

Bijlage 9

Minimale inhoud Service Level Agreement

Europese openbare aanbesteding ATS en VMS — Regio West-Brabant | kenmerk K011612

Gewijzigd naar aanleiding van de 1e en de 2e Nota van Inlichtingen

1. Doel en status van dit document

Deze bijlage bevat de minimumeisen waaraan het Service Level Agreement (hierna: SLA) moet voldoen. De inschrijver stelt de SLA zelf op, gebaseerd op zijn eigen standaardformat, en levert deze bij de inschrijving aan als concept-SLA.

De in deze bijlage opgenomen minimumeisen zijn leidend. Voor zover de concept-SLA daarvan afwijkt, prevaleren het Programma van Eisen en de overeenkomst. Een concept-SLA leidt tot een ongeldige inschrijving indien één of meer onderdelen van de controlelijst in paragraaf 17 ontbreken, of indien normen worden aangeboden die ruimer zijn dan de in deze bijlage opgenomen minimumnormen. Een norm die voor de opdrachtgever gunstiger is dan de minimumnorm, geldt niet als een ruimere norm en is toegestaan. De toets op ruimere normen ziet uitsluitend op de normen die in deze bijlage uitdrukkelijk als minimumnorm zijn opgenomen, te weten de normen van de paragrafen 4, 5 en 14. Overige bepalingen uit het eigen format van de inschrijver die afwijken van de aanbestedingsstukken leiden niet tot ongeldigheid; daarvoor prevaleren de aanbestedingsstukken. Een conformiteitsmatrix per onderdeel van de controlelijst volstaat als verwijzing.

De SLA maakt na gunning integraal onderdeel uit van de overeenkomst. De in de SLA vastgelegde prestatie-indicatoren gelden als contractuele norm met een rapportageplicht. Op tekortkomingen in de prestatie-indicatoren voor beschikbaarheid, API-responstijd, Recovery Point Objective en Recovery Time Objective is het boetebeding van paragraaf 3.2.4 onder a van het beschrijvend document van toepassing. Aan de overige prestatie-indicatoren van paragraaf 14 is geen boete verbonden; overschrijding daarvan leidt tot rapportage en tot het verbetertraject van paragraaf 14.

De SLA wordt per perceel afgesloten. Indien beide percelen aan dezelfde opdrachtnemer worden gegund, gelden de normen en de daaraan verbonden boetemaxima per afzonderlijke overeenkomst. Voor perceel 1 (ATS) wordt onder 'de centrale beheerder van Flex West-Brabant' verstaan: de door de opdrachtgever voor het ATS aangewezen centrale beheerder. De bepalingen over kosteloze ondersteuning van leveranciers, zzp'ers en flexibele arbeidskrachten en over de piekperioden rond de urenregistratie en de facturatieuren gelden uitsluitend voor perceel 2 (VMS).

2. Definities

De SLA bevat ten minste de volgende definities, met de hieronder aangegeven strekking.

Begrip	Omschrijving
Diensttijd	De periode waarbinnen de servicedesk bereikbaar is en waarbinnen reactie- en hersteltijden worden gemeten: ten minste maandag tot en met vrijdag van 08.00 tot 18.00 uur, met uitzondering van nationale feestdagen. Voor incidenten in prioriteitsklasse P1 geldt de diensttijd 24 uur per dag en 7 dagen per week, met het volgende onderscheid per perceel. Voor perceel 2 (VMS) geldt het 24/7-regime bij volledige onbeschikbaarheid en bij een beveiligingsincident of (vermoedelijk) datalek onverkort, inclusief de workaround- en hersteltermijnen. Voor perceel 1 (ATS) geldt bij volledige onbeschikbaarheid buiten de diensttijd een reactietijd van vier uur op basis van 24/7 geautomatiseerde monitoring met automatische alarmering en een bereikbaarheidsdienst, en vangen de workaround- en hersteltermijnen aan bij de start van de eerstvolgende diensttijd; bij een beveiligingsincident of (vermoedelijk) datalek geldt ook voor perceel 1 buiten de diensttijd een reactietijd van één uur, waarbij die termijn ziet op het aanvangen van de insluitende maatregelen.
Piekperiode	De perioden waarin uitval onevenredig grote gevolgen heeft: voor het VMS de week waarin urenstaten worden ingediend en goedgekeurd en de vierweekse facturatieuren; deze perioden worden vastgelegd in een jaarkalender die bij de implementatie wordt vastgesteld. Voor het ATS gelden geen piekperioden; uitval van

