SLA Overeenkomst behorende tot de Europese aanbesteding SOC (Monitoring & Response) dienstverlening

en

OPDRACHTNEMER

Versie: concept

datum

1 INTRODUCTIE

Deze SLA is overeengekomen tussen SSC ONS en OPDRACHTNEMER ten behoeve van de uitvoering van de tender *<naam en kenmerk>*

Doel van de SLA

Service Center SSC ONS (SSC ONS) heeft met haar partners een Service Level Agreement (SLA) afgesloten. Externe leveranciers dienen altijd minimaal aan deze SLA afspraken te voldoen. Afhankelijk van de in te kopen producten of diensten worden servicelevels vastgelegd en vertaald in zogenaamde kritische prestatie indicatoren (KPIs). Deze KPI's zijn meestal alleen te realiseren wanneer er aan een basis set van onderliggende prestatie indicatoren wordt voldaan. Bijvoorbeeld: De KPI voor een servicedesk is gesteld op het aannemen en verwerken van een door de klant gemeld incident binnen 5 minuten na melding door de klant. Dan is de KPI 5 minuten maar dient de leverancier een tal van prestatie indicatoren te besturen om hieraan te voldoen, zoals voldoende beschikbaar en gekwalificeerd personeel, voldoende vrije telefoonlijnen, een (hoog) beschikbare self service portal enzovoorts. Deze onderliggende indicatoren zijn voor SSC ONS niet van belang maar dienen voor interne sturing van de leverancier. Er is inmiddels een trend waarneembaar naar XLA afspraken (eXperience Level Afspraken), hierbij staat de ervaring van de eindgebruiker centraal en moet deze bijvoorbeeld gemiddeld een 8 (schaal 1-10) geven op de ervaren dienstverlening. Hoe de leverancier dit verder bewerkstelligd is aan de leverancier en ziet men dan als onderliggende prestatie indicatoren.

In deze SLA worden de kwalitatieve en kwantitatieve afspraken met betrekking tot ondersteuning en onderhoud op de door SSC ONS bij OPDRACHTNEMER afgenomen dienstverlening vastgelegd. Deze SLA vormt een integraal onderdeel van de overeenkomst tussen OPDRACHTNEMER en SSC ONS. Het doel is om de twee partijen in staat te stellen om effectief samen te werken.

Versie	0.1
Omschrijving	concept
Modificatiedatum	datum
Auteur	naam

2 ALGEMEEN

2.1 **Uitgangspunten:**

A. OPDRACHTNEMER zorgt voor optimale werking, beschikbaarheid en uitstekende prestaties van geleverde Diensten.

B. OPDRACHTNEMER verleent diensten aan SSC ONS met toewijding aan klanttevredenheid en gepersonaliseerde ondersteuning en zal voortdurend investeren in het verwerven en behouden van vereiste expertise binnen haar organisatie.

C. Het softwareonderhoud van het aangeboden portaal zal door OPDRACHTNEMER worden verzorgd.

2.2 **Te leveren diensten:**

<opsomming van te leveren diensten, niet limitatief>

		Wat:	**Toelichting**
1	***Hosting***	Omvat alle diensten welke te maken hebben met het (technisch) beschikbaar maken en houden van de dienst voor SSC ONS, inclusief het technisch beheer en de support op het beschikbaar zijn van het portaal.	Het portaal wordt 24/7 automatisch bewaakt.
2	***Support***	- 1ste en 2de lijn support voor technische ondersteuning en probleembeheer. - 3e lijn support zal worden ondersteund in samenwerking met leverancier software - In *<naam portal>* is informatie opgenomen zoals handleidingen, releasenotes en configuratiedocumenten	De intake van incidenten/problemen en informatievragen, volgens afgesproken servicelevels. Het indienen van incidenten geschiedt via het supportportaal van OPDRACHTNEMER. Deze is 24/7 beschikbaar. Documentatie wordt door OPDRACHTNEMER in portal geplaatst. Geautoriseerde medewerkers van SSC ONS hebben leesrechten.
3	***Incidenten-beheer***	Het neutraliseren van een incident al dan niet door middel van een work around;	Het afhandelen, beheren en verhelpen van incidenten, volgens afgesproken servicelevels. In het geval van het toepassen van een work around wordt daarna via onderhoud en beheer gewerkt aan de structurele dienst.

