Bijlage 4 – Service Level Agreement (SLA)

'SIEM, SOC, SOAR-dienstverlening'

Deze Service Level Agreement (SLA) bevat de servicenormen voor de SIEM-, SOC- en SOAR-dienstverlening en geldt gedurende de volledige looptijd van de overeenkomst. Nadere werkafspraken worden vastgelegd in het Dossier Afspraken en Procedures (DAP). Het DAP kan niet afwijken van deze SLA (eis 1.18 Programma van Eisen).

Algemene SLA eisen	
SLA-01	Opdrachtnemer registreert en prioriteert iedere melding conform de matrix in Bijlage 4A – Reactie- en oplostijden bij deze SLA, en levert reactie en oplossing binnen de daarbij genoemde tijden. Bij verschil van inzicht over de toe te kennen prioriteit is het oordeel van VNOG leidend. Opdrachtnemer kan een afwijkende opvatting gemotiveerd inbrengen via de escalatieprocedure in het DAP; dit schort de afhandeling van de melding niet op.
SLA-02	Indien VNOG in het kader van haar crisisorganisatie operationeel is opgeschaald volgens de GRIP-structuur (20170523-IFV-GRIP-en-de-flexibele-toepassing.pdf) en de SIEM-, SOC-, SOAR- of incidentresponsdienstverlening daarbij relevant is, treden op eerste verzoek van VNOG de overeengekomen escalatie- en samenwerkingsafspraken in werking. Opdrachtnemer handelt daarbij overeenkomstig de bij inschrijving ingediende en door VNOG geaccepteerde uitwerking van gunningscriterium **K2 – Implementatie, transitie en samenwerking**, voor zover deze betrekking heeft op de samenwerking, escalatie en dienstverlening tijdens grootschalige crisissituaties. De geaccepteerde uitwerking maakt na definitieve gunning integraal en contractueel afdwingbaar onderdeel uit van de overeenkomst en wordt nader geconcretiseerd in het Dossier Afspraken en Procedures (DAP). Opdrachtnemer wijst hiervoor minimaal één primair en één vervangend aanspreekpunt aan. Deze aanspreekpunten zijn gedurende de opschaling beschikbaar conform de overeengekomen afspraken, sluiten aan op de relevante overlegstructuur van VNOG en zorgen voor technische duiding, advisering, coördinatie en afstemming tussen het SOC, eventuele CERT-/CSIRT-specialisten en de crisisorganisatie van VNOG. De definitieve uitwerking van K2 van de winnende Inschrijver wordt als bijlage bij de overeenkomst gevoegd. Hiermee worden de daarin gedane toezeggingen onderdeel van de contractuele verplichtingen van Opdrachtnemer.

SLA-03	Opdrachtnemer levert uiterlijk binnen tien (10) werkdagen na afloop van iedere kalendermaand een operationele rapportage aan VNOG. De rapportage bevat ten minste: • het aantal meldingen en incidenten, uitgesplitst naar prioriteit, classificatie, bron en status; • de gerealiseerde detectie-, triage-, reactie-, notificatie- en escalatietijden per prioriteitsklasse, afgezet tegen de normen uit Bijlage 4A; • het aantal en percentage meldingen dat binnen en buiten de overeengekomen normen is afgehandeld, inclusief een toelichting op eventuele afwijkingen; • het aantal en percentage foutpositieve meldingen, inclusief trends en getroffen optimalisatiemaatregelen; • het aantal openstaande meldingen en incidenten en de ouderdom daarvan; • (indien van toepassing) een overzicht van opschalingen naar CERT-/CSIRT-specialisten en/of de crisisorganisatie van VNOG; • een overzicht van uitgevoerde containment- en responsmaatregelen; • relevante wijzigingen in usecases, detectieregels en playbooks; • de gerealiseerde beschikbaarheid van het serviceportaal en eventuele uitval van aangesloten logbronnen (SLA-09 en SLA-10); • gesignaleerde risico's, trends, verbeterpunten en voorgenomen maatregelen. Opdrachtnemer consolideert deze informatie per kwartaal in een trend- en servicerapportage. Deze wordt besproken tijdens de operationeel-tactische kwartaalreview, waarbij partijen gezamenlijk verbetermaatregelen, prioriteiten, verantwoordelijkheden en termijnen vaststellen. De overeengekomen acties worden vastgelegd en in de daaropvolgende rapportages gevolgd.

