Bijlage G- Concept Service Level Agreement (SLA)

1. Inleiding

1.1 Doel

Deze Service Level Agreement (SLA) is een bijlage van de Overeenkomst tussen Opdrachtnemer en Opdrachtgever Het Waterschapshuis (HWH). HWH vertegenwoordigd de Nederlandse waterschappen. De waterschappen zullen deelnemen aan deze overeenkomst en worden verder genoemd 'deelnemers'.

Binnen het proces Service level management worden afspraken gemaakt en vastgelegd tussen Opdrachtgever en Opdrachtnemer over het door Opdrachtnemer te leveren niveau van dienstverlening. Bovendien worden binnen dit proces de afgesproken service levels bewaakt en gerapporteerd. Om die reden zijn alle eisen vertaald naar (eenvoudig) meetbare en beheersbare service levels.

De vastgelegde normen worden gezien als het minimum niveau van de dienstverlening dat door Opdrachtnemer gegarandeerd wordt.

In de Overeenkomst is vastgelegd wat de dienstverlening met betrekking tot de SOC-dienstverlening "Monitoring & Alarmering" inhoudt. In deze SLA is vastgelegd welke service levels daarbij horen en hoe de service levels worden gemeten.
Hoe de procesgang is tussen Opdrachtgever, Opdrachtnemer, deelnemers en wie de actoren zijn, wordt vastgelegd in het Dossier Afspraken en Procedures (DAP). Deelnemer-specifieke afspraken, zoals contacten en procesinhoudelijke afspraken worden per Deelnemer in een deelnemer-DAP vastgelegd. In geval van strijdigheid in definities en normen zullen de in de SLA genoemde definities en normen prevaleren boven de DAP.

Deze overeenkomst is van kracht voor een deelnemer, vanaf het moment dat deze deelnemer operationeel van de dienstverlening gebruik gaat maken. De looptijd van de SLA is gelijk aan de looptijd van de Overeenkomst.

1.2 Gehanteerde begrippen

In de Overeenkomst is een begrippenlijst opgenomen. De in deze SLA gehanteerde begrippen die met een hoofdletter worden aangeduid refereren naar de begrippenlijsten uit de Overeenkomst en de AWBIT-2023. Daarnaast worden onderstaande begrippen gehanteerd in deze SLA en de DAP.

Alert: Een waarschuwing van een gedetecteerde afwijking die naar het SOC wordt gestuurd.

Case: Een alert met een risiconiveau van 1 of 2 die voor analyse aan een SOC-analist wordt voorgelegd.

Classificatie: Indeling in niveaus die de ernst bepalen van de incidenten en de hierbij afgesproken reactietijd.

Analyse platform, methoden of inzichtverschaffing < in te vullen door opdrachtnemer>: De technologie die het SOC gebruikt voor het analyseren van security-incidenten en het genereren van informatie. Het platform biedt de deelnemers ook informatie over de diensten en de status van de bewaakte infrastructuur, inclusief gedetailleerde incidentrapporten en zoekmogelijkheden.

Detectiedienst: Dienstverlening voor de opvolging (analyse en mitigatieadvies) naar aanleiding van alerts die gegenereerd worden.

Dienst-Incident: Een dienst-incident is verstoring van de dienstverlening die leidt tot gehele of gedeeltelijke niet-beschikbaarheid van functionaliteit of een reductie van kwaliteit of performance, die gerapporteerd wordt aan de opdrachtgever, de deelnemers en het CERT-WM.

Functiehersteltijd: Bij uitval van de dienst: de tijd tussen het melden van een incident en het herstel van de SOC-dienstverlening.

Infrastructuur: De verzameling van computersystemen, netwerkcomponenten en PA-objecten in de infrastructuur van de deelnemers waarop security monitoring & alarmering van toepassing is.

Deelnemer: De partij die is aangesloten op de SOC-dienstverlening.

Managed Detection and Response (MDR): Het geheel van preventie-, detectie- en responsdiensten en de aanpak die mensen, inzichten en technologie samenbrengt in het geïntegreerde dienstenpakket van de opdrachtnemer. Met 24/7 monitoring en alarmering op incidenten gebruikt MDR meerdere verdedigingslinies om de deelnemers te helpen aanvallers voor te blijven en de gevolgen te beperken.