			Incidenten met prioriteit P1 en P2 moeten altijd telefonisch gemeld worden, dit kan gedurende kantoortijden en piket window.
4	***Onderhoud & beheer***	Software onderhoud	De release van nieuwe versies, patches en / of releases om: - Te voldoen aan beveiligingsstandaarden; - Het structureel oplossen van eerder gesignaleerde problemen; - Het voorkomen van (toekomstige) storingen; - Het verbeteren van functionaliteit en / of prestaties.
5	***SOC-diensten***	Omvat alle diensten die te maken hebben met het monitoren van de digitale infrastructuur van SSC ONS	Betreft activiteiten zoals: - Actieve en realtime monitoring & detectie van dreigingen en security incidenten; - Analyse en onderzoek; - Kwalificatie & triage meldingen; - Threat response advies; - Advies en optimalisatie digitale weerbaarheid SSC ONS;
5	***Rapportage***	Regulier te verstrekken rapportages	Betreft rapportage's zoals beschreven in H11.
6	***…***		

2.3 KPI's

Aan elke KPI is een norm gekoppeld, die de minimaal te behalen grenswaarde van de KPI aangeeft. Aan normen zijn sancties gekoppeld, die gelden als de norm niet wordt behaald.
Ten aanzien van de KPI's die in deze SLA worden genoemd gelden de volgende algemene bepalingen:

- De KPI's zijn gebaseerd op het Programma van Eisen;
- Alle KPI's en normen worden gemeten en beoordeeld over een periode. De perioden zijn bij de KPI aangegeven.
- De gerealiseerde KPI's worden periodiek door OPDRACHTGEVER gerapporteerd.
- In de rapportages is duidelijk zichtbaar welke KPI's wel of niet behaald zijn

Er kunnen redenen zijn om situationeel en/of tijdelijk af te wijken van de KPI Normen. Afwijken zal in onderling overleg tussen OPDRACHTGEVER en SSC ONS plaatsvinden. SSC ONS dient akkoord te gaan met de afwijking. De afspraken met betrekking tot een afwijking, waaronder de norm, de tijdsduur en kosten, worden schriftelijk vastgelegd.

3 BESCHIKBAARHEID

OPDRACHTNEMER streeft een hoge beschikbaarheid (uptime) na waarbij *<applicatie/software/services>* langdurig zonder storingen zullen werken. Het systeem is volledig getest. Er zijn voorzieningen ter voorkoming van storing in de vorm van redundante componenten.

3.1 Toelichting op beschikbaarheidseisen (uptime)

- De afgenomen service **moet** bestand zijn tegen storingen (resilient) waarbij storingen direct worden verholpen.
- Geplande downtime wordt niet meegerekend bij het bepalen van de beschikbaarheid, geplande downtime moet ten minste 5 werkdagen op voorhand worden gecommuniceerd door OPDRACHTNEMER. Uitzonderingen daargelaten zal geplande downtime buiten kantooruren van SSC ONS worden gepland.
- OPDRACHTNEMER levert maandelijks een beschikbaarheidsrapport op.

3.2 Beschikbaarheid KPI's

OPDRACHTNEMER Support en de SSC ONS komende volgende beschikbaarheid overeen:

KPI 1: Beschikbaarheid portaal	
Doel	Dienst is beschikbaar voor gebruik en bedient de overeengekomen functionaliteit en kwaliteit.
Meetmethodiek	Beschikbaarheid berekend per maand. Uptime systemen minus geplande downtime minus ongeplande downtime gedeeld door maximale uptime gedurende rapportageperiode.
Norm	95,0 % 24 uur per dag, 7 dagen per week

4 SUPPORT

4.1 Uitgangspunten

A. OPDRACHTNEMER verklaart vooraf dat hij, daartoe door SSC ONS uitgenodigd, bereidt is om met SSC ONS en mogelijk derde betrokken partijen te overleggen om oorzaken van storingen of onbevredigende werking van de geleverde software op te sporen en te verhelpen.

B. Mocht blijken dat de storingen of onbevredigende handelingen niet kunnen worden toegeschreven aan de door OPDRACHTNEMER geleverde software, dan worden de verbonden kosten van OPDRACHTNEMER alleen vergoed indien deze tussen Partijen zijn overeengekomen.

4.2 OPDRACHTNEMER Support

Er wordt een Nederlandstalige supportdesk geboden voor zowel technische als functionele ondersteuning. De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie inzicht in de afhandeling daarvan en is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de dienst. De helpdesk levert zowel telefonische ondersteuning of vergelijkbaar zoals Microsoft Teams, als ondersteuning via e-mail en een supportsite.

Het SOC van OPDRACHTNEMER is 24 uur per dag, 7 dagen per week, beschikbaar voor het identificeren, vaststellen, analyseren van security incidenten en geven van mitigatie-advies.

De supportdesk wordt zoveel mogelijk gebruikt voor (urgente) incidenten en is op werkdagen minimaal bereikbaar tijdens kantooruren van 7:00 uur tot 17:00 uur.

Prioriteit 1 (P1) (security) incidenten dienen te allen tijde naast schriftelijk ook telefonisch gemeld te worden!

Naast de openingstijden van de Servicedesk en SSC ONS Piketdienst is Security 24/7 bereikbaar voor P1 en P2 geclassificeerde security incidenten.