Begrip	Omschrijving
	de sollicitatiefunctiefunctionaliteit geldt voor het ATS als P1. In piekperioden vindt geen gepland onderhoud plaats. Onderhoudsvenster: gepland onderhoud vindt uitsluitend plaats binnen het in paragraaf 4.2 omschreven venster en volgens de jaarlijks vast te stellen onderhoudskalender. Voor perceel 2 (VMS) is dat op werkdagen tussen 22.00 en 06.00 uur en in het weekend. Voor perceel 1 (ATS) geldt een tweeledig regime: op werkdagen van 19.00 tot 06.00 uur en in het weekend voor onderhoud waarbij de sollicitatiefunctiefunctionaliteit beschikbaar blijft, en op werkdagen van 22.00 tot 06.00 uur en in het weekend voor onderhoud waarbij die functionaliteit niet beschikbaar is.
Incident	Een gebeurtenis die leidt tot een onderbreking of vermindering van de kwaliteit van de dienstverlening ten opzichte van de overeengekomen norm.
Reactietijd	De tijd tussen de registratie van een melding en het moment waarop de opdrachtnemer de melding heeft geclassificeerd en aan de melder heeft bevestigd, met opgave van prioriteit en de eerstvolgende terugkoppeling.
Workaround	Een tijdelijke voorziening waarmee de gebruiker het proces kan vervolgen, ook al is de onderliggende oorzaak nog niet weggenomen.
Hersteltijd	De tijd tussen registratie van het incident en het moment waarop de dienstverlening structureel is hersteld, gemeten binnen de dienstdtijd van de betreffende prioriteitsklasse.
Beschikbaarheid	Het percentage van de tijd per kalendermaand dat de applicatie voor gebruikers bereikbaar is en de kernfunctionaliteit naar behoren werkt, gemeten door onafhankelijke externe monitoring.
Wijzigingsverzoek	Een verzoek tot aanpassing of uitbreiding van de dienstverlening dat geen incident is.

3. Serviceorganisatie en bereikbaarheid

De SLA beschrijft ten minste:

- de opbouw van de serviceorganisatie, met een benoemde servicemanager als vast aanspreekpunt voor de opdrachtgever en een vervangingsregeling;
- de beschikbare meldkanalen, waaronder ten minste een selfserviceportaal, e-mail en telefoon, en het kanaal waarlangs P1-meldingen buiten de dienstdtijd kunnen worden gedaan;
- de openingstijden per kanaal en de wijze waarop meldingen buiten de dienstdtijd worden opgepakt;
- dat de servicedesk Nederlandstalig is en dat alle communicatie, documentatie en rapportage in het Nederlands plaatsvindt;
- welke gebruikersgroepen rechtstreeks mogen melden en welke via de centrale beheerder van Flex West-Brabant lopen, waarbij leveranciers, zzp'ers en flexibele arbeidskrachten kosteloos toegang hebben tot ondersteuning;
- de escalatieladder met ten minste drie niveaus, inclusief naam, functie en bereikbaarheid per niveau en de termijn waarna automatisch wordt geëscaleerd.

4. Beschikbaarheid, onderhoud en performance

4.1 Beschikbaarheid

De applicatie kent een beschikbaarheid van ten minste 99,7% per kalendermaand. De SLA beschrijft de meetmethode, het meetpunt en de wijze waarop de beschikbaarheid wordt gerapporteerd. Buiten de berekening van de beschikbaarheid blijven: vooraf aangekondigd onderhoud binnen het overeengekomen onderhoudsvenster; spoedonderhoud in verband met beveiliging en kritieke beveiligingsupdates of hotfixes als bedoeld in paragraaf 4.2; overmacht als bedoeld in artikel 20 GIBIT 2025; onbeschikbaarheid van systemen, netwerken of diensten die niet onder de verantwoordelijkheid van de opdrachtnemer vallen, waaronder de identity provider en de bronsystemen van de opdrachtgever en de Deelnemende Organisaties en het openbare internet; en onbeschikbaarheid die het gevolg is van handelen of nalaten van de opdrachtgever, een

