

**ADVIESNOTA voor burgemeester en wethouders**

**Openbare besluitenlijst**

Zaaknummer: 15836-2026

Medewerker	:	Henrike Reinders
Team	:	Werk Inkomen Zorg
Datum	:	13 april 2026
Portefeuillehouder	:	wethouder Herman Engberink

<p><b>BIJLAGEN:</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Beveiligingsplan Suwinet (def) (15829-2026)</li> <li><input checked="" type="checkbox"/> Informatiebeveiliging en Privacy De Gouden Regels (15829-2026)</li> <li><input checked="" type="checkbox"/> Werkinstructie Weet hoe het zit met Suwinet (15829-2026)</li> <li><input checked="" type="checkbox"/> Procedure Autorisatie tot Suwinet (15829-2026)</li> <li><input checked="" type="checkbox"/> Procedure controleren gebruik Suwinet (15829-2026)</li> <li><input checked="" type="checkbox"/> Verklaring zorgvuldig gebruik Suwinet (15829-2026)</li> <li><input checked="" type="checkbox"/> Taakomschrijving Security Officer Suwinet (15829-2026)</li> <li><input checked="" type="checkbox"/> Autorisatiematrix (april 2026) (15829-2026)</li> <li><input checked="" type="checkbox"/> Suwinet-guidance-2025 (15829-2026)</li> </ul>
<p><b>AFSTEMMING MET</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> team Communicatie en Ondersteuning <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Geen actieve communicatie</li> </ul> </li> <li><input checked="" type="checkbox"/> anders, nl. Rachel Brouwer, Ensia Coördinator/ICT Security Officer DOWR, gemeente Deventer en gemeente Raalte</li> </ul>
<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Openbaar</li> <li><input type="checkbox"/> Vertrouwelijk</li> </ul>
<p><b>ONDERWERP</b> Beveiligingsplan Suwinet Olst-Wijhe</p>

**BESLUIT burgemeester en wethouders**

1. Het Beveiligingsplan Suwinet Olst-Wijhe vast te stellen.

**SAMENVATTING**

Voor het delen van persoonsgegevens binnen de wettelijke taken op het gebied van werk en inkomen maken gemeenten gebruik van het informatiesysteem Suwinet. Dit biedt een veilige omgeving voor het delen van persoonsgegevens en privacygevoelige informatie tussen organisaties. Zorgvuldig en veilig gebruik van de gegevens moet goed worden geborgd binnen de gemeentelijke organisatie.

Jaarlijks wordt er verantwoording afgelegd over het gebruik van Suwinet op basis van het normenkader, dat is gebaseerd op de BIO-normen (Baseline Informatiebeveiliging Overheid). Dit beveiligingsplan beschrijft hoe we in Olst-Wijhe aan deze normen voldoen en hoe we een zorgvuldig en controleerbaar gebruik van Suwinet waarborgen.

Op 17 juli 2024 is het Strategisch informatiebeveiligingsbeleid DOWR-gemeenten 2024 vastgesteld. Dit beveiligingsplan Suwinet past binnen dit strategisch informatiebeveiligingsbeleid.

## AANLEIDING

Voor een goede uitvoering van de Participatiewet, de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte werkloze werknemers (IOAW) en de wet Inkomensvoorziening oudere of gedeeltelijk arbeidsongeschikte gewezen zelfstandigen (IOAZ) heeft de gemeente gegevens nodig van andere partijen. Bijvoorbeeld bij het vaststellen van het recht op een uitkering. Partijen, waaronder gemeenten, UWV en de Belastingdienst, maken hiervoor gebruik van Suwinet. Dit is een informatiesysteem dat een veilige omgeving biedt voor het delen van gegevens. Het gaat hier om privacygevoelige gegevens, zoals inschrijvingen in de Basisregistratie Persoonsgegevens, arbeidsverleden, loon, bijstandsuitkeringen en opleiding van burgers die in aanmerking (willen) komen voor een uitkering.

Bij behandeling van deze gegevens is zorgvuldigheid en controleerbaarheid erg belangrijk. Gemeenten moeten daarom verantwoording afleggen over het gebruik van Suwinet. Gemeenten verantwoorden zich jaarlijks over het gebruik van Suwinet volgens de ENSIA systematiek. Zij geven zo inzicht in de mate waarin de gemeente compliant is aan de Baseline Informatiebeveiliging Overheid (BIO). Door gemeenten wordt verantwoording afgelegd langs twee pijlers:

1. Intern ten behoeve van de verantwoording van het college aan de raad over de mate waarin de gemeentelijke bedrijfsvoering in control is op het gebied van informatiebeveiliging met als norm de BIO.
2. Extern ten behoeve van de verantwoording aan de toezichthouders en stelselhouders van het Rijk.

De verantwoording Suwinet vindt plaats op basis van een jaarlijkse zelfevaluatie aan de hand van de BIO-vragenlijst ENSIA. Dit gebeurt op basis van een aantal normen. Deze normen zijn opgenomen in de Suwinet guidance, zie bijlage 8.

Het laatst vastgestelde beveiligingsplan dateert uit 2021 en had een geldigheidsduur tot en met 2025. Het nieuwe beveiligingsplan heeft een onbeperkte looptijd. Hiervoor wordt gekozen omdat er intern periodiek (eens per maand) en jaarlijks met de zelfevaluatie ENSIA wordt gecontroleerd op het veilig gebruik van Suwinet. Als er aanleiding voor is, dan wordt het beveiligingsplan Suwinet geactualiseerd.

