

Bijlage bij het Assurancerapport inzake Suwinet – Gemeente Lansingerland

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
B.01	De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld.	Via inspectie van documentatie vastgesteld dat een actueel en door het College vastgesteld informatiebeveiligingsbeleid en beveiligingsplan Suwinet-Inkijk aanwezig zijn waarin ingegaan wordt op de beveiligingsmaatregelen voor Suwinet.	Voldoet
B.04	De Afnemer heeft een Beveiligingsfunctie Suwinet (GeVS) benoemd en taken en verantwoordelijkheden vastgesteld.	Via inspectie van documentatie vastgesteld dat de functie van Security Officer SUWI is beschreven inclusief de taken, verantwoordelijkheden en bevoegdheden. Daarnaast is vastgesteld via inspectie van documentatie dat een Security Officer SUWI is aangemeld bij het BKWI. Via inspectie van documentatie vastgesteld dat het melden van beveiligingsincidenten is opgenomen in het beveiligingsplan en dat een procedure voor het melden van beveiligingsincidenten is beschreven. Via inspectie van documentatie vastgesteld dat beveiligingsincidenten geregistreerd worden en opgevolgd.	Voldoet
B.05	De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven.	Via inspectie van documentatie vastgesteld dat taken en verantwoordelijkheden inzake informatiebeveiliging en Suwinet zijn beschreven, waarbij functiescheiding is toegepast. Via inspectie van documentatie vastgesteld dat een autorisatiematrix Suwinet is opgesteld en overeenkomt met de inrichting in de applicatie Suwinet. Tevens is via inspectie van documentatie vastgesteld dat het autorisatiebeheerproces is beschreven.	Voldoet
U.02	De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is dat het wijzigen (ook intrekken of	Via inspectie van documentatie is vastgesteld dat het autorisatiebeheerproces is beschreven.	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
	blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd.	Via inspectie van documentatie vastgesteld dat periodieke review van verleende toegangsrechten is uitgevoerd. Via inspectie van een indiensttreder vastgesteld dat hiervoor een autorisatieverzoek was ingediend en dat de verkregen toegangsrechten overeenkwamen met de aanvraag. Via inspectie van een mover vastgesteld dat hiervoor een autorisatieverzoek was ingediend en dat de verkregen toegangsrechten overeenkwamen met de aanvraag. Via inspectie van een uitdiensttreder vastgesteld dat de toegangsrechten tijdig zijn verwijderd.	
U.03	Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen.	Via inspectie van documentatie vastgesteld dat het wachtwoordbeleid is beschreven. Via inspectie van documentatie van het BKWI en in Suwinet vastgesteld dat aan het Suwinet wachtwoord specifieke eisen worden gesteld. Hier heeft de gemeente zelf geen invloed op. Via inspectie van de Suwinet gebruikers vastgesteld dat alleen persoonsgebonden en unieke user ID's worden gebruikt.	Voldoet
U.11	De Afnemer behoort alle netwerkverbindingen waarover Suwinet gegevens worden uitgewisseld beveiligd te hebben tegen ongeautoriseerde toegang overeenkomstig het aansluitingsbeleid Suwinet.	Via inspectie van documentatie vastgesteld dat classificatie van Suwinet gegevens heeft plaatsgevonden. Via inspectie van documentatie vastgesteld dat een cryptografie beleid is opgesteld. Via inspectie van documentatie vastgesteld dat een contract is afgesloten voor de aansluiting op het Gemnet. Via inspectie van de verbindingen met Suwinet vastgesteld dat deze over een beveiligde verbinding verloopt. Hier heeft de	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
		gemeente geen invloed op. Via inspectie van documentatie vastgesteld dat de netwerkarchitectuur inclusief de aansluiting op het Gemnet is beschreven.	
C.01	(De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologieën.	Via inspectie van het aansluitbeleid vastgesteld dat hierin is opgenomen dat deze elke 3 jaar wordt geëvalueerd. Via interview vastgesteld dat het aansluitbeleid in 2018 wordt geëvalueerd. Via inspectie van documentatie vastgesteld dat de procedure voor het periodiek controleren van verleende toegangsrechten is beschreven. Via inspectie van documentatie vastgesteld dat periodieke review van verleende toegangsrechten is uitgevoerd. Via inspectie van documentatie vastgesteld dat binnen de gemeente aandacht wordt geschonken aan awareness voor informatiebeveiliging.	Voldoet
C.04	Het verantwoordelijke management behoort de toegangsrechten van gebruikers/beheerders tot de Suwinet diensten regelmatig te beoordelen in een formeel proces (cyclisch proces).	Via inspectie van documentatie vastgesteld dat de procedure voor het periodiek controleren van verleende toegangsrechten is beschreven. Via inspectie van documentatie vastgesteld dat periodieke review van verleende toegangsrechten is uitgevoerd. Via inspectie van documentatie vastgesteld dat een autorisatiematrix voor Suwinet rechten is opgesteld.	Voldoet
C.05	Activiteiten van gebruiker en beheerders, uitzonderingen en informatiegebeurtenissen behoren te worden	Via inspectie van documentatie vastgesteld dat lograpportages Suwinet aanwezig zijn.	Voldoet

Nr.	Beheersmaatregel	Uitgevoerde testwerkzaamheden	Conclusie / aanbevelingen
	vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles.	Via inspectie van documentatie vastgesteld dat de procedure voor het bijhouden en monitoren van de logging is beschreven. Via inspectie van systeeminstellingen vastgesteld dat alleen internal control bij de lograpportages kunnen.	
C.06	De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen)	Via inspectie van documentatie vastgesteld dat monitoring van de logging heeft plaatsgevonden waarbij eventuele vervolgacties zijn beschreven. Via inspectie van documentatie vastgesteld dat een rapportage over o.a. de analyse van de logging aan het management is opgesteld en doorgestuurd. Via inspectie van documentatie vastgesteld dat de procedure voor het bijhouden en monitoren van de logging is beschreven.	Voldoet
C.07	De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties.	Via inspectie van documentatie vastgesteld dat lograpportages Suwinet aanwezig zijn en dat deze zijn beoordeeld. Verder is via inspectie vastgesteld dat controle op verleende toegangsrechten plaatsvindt. Tot slot is via inspectie vastgesteld dat gerapporteerd wordt aan het management over de beveiliging van IAA inzake Suwinet.	Voldoet