Registratie & Support	
SLA-04	Opdrachtnemer stelt geen limiet aan het aantal meldingen (ongeacht prioriteit) vanuit VNOG.
SLA-05	Iedere melding wordt direct geregistreerd en blijft gedurende de overeengekomen bewaartermijn beschikbaar in het serviceportaal van Opdrachtnemer. VNOG ontvangt voor iedere melding tevens per e-mail een bevestiging en, zodra de koppeling beschikbaar is, automatisch via het ITSM-/ticketsysteem van VNOG. De bevestiging bevat ten minste: • het unieke ticket- of incidentnummer; • de datum en het tijdstip van detectie en registratie; • het meldingstype en de toegekende prioriteit; • een duidelijke omschrijving en eerste duiding van de melding; • de getroffen systemen, gebruikers of diensten, voor zover bekend; • de actuele status en reeds uitgevoerde acties; • het geadviseerde vervolg en de eventuele actie die van VNOG wordt verwacht; • de contactgegevens van het verantwoordelijke aanspreekpunt bij Opdrachtnemer. Bij meldingen met prioriteit 1 of 2 informeert Opdrachtnemer VNOG aanvullend telefonisch. VNOG kan desgewenst per prioriteit of type melding een aanvullende sms-notificatie laten instellen. De ontvangers, communicatiemiddelen, escalatievolgorde en vervangende contactpersonen worden vastgelegd in een actuele contact- en escalatiematrix in het Dossier Afspraken en Procedures (DAP).

SLA-06	Na afronding van iedere melding of ieder incident ontvangt VNOG een afsluitmelding. Deze wordt vastgelegd in het serviceportaal van Opdrachtnemer en per e-mail en, zodra de koppeling beschikbaar is, via het ITSM-/ticketsysteem van VNOG verstrekt. De afsluitmelding bevat ten minste: • het unieke ticket- of incidentnummer; • het oorspronkelijke meldingstype en de oorspronkelijke prioriteit; • de datum en het tijdstip van detectie, registratie en eerste melding; • een omschrijving van de melding en de vastgestelde oorzaak, voor zover bekend; • de getroffen systemen, gebruikers, gegevens of diensten en de vastgestelde impact; • een overzicht van de uitgevoerde onderzoeks-, containment-, herstel- en overige responsmaatregelen; • de datum en het tijdstip waarop de melding of het incident is opgelost en afgesloten; • de gerealiseerde doorlooptijden, afgezet tegen de overeengekomen servicenormen; • eventuele restrisico's, openstaande acties en verantwoordelijke partijen; • aanbevelingen voor aanvullende maatregelen of aanpassing van usecases, detectieregels en playbooks. Meldingen en incidenten met prioriteit 1 of 2 worden uitsluitend na afstemming met VNOG definitief afgesloten. Indien nader onderzoek nog loopt, wordt dit duidelijk vermeld en blijft een gekoppelde vervolgactie of onderzoekstaak geopend.

SLA-07	VNOG kan op ieder moment aan de hand van het unieke ticket- of incidentnummer de actuele status, voortgang, uitgevoerde acties en openstaande vervolgacties raadplegen in het serviceportaal van Opdrachtnemer en, zodra de koppeling beschikbaar is, via het ITSM-/ticketsysteem van VNOG. Bij meldingen en incidenten met prioriteit 1 of 2 informeert Opdrachtnemer VNOG proactief over het verloop. Dit gebeurt: • bij iedere wijziging in impact, prioriteit, risico of aanpak; • bij uitvoering van een belangrijke containment- of herstelmaatregel; • wanneer besluitvorming, toestemming of inzet van VNOG noodzakelijk is; • wanneer een overeengekomen servicenorm mogelijk niet wordt gehaald; • met de minimale updatefrequentie uit Bijlage 4A. Iedere voortgangsupdate bevat ten minste de actuele status, impact, reeds genomen maatregelen, openstaande acties, eventuele beslispunten en het verwachte moment van de volgende update. De wijze van communicatie en ontvangers worden vastgelegd in de contact- en escalatiematrix.
SLA-08	Wijzigingen van de reactie-, triage-, escalatie-, herstel- of overige servicenormen in Bijlage 4A en wijzigingen van overige bepalingen van de SLA vinden uitsluitend plaats met schriftelijke instemming van beide partijen. De gevolgen voor kwaliteit, capaciteit, continuïteit, verantwoordelijkheden, risico's en kosten worden vooraf inzichtelijk gemaakt. Overeengekomen wijzigingen worden voorzien van een ingangsdatum en vastgelegd in een gewijzigde versie van de SLA en, indien van toepassing, het Dossier Afspraken en Procedures (DAP). Totdat een wijziging schriftelijk is overeengekomen, blijven de bestaande bepalingen onverkort van kracht. **Toelichting** Er is bewust niet gekozen voor een eenzijdig wijzigingsrecht van VNOG. De SOC-dienstverlening is mede gebaseerd op vooraf gereserveerde personele capaciteit, expertise en beschikbaarheid. Een wijziging van servicenormen kan daardoor gevolgen hebben voor de operationele inrichting en kosten van Opdrachtnemer. Dit laat onverlet dat Opdrachtnemer wijzigingen die noodzakelijk zijn om te blijven voldoen aan de overeenkomst, toepasselijke wet- en regelgeving of de actuele stand van de techniek binnen de overeengekomen prijs en termijnen moet uitvoeren.