Notificatietijd: De tijd die is gedefinieerd voor het SOC van opdrachtnemer om te reageren op een alert of incident.

Onderhoud: Alle activiteiten die nodig zijn om wijzigingen door te voeren die noodzakelijk worden geacht om de dienstenniveaus operationeel te houden. Dit omvat, maar is niet beperkt tot, aanpassingen aan ontwerp, software en configuraties als gevolg van veranderingen in het beveiligingsprofiel en beveiligingsbeleid van een instelling, infrastructurele en technologische veranderingen of een verschuiving in netwerkverkeerspatronen.

Operationele dienstverlening: Elke deelnemer wordt tijdens een aansluitfase aangesloten op de dienstverlener van de opdrachtnemer. De aansluitfase wordt afgesloten met een acceptatie door de deelnemer van de aansluiting op de dienstverlening. Na acceptatie van de deelnemer, treed de operationele dienstverlening in werking en gelden de in deze overeenkomst overeengekomen afspraken.

Rapportage: Incidenten worden aan de opdrachtgever, deelnemers en het CERT-WM gerapporteerd. In samenspraak met de deelnemers wordt afgesproken of er telefonisch

en/of schriftelijk gerapporteerd wordt over een incident. In tabel 4.2.2. wordt nader toegelicht welke vorm van rapporteren van toepassing is bij betreffende risiconiveaus.

Security Incident: Een security-incident is een case die na analyse wordt bestempeld als succesvolle hack, high risk, medium risk of low risk en die vervolgens wordt gerapporteerd aan de deelnemer en het CERT-WM.

Security Operations Center (SOC): Het zenuwcentrum van <opdrachtnemer> waar alle alerts binnenkomen. Vraagt een alert om nader onderzoek, dan zijn er 24/7 beveiligingsanalisten beschikbaar voor ondersteuning en onderzoek.

Sensor: Een probe of sonde in het netwerk die is verbonden met een sensorserver die al het passerende verkeer analyseert.

SIEM: Afkorting voor Security Incident & Event Management. Op een SIEM-platform worden databronnen ontsloten en geanalyseerd. De informatie uit deze databronnen wordt onderzocht op afwijkingen.

Storing: Een ongeplande onderbreking in de beschikbaarheid van de SOC-dienstverlening.

Werkdag: Elke dag in een kalenderjaar, met uitzondering van zaterdagen, zondagen en (nationale) feestdagen.

1.3 Randvoorwaarden

Beide Partijen zijn gehouden de procedures en afspraken op te volgen die in de DAP zijn overeengekomen. Indien de Opdrachtgever of de Deelnemers deze procedures en afspraken niet opvolgen en de Opdrachtnemer daardoor voor (een deel van) de dienstverlening niet in staat is het service level te halen, wordt dat betreffende deel van de Prestatie niet meegenomen in de bepaling van het gehaalde service level.

De Opdrachtgever en de Opdrachtnemer hebben wederzijds de verplichting elkaar tijdig te attenderen op de gemaakte afspraken en welke consequenties het niet nakomen van deze afspraken tot gevolg hebben.

1.4 Beheer en onderhoud van de SLA

Periodiek zal een evaluatie en eventuele bijstelling van de hoogte van de service levels plaatsvinden. Tegelijkertijd kan ook een uitbreiding of inkrimping van het aantal service levels of de scope van de dienstverlening plaatsvinden.

De beheerders van de SLA zijn de Service Delivery Manager van hWh en de Service Coördinator van de Opdrachtnemer. Wijzigingsvoorstellen worden door de beheerders van de SLA ter goedkeuring voorgelegd aan Contractmanager van hWh en aan de Servicemanager van de Opdrachtnemer.

2 Servicedefinitie

2.1 Inleiding

De servicedefinitie geeft een high level-beschrijving van de dienstverlening. In het vervolg van deze SLA is de scope van de dienstverlening beschreven, evenals de normering. Voor de procedures en nadere afspraken wordt verwezen naar het DAP.

2.2 Scope van de dienstverlening

Deze overeenkomst heeft betrekking op de SOC-dienstverlening die opdrachtnemer aan de Deelnemers levert zoals in deze overeenkomst gespecificeerd.