Deelnemende Organisatie of een door hen aangewezen derde. Onbeschikbaarheid van een door de opdrachtnemer ingeschakelde (sub)verwerker of hostingpartij valt wél binnen de meting (artikel 14.3 van de overeenkomst). De beschikbaarheid wordt gemeten op het koppelvlak aan de rand van de infrastructuur van de opdrachtnemer, op dezelfde wijze als de API-responstijd.

De opdrachtnemer stelt een realtime statuspagina of dashboard beschikbaar waarop actuele en historische verstoringen en onderhoudsmomenten zichtbaar zijn.

4.2 Onderhoud

De SLA legt ten minste vast dat:

- regulier en impactvol onderhoud vindt uitsluitend plaats buiten de reguliere kantooruren, in de avond, nacht of het weekend, binnen het vaste onderhoudsvenster en volgens de jaarlijks vast te stellen onderhoudskalender. Het vaste onderhoudsvenster luidt: voor perceel 2 (VMS) op werkdagen van 22.00 tot 06.00 uur en in het weekend; voor perceel 1 (ATS) op werkdagen van 19.00 tot 06.00 uur en in het weekend voor onderhoud waarbij de sollicitatiefunctie beschikbaar blijft, en op werkdagen van 22.00 tot 06.00 uur en in het weekend voor onderhoud waarbij de sollicitatiefunctie niet beschikbaar is. De onderhoudskalender vermeldt per venster welk regime van toepassing is;
- gepland onderhoud wordt ten minste vijf werkdagen vooraf aangekondigd, met opgave van tijdvak, verwachte impact en terugvalscenario;
- in de piekperiodes van het VMS vindt geen gepland onderhoud plaats;
- spoedonderhoud in verband met beveiliging, en kritieke beveiligingsupdates en hotfixes die niet kunnen wachten tot het volgende geplande onderhoud, kunnen zonder de genoemde termijn en buiten het onderhoudsvenster en de onderhoudskalender plaatsvinden, mits de onderbreking tot een minimum wordt beperkt, de opdrachtgever zo spoedig als mogelijk wordt geïnformeerd en de opdrachtnemer achteraf onderbouwt waarom de aankondigingstermijn niet kon worden aangehouden. Een dergelijke noodzakelijke onderbreking geldt niet als tekortkoming en wordt niet als P1-incident geregistreerd. Deze uitzondering geldt eveneens voor spoedonderhoud door een in de subverwerkerslijst opgenomen (sub)verwerker van het platform.
- een spoedpatch die een softwarefout herstelt en geen beveiligingsrisico wegneemt, wordt ten minste 48 uur vooraf aangekondigd en waar mogelijk buiten kantooruren uitgerold; het uitrollen van een herstel voor een P1- of P2-incident valt onder de afhandeling van dat incident;
- software releases behoeven niet afzonderlijk in de jaarlijkse onderhoudskalender te worden opgenomen. Een release die een onderbreking van de dienstverlening met zich brengt, vindt plaats binnen het onderhoudsvenster en wordt ten minste vijf werkdagen vooraf aangekondigd, met een release note. Een release zonder onderbreking kan op elk moment worden uitgerold;
- een vooraf aangekondigde onderbreking binnen het onderhoudsvenster blijft buiten de berekening van de beschikbaarheid en wordt niet als P1-incident aangemerkt. Duurt de onderbreking langer dan aangekondigd of loopt zij door buiten het onderhoudsvenster, dan telt uitsluitend het meerdere mee in de beschikbaarheidsberekening en wordt dat meerdere bij volledige onbeschikbaarheid als P1-incident behandeld;
- gepland onderhoud door een in de subverwerkerslijst opgenomen (sub)verwerker van het platform voldoet aan deze bijlage wanneer de opdrachtnemer het direct na de aankondiging door die (sub)verwerker doorgeeft, ook als het niet in de onderhoudskalender staat. Valt dat onderhoud in een piekperiode van het VMS, dan spant de opdrachtnemer zich aantoonbaar in om uitstel te verkrijgen en informeert hij de centrale beheerder over de uitkomst.

