

Aansluitbeleid (beveiligingsplan) voor het gebruik van Suwinet-Inkijk Fijnder 2026-2030

1. Inleiding

De gemeenten Berkelland, Oost Gelre en Winterswijk hebben hun taken op het gebied van werk en inkomen uitbesteed aan Fijnder. Voor de uitvoering van een aantal SUWI-taken (Suwi = Structuur uitvoeringsorganisatie werk en inkomen) maakt Fijnder gebruik van Suwinet Inkijk. De afdelingen Inkomen en Dienstverlening en Re-integratie gebruiken Suwinet-Inkijk als een verificatie-instrument voor het rechtmatig verstrekken van uitkeringen. Het is een internetapplicatie voor het uitwisselen van informatie over cliënten met een uitkering tussen de ketenpartners Uitvoering Werknemersverzekeringen, UWV Werkbedrijf, gemeenten en Sociale Verzekeringsbank. Het gaat om inkomens-, vermogens- en re-integratiegegevens. Ook is het mogelijk om informatie uit de administraties van de Basisregistratie Personen, de Rijksdienst voor het wegverkeer, de Dienst Uitvoering Onderwijs, de Kamer van Koophandel, het Kadaster en de Belastingdienst te raadplegen. Toegang tot de gegevens van cliënten met een uitkering gebeurt op basis van hun Burgerservicenummer. In bijzondere situaties kan ook op naam, adres, geboortedatum, kenteken van voertuig, kadastrale gegevens, etc. worden gezocht.

De ketenpartners sturen de gegevens van cliënten met een uitkering digitaal naar het Bureau Informatiediensten Nederland (voorheen het Inlichtingenbureau), dat ervoor zorgt dat de gegevens op Suwinet-Inkijk kunnen worden geraadpleegd. Het Bureau Keteninformatisering Werk en Inkomen (BKWI) is de beheerder van Suwinet-Inkijk.

In het kader van de Wet eenmalige gegevensuitvraag werk en inkomen is Suwinet-Inkijk ook de bron voor het vaststellen van bepaalde gegevens van de cliënten met een uitkering. Bijvoorbeeld naam, adres en woonplaats. De ketenpartners mogen, als het Burgerservicenummer bekend is, die gegevens niet meer aan de cliënt vragen. Wel mogen ze controleren of de gegevens nog steeds kloppen.

Het Dagelijks Bestuur van Fijnder heeft een strategisch beleidskader Informatiebeveiliging vastgesteld dat ook van toepassing is op het gebruik van Suwinet-Inkijk. In dit beleidskader wordt het management gevraagd aanvullend aansluitbeleid voor het gebruik van Suwinet-Inkijk te definiëren en aan het Dagelijks Bestuur ter vaststelling voor te leggen.

In het Strategisch Informatiebeveiligingsbeleid van Fijnder (vastgesteld door het Dagelijks Bestuur) zijn aanvullende risico's, maatregelen en verantwoordelijkheden vastgesteld.

Bij het raadplegen van Suwinet-Inkijk gaat het om privacygevoelige informatie. Daarom is aanvullend op het informatiebeveiligingsbeleid ook het Privacybeleid van toepassing.

Om het gehele jaar in control te zijn en om alle (verplichte) onderdelen rondom zowel informatiebeveiliging en privacy (waar onder dus ook het gebruik van Suwinet-Inkijk) jaarlijks te plannen wordt door de Privacy Officer controles uitgevoerd. Deze controles worden aan het management voorgelegd. Tevens wordt dit jaarlijks besproken met de CISO's van de drie gemeenten. Jaarlijks beoordeelt een externe daarvoor bevoegde IT auditor of het gebruik van Suwinet-Inkijk door Fijnder aan de beveiligingseisen voldoet. De uitkomsten van deze beoordeling worden via een TPM aan de deelnemende gemeentebesturen vóór 1 december kenbaar gemaakt.

Het Aansluitbeleid (Beveiligingsplan) voor het gebruik van Suwinet-Inkijk van Fijnder wordt minstens elke 5 jaar of bij grote wijzigingen opnieuw beoordeeld en vastgesteld. De volgende periodieke beoordeling van dit beleid zal in 2030 plaatsvinden.

2. Digitale bescherming

Voor de digitale bescherming zijn de volgende maatregelen genomen:

- de aansluiting en toegang tot Suwinet-Inkijk loopt via het beveiligde diginetwerk aansluiting welke een beveiligde verbinding van overheidsorganisaties is onder regie van Logius;
- alleen de in dit plan genoemde functies hebben toegang tot Suwinet-Inkijk;
- autorisaties voor Suwinet-Inkijk worden toegewezen door de teamleiders en verwerkt door de gebruikersbeheerder (applicatiebeheer Fijnder);