SSC ONS heeft na kantoortijden een Piketdienst. De openingstijden hiervan staan in onderstaande tabel:

Openingstijden Servicedesk	
Maandag t/m vrijdag	07.00 – 17.00
Openingstijden SSC ONS Piketdienst	
Maandag t/m vrijdag	17.00 – 22.00
Weekend en feestdagen	10.00 – 22.00
Openingstijden Security Incident Management	
Maandag t/m vrijdag	24/7
Weekend en feestdagen	24/7
Reactietijden SSC ONS Piketdienst & Security Incident Management	
Telefoon	90% reactie binnen 30 minuten

P1 en P2 (security) incident buiten kantoortijd:

- Verifiëren oplossing incident bij SSC ONS kan tot uiterlijk 22:00 uur. Voor security incidenten geldt 24/7 beschikbaarheid voor P1 en P2 security incidenten.
- Indien assistentie voor reguliere incidenten benodigd is van SSC ONS kan dit tot uiterlijk 22:00 uur, daarna wordt het incident “on hold” gezet tot de volgende werkdag

- P1 en P2 incidenten gemeld vanuit monitoring worden 24/7 opgepakt, SSC ONS is bereikbaar volgens tabel hierboven.

Overdracht van tickets van 24/7 naar kantoortijd is geborgd zowel binnen OPDRACHTNEMER als SSC ONS.

4.3 Support site

De supportsite van OPDRACHTNEMER is bereikbaar via <link> en is 24/7 bereikbaar. De servicedesk- en technisch applicatiebeheer en security medewerkers van SSC ONS ontvangen van een geautoriseerd contactpersoon een gebruikers-ID en wachtwoord waarmee toegang verkregen kan worden tot de supportsite. Op deze site kan SSC ONS incidenten melden, de voortgang van gemelde incidenten monitoren en informatievragen stellen. Meldingen kunnen ook per e-mail via het adres <emailadres> worden ingediend. De gegevens die minimaal moeten worden ingevoerd staan beschreven in het DAP.

KPI 3: Beschikbaarheid serviceportaal OPDRACHTNEMER	
Doel	Kunnen melden van incidenten en verzoeken
Meetmethodiek	Aantal minuten dat serviceportaal niet beschikbaar was gedurende kantoortijden beschikbaarheid berekend per maand.
Norm	99%

BELANGRIJK

Gegeven het intensieve karakter van de te verwachten dienstverlening tussen SSC ONS en OPDRACHTNEMER wordt t.a.v. deze dienst een koppeling verwacht waarbij bi-directionele communicatie mogelijk is tussen het servicemanagement systeem van SSC ONS, zijnde TOPdesk, en het service management systeem van OPDRACHTGEVER voor minimaal incidenten en wijzigingsverzoeken bij voorkeur via een standaard API zonder maatwerk.

5 INCIDENTENBEHEER - GENERIEK

Een incident kan betrekking hebben op de dienst of dienstverlening omtrent het portaal. Het kan het melden van een fout zijn of het stellen van een vraag over de dienst. Indien een incident een gebruikers- of configuratievraag betreft, zal deze vraag direct worden behandeld door de supportmedewerker. ONS ontvangt van elk incident een bevestiging voorzien van het incidentnummer. Dit incidentnummer is uniek en dient als referentie bij correspondentie met OPDRACHTGEVER met betrekking tot het incident.

5.1 KPI-normen

KPI 2: Oplostijden incident management generiek	
Doel	Garantie op spoedig herstel van voorkomende verstoringen.
Meetmethodiek	Alle geregistreerde en afgesloten incidenten in rapportage periode per maand waarbij wordt aangegeven of deze binnen of buiten norm vallen.
Norm	90% van alle P1 incidenten is opgelost binnen 4 klokuur. 90% van alle P2 incidenten is opgelost binnen 8 werkuur 90% van alle P3 incidenten is opgelost binnen 2 werkdagen 90% van alle P4 incidenten is opgelost binnen 5 werkdagen 90% van alle P5 incidenten is opgelost binnen 10 werkdagen Voor alle prioriteiten geldt dat de resterende 10% incidenten binnen 2x de geldende oplostijd is opgelost.

Partijen komen overeen dat bij de volgende impact definities de volgende response- en oplostijden van toepassing zijn:

Impact	Situatie	Respons Tijd	Oplos Tijd
1: Kritisch - Dienst is down zonder herstart mogelijkheid of work around en/of - Bedrijfskritieke interfaces down zonder herstart dienst of work around en/of - Groot aantal getroffen gebruikers (~ 50%), volledige uitval dienstverlening één of meerdere partners.	De dienst kan niet worden gebruikt, is niet operationeel; kritische impact op de hostingomgeving; situatie vereist onmiddellijke actie.	2 uur	4 klokuur
2: Hoog - Applicatie issue waarbij work around mogelijk is en/of - Meerdere gebruikers over meerdere partners getroffen en/of - Systeeminterfaces niet beschikbaar	De dienst kan niet worden gebruikt is wel operationeel, maar heeft ernstige beperkingen; een work around is beschikbaar, situatie vereist snel herstel.	4 klokuur	8 werkuur
3: Medium - Kleinere systeemproblemen, ernstige performance degradatie en/of - Kritische bugfix met work around en/of - Lage impact op gebruikers-organisatie	De applicatie is beperkt operationeel met ernstige hinder.	4 werkuur	2 werkdagen
4: Laag - Kleinere systeemproblemen, performance degradatie en/of. - Niet-kritische bugfix met work around en/of - Geen directe impact op gebruikers-organisatie	De applicatie is operationeel met beperkte hinder.	2 werkdagen	5 werkdagen
5: Info - Rapportages - Informatievragen - Suggesties	Er zijn wensen met betrekking tot verbeteringen aan de applicatie (> 8 uur)	4 werkdagen	10 werkdagen