4.3 Performance

De SLA legt normen vast voor de responstijd van het systeem en van de aangeboden API's, waaronder een responstijd van minder dan 800 milliseconden voor 95% van de standaard CRUD-requests, alsmede de meetmethode en de wijze van rapportage. Tevens wordt vastgelegd hoe de performance wordt geborgd bij piekbelasting en bij groei van het aantal Deelnemende Organisaties, gebruikers en transacties. De API-responstijd wordt gemeten op het koppelvlak aan de rand van de infrastructuur van de opdrachtnemer (bijvoorbeeld de API-gateway), exclusief netwerk- en internetlatentie aan de zijde van de opdrachtgever en van derden.

5. Incidentmanagement en prioriteitsklassen

De SLA hanteert ten minste de volgende vier prioriteitsklassen en de daarbij behorende normen. De prioriteit wordt bepaald door de opdrachtgever; bij verschil van inzicht geldt de door de opdrachtgever vastgestelde prioriteit tot het moment waarop partijen overeenstemming bereiken.

Klasse	Omschrijving	Reactietijd	Workaround	Structureel herstel
P1 – Kritiek	De applicatie is onbeschikbaar, of een kernproces is voor meerdere Deelnemende Organisaties geblokkeerd, of er is sprake van een beveiligingsincident of (vermoedelijk) datalek. Ook: uitval tijdens een piekperiode van het VMS en uitval van de sollicitatiefunctie van het ATS. De reactietijd van 1 uur geldt 24 uur per dag en 7 dagen per week bij volledige onbeschikbaarheid van de applicatie of van het sollicitatie-respectievelijk urenregistratieproces en bij beveiligingsincidenten en (vermoedelijke) datalekken; voor overige P1-incidenten geldt een reactietijd van 1 uur binnen de diensttijd. De workaround (functieherstel) binnen 4 uur geldt als resultaatsverplichting; overschrijding van het structurele herstel binnen 8 uur leidt tot het verbetertraject van paragraaf 14 en niet zelfstandig tot een boete.	1 uur 24/7 (VMS); binnen de diensttijd 1 uur en daarbuiten 4 uur bij volledige onbeschikbaarheid (ATS), en 1 uur bij een beveiligingsincident of datalek	4 uur	8 uur
P2 – Hoog	Een belangrijk deelproces is onbruikbaar zonder werkbare workaround, of een Deelnemende Organisatie kan niet werken, of gegevens worden aantoonbaar onjuist verwerkt.	2 uur binnen diensttijd	8 uur	2 werkdagen
P3 – Middel	Functionaliteit werkt niet zoals overeengekomen, maar er is een werkbare workaround beschikbaar en de voortgang van het proces komt niet in gevaar.	1 werkdag	n.v.t.	10 werkdagen
P4 – Laag	Cosmetische afwijking, vraag om ondersteuning of kleine onvolkomenheid zonder procesimpact.	2 werkdagen	n.v.t.	eerstvolgende release, dan wel in overleg

De SLA legt daarnaast vast:

- de frequentie van tussentijdse terugkoppeling per klasse: bij P1 ten minste elk uur, bij P2 ten minste elke vier uur en bij P3 ten minste wekelijks;
- dat de melder een ontvangstbevestiging met meldingsnummer ontvangt en de status van de melding zelfstandig kan volgen;
- dat het incident pas wordt gesloten na bevestiging door de melder;
- dat bij P1- en P2-incidenten binnen vijf werkdagen na herstel een schriftelijke evaluatie wordt opgeleverd met oorzaakanalyse en structurele maatregelen; Indien een incident meerdere prestatie-indicatoren of meerdere Deelnemende Organisaties raakt, geldt het als incident met verhoogde impact: de opdrachtnemer handelt het met de hoogste prioriteit af en past onverwijld de escalatieprocedure toe.