De scope van de dienstverlening betreft het leveren van dienstverlening (zowel technische oplossing als operationele uitvoering) voor de volgende SOC-processen:

- Monitoring – Het vinden en analyseren van mogelijke cyberbeveiligingskwetsbaarheden, -aanvallen en -incidenten (cf. "Detect" uit het NIST Cybersecurity Framework 2.0)
- Alarmering - Actie ondernemen met betrekking tot een gedetecteerd cyberbeveiligingskwetsbaarheid en -incident (cf "Respond" uit het NIST Cybersecurity Framework 2.0

SOC-dienstverlening omvat de mensen, de procedures en de middelen die nodig zijn om beveiligingsincidenten op de aangesloten netwerken en systemen te signaleren, te analyseren en te adviseren over maatregelen en opvolgacties aan de deelnemers en hWh. Deze diensten worden geleverd door de opdrachtnemer.

2.3 Inhoud van de dienstverlening

Deze SOC-dienstverlening heeft als doel om detectie van digitale dreigingen en/of afwijkend gedrag, en de response hierop toekomstbestendig uit te voeren, zodat de Deelnemers hiermee hun cyberweerbaarheid vergroten.

De volgende (beheer)diensten zijn onderdeel van de Overeenkomst:

Security Monitoring

- Inrichten en operationeel werkend houden van security monitoring op basis van de overeengekomen security use cases en detectie van afwijkend gedrag op zowel de OT- als de KA-omgeving van de deelnemers;

Security analyse, dreigingskennis en geavanceerde dreigingsopsporing

- Analyse van de ingelezen data, gecombineerd met diepgaande kennis van dreigingen en geavanceerde zoekmechanismen vormen de basis van het onderdeel Alarmering. De detectiemethoden om dreigingen vast te stellen zijn enerzijds gebaseerd op de aanvalsscenario's benoemd in de use cases en anderzijds op het constateren van afwijkingen in de gemonitorde datastromen, anomalie detectie;

Alarmeren bij een incident of gebeurtenis

- Bij een incident wordt een analyse door SOC-analist uitgevoerd, inclusief eerste triage. Dat levert 1 of meerdere oplossingsmogelijkheden op met een advies van de SOC-analist welke oplossing wordt geadviseerd om uit te voeren. De alarmering en advies gaan naar de betreffende afnemer en het CERT-WM. Bij een incidentnemer moet het incident oplossen.

Use Case management

- Optimalisatie en actualisatie van de bestaande geïmplementeerde use cases. Inclusief vernieuwing of aanscherping van de use cases set en nieuwe of verscherpte detectieregels;

- Beheren en doorontwikkeling van voor de watersector relevante security use cases die voorzien zijn van een detectiemechanisme om de monitoring inhoud geven;
- Opnemen in de dienstverlening van use cases die deelnemers en het CERT-WM selecteren als relevant voor de cyberveiligheid. De opdrachtnemer draagt proactief nieuwe use cases en detectieregels aan voor implementatie en adviseert de deelnemers welke use cases vanuit veiligheidsoverwegingen opgenomen kunnen/ moeten worden;

Security Incident Management

- het registreren, analyseren en afhandelen van gebeurtenissen, waaronder incidenten, wijzigingsverzoeken (changes), klachten en Serviceverzoeken;
- Het hebben en openstellen van een Servicedesk;

Penvoering en rapportage over de dienstverlening.

3. Service Normen

3.1 Inleiding

Dit hoofdstuk beschrijft in detail de diensten die onder deze SLA beschreven worden en de normen waaraan deze diensten moeten voldoen. De beschrijving van de werkafspraken wordt opgenomen in het DAP.

We maken in deze SLA onderscheid tussen 2 vormen van gebeurtenissen en bijbehorende service levels:

1. Gebeurtenissen, inclusief incidenten (security-incidenten), voorvloeiend uit de security monitoring als onderdeel van de dienst 'Monitoring & alarmering' waarop een reactie nodig is om de cyberveiligheid van de deelnemers te waarborgen;
2. Gebeurtenissen, inclusief incidenten (dienst-incidenten), voorvloeiend uit het leveren van de SOC-dienstverlening. Deze gebeurtenissen hebben invloed op de geleverde 'Monitoring & Alarmering'-dienst en als afgeleide daarvan een mogelijke invloed op de effectiviteit van de security monitoring.