5.2 Technische ondersteuning

De OPDRACHTGEVER benoemt één of meer contactpersonen die gemachtigd zijn om incidenten te melden. Deze functies van deze personen zijn opgenomen in de communicatiematrix vastgelegd in het DAP. Deze personen krijgen de beschikking over een persoonlijke toegangscode en wachtwoord waarmee toegang wordt verkregen tot het supportportaal.

Er dienen meerdere contactpersoon te worden toegekend die bij calamiteiten het directe aanspreekpunt. Deze functies van deze personen zijn opgenomen in de communicatiematrix. Deze personen zijn in het DAP benoemd.

Indien een medewerker uit dienst treedt bij SSC ONS, stelt de SSC ONS OPDRACHTNEMER daarvan tijdig op de hoogte, waarna OPDRACHTNEMER zal zorgdragen voor het per direct uitschrijven van de betreffende medewerker voor toegang tot de support site.

5.3 Calamiteiten

OPDRACHTNEMER stelt het doel om de beschikbaarheid, integriteit en vertrouwelijkheid van haar systemen en informatie te borgen en continueren. OPDRACHTNEMER hanteert daarom een continuïteitsplan om de impact van calamiteiten te kunnen opvangen en de bedrijfscontinuïteit van haar en haar klanten zo goed mogelijk te kunnen borgen.

Daar waar in de risicoanalyse van OPDRACHTNEMER preventieve maatregelingen worden opgesteld voor risico's, wordt in het continuïteitsplan reactieve maatregelen beschreven voor de continuïteit van bedrijfsprocessen in geval van een calamiteit. Het kan voorkomen dat tijdens het voordoen van een calamiteit alsnog wordt afgeweken van dit continuïteitsplan om de veiligheid van mensen, systemen en informatie beter te waarborgen.

Na het opstellen van het continuïteitsplan zal het jaarlijks geactualiseerd worden. Het bespreken van de geactualiseerde continuïteitsplan wordt minimaal jaarlijks besproken op strategisch niveau.

Notities

- ***Incident Respons tijden:*** Reactietijd: de tijd tussen het moment waarop een storing aan OPDRACHTNEMER wordt gemeld en het moment waarop OPDRACHTNEMER begint met het repareren van de storing.
- ***Incident Oplostijd***: Hersteltijd: de tijd tussen het moment waarop een storing wordt gemeld en het moment waarop gemeld wordt dat de storing is hersteld.
- Ten aanzien van de inhoudelijke reactie van P1 incidenten, wordt opgemerkt dat deze bestaat uit een probleemanalyse, een oplossing dan wel indien mogelijk een work-around voor het incident. Ook voor prioriteit 2 en 3 incidenten geldt dat, indien niet kan worden voldaan aan gestelde eisen, er een work-around wordt aangeboden.
- Incidenten welke buiten de normale openingstijden van de helpdesk zijn aangemeld zullen de eerstvolgende werkdag in behandeling worden genomen met uitzondering van de P1 incidenten. Een reactie volgt dan op basis van de prioriteit van het incident. Om de hersteltijd te kunnen garanderen dient de melder beschikbaar te zijn voor het beantwoorden van eventuele vragen.

6 SECURITY INCIDENT MANAGEMENT

Een security incident kan betrekking hebben op de dienst of dienstverlening. Het kan gaan om een datalek, een hack, zero-day of ransom, etc. Een security incident kan gemeld worden door SSC ONS of door OPDRACHTGEVER. In geval van melding door OPDRACHTGEVER verwacht SSC ONS dat triage al gestart is.

SSC ONS ontvangt van elk incident een bevestiging voorzien van het incidentnummer. Dit incidentnummer is uniek en dient als referentie bij correspondentie met OPDRACHTGEVER met betrekking tot het incident.

6.1 Responsetijden

Kerncijfers:

KPI 3: Responstijden security incident management naar prioriteit	
Doel	Inzicht geven in reactiesnelheid security incidenten.
Meetmethodiek	Alle geregistreerde en afgesloten security incidenten in rapportage periode per maand waarbij wordt aangegeven of deze binnen of buiten norm vallen.
Norm	95% van alle P1 incidenten wordt *onmiddellijk* gereageerd. 95% van alle P2 incidenten wordt gereageerd binnen 30 minuten. 95% van alle P3 incidenten wordt gereageerd binnen 1 klokuur. 95% van alle P4 incidenten wordt gereageerd binnen 2 werkuur. 95% van alle P5 incidenten wordt gereageerd binnen 8 werkuur. Voor alle prioriteiten geldt dat de resterende 5% incidenten binnen 2x de geldende reactietijd is gereageerd.