- na elke wijziging in de autorisaties wordt een overzicht Autorisaties, rollen en taken gemaakt, die wordt goedgekeurd door de directeur;
- per rol is aangegeven welke gegevens er te raadplegen zijn;
- de toegang tot het netwerk en de digitale werkplek is beveiligd door middel van een persoonlijk gebruikersnaam en wachtwoord;
- de gebruiker heeft met een ander persoonlijk gebruikersnaam en wachtwoord toegang tot Suwinet-Inkijk;
- dit wachtwoord moet iedere 30 dagen worden gewijzigd (is in de applicatie Suwinet-Inkijk verankerd);
- als Suwinet-Inkijk even niet is gebruikt, dan sluit de applicatie automatisch (is in de applicatie Suwinet-Inkijk verankerd);
- als de gebruiker Suwinet-Inkijk lange tijd niet raadpleegt, dan vervalt het wachtwoord na 56 dagen (is in de applicatie Suwinet-Inkijk verankerd);
- er is een beeldschermbeveiliging wat inhoudt dat het scherm vergrendeld wordt als het 10 minuten niet is gebruikt;
- er wordt gebruik gemaakt van een whitelist. Dit betekent dat gebruikers uitsluitend gegevens kunnen opvragen van de personen die bekend zijn in de uitkeringsadministratie. Andere personen kunnen alleen via de escapefunctie worden opgevraagd;
- opgevraagde gegevens mogen niet lokaal worden opgeslagen (op de harde schijf of elk ander medium);
- beveiligingsincidenten met betrekking tot Suwinet-Inkijk worden doorgegeven aan de Security Officer van het BKWI en de Security Officer van Fijnder en aan de deelnemende gemeenten of betrokken gemeenten waarvan persoonsgegevens zijn gelect.

3. Papieren bescherming

Informatie uit Suwinet-Inkijk kan op papier worden afgedrukt. Het afdrukken gebeurt op een printer waarvoor de gebruiker een persoonlijke pincode heeft. De afdrukken worden zo nodig in de cliëntdossiers bewaard. De fysieke cliëntdossiers met betrekking tot de uitkering en/of re-integratie zijn opgeborgen bij een externe partij (van Dam) en kunnen per mail bij de archiefmedewerkers worden opgevraagd. Afdrukken die niet worden bewaard, worden gedeponereerd in de afgesloten containers voor te vernietigen documenten. Deze worden door een daartoe bevoegd persoon dagelijks vernietigd.

4. Autorisaties, rollen en taken

Er zijn 9 functies (rollen) betrokken bij het gebruik van Suwinet-Inkijk:

1. Inkomensconsulent
2. Medewerker Uitkeringsadministratie
3. Re-integratieconsulent
4. Medewerker Service unit
5. Kwaliteitsmedewerker
6. Medewerker Terugvordering en verhaal
7. Medewerker Preventie en handhaving
8. Controle/Security Officer
9. Gebruikersbeheerder (voorgedefinieerd vanuit Suwidesk)

De Whitelist escapefunctie wordt aan de rollen 1, 4, 5 en 6 toegekend.

Doordat de rollen onverenigbaar zijn is de controlefunctie bij de toezichthouder ondergebracht en is er sprake van functiescheiding. De toegewezen autorisaties zijn op functieniveau vastgelegd in een autorisatiematrix waarin de bijbehorende rollen en taken zijn beschreven. Deze autorisatiematrix wordt door de directeur van Fijnder ondertekend. Bij wijzigingen in de autorisatiematrix wordt deze opnieuw door de directeur ondertekend. De autorisaties vormen de maximaal toegestane bevoegdheden. Wanneer de werkzaamheden van medewerkers dit toelaten zal de gebruikersbeheerder deze verder beperken. Bij verschil van inzicht tussen gebruikers en gebruikersbeheerder beslist de teamleider.

De betreffende teamleider bepaalt op basis van de functie-inhoud of het noodzakelijk is dat een medewerker toegang krijgt tot Suwinet-Inkijk. Bij beëindiging van een dienstverband stelt het secretariaat de gegevensbeheerder op de hoogte, zodat de toegang tot Suwinet-Inkijk wordt beëindigd. Wanneer er tussentijds wijzigingen optreden bij een medewerker die in dienst is of blijft, of wanneer toegang

niet langer noodzakelijk is voor de uitoefening van de functie, stelt de teamleider de gegevensbeheerder hiervan op de hoogte via Topdesk.

De Security Officer houdt in een autorisatiematrix de administratie bij over de toegekende autorisaties en de rollen in Suwinet-Inkijk. Autorisaties worden uitsluitend toegekend aan medewerkers in vaste en tijdelijke dienst van Fijnder die taken uitvoeren met betrekking tot de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen, Tijdelijke Wet Opvang Ontheemden Oekraïne, Regeling opvang ontheemden Oekraïne, het Besluit bijstandsverlening zelfstandigen 2004, Wet Inburgering 2021 en adrescontrole voor de gemeenten Winterswijk, Oost Gelre en Berkelland.