3.2 Servicevenster

Het servicevenster is de periode per dag waarin de SOC-dienstverlening wordt geleverd. Het geldende servicevenster voor deze overeenkomst is 24 uur per dag, gedurende 7 dagen per week. Dit servicevenster omvat tevens alle feestdagen.

Alle gebeurtenissen die van belang zijn worden binnen het servicevenster opgepakt. Incidentregistratie en afhandeling vindt plaats via een incident managementsysteem <nader in te vullen met opdrachtnemer>.

3.3 Onderhoudsvenster

Werkzaamheden die NIET tot een verstoring/ incident leiden, zijn 'gewoon' beheer-werkzaamheden.

Onderhoud vindt altijd plaats tussen 19.00 en 07.00 (ook onaangekondigd onderhoud in noodgevallen. Het benodigde tijdsframe wordt gezien als onderhoudsvenster).

Bij onderhoud wordt onderscheid gemaakt tussen regulier gepland onderhoud en niet gepland onderhoud. Onder 'niet gepland' onderhoud wordt verstaan die werkzaamheden die ongepland,

onaangekondigd of minder dan 5 dagen van tevoren aangekondigd voor herstel van de dienst of functionaliteit moeten worden uitgevoerd. Niet gepland onderhoud wordt gezien als niet-beschikbaarheid, tenzij in onderling overleg wordt vastgesteld dat de werkzaamheden niet als zodanig worden aangemerkt. Ongepland onderhoud (spoed wijziging) vindt ongepland plaats, afhankelijk van de ernst van het veroorzakende incident. De contactpersoon van een deelnemer zal te allen tijde op de hoogte worden gesteld van ongepland onderhoud. Ongepland onderhoud (spoed wijziging) wordt altijd gevolgd door een analyse naar de oorzaak (root-cause analyse). Deze analyses wordt besproken in het reguliere service-overleg.

3.4 Classificatieniveau en reactietijden

In onderstaande tabel staat de classificatie van gebeurtenissen voorvloeiend uit de security monitoring, leidend tot incidenten die de cyberveiligheid beïnvloeden en de snelheid waarmee de opdrachtnemer op die incidenten reageert.

Classificatie	Omschrijving	Notificatietijd	Rapportagetijd & vorm
Succesvolle hack (Critical)	Een geslaagde, gerichte aanval is uitgevoerd op een systeem hetgeen resulteert in een ernstige inbreuk op de beveiliging, dan wel data exfiltratie wordt waargenomen. De impact hiervan moet zo snel mogelijk worden geminimaliseerd.	10 minuten	45 minuten Incident rapportage mailen aan de deelnemer
Succesvolle inbreuk (Critical)	Er is een inbreuk op de beveiliging die een hoog risico vormt. Directe aandacht is vereist.	10 minuten	45 minuten Incident rapportage mailen aan de deelnemer
High risk	Er is een poging gedaan om door de beveiliging heen te breken. Deze poging is mislukt, omdat de aanval niet succesvol was of omdat een beveiligingsvoorziening de activiteit blokkeerde. De oorzaak hiervan moet worden onderzocht.	1 uur	2 uur Incident rapportage mailen aan de deelnemer
Benign Positive High Risk	Er wordt verdacht gedag geconstateerd (True Positive) dat niet als kwaadaardig hoeft te worden beschouwd. Bijvoorbeeld een penetratietest.	1 uur	2 uur Incident rapportage mailen aan de deelnemer
Malicious Medium risk	Er heeft zich een aanvalspoging voorgedaan maar deze is niet geslaagd. Er is geen actie vereist, maar deze poging kan inzage geven in het dreigings-landschap of in de veiligheid van de eigen omgeving.	4 uur	4 uur Incident rapportage wordt beschikbaar gesteld

False positive Low risk	Er is ten onrechte een alert afgegaan op gedetecteerd gedrag. Dit gedrag bleek tevens na analyse legitiem te zijn.	16 uur	16 uur Conclusie bijgevoegd bij case
Not malicious	Detectie heeft gedrag geobserveerd dat als legitiem wordt bevonden binnen deze omgeving.	16 uur	16 uur Conclusie bijgevoegd bij case

3.5 Prioriteitsbepaling incidenten

Onderstaande prioriteitsbepaling heeft betrekking op de service levels voor het leveren van de dienst. In het leveren van de SOC-dienstverlening onderscheiden we 4 verschillende prioriteiten, waarbij we P1, P2 en P3 zien als incidenten en P4 als vragen en verzoeken. Incidenten en vragen/verzoeken worden gelogd/aangevraagd via <nader te specificeren in overleg met opdrachtnemer>.