- een proces voor probleembeheer, waarin terugkerende incidenten worden geanalyseerd en de onderliggende oorzaak wordt weggenomen.

6. Continuïteit, back-up en herstel

De SLA legt ten minste vast:

- een Recovery Point Objective van maximaal 24 uur en een Recovery Time Objective van maximaal 8 uur;
- de back-upfrequentie, de bewaartermijn van back-ups en de geografisch gescheiden opslag daarvan binnen de Europese Economische Ruimte;
- gedocumenteerde herstelprocedures die ten minste eenmaal per jaar aantoonbaar worden getest, waarbij de opdrachtgever de testrapportage ontvangt;
- de wijze waarop bij storingen en calamiteiten de volledigheid, beschikbaarheid en integriteit van de opgeslagen gegevens wordt gewaarborgd;
- een actueel en getoetst Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP) voor het platform, waarvan de opdrachtgever op verzoek inzage krijgt en waarvan de testresultaten jaarlijks met de opdrachtgever worden gedeeld;
- de werking van de escrow- of continuïteitsvoorziening en het moment waarop deze in werking treedt;
- het uitwijksценario en de wijze waarop de opdrachtgever daarover wordt geïnformeerd.

7. Informatiebeveiliging en kwetsbaarhedenbeheer

De SLA legt de operationele afspraken vast die volgen uit het Programma van Eisen, waaronder ten minste:

- een jaarlijkse onafhankelijke penetratietest, waarvan de managementsamenvatting en het herstelplan aan de opdrachtgever worden verstrekt;
- een risicogebaseerd proces voor kwetsbaarhedenbeheer met continue scanning in de ontwikkel- en releaseketen, wekelijkse scanning van internetbenaderbare productiecomponenten en maandelijkse scanning van overige componenten;
- hersteltermijnen per ernstklasse: kritieke kwetsbaarheden binnen 7 kalenderdagen en bij actief misbruik binnen 48 uur, hoge binnen 30 kalenderdagen, middelhoge binnen 90 kalenderdagen en lage bij de eerstvolgende release;
- het beschikbaar stellen en actualiseren van de Software Bill of Materials na iedere major release;
- logretentie van ten minste 12 maanden, de exporteerbaarheid van logging naar een SIEM en de wijze waarop de opdrachtgever daarover beschikt;
- periodieke controle van autorisaties en gebruikersrechten en de rapportages die de opdrachtnemer daarvoor beschikbaar stelt;
- de werking van de detectie van afwijkend gebruik, waaronder bulkdownloads en uitzonderlijke exportvolumes, en de wijze waarop signalen aan de opdrachtgever worden gemeld;
- een operationeel overleg over informatiebeveiliging ten minste eenmaal per halfjaar, met een rapportage over beveiligingsincidenten, kwetsbaarheden, risico's, audits, patchstatus en verbetermaatregelen, waarbij acties en besluiten worden vastgelegd en opgevolgd.

8. Beveiligingsincidenten en datalekken

De SLA beschrijft het incidentproces bij een (vermoedelijk) datalek of zwaar beveiligingsincident. Daarin is ten minste vastgelegd:

- dat de eerste formele melding zo spoedig mogelijk en uiterlijk binnen 24 uur na ontdekking plaatsvindt aan het door de opdrachtgever aangewezen functionele meldpunt, bestaande uit een afdelingspostbus en een telefonisch aanspreekpunt dat ook buiten kantooruren bereikbaar is. De melding wordt niet aan een met naam of functie aangeduide persoon gedaan; de opdrachtgever draagt zorg voor de interne doorgeleiding naar de betrokken functionarissen, waaronder de CISO

en de Functionaris Gegevensbescherming. Het meldpunt en de escalatieroute zijn opgenomen in Bijlage 16;

