

Bijlage 16 – Concept Service Level Rapport (SLR) Normenkader IBP-FO Netwerk & beheer

Versie: 1.0

Perceel: Basis

TLP: **GREEN**: openbaar inzichtelijk, maar alleen te gebruiken
binnen het kader van deelname aan de aanbesteding.

Inleiding

Dit document beschrijft de Service Level Requirements (SLR) voor de dienstverlening Netwerk & Beheer binnen de aanbesteding van SIVON.

Het doel van dit document is om een duidelijk en toetsbaar kader te bieden waarmee SIVON gedurende de samenwerking met leveranciers de geleverde prestaties kan beoordelen. De SLR's zijn gebaseerd op het bijgevoegde Normenkader Informatiebeveiliging & Privacy (IBP) en de daaruit voortvloeiende verplichtingen op het gebied van integriteit, vertrouwelijkheid en beschikbaarheid van de netwerkdiensten.

De SLR's vormen samen met de overeengekomen Service Level Agreement (SLA) in het Programma van Eisen het uitgangspunt voor de operationele en contractuele sturing op de dienstverlening.

Classificatie	Vraag	Antwoord
Algemeen	Hoeveel incidenten hebben er plaats gevonden in de afgelopen periode? Lever eventueel incidentrapportages aan.	
	Oefenen jullie met crisisscenario's (met als scope de dienst/het product)?	
	Hoe zorgen jullie voor dat de betrokken medewerkers bewust omgaan met de dienst/het product? (Bewustzijn van medewerkers)	
	Hoe wordt geborgd dat toegang tot persoonsgegevens beperkt blijft tot bevoegde medewerkers (denk aan logging, autorisaties)?	
	Is er een vorm van monitoring aanwezig, zoals een IDS/IPS of SOC/SIEM?	
	Hoe ziet jullie ontwikkelstraat eruit voor de dienst/het product (denk aan OTAP, SDLC, CI/CD, continue dienstverlening)?	
	Zijn er privacy-audits, penetratietests of DPIA's uitgevoerd en wat waren de uitkomsten?	

	Worden AI-modellen periodiek getest op bias, accuracy en performance?	
	Zijn afwijkingen in AI-modellen of kritieke fouten gerapporteerd en gedocumenteerd?	
	Welke overige beveiligingsmaatregelen treffen jullie voor de levering van de dienst/het product?	
Beschikbaarheid	Wat is de uptime van afgelopen periode?	
	Is er (gepland) onderhoud geweest?	
	Wat is het RTO en kunt u aantonen dat hieraan is voldaan op basis van testen/praktijk ervaringen?	
	Hoe snel is er gereageerd op incidenten? Lever eventueel incidentrapportages aan.	
Integriteit	Zijn er patches uitgevoerd en hoe is dit uitgevoerd, zonder dataverlies?	

	Wat is het RPO en kunt u aantonen dat hieraan is voldaan op basis van testen/praktijk ervaringen?	
	Zijn er hersteltesten uitgevoerd en is er onderzocht of er dataverlies heeft plaats gevonden? (RTO en RPO)	
	Wat is de back-up strategie en hoe worden back-ups beveiligd?	
	Hoe wordt geborgd dat logging beschermd is tegen manipulatie?	
Vertrouwelijkheid	Is er een periodieke audit van de toegangsbeveiliging uitgevoerd? Zo ja, wat waren de bevindingen?	
	Is er monitoring van de logging op toegang? Lever eventueel inbreukrapportages op.	
	Hoe is de dienst/applicatie/communicatie versleuteld? En welke cryptografie wordt er toegepast?	
	Is er een proces voor sleutelbeheer, en hoe wordt de naleving hiervan gemonitord?	

	Hoe wordt afgeschreven media gecontroleerd vernietigd/verwijderd? Is dit in de afgelopen tijd gebeurd? Lever eventueel bewijs aan.	
Bewijslast	ISO27001 certificaat met VVT.	
	ISAE3402 of SOC2 Type2	
	Pentest, Third Party Memorandum (TPM), (op de operationele systemen of identiek aan) zowel infra als specifieke dienst/product)	
	Cloud Controls Matrix (CCM)	
	Cloud Security Alliance (CS)	
	Externe- of interne auditrapportages (mag ook een TPM zijn)	
	Vulnerability rapportages	
	Dataportabiliteit beleid/proces	
	Locatie van gegevens (lever bewijs aan)	