaken, verwijderen en rolwijzigingen van Suwinet accounts wordt hieronder verstaan. De autorisatiebeheerder is verantwoordelijk voor de uitvoer van het toekennen/wijzigen/intrekken van autorisaties binnen de Suwinet-inkijk applicatie. Hierbij zijn de volgende taken te onderkennen:

- Het instrueren en doen toekomen van relevante documenten aan de potentiële nieuwe gebruiker.
- Het doorvoeren van het autorisatieverzoek op basis van een standaard formulier dat geformaliseerd wordt door ondertekening van de domeinmanager Dienstverlening.
- Het na verwerking zorgdragen voor archivering van het autorisatieformulier en de Verklaring rechtmatig gebruik Suwinet.
- Maakt na iedere gebruikersmutatie hiervan melding in het logboek
- Na de gebruikersmutatie wordt de gebruikersmatrix bijgewerkt.

**3.7 Proces autorisatiebeheer Suwinet-Inkijk**
Het proces van autorisatiebeheer Suwinet-Inkijk wordt gekenmerkt door de volgende stappen.

- Een gebruiker kan alleen toegang tot Suwinet krijgen als de domeinmanager Dienstverlening hier toestemming voor geeft. De domeinmanager Dienstverlening is verantwoordelijk voor het tijdig toekennen/wijzigen/intrekken van accounts.
- Een verzoek aan de autorisatiebeheerder tot toekenning, wijziging van rol of beëindiging van autorisaties gebeurt aan de hand van een standaardformulier (zie bijlage 2).
- Bij intrekking van een account wordt de autorisatiebeheerder per omgaande geïnformeerd.
- De domeinmanager Dienstverlening ondertekent het autorisatieformulier. De autorisatiebeheerder kent vervolgens de rol(len) met bijbehorende rechten toe aan de gebruiker.
- De autorisatiebeheerder verstuurt per mail aan gebruiker het Beveiligingsplan Suwinet, de actuele versie van de Factsheet Wie-mag-Suwinet-gebruiken van de VNG en ter ondertekening de Verklaring rechtmatig gebruik Suwinet. De mail wordt ter archivering opgeslagen (bij autorisatiedossier in JOIN).
- De autorisatiebeheerder digitaliseert het originele autorisatieformulier en archiveert het, evenals de door de medewerker ondertekende Verklaring rechtmatig gebruik Suwinet. De medewerker DIV draagt er zorg voor dat ook de Verklaring rechtmatig gebruik Suwinet aan het personeelsdossier wordt toegevoegd. De autorisatiebeheerder draagt hierna zorg voor de vernietiging van beide papieren exemplaren.
- De werkzaamheden van medewerkers kunnen veranderen. Dit kan een uitbreiding of beperking betekenen. Wijzigingen als gevolg van veranderende taken doorlopen dezelfde stappen als bij een autorisatie toekenning.
- De autorisatiebeheerder werkt bij iedere accountmutatie (toekennen/wijzigen/intrekken) het logboek bij met vermelding van de handeling. Tevens wordt de gebruikersmatrix bijgewerkt.
- De domeinmanager Dienstverlening is verantwoordelijk voor het tijdig melden van accountmutaties aan de autorisatiebeheerder Suwinet.

**3.8 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 domeinmanager Dienstverlening. Het college is bestuurlijk eindverantwoordelijk voor een adequaat stelsel van procedures, afspraken en werkwijzen rondom het gebruik en beheer en de interne verantwoording daarover.
De domeinmanager Dienstverlening is verantwoordelijk voor het gebruik en de beveiliging van Suwinet-Inkijk.