KPI 4: Mitigatie advies security incidenten naar prioriteit	
Doel	Inzicht geven in de snelheid van het opleveren van een adequaat mitigatie advies
Meetmethodiek	Alle geregistreerde en afgesloten security incidenten in rapportage periode per maand waarbij wordt aangegeven of deze binnen of buiten norm vallen.
Norm	90% van alle P1 incidenten is adequaat mitigatie advies bekend binnen 1 klokuur. 90% van alle P2 incidenten is adequaat mitigatie advies bekend binnen 1 klokuur. 90% van alle P3 incidenten is adequaat mitigatie advies bekend binnen 2 werkuur. 90% van alle P4 incidenten is adequaat mitigatie advies bekend binnen 1 dag. 90% van alle P5 incidenten is adequaat mitigatie advies bekend binnen 2 dagen. Voor alle prioriteiten geldt dat de resterende 10% incidenten binnen 2x de geldende oplostijd is opgelost.

KPI 5: Emergency capaciteit beschikbaar	
Doel	Capaciteit beschikbaar stellen t.b.v. ondersteuning forensisch onderzoek derden partij
Meetmethodiek	Alle capaciteitsverzoeken binnen 1 kwartaal
Norm	90% van alle capacteitsverzoek wordt binnen 2 uur gehonoreerd

Partijen komen overeen dat bij de volgende impact definities de volgende respons- en mitigatie adviestijden van toepassing zijn:

Impact	Situatie	Respons Tijd	Oplevering mitigatie advies
1: Kritisch - Dienst is down zonder herstart mogelijkheid of work around en/of - Bedrijfskritieke interfaces down zonder herstart dienst of work around en/of - Groot aantal getroffen gebruikers (~ 50%), volledige uitval dienstverlening één of meerdere partners.	Kritieke service(s) verstoord, dienst kan niet worden gebruikt, kritische impact op de hosting omgeving; situatie vereist directe actie. Groot datalek, directe melding bij autoriteiten	Onmiddellijk	1 klokuur
2: Hoog - Applicatie issue waarbij work around mogelijk is en/of - Meerdere gebruikers over meerdere partners getroffen en/of - Systeeminterfaces niet beschikbaar	De dienst kan niet worden gebruikt is wel operationeel, maar heeft ernstige beperkingen; een work around is beschikbaar, situatie vereist snel herstel. Eén of meer services verstoord, en/of verlies van (privacy) gevoelige informatie	30 minuten	1 klokuur
3: Medium - Kleinere systeemproblemen, ernstige performance degradatie en/of - Kritische bugfix met work around en/of - Lage impact op gebruikers-organisatie	De applicatie is beperkt operationeel met ernstige hinder. Minimale impact op gebruikers, de organisatie kan zijn kritieke diensten nog leveren. Geen gevoelige en/of persoons-gegevens gelekt.	1 werkuur	2 werkuur
4: Laag - Kleinere systeemproblemen, performance degradatie en/of. - Niet-kritische bugfix met work around en/of - Geen directe impact op gebruikers-organisatie	De applicatie is operationeel met beperkte hinder. Impact op continuïteit is minimaal, geen dataverlies of risico op een datalek.	2 werkuur	1 werkdag
5: Info - Rapportages - Informatievragen - Suggesties	Er zijn wensen met betrekking tot verbeteringen aan de applicatie (> 8 uur)	8 werkuur	2 werkdagen

Notities

- ***Security Incident Responstijden:*** Reactietijd: de tijd tussen het moment waarop een security incident wordt opgemerkt door OPDRACHTNEMER of aan OPDRACHTNEMER wordt gemeld door SSC ONS en het moment waarop OPDRACHTNEMER begint met de triage voor het opleveren van het mitigatie advies.
- ***Oplevering mitigatie advies***: Doorlooptijd: de tijd tussen het moment waarop een security incident wordt opgemerkt door OPDRACHTNEMER of aan OPDRACHTNEMER wordt gemeld door SSC ONS en het moment waarop het mitigatie advies aan SSC ONS wordt opgeleverd.

7 HOSTING

Een Cloud dienst is een totaal dienst (ook wel Infrastructure-as-a-Service genoemd) waarbij hardware, beheer, licenties en verbindingen aangeboden en onderhouden worden door de leverancier.

7.1 Hosting Platform

OPDRACHTNEMER SaaS wordt gehosted in een (Tier 3) datacenter in Nederland. Hierbij zijn alle noodzakelijke maatregelen aanwezig voor een optimale uptime, performance en fallback.

7.2 Dienst specifieke KPI's

BELANGRIJK

Het staat OPDRACTHGEVER vrij hier dienst specifieke KPI's op te nemen die een bijdragen leveren aan de toegevoegde waarde van door OPDRACHTGEVER geleverde dienst.