Monitoring, beschikbaarheid en realisatie	
SLA-09	Opdrachtnemer bewaakt continu de aanlevering van log- en eventdata door de aangesloten bronnen. Uitval van, of een significante afwijking in, de aanlevering door een aangesloten bron wordt uiterlijk binnen één (1) uur gedetecteerd en aan VNOG gemeld. De drempelwaarden per bron worden vastgelegd in het DAP. Uitval van een bron die in het DAP als kritiek is aangemerkt, wordt behandeld als een melding met prioriteit 2.
SLA-10	Het serviceportaal van Opdrachtnemer heeft een beschikbaarheid van ten minste 99,5% per kalendermaand, gemeten 24/7, exclusief gepland onderhoud van maximaal acht (8) uur per maand. Gepland onderhoud wordt ten minste vijf (5) werkdagen vooraf aangekondigd en met VNOG afgestemd. Tijdens onbeschikbaarheid van het serviceportaal lopen monitoring, detectie en notificatie conform SLA-05 onverminderd door.
SLA-11	De reactie- en oplostijden uit Bijlage 4A worden per kalendermaand gemeten en gerapporteerd conform SLA-03. Daarbij gelden de volgende realisatienormen: • prioriteit 1 en 2: 98% van de meldingen binnen de reactietijd en ten minste 95% binnen de oplostijd; • prioriteit 3 tot en met 5: ten minste 95% van de meldingen binnen de reactietijd en ten minste 90% binnen de oplostijd.
SLA-12	Indien een realisatienorm uit SLA-11 of de beschikbaarheidsnorm uit SLA-10 in drie (3) opeenvolgende kalendermaanden, of in vier (4) kalendermaanden binnen één contractjaar, niet wordt behaald, dan treedt de in het Dossier Afspraken en Procedures (DAP) vastgelegde escalatieprocedure op het hoogste niveau in werking. Opdrachtnemer levert in dat geval binnen tien (10) werkdagen een concreet en schriftelijk verbeterplan aan VNOG. Dit verbeterplan bevat ten minste: • een analyse van de oorzaken van de tekortkoming; • de reeds getroffen en nog te treffen corrigerende maatregelen; • de beoogde resultaten en wijze waarop deze worden gemeten. Opdrachtnemer rapporteert periodiek over de voortgang totdat aantoonbaar en gedurende een met VNOG overeengekomen periode weer aan de norm wordt voldaan. De voortgang wordt besproken in de kwartaalreview (SLA-03). De overige rechten van VNOG op grond van de overeenkomst en de ARBIT 2022 (Bijlage 5) blijven onverlet.

Bijlage 4A – Reactie en oplostijden bij deze Service Level Agreement (SLA)

Voor de prioritering van security-incidenten wordt gebruikgemaakt van onderstaande matrix. De combinatie van urgentie en impact van een incident bepaalt de toe te kennen code.

Urgentie \ Impact	Hoog	Midden	Laag
Hoog	**1**	**2**	**3**
Midden	**2**	**3**	**4**
Laag	**3**	**4**	**5**

Aan iedere code zijn de volgende reactie- en oplostijden en bereikbaarheid gekoppeld:

Prio	Omschrijving	Reactietijd	Status update frequentie	Oplostijd	Bereikbaarheid
1	**Kritiek**	*≤ 15 minuten*	*Elke 60 minuten*	*≤ 4 uur*	*24/7, alle dagen*
2	**Hoog**	*≤ 30 minuten*	*Elke 2 uur*	*≤ 8 uur*	*24/7, alle dagen*
3	**Medium**	*≤ 2 uur*	*Elke 4 uur (werkdagen)*	*≤ 24 uur*	*werkdagen 08:00-18:00*
4	**Laag**	*≤ 8 uur*	*Dagelijks (werkdagen)*	*≤ 40 uur*	*werkdagen 08:00-18:00*
5	**Zeer laag**	*≤ 24 uur*	*Wekelijks (werkdagen)*	*best effort*	*werkdagen 08:00-18:00*