**3.9 Misbruik**
Geautoriseerde medewerkers bij de GSD van gemeenten die belast zijn met de uitvoering van de wettelijke taken die vallen onder de P-wet, IOAW en IOAZ, mogen gebruik maken van Suwinet.
Suwinet wordt onder andere gebruikt in processen om de grondslag voor het toekennen of afwijzen van een uitkering te bepalen of voor re-integratie. In de onderlinge wet- en regelgeving wordt ook nadrukkelijk uitgesloten waar Suwinet niet voor mag worden gebruikt. Dit betreft raadpleging voor uitvoering van wetten anders dan de drie voornoemde wetten. Zo is het niet toegestaan Suwinet te gebruiken voor taken rondom schuldhulpverlening en de uitvoering van de WMO of Jeugdzorg. Ook voor bijvoorbeeld de wet Taaleis is raadpleging van Suwinet niet toegestaan. De handreiking van de VNG geeft een goede beschrijving van wat wel en niet mag (zie factsheet).
Als de Security Officer Suwinet op basis van nadere inspectie van specifieke rapportages misbruik vermoed of constateert wordt een onderzoek ingesteld en betrekt hierbij altijd de domeinmanager Dienstverlening. Onderzocht wordt of er sprake was van doelmatig en rechtmatig gebruik van de Suwinet-Inkijk voorziening. Het kan nodig zijn met de betrokken medewerker te spreken om dit uiteindelijk vast te stellen.
Bij geconstateerd misbruik van Suwinet geldt het algemeen geldende misbruik beleid van de organisatie. Conform de Ambtenarenwet en de WNRA zijn rechtspositionele maatregelen mogelijk.

## 4) Procedure logging rapportages

Het BKWI is verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per medewerker kan worden nagegaan. De logging wordt gebruikt voor controles over onrechtmatige, onregelmatige of doel overschrijdende verwerking.
Door de Security Officer Suwinet worden er maandelijks voor controledoeleinden een algemene (generieke) rapportage van zoekopdrachten opgevraagd. Wanneer afwijkingen worden geconstateerd in de Burgerzaken-rapportage is het zaak hiervoor een specifieke rapportage aan te vragen. De specifieke rapportages zijn alleen opvraagbaar door de Security Officer Suwinet en zijn niet openbaar. De Security Officer Suwinet stelt jaarlijks zijn bevindingen vast en rapporteert deze samen met een eventueel advies aan de domeinmanager Dienstverlening. De domeinmanager Dienstverlening geeft aan welke eventuele actie hij onderneemt en ondertekent daarna het controle rapport. Deze controle rapporten worden gearchiveerd.
Indien controle daar aanleiding toe geeft stelt de Security Officer Suwinet een onderzoek in naar rechtmatig en doelmatig gebruik en betrekt daarbij altijd de volgende personen;

- autorisatiebeheerder Suwinet
- domeinmanager Dienstverlening

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.
De gebruikers en beheerders van Suwinet weten dat gegevens over hun gebruik van Suwinet worden verzameld en vastgelegd. Voorafgaand aan toegang tot Suwinet krijgen zij door de Autorisatiebeheerder uitleg over het gebruik van Suwinet en worden zij gevraagd het centraal opgeslagen beveiligingsplan door te nemen. Tevens tekenen zij een “Verklaring rechtmatig gebruik Suwinet” (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;
- In geval van onrechtmatig of doel overschrijdend gebruik van Suwinet-Inkijk bespreekt de domeinmanager Dienstverlening dit met de betreffende medewerker, met mogelijke sancties tot gevolg (zie paragraaf 3.9).

gemeente BORSELE

## 5) Procedures Suwinet-Inkijk

Voor het werken 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 Borsele in relatie tot al hun werkzaamheden en bij het gebruik van Suwinet-Inkijk voor medewerkers van het team Burgerzaken in het bijzonder.
Concreet kunnen deze regels als volgt worden vertaald:

### 5.1 Beheren van wachtwoorden

Bij het aanmaken van een gebruikersaccount wordt een tijdelijk wachtwoord gegenereerd. Dit tijdelijke wachtwoord wordt naar de gebruiker gemaild in de voorbeeldmail voor het verstrekken van gebruikersgegevens. De gebruiker moet het toegekende wachtwoord wijzigen zodra de eerste inlog plaatsvindt. Suwinet dwingt in alle gevallen een sterk wachtwoord af. Vervolgens vervalt dat wachtwoord periodiek. De gebruiker heeft dus het eigen beheer over het wachtwoord. Een wachtwoord is strikt persoonlijk en mag niet gedeeld worden met anderen. Het account blokkeert automatisch wanneer het 90 dagen niet is gebruikt.

