Compact verbeterplan bevindingen Suwinet 2025 (niet uitgesplitst per Suwi-aansluiting)

| Norm waaraan niet wordt voldaan | Risico | Verbeterplan |
|---|---|---|
| 5.1.2.1 Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld. | De getroffen beveiligingsmaatregelen kunnen ontoereikend zijn in relatie tot aangescherpte wetgeving, verandering van risicoklasse van gegevens en de toegepaste technologieën. | Formele beoordeling van het huidige beleidskader vindt plaats in Q1 2026. De geldigheidsduur van het huidige beleidskader wordt verlengd; actualisatie volgt in 2026, in navolging van verwachte nieuwe wet- en regelgeving. |
| 6.1.1.1 De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie. | Het risico bestaat dat door gebrek aan coördinatie van activiteiten niet op beveiligingsincidenten wordt geacteerd en dat door wijzigingen nieuwe kwetsbaarheden ontstaan. | Toegangsrechten voor Suwi-RooO zijn persoonsgebonden en niet onder te brengen in een standaardrol, waardoor reguliere functiescheiding beperkt toepasbaar is. Ter beheersing van dit risico wordt gewerkt volgens een protocol, waarbij rekening wordt gehouden met bestaande Suwi-Inkijk-rechten. Daarnaast wordt inzichtelijk gemaakt welke medewerkers zowel RoO- als Inkijk-rechten hebben en wordt bezien hoe signalering en opvolging via de halfjaarlijkse autorisatiecontrole bij de leidinggevende kan worden belegd. Tijdlijn:Q3 2026 |
| 6.1.2.1 Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen* waarnemen of voorkomen.<br>* Onder bedrijfsmiddelen worden in dit verband de Suwinet gegevens (mede) begrepen. | Onduidelijke taken en verantwoordelijkheden en het ontbreken van juiste functiescheiding kunnen leiden tot:<br>- misbruik van bevoegdheden,<br>- te ruim toegekende bevoegdheden,<br>- over het hoofd zien van en/of tot implementatie van tegenstrijdige beveiligingsmaatregelen. | Voor de afdeling kwaliteit zullen we de manier van opstellen van de autorisatiematrix opnieuw beoordelen en aanpassen naar gewenste format. Streefdatum: mei 2026 |
| 7.2.2.2 Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd | Indien gebruikers van Suwinet- gegevens zich niet of onvoldoende bewust zijn van de (hoge) vertrouwelijkheid, bestaat het risico dat deze gegevens onvoldoende worden beschermd. | De naleving van de verplichte Suwi-training wordt periodiek gemonitord. Indien blijkt dat een medewerker de training niet tijdig heeft gevolgd, wordt de betreffende leidinggevende hierover benaderd met het verzoek hierop actie te ondernemen. Wanneer de training vervolgens niet alsnog tijdig wordt afgerond, wordt de toegang tot Suwinet ontzegd totdat aan de opleidingsverplichting is voldaan. |
| 9.2.5.2 De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident. | Bij het ontbreken controles op het gebruik van autorisaties wordt misbruik niet gesignaleerd | Voor de afdeling kwaliteit beoordelen we dit maandelijks, we zullen dit beter traceerbaar vastleggen in de matrix; streefdatum: per direct.<br>De periodieke beoordeling is ook van toepassing op Suwi-Doorstroompunt. |
| 9.2.5.3 Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld | Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens | Voor de afdeling kwaliteit beoordelen we dit maandelijks, we zullen dit beter traceerbaar vastleggen in de matrix; streefdatum: per direct. |

| | | |
|---|---|---|
| 9.2.6 Aanvullende maatregel:<br>Het lijnmanagement heeft een procedure vastgesteld en geïmplementeerd voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie | Als toegangsrechten niet bijtijds worden beëindigd of gewijzigd, bestaat het risico op onbevoegde kennisname van Suwinet gegevens | Voor de afdeling kwaliteit was dit van toepassing op uit dienst - we zullen we de tijdigheid van verwerking bij mutaties beter opvolgen. Streefdatum; per heden |
| 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen. | Ondanks het besloten karakter van Suwinet bestaat het risico dat de toegang tot gegevens niet adequaat is beschermd. | Het cryptografiebeleid wordt in 2026 opgesteld. |
| 18.1.4.2 Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. | Als de verwerking van Suwinet (persoons)gegevens niet overeenkomstig toepasselijke wet- en regelgeving plaatsvindt, wordt hierdoor de AVG overtreden. | Het verwerkingsregister wordt in het eerste kwartaal van 2026 bijgewerkt. |