8 BACKUPS

Gegevensback-up wordt gedefinieerd als het onderhouden van een of meer versies van inhoud in een fysiek en logisch gescheiden systeem. Deze gegevens zijn bedoeld om snel toegankelijk te zijn om inhoud te vervangen die beschadigd is, corrupt raakt of per ongeluk verwijderd is. Hersteltijddoelen en beschreven herstelpuntdoelen zijn maximale waarden.

Kerncijfers	Norm
Gedocumenteerd back-upbeleid	Aanwezig
Retentie SLA	60 dagen
RPO SLA	24 uur
RTO SLA	2 uur
Backup isolatie	Aanwezig
PITR SLA	Aanwezig

8.1 Overzicht back-upvereisten

Level	Beschrijving
1	Er is een gedocumenteerd back-upbeleid voor alle gegevens. Er moet een back-up van 60 dagen worden onderhouden, met een doelstelling van 2 uur **hersteltijd** (**RTO**) en een doelstelling van maximaal 24 uur **herstelpunt** (**RPO**). Er moeten stappen worden genomen om ervoor te zorgen dat de back-up niet op dezelfde omgeving wordt gehost als de primaire gegevens (back-upisolatie). **Point-In-time-Recovery**, kortweg PITR, betekent dat data vanaf een backup teruggehaald kan worden tot een willekeurig moment. In de praktijk betekent dit dat je in een geval van een incident een database (in de meeste gevallen) kunt herstellen tot vlak voor het moment dat het incident zich voordeed.

8.2 Noodherstel (Disaster Recovery - DR)

Noodherstel omvat een reeks beleidsmaatregelen, hulpmiddelen en procedures om het herstel of de voortzetting van het proces c.q. technische infrastructuur en toepassingen mogelijk te maken na een natuurlijke of door de mens veroorzaakte ramp.

Kerncijfers	Norm
DR policy	Aanwezig
Business Continuity Draaiboek	Overeengekomen
DR Testing	Jaarlijks

9 SECURITY

SSC ONS en OPDRACHTNEMER hechten grote waarde aan de beveiliging van de gegevens die in de dienst worden gebruikt en verwerkt. Standaard is de dienst voorzien van een aantal technische maatregelen om in de beveiliging van deze gegevens te voorzien. Voorbeelden van deze technische maatregelen zijn logging en logische toegangsbeveiliging.

Een goede beveiliging rust op een stelsel van maatregelen dat is opgebouwd uit de passende combinatie van technische, organisatorische en procedurele maatregelen. Daarbij is het van belang te kijken naar de risico's ten aanzien van de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in de te vormen situatie van de Dienst ten behoeve van en in gebruik door de Opdrachtgever.

9.1 Verwachtingen bij response op beveiligingsincidenten

Incidentrespons is een georganiseerde aanpak voor het aanpakken en beheren van de nasleep van een beveiligingslek of cyberaanval, ook bekend als een IT-incident, computerincident of beveiligingsincident. Het doel is om de situatie op een manier aan te pakken die schade beperkt en hersteltijd en -kosten vermindert.

Security incidenten volgen het standaard incident management proces maar worden apart geidentificeerd en geclassificeerd.

9.2 Aantoonbaarheid naleving informatiebeveiliging

Onderzoek:

- Jaarlijks wordt door OPDRACHTNEMER een pentest uitgevoerd op onderdelen die voor de SSC ONS relevant zijn. De SSC ONS ontvangt een verslag met bevindingen en het plan van aanpak voor de opvolging.
- Minimaal eens per jaar wordt een kwetsbaarheidsscan uitgevoerd op de onderdelen die voor de SSC ONS relevant zijn. De SSC ONS ontvangt een verslag met bevindingen en het plan van aanpak voor de opvolging.
- Minimaal eens per jaar wordt een disaster en recovery-test uitgevoerd.

Status van de opvolging n.a.v. uitgevoerde pentest en kwetsbaarheidsscan Verdere afspraken die gelden:

- Versies van de software worden voor de in productiename door de leverancier onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.).
- Applicaties worden ontwikkeld en getest op basis van landelijke normen en richtlijnen voor beveiliging, zoals de richtlijnen voor beveiliging van webapplicaties. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de Open Web Application Security Project (OWASP) top 10.
- De leverancier geeft transparant en kostenloos inzicht in certificeringsdocumenten en rapportages opgesteld door EDP-auditors.
- Leverancier staat er voor in dat met de ICT Prestatie door Opdrachtgever kan worden voldaan aan de Baseline Informatiebeveiliging Overheid (ISO 27001/2). Leverancier staat er ook voor in dat het door hem ingeschakelde personeel en andere derden zullen werken overeenkomstig de overeengekomen normen voor informatiebeveiliging.

10 ONDERHOUD EN BEHEER

De diensten voor onderhoud en beheer worden door OPDRACHTNEMER op afstand uitgevoerd. Indien onderhoud en beheer op locatie moet worden uitgevoerd zal dit in overleg gaan en SSC ONS zal hieraan medewerking verlenen.