### 5.2 Melden van beveiligingsincidenten

Het is belangrijk dat beveiligingsincidenten worden gemeld bij de CISO, de domeinmanager Dienstverlening en de Security Officer Suwinet. Voorbeelden van incidenten 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). Mocht een incident leiden tot een datalek dan wordt de functionaris gegevensbescherming ingeschakeld.
Zie ook de gemeentelijke procedure: Plein 6, Weten en regelen, iBewust Borsele.

### 5.3 Rechtmatig gebruik

Voor gebruikers van Suwinet geldt het essentiële voorschrift dat de persoonsgegevens waarmee gewerkt wordt, niet verder bekend mogen worden gemaakt dan voor het uitvoeren van de taak noodzakelijk is. Ten behoeve van de borging van de vertrouwelijke omgang met persoonsgegevens, laat de gemeente Borsele de gebruikers en autorisatiebeheerders van Suwinet een “Verklaring rechtmatig gebruik Suwinet” ondertekenen (zie bijlage 1).

### 5.4 Kennisname van het beveiligingsplan Suwinet

Het onderhavige beveiligingsplan Suwinet is van toepassing op iedereen die gebruik maakt van Suwinet of beheer voert op de gebruikersaccounts van Suwinet binnen de gemeente Borsele. Het beveiligingsplan wordt na vaststelling gepubliceerd op intranet. Alle gebruikers worden er minimaal tweemaal per jaar in een periodiek teamoverleg op geattendeerd dat ze kennis moeten nemen van het plan.
Nieuwe medewerkers worden via de domeinmanager Dienstverlening uitdrukkelijk op het plan 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 hun gedrag kan worden gecontroleerd. Van dat laatste moeten ze zich bewust zijn in relatie tot hun eigen privacy en dat van de klant.
Nieuwe gebruikers volgen voordat de autorisatie plaatsvindt online de training Suwinet via de Bevelandacademie. Het certificaat wordt gedeeld met de domeinmanager Dienstverlening. Naast de Suwinet-specifieke training volgt de nieuwe gebruiker ook algemene informatieveiligheidstrainingen in de academie.

### 5.5 Gegevensverstrekking aan derden via de telefoon

In principe wordt geen telefonische informatie over inwoners verstrekt aan personen of instanties die beweren namens betrokkene te bellen. Het uitgangspunt is dat zeer terughoudend wordt omgegaan met verzoeken van 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.

### 5.7 Clean desk en clear screen policy

Het is noodzakelijk ook ten opzichte van collega’s en dienstverleners zorgvuldig om te gaan met de privacy van klanten. Onbevoegden, zowel binnen als buiten de organisatie, mogen niet de beschikking krijgen over vertrouwelijke informatie.
Zie de gemeentelijke procedure clean desk en clear screen: Plein 6, Weten en regelen, iBewust Borsele.

### 5.8 Vernietiging van vertrouwelijke gegevens

Het is erg belangrijk om correct om te gaan met vertrouwelijke gegevens. Ook het vernietigen van deze gegevens moet op een veilige manier plaatsvinden. Daarom zijn er bij de gemeente Borsele speciale

gemeente BORSELE

afgesloten containers geplaatst, waarin het te vernietigen materiaal verzameld wordt. De verzamelde papieren worden regelmatig aangeleverd bij een vernietigingsbedrijf. Indien er een onverhoopt toch een print is gemaakt van Suwinet-Inkijk gegevens, moet deze na afhandeling van het werkproces worden vernietigd.