Op maandag t/m vrijdag, tussen 09.00 en 17.00 kan telefonisch contact worden opgenomen met contactpersonen van de deelnemers. Tussen 17.00 en 09.00, op zaterdagen, zondagen en nationale feestdagen wordt contact met een deelnemer gelegd zoals overeengekomen in de DAP.

De functiehersteltijd van de verstoring van de dienstverlening start op het moment dat het verstoring is geconstateerd. Als de constatering en melding door een deelnemers wordt gedaan, start de functiehersteltijd op het moment van melding bij de opdrachtnemer.

Prioriteit	Reactietijd	Updatetijd	Geplande functieherstel-tijd
Noodgeval (P1)	10 min.	1 uur	80%<2u, 90%<8u, 99%<16u
Hoog (P2)	1 werk uur	2 werk uren	80%<8u, 99%<48u
Gemiddeld (P3)	2 werk uren	4 werk uren	80%<16u, 99%<60u
Laag (P4)	4 werk uren	1 werkdag	Maximaal 10 werkdagen

Prioriteit 4 vragen worden door deelnemers aangemeld via <nader te specificeren in overleg met opdrachtnemer>. Als een Prioriteit 4 betrekking heeft op een verzoek of een vraag, kan afhankelijk van de aard en de complexiteit van het verzoek of de vraag de doorlooptijd meerdere dagen zijn. In onderling overleg wordt vastgesteld wat een acceptabele tijd is om aan het verzoek of de vraag te voldoen.

In het Delivery Overleg worden incidenten en de adequaatheid van de afhandeling maandelijkse besproken.

3.6 Beschikbaarheid van de dienstverlening

Onder beschikbaarheid van de SOC-dienstverlening verstaan we het percentage van de tijd dat de SOC-dienstverlening beschikbaar is binnen het servicevenster. Dit berekenen we per kalendermaand aan de hand van het aantal beschikbare uren en het aantal geregistreerde uren dat de dienst niet beschikbaar is. Een dienst wordt tevens als niet beschikbaar geregistreerd voor de werkelijke duur van een prioriteit 1 dienst-incident. Het aantal beschikbare uren is het aantal uren in een kalendermaand.

Onderstaande beschikbaarheidseisen gelden voor deze overeenkomst.

Beschikbaarheid	Eis
SOC-dienstverlening	99,99%
Faalfrequentie prioriteit 1	Maximaal 1x per maand
Faalfrequentie prioriteit 2	Maximaal 3x per maand

3.7 Beschikbaarheid meeting

De gerealiseerde maandelijkse beschikbaarheid van de geleverde dienst wordt vastgesteld aan de hand van incidenten die hebben plaatsgevonden. De berekening wordt gedaan op basis van de gegevens uit het incidentenregistratie systeem.

M.a.w. de 100% beschikbaarheid-norm wordt vastgesteld aan de hand van het aantal minuten in de betreffende kalendermaand (bijvoorbeeld 31 dagen = 44.640 minuten). De door incidenten veroorzaakte niet-beschikbaarheid in minuten wordt in mindering gebracht op de 100% norm, waarna het feitelijke beschikbaarheidspercentage voor de betreffende kalendermaand kan worden vastgesteld.

Afspraak is: gedurende de reactietijd (responstijd) en de functieherstelttijd (oplostijd) van een prioriteit 1 incident is er sprake van niet-beschikbaarheid (vanaf melding tot geïmplementeerd en werkende oplossing of work-around).