De directeur parafeert op de uitdraai van de 'Autorisatiematrix Fijnder autorisaties, rollen en taken' en op de uitdraai 'Gebruikersadministratie – Navigatie' van Suwinet-Inkijk elke wijziging in de autorisatie en de rol voor gezien en akkoord. Gebruikers van Suwinet-Inkijk moeten zich houden aan de algemene regels voor het werken met persoonsgegevens, zoals vermeld in 'Bijlage 1 – Regels werken met persoonsgegevens' en aan de specifieke regels die in dit beveiligingsplan zijn opgenomen. Nieuwe medewerkers van Fijnder dienen verplicht een e-learning Suwinet te volgen via de site van de VNG (Vereniging Nederlandse gemeenten).

Tijdens thuiswerken is het raadplegen van Suwinet-Inkijk toegestaan als onbevoegden op geen enkele wijze toegang hebben tot Suwinet.

5. Logging rapportages

Het Bureau Keteninformatisering Werk en Inkomen is wettelijk verplicht om gegevens te loggen waarmee het gebruik van Suwinet-Inkijk per gebruiker kan worden nagegaan. Het doel van de logging is het tegengaan en controleren van onrechtmatige, onregelmatige of doeloverschrijdende raadpleging en voor wetenschappelijk/statistisch gebruik.

De volgende gegevens worden gelogd:

- het tijdstip van iedere log-in en log-out en andere actie;
- de naam van de gebruiker die inlogt en uitlogt;
- elk Burgerservicenummer (of andere zoek sleutel) waarvan gegevens worden opgevraagd;
- elke geraadpleegde bron.

De gebruikers van Suwinet-Inkijk worden geïnformeerd dat over de toegang en handelingen gegevens worden verzameld en vastgelegd. Hij informeert nieuwe gebruikers direct na de autorisatie. Dit is een belangrijk onderdeel van de privacybescherming van de gebruikers. Om die reden wordt de volgende informatie verstrekt aan de gebruikers die werken met Suwinet-Inkijk:

- het bestaan en de vindplaats van dit aansluitbeleid;
- het bestaan van de loggingapplicatie en de mogelijkheid hieruit te rapporteren;
- de (aard van de) gegevens die binnen deze applicatie worden gelogd;
- de doelen van de logging;
- dat de gegevens niet voor andere doeleinden worden gebruikt dan waarvoor ze zijn vastgelegd;
- omschrijving van de werkzaamheden die met behulp van Suwinet-Inkijk mogen worden verricht, respectievelijk omschrijving van het gebruik van (de persoonsgegevens binnen) Suwinet-Inkijk dat verboden is;
- de gevolgen voor de gebruiker bij een geconstateerd onrechtmatig, onregelmatig of doel overschrijdend gebruik van (de persoonsgegevens binnen) Suwinet-Inkijk;
- de wijze waarop en door wie een (mogelijk) geconstateerd onrechtmatig, onregelmatig of doeloverschrijdend gebruik van (de persoonsgegevens binnen) Suwinet-Inkijk wordt besproken met de betreffende gebruiker(s);
- overzicht van degenen die bevoegd zijn de informatie van de loggingapplicatie op te vragen en daarover te rapporteren.

6. Controle gebruik Suwinet-Inkijk

De toezichthouder informatiebeveiliging (Security Officer) vraagt minimaal na afloop van elk half jaar in maart en september via Suwinet-Inkijk de gebruikersrapportage van de afgelopen 6 maanden op. De rapportage verstrekt informatie over de kwantiteit van de opvragingen en het gebruik van de escape-functie. De rapportage bevat geen per gebruiker herleidbare gegevens.

De toezichthouder controleert het gebruik van Suwinet-Inkijk en de autorisaties over de afgelopen periode en rapporteert hierover aan het Management Overleg. Bij mogelijke signalen van oneigenlijk gebruik en als er anders aanleiding toe is raadpleegt de Security Officer Suwinet via Suwinet-Inkijk de

specifieke rapportage voor verdere analyse. Als er sprake is van oneigenlijk gebruik van Suwinet-Inkijk licht de teamleider de Functionaris gegevensbescherming en het dagelijks bestuur in. Hij spreekt de gebruiker op het oneigenlijk gebruik van Suwinet-Inkijk aan en neemt zo nodig maatregelen. De teamleider en de manager nemen maatregelen.

7. Inzage in Suwinet-Inkijk door cliënt en/of gemachtigde

Om de privacy van de cliënt te waarborgen is zorgvuldigheid in de omgang met zijn/haar gegevens vereist. In bepaalde gevallen is gegevensinzage door derden mogelijk. In de Bijlage 2 - Handleiding inzage in Suwinet-Inkijk door cliënt en/of gemachtigde staat de werkwijze voor een aantal situaties waar de gebruiker van Suwinet-Inkijk mee te maken kan krijgen. De via Suwinet-Inkijk opvraagbare gegevens zijn in elektronische vorm te zien en als dit noodzakelijk is voor de rechtmatigheid van de uitkering mogen deze in het persoonsdossier worden opgenomen.

In Bijlage 3 – Toegewezen rollen (BKWI) staat een overzicht van de toegewezen rollen met paraaf van de directeur.