**5.9 Dagelijkse werkzaamheden en informatiebeveiliging**
Informatiebeveiliging is belangrijk voor het werk binnen een team waar veelvuldig met privacygevoelige informatie wordt gewerkt en hoort dan ook bij de professionele en bekwame uitvoering van het werk. Klanten vertrouwen op een zorgvuldige wijze van omgang met en verwerken van hun gegevens. Reden waarom in het werk- en of teamoverleg informatiebeveiliging altijd een terugkerend agendapunt moet zijn.

**5.10 Sancties**
Een medewerker die de beveiligingsregels onvoldoende naleeft wordt daar door de domeinmanager op aangesproken. Conform de Ambtenarenwet en de WNRA zijn daarop rechtspositionele maatregelen mogelijk. Bij ernstige vergrijpen kan ook het strafrecht in beeld komen.

**5.11 Suwinet-audit**
In het kader van ENSIA zijn we verplicht jaarlijks een externe audit naar de beveiligingsmaatregelen van Suwinet te laten uitvoeren. Het college van B&W legt een collegeverklaring af over het wel of niet voldoen aan de gestelde beveiligingseisen. Een bevoegde onafhankelijke auditor, die is ingeschreven bij de Nederlandse Orde van Register Auditors (NOREA), beoordeelt deze collegeverklaring en levert een assurancerapportage op.

*Aldus besloten in de vergadering van het college van burgemeester en wethouders van de gemeente Borsele op 27 september 2022.*

*de burgemeester.*

*de secretaris.*

gemeente BORSELE

**Bijlage 1: Verklaring rechtmatig gebruik Suwinet**
Verklaring rechtmatig gebruik Suwinet-inkijk

| Naam | Team | Datum in dienst/start werkzaamheden |
|---|---|---|
| | | |

Bij besluit van het college van burgemeester en wethouders van de gemeente Borsele, geautoriseerd tot het opvragen van gegevens uit de gemeentelijke en andere gegevensbestanden, verklaart ondergetekende zijn/haar werkzaamheden te zullen verrichten onder de volgende voorwaarden:

- Geen andere informatie uit Suwinet te zullen opvragen dan die welke voor de hem/haar opgedragen werkzaamheden nodig zijn;
- Zich te verplichten tot geheimhouding van al datgene wat hem/haar in zijn/haar dienstverband ter kennis komt, tenzij enig wettelijk voorschrift mededeling vordert;
- Bekend te zijn met wat ten aanzien van geheimhouding in de wet is bepaald (zie artikel 272 van het Wetboek van Strafrecht) en met het feit dat schending van de geheimhoudingsplicht als uiterste consequentie tot strafontslag kan leiden;
- Bekend te zijn met de controles die door de Beveiligingsfunctionaris Suwinet op het gebruik van Suwinet worden gehouden en bekend te zijn met de mogelijke consequenties van onrechtmatig gebruik.
- Geen andere personen gebruik te zullen laten maken van zijn/haar unieke gebruikersnaam en/of wachtwoord voor Suwinet of die op enige andere wijze aan hen te doen toekomen;
- Ondergetekende zal geen andere personen, ook niet de in dienstverband werkende teamleden, toelaten tot de persoonsgebonden toegang tot Suwinet;
- Bij het tijdelijk verlaten van de werkplek (op kantoor of elders) zal het beeldscherm op de werkplek, door ondergetekende worden afgesloten m.b.v. de schermbeveiliging;
- Bij het verlaten van de werkplek (op kantoor of elders) voor lange duur, zullen alle sessies van applicaties die toegang geven tot de gegevensbestanden en van portalen, dus ook van Suwinet, op de werkplek door ondergetekende worden afgesloten;
- Uitdraaien van Suwinet ten behoeve van het onderzoeksdossier Burgerzaken worden bij het werken buiten kantoorlocaties van gemeente Borsele buiten bereik en zicht van huisgenoten en bezoekers gehouden.
- Deze verklaring blijft voor lid 1b van kracht, ook na beëindiging van bovengenoemde werkzaamheden.