10.1 OPDRACHTNEMER Monitoring

Door monitoring ontstaan veel minder supporttickets want OPDRACHTNEMER is de meldingen voor. Het Bestaat concreet uit:

- 24/7 monitoring van door OPDRACHTNEMER geleverde Dienst.
- Bij afwijkingen wordt OPDRACHTGEVER direct geïnformeerd.
- De volgende onderdelen worden gemonitord:
  - Het 'live zijn' van de applicatie
  - Aantal gebruikers
  - Response tijd
  - Audit failure(s) (7 dagen / 1 dag / 1 hr)
  - Detectie van ongewenste pogingen tot inloggen

10.2 Definities

Onderhoud en beheer vindt plaats op basis van de onderstaande definities:

Definitie	Beschrijving
Proactief en planmatig onderhoud	Onderhoud om verstoringen te voorkomen, te voldoen aan wettelijke vereisten, veranderende infrastructuur en op basis van in de DAP vast te leggen releasekalender het bieden van nieuwe functionaliteiten.
…	

Notities:

- De intiële respons van een consulant op een changeverzoek door de juiste functionaris van opdrachtgever zal binnen 5 werkdagen plaatsvinden. De daadwerkelijke uitvoering van de change zal in overleg met de cSSC ONSulant worden bepaald, echter het moment van uitvoering zal zoveel mogelijk in lijn met in de DAP vastgestelde momenten van het releaseschema plaatsvinden.

KPI 6: Opleveren offerte n.a.v. wijzigingsverzoek	
Doel	Inzicht geven in impact, kosten en doorlooptijd niet-standaard wijzigingsverzoek
Meetmethodiek	Aantal geregistreerde niet-standaard wijzigingsverzoek waarbij binnen 5 dagen na ontvangstdoor OPDRACHTGEVER een adequate respons in de vorm van een offerte is afgegeven.
Norm	100% binnen 5 dagen

10.3 Termijnen

1. Voor al het onderhoud en in ieder geval het planmatige en adaptieve onderhoud, geldt dat dit zoveel mogelijk buiten de kantoortijden van SSC ONS plaatsvindt
2. Geplande onderhoudsactiviteiten worden minimaal 10 werkdagen van tevoren schriftelijk aangekondigd bij SSC ONS.
3. Voor het oplossen van urgente productieverstoringen (Calamiteiten) kunnen ad-hoc crashreleases worden ingepland; dit gebeurt uitsluitend na goedkeuring van de Opdrachtgever.

10.4 Kosten van releases

In het geval van kleine aanpassingen (< 8 uur en/of binnen overeengekomen supporturen dekking) zijn er geen additionele kosten bij doorvoer van de nieuwe versie of release. Indien blijkt dat een nieuwe versie of release grote impact heeft (> 8 uur en/of buiten overeengekomen supporturen dekking) dan kan de nieuwe versie of release op basis van begroting en tegen additionele kosten worden uitgevoerd. Dit kan alleen na schriftelijk akkoord door SSC ONS.

11 RAPPORTEREN

OPDRACHTNEMER levert rapportages aan de conform onderstaande:

Onderwerp	Frequentie
KPI's beschikbaarheid	Maandelijks, incl. korte toelichting
(Security) Incidentenbeheer	Maandelijks, inclusief response- en remediatietijden
Alle overige KPI's	Maandelijks, incl korte toelichting
Wijzigingenbeheer	Per kwartaal, inclusief forecast komende kwartaal

Security	- Incidenten (incl. datalekken)
	- Capaciteitsbeheer
	- Back-up
	- Informatiebeveiliging:
	  ○ Uitgevoerde pentesten (incl status opvolging)
	  ○ uitslag uitgevoerde kwetsbaarheidsscans (incl. status opvolging)
	  ○ Uitslag disaster recoverytest
	  ○ Uitkomst jaarlijkse security scan

KPI 7: Opleveren rapportages	
Doel	Tijdige beschikbaarheid rapportages.
Meetmethodiek	Alle rapportages binnen overeengekomen servicelevel beschikbaar voor SSC ONS via portaal of verzonden via mail naar contactpersonen.
Norm	Binnen 10 werkdagen na de eerste dag van de maand (of kwartaal).

12 VERANTWOORDELIJKHEDEN

OPDRACHTNEMER draagt zorg voor:

1. Adequate en ter zake kundige dienstverlening
2. Ondersteuning
3. Tijdige rapportage van bevindingen
4. Adequate afhandelingen van incidenten en problemen conform gemaakte afspraken
5. Beschikbaarheid van het onlinesupportsysteem ten behoeve van het melden van incidenten en indienen van wijzigingsverzoeken (Software Change Request)

12.1 Wijzigen van de SLA

Een SLA komt tot stand door rechtsgeldige ondertekening van de overeenkomst tussen SSC ONS en OPDRACHTNEMER of door de feitelijke aanvang van onder deze SLA vallende werkzaamheden door OPDRACHTNEMER met toestemming van SSC ONS.

De SLA kan gewijzigd worden door het indienen van een verzoek daartoe door zowel SSC ONS als OPDRACHTNEMER. Een dergelijk verzoek wordt door partijen rechtsgeldig ondertekend alvorens de wijziging op de SLA in werking treedt.