De belangrijkste normen worden hieronder kort toegelicht:

### 1. Inrichten van een Beveiligingsfunctie Suwinet

De gemeente Olst-Wijhe heeft een Security Officer. Deze functionaris is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit dit document en bevordert de informatiebeveiliging en de communicatie naar de medewerkers over het gebruik van Suwinet.

### 2. Scheiding van taken, verantwoordelijkheden en functies

Er is een autorisatiematrix, waarin de scheiding van taken, verantwoordelijkheden en functies staan beschreven. Er is een zodanig onderscheid gemaakt in functie en rol binnen de autorisatiestructuur, dat de medewerker alleen die gegevens kan raadplegen die van belang zijn voor zijn/haar werkzaamheden.

### 3. Monitoring, rapportage en controle

Alle handelingen die in Suwinet plaatsvinden worden door het Bureau Keteninformatisering werk en inkomen (BKWI) gelogd, oftewel opgeslagen. Deze informatie wordt maandelijks in een rapportage door BKWI beschikbaar gesteld. Het is de taak van de Security Officer om deze informatie te controleren en te analyseren op het zorgvuldig gebruik van Suwinet. Ook wordt in een controle beoordeeld of alle autorisaties nog overeenkomstig de matrix zijn afgegeven. Signalen van mogelijk onrechtmatig gebruik worden vastgelegd en onderzocht. Ieder half jaar wordt over de uitkomsten van de maandelijkse controles en de eventuele verbeteracties gerapporteerd aan de teamleider Werk, Inkomen en Zorg en de DOWR-brede Chief Information Security Officer (CISO).

### 4. Verantwoording

Jaarlijks moet door middel van beantwoording van de ENSIA-vragenlijst (in de digitale omgeving van de ENSIA-tool) verantwoord worden hoe de gemeente Olst-Wijhe invulling geeft aan de gestelde normen. Hiermee voldoen we aan de eisen van transparantie. De beheerder (BKWI) kan van de ENSIA-verantwoording/controleverklaring gebruikmaken. Over 2025 is de ENSIA-vragenlijst ingevuld door de Security Officer Suwinet. Verantwoording aan het college en de gemeenteraad over de normen gebeurt ook via de ENSIA-tool.

Vanaf 2026 wordt niet meer alleen de opzet en het bestaan getoetst maar ook de werking (daadwerkelijke uitvoering). Het beveiligingsplan Suwinet Olst-Wijhe is ook als zodanig opgebouwd. Dit beveiligingsplan is gezamenlijk met de gemeenten Deventer en Raalte opgesteld en daar waar nodig gemeentespecifiek gemaakt.

#### BEOOGD RESULTAAT

Vaststellen van het Beveiligingsplan Suwinet Olst-Wijhe, zodat het een duidelijk kader biedt voor een zorgvuldig en controleerbaar gebruik van Suwinet.

#### KADER

Het Beveiligingsplan Suwinet Olst-Wijhe kadert binnen de volgende regelingen en wetten:

- Baseline Informatiebeveiliging Overheid (BIO)
- Wet SUWI (Wet Structuurorganisatie Uitvoering Werk en Inkomen)
- Regeling SUWI
- AVG (Algemene Verordening Gegevensbescherming)
- Strategisch Informatiebeveiligingsbeleid DOWR-gemeenten 2024

Verder wordt het verwerken van persoonsgegevens geregeld in specifieke wetten zoals de Participatiewet.

#### ARGUMENTEN VOOR

Een vastgesteld Beveiligingsplan Suwinet is voorwaardelijk om aangesloten te kunnen zijn op Suwinet. Deze aansluiting is nodig voor het uitvoeren van wettelijke taken binnen de keten van werk en inkomen. Ook is de aansluiting nodig om het recht op een uitkering binnen de Participatiewet te kunnen vaststellen.

#### ARGUMENT TEGEN

Niet van toepassing

#### RISICO'S

Dit plan draagt bij aan het beperken van risico's in het gebruiken en delen van persoonsgegevens. Aan het plan zelf zijn geen risico's verbonden.

#### FINANCIËN

Er zijn geen financiële consequenties

#### DUURZAAMHEID

Niet van toepassing

#### PARTICIPATIE

Omdat Suwinet privacygevoelige gegevens bevat, moeten klanten erop kunnen vertrouwen dat hun gegevens op een zorgvuldige en controleerbare wijze worden behandeld. Dit beveiligingsplan dient dan ook als kader waarbinnen we het zorgvuldig gebruik van Suwinet willen borgen.

#### COMMUNICATIE

Niet van toepassing

#### PLANNING EN UITVOERING

Het beveiligingsplan sluit inhoudelijk nauw aan op het aflopende Suwinet beveiligingsplan 2022-2025. Er zijn geen noemenswaardige inhoudelijke wijzigingen. Voor de Security Officer Suwinet blijven taken en verantwoordelijkheden grotendeels hetzelfde. De uitvoering van taken wordt dus voortgezet.

De Security Officer Suwinet draagt de inhoud van het beveiligingsplan uit aan alle medewerkers die gebruik maken van Suwinet. Dit gebeurt door voorlichting en een-op-een contact. Dit draagt bij aan draagvlak voor een zorgvuldig gebruik van Suwinet binnen onze gemeente.

Als u instemt dan wordt het beveiligingsplan gedeeld met de CISO en Functionaris voor de Gegevensbescherming.