Ondergetekende heeft voorafgaand aan de ondertekening van deze verklaring een exemplaar ontvangen van het Beveiligingsplan Suwi-inkijk Burgerzaken gemeente Borsele 2022 en voldoende tijd gehad om kennis te nemen van de inhoud ervan.
Ondergetekende verklaart akkoord te zijn met de inhoud van het Beveiligingsplan Suwi-inkijk Burgerzaken gemeente Borsele 2022 en in overeenstemming met de hierin genoemde bepalingen en gedragsregels te handelen.

Heinkenszand (datum)
De ambtenaar/medewerker (handtekening),

gemeente BORSELE

**Bijlage 2: Autorisatieformulier Suwinet**
Formulier autorisatieverzoek Suwinet-Inkijk

| | |
|---|---|
| **Gegevens medewerker** | |
| Naam: | |
| Team: | |
| **Autorisatie** | |
| Domeinmanager Dienstverlening geeft opdracht om met ingang van ……<br>o de medewerker volgens onderstaand profiel toegang te verlenen tot Suwinet.<br>o de rechten in Suwinet voor de medewerker te wijzigen volgens onderstaand profiel<br>o de toegang tot Suwinet voor deze medewerker in te trekken | |
| **Autorisatieprofiel** | |
| o Medewerker Burgerzaken<br>o Autorisatiebeheer<br>o Security Officer | |
| **Ondertekening** | |
| Voor akkoord, domeinmanager Dienstverlening | Datum:<br>Naam:<br>Handtekening: |

| | |
|---|---|
| Verwerking Autorisatieverzoek, Applicatiebeheerder | Datum:<br>Naam:<br>Handtekening: |

gemeente
BORSELE

**Bijlage 3: Protocol inzage in Suwinet-Inkijk door cliënt en/of gemachtigde**
Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met diens gegevens vereist. In bepaalde, hieronder beschreven gevallen, is gegevensinzage door derden mogelijk.
De via Suwinet opvraagbare gegevens zijn alleen in elektronische vorm te zien. De gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of op gegevensdrager). Er mag wel een afdruk worden gemaakt voor de cliënt of zijn gemachtigde. Een cliënt kan zijn gegevens op 2 manieren inzien:

- Online via http://www.bkwi.nl/over-bkwi/wat-doet-bkwi-met-mijn-gegevens/ bevindt zich daar een link "mijn gegevens inzien"
- Schriftelijk verzoek aan team Burgerzaken

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

**De cliënt verzoekt om inzage in zijn gegevens, schriftelijk of mondeling**
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 team. 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 cliënt vast aan de hand van een geldig legitimatiebewijs;
- Maak een uitdraai van de geraadpleegde gegevens of laat de cliënt meekijken op het scherm;
- Vernietig het uitgedraaide exemplaar als de cliënt het niet meeneemt;
- Beëindig inkijksessie.

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

**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;
- Stel de identiteit en het BSN van de cliënt 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 inwonergegevens**
Dit is niet mogelijk.

gemeente BORSELE

**Bijlage 4: Autorisatiematrix Suwinet-inkijk**

| Functionaris | Naam | Rol | | | Datum ingang | Datum einde |
|---|---|---|---|---|---|---|
| | | Medewerker team Burgerzaken | Autorisatiebeheer | Security Officer Suwinet | | |
| | | Raadplegen actuele adresgegevens | Gebruikersbeheer Accountbeheer | Opvragen generieke en specifieke gebruikersrapportage | | |
| Sr. beleids-medewerker Burgerzaken | | | | X | | |
| Beleids-medewerker Burgerzaken (tevens applicatiebeheerder, geen toezichthouder BRP) | | | X | | | |
| Medewerker team Burgerzaken, tevens toezichthouder BRP | | X | | | | |
| Medewerker team Burgerzaken, tevens toezichthouder BRP | | X | | | | |
| Medewerker team Burgerzaken, tevens toezichthouder BRP | | X | | | | |