OPDRACHTNEMER is verantwoordelijk voor het (versie)beheer van deze SLA.

13 OVERLEGSTRUCTUREN

Beide partijen zullen in het overleg worden vertegenwoordigd door de contactpersonen (zie Hoofdstuk 14 Contactpersonen). OPDRACHTNEMER verzorgt het verslag van elk overleg. Het verslag wordt uiterlijk 10 werkdagen na het overleg aan SSC ONS via verzonden of beschikbaar gemaakt via een potaal.

Serviceoverleg (operationeel)

- minimaal 4 keer per jaar
- Bespreken van de rapportages (zie hoofdstuk 11 rapporteren), de verbetervoorstellen en de wederzijdse ontwikkelingen op korte en middellange termijn. De rapportages bevatten de relevante parameters voor alle in het SLA genoemde dienstverlening.

Service review (strategisch), jaarlijks

- Bespreken van de wederzijdse ontwikkelingen middellange en lange termijn, het evalueren van de samenwerking, afspraken voor het komende jaar. Deze bespreking vindt aan het einde van een jaar plaats.

Details van de overleggen zijn verder uitgewerkt in het DAP.

13.1 Escalatie

Bij onenigheid m.b.t. knelpunten in de dienstverlening, één van beide Partijen komt de afspraken niet na, zal eventuele escalatie plaatsvinden volgens de hiërarchie van de contractorganisatie zoals beschreven in hoofdstuk 14 Contactpersonen conform in het DAP overeengkomen escalatieschema.

In geval van verschil van mening tussen partijen over de uitleg en toepassing van de overeenkomst, zullen zij in gezamenlijk overleg trachten een dienst te vinden met inachtneming van de regels van redelijkheid en billijkheid.

Escalatieniveaus zijn niveaus waar een escalatie zich bevindt. Bij elk niveau wordt een echelon hoger betrokken. Er wordt onderscheid gemaakt in drie escalatie niveaus. (zie paragraaf 14.3). Standaard is er geen sprake van escalatie en is het escalatieniveau 0

13.2 Escalatieniveau verhogen

Indien één van beide partijen van mening is dat de ander zich niet aan de afspraken houdt, kan zij overgaan tot escalatie. Een hoger niveau manager wordt betrokken. Het escalatieniveau wordt met één niveau verhoogd

Bij escalatie treden de functionarissen die bij het escalatieniveau horen, in contact met elkaar. Zij zullen de situatie bespreken, afspraken maken en de voortgang bewaken.

14 CONTACTPERSONEN

14.1 Communicatiematrix regulier overleg

SSC ONS	Verantwoordelijkheden	OPDRACHTNEMER	
Contractmanager	Afsluiten, ontbinden, wijzigingen van de overeenkomst en/of het SLA. Nakomen (SLA) verplichtingen	Contractmanager	Contractmanager
Project Manager	Projectcoördinatie en eerste aanspreekpunt. Afstemmen en bewaken van de (uren)planning en de werkzaamheden tijdens projecten	Projectleider/Consultant	Projectleider/Functioneel beheerder
Servicedesk	Eerste contact met gebruikers, eerste analyse van bevindingen. Communiceren over de voortgang	Medewerker ondersteuning	Contactpersoon ondersteuning
Functioneel-applicatie beheer	Functionele ondersteuning van gebruikers en contactpersoon naar de servicemedewerkers van OPDRACHTNEMER, opvoeren bevindingen. Tevens coördineren van wensen en daaruit voortvloeiende uitbreidingen van de Dienst	Medewerker ondersteuning	Contactpersoon ondersteuning
Technisch beheerder	2e lijn technische ondersteuning van gebruikers	Consultant	Functioneel beheerder
Operationeel overleg	Bespreken doorontwikkeling Software	Projectleider / contractmanager	Vertegenwoordiger Opdrachtgever

14.2 **Communicatiematrix escalatie**

Niveau	Status	SSC ONS	OPDRACHTNEMER
Niveau 0	Geen escalatie	Operationeel beveiligings team	SOC
Niveau 1	Eerste escalatieniveau	Contract- of service manager	Project- of delivery manager
Niveau 2	Tweede escalatieniveau	Manager IT Regie of IT Ops	Account- of Sales Manager
Niveau 3	Derde escalatieniveau	Directie	Directie

Het escalatieproces is verder uitgewerkt in het DAP.

15 ONDERTEKENING

Overeenkomst en betrokken partijen

Het SLA is een bijlage bij de (NAAM / Kenmerk)' t.b.v. SSC ONS en kent dezelfde duur als de Overeenkomst. Deze SLA eindigt van rechtswege wanneer de bovenliggende overeenkomst eindigt.

De partijen betrokken bij dit SLA zijn de SSC ONS in de rol van opdrachtgever en OPDRACHTNEMER in de rol van OPDRACHTNEMER.

Voor akkoord:

OPDRACHTNEMER	SSC ONS
OPDRACHTNEMER	Opdrachtgever
Naam	Naam