Van de overeengekomen beschikbaarheidsmeeting worden uitgesloten:

- Calamiteiten, zoals aardbevingen overstromingen, enz.,
- Gebruikersfouten die leiden tot niet-beschikbaarheid van de dienst.
- Activiteiten of handelingen door een derde partij die leiden tot niet-beschikbaarheid van de dienst.
- Indien werkzaamheden niet uitgevoerd kunnen worden door de opdrachtnemer door bijvoorbeeld gebrek aan rechten.

4. Rapportage

4.1 Toelichting

Opdrachtnemer rapporteert over de uitgevoerde werkzaamheden in een digitale vorm via een dashboard of portalfunctie op basis van een (near) real time rapportage.

Deze rapportage bevat minimaal de onderdelen:

- Kwaliteit van de dienstverlening, inclusief te verwachten ontwikkelingen op korte termijn (1 kwartaal vooruit kijkend)
- Incidenten - alle benodigde informatie voor sturing op incidenten (o.a. opgetreden, afgesloten en openstaand)
- Waarschuwingen ter voorkoming van incidenten
- Time to respond van incidenten en waarschuwingen
- False positives - alle benodigde informatie voor sturing op reductie
- Brondata - alle benodigde informatie voor optimalisatie van- en continuïteit in brondata aanlevering
- Trends in de markt
- Lifecycle Management t.a.v. use cases en detectiemechanismen
- Dekkingsgraad van de security monitoring
- Verbetermogelijkheden van de monitoring en response processen

4.2 Communicatiematrix

Naam	Organisatie	Telefoon	Email	Functie	Verantwoordelijkheden en escalatieniveau

4.2 Overlegvormen

Naam overleg	Omschrijving	Frequentie
Service Level Overleg	Overleg om de voortgang en de kwaliteit van de dienstverlening te bespreken	1 x per maand

Naam overleg	Omschrijving	Frequentie
Operationeel overleg	Operationele afstemming over procesgang en onderhanden werkzaamheden	Wordt ingepland op basis van noodzaak
Kwartaal overleg	Elk derde service overleg is een kwartaaloverleg, waarbij tevens de contractmanager van hWh deelneemt.	4 x per jaar

5. Kalibratie van de Service Levels

De Service Levels zullen onderhevig zijn aan verandering: zowel de eisen aan de zijde van Opdrachtgever of deelnemers kunnen veranderen als de eisen en mogelijkheden aan de zijde van Opdrachtnemer. Opdrachtgever en Opdrachtnemer hebben samen het doel om vast te stellen in hoeverre de Service Levels redelijk en billijk zijn, of ze een afspiegeling vormen van de behoeften uit het bedrijfsproces, of ze markconform zijn en of de kosten opwegen tegen het verlangde serviceniveau. Waar en wanneer nodig zal aanpassing van de afspraken plaatsvinden.

Wijzigingsvoorstellen op de SLA worden schriftelijk ingediend en kunnen zowel van hWh (als vertegenwoordiger van de deelnemers) als Opdrachtnemer afkomstig zijn en worden schriftelijk ingediend bij de bij de Service Delivery Manager van opdrachtgever en de servicemanager van opdrachtnemer.

De beheerders van de SLA zijn verantwoordelijk voor eventuele verspreiding van nieuwe ondertekende versies binnen de eigen organisatie naar een ieder die een rol speelt in of een direct belang heeft bij een of van de beschreven afspraken en procedures. Voor verspreiding buiten dit gestelde kader is toestemming nodig van de andere partij.

5.1 Service Delivery Overleg

1 x per kalendermaand zal een service delivery overleg worden gepland tussen opdrachtnemer, hWh en een delegatie van de deelnemers om de geleverde dienst te bespreken, klanttevredenheid en kwaliteit van het werk te evalueren. Uit dit overleg voortvloeiende deelnemer-specifieke-afspraken worden vastgelegd in de deelnemer-DAP.

Ondertekening

Aldus overeengekomen en getekend.

Deze SLA heeft dezelfde looptijd als de looptijd van de Overeenkomst, of tot de eerstvolgende revisie als dit schriftelijk tussen partijen is overeengekomen.

Namens Het Waterschapshuis	Namens Opdrachtnemer
Datum:	Datum:
Handtekening:	Handtekening:
drs. G.J. Smits secretaris-directeur	<naam> <functie>