- welke informatie de melding minimaal bevat: aard en oorzaak, betrokken gegevenscategorieën, aantal betrokkenen, getroffen Deelnemende Organisaties, reeds genomen maatregelen en het aanspreekpunt;
- dat de opdrachtnemer onverwijld meewerkt aan de beoordeling van de meldplicht en aan een melding aan de Autoriteit Persoonsgegevens of aan betrokkenen, en zelfstandig geen mededelingen doet aan derden;
- de frequentie van tussentijdse terugkoppeling gedurende de afhandeling, met als uitgangspunt ten minste dagelijks zolang het incident niet is beheerst, en de termijn waarbinnen de eindevaluatie wordt opgeleverd. De eerste melding vermeldt uitdrukkelijk welke informatie nog ontbreekt en wordt niet uitgesteld in afwachting van nader onderzoek; zodra blijkt dat persoonsgegevens zijn betrokken, wordt de opdrachtgever onverwijld geïnformeerd, ook binnen de 24 uur;
- de bewaring van bewijsmateriaal ten behoeve van onderzoek.

9. Privacy in de uitvoering

Onverminderd de verwerkersovereenkomst legt de SLA de operationele uitvoering vast van:

- de configureerbare bewaartermijnen en de automatische verwijdering van gegevens na afloop daarvan, inclusief de wijze waarop verwijdering ketenbreed aantoonbaar is;
- de afhandeling van verzoeken van betrokkenen, waaronder inzage, correctie en het recht op vergetelheid, en de termijn waarbinnen de opdrachtnemer daaraan medewerking verleent;
- de actuele lijst van subverwerkers, de wijze en termijn van melding van voorgenomen wijzigingen daarin en het bezwaarrecht van de opdrachtgever;
- de bevestiging dat alle gegevens, inclusief back-ups, logs, bijlagen en metadata, uitsluitend binnen de Europese Economische Ruimte worden verwerkt en opgeslagen, en de wijze waarop dit periodiek wordt aangetoond;
- het beschikbaar houden en actualiseren van de DPIA en het auditrecht van de opdrachtgever.

10. Release-, wijzigings- en versiebeheer

De SLA legt ten minste vast:

- een gestructureerd proces voor release- en wijzigingsbeheer, met documentatie van wijzigingen en tijdig beschikbare releasenotes in het Nederlands;
- dat updates kosteloos worden doorgevoerd, zowel op de acceptatie- als op de productieomgeving;
- dat updates, met uitzondering van systeembrede beveiligingsupdates, ten minste vijf werkdagen vóór de uitrol naar productie beschikbaar komen op de acceptatieomgeving, met een release note waarin de wijzigingen en de gevolgen voor de processen zijn beschreven. Die termijn van vijf werkdagen is een minimumtermijn. De uitrol vindt niet plaats tijdens een piekperiode zoals vastgelegd in de onderhoudskalender; valt het einde van de acceptatietermijn in een piekperiode, dan wordt de uitrol uitgesteld tot na die periode en wordt de acceptatietermijn met die periode verlengd;
- dat de opdrachtnemer de uitrol van een update uitstelt bij een door de centrale beheerder binnen de acceptatietermijn gemelde en aantoonbaar procesblokkerende bevinding, tenzij sprake is van een noodzakelijke beveiligings- of wettelijk verplichte release. Onder een procesblokkerende bevinding wordt in ieder geval verstaan een verstoring waardoor aanvragen, beoordelingen, opdrachtvorming, urenverwerking of facturatie niet meer conform het proces kunnen plaatsvinden. De opdrachtnemer besluit over het al dan niet uitstellen en motiveert dat besluit binnen één werkdag schriftelijk aan de centrale beheerder. Nieuwe optionele functionaliteit kan per opdrachtgever uitgeschakeld blijven;
- de aankondigingstermijn per type release en de wijze waarop de impact voor de Deelnemende Organisaties wordt beschreven;
- het terugdraaiscenario indien een release tot verstoringen leidt;

- het versie- en einde-levensduurbeleid, met de termijn waarbinnen de opdrachtgever wordt geïnformeerd over het uitfaseren van functionaliteit of van een versie;
- de actualisatie van het inrichtingsdocument, de handleidingen en het instructiemateriaal op B1-taalniveau bij functionele wijzigingen.

11. Behandeling van meldingen, vragen en wensen

Dit onderwerp wordt niet binnen de gunningscriteria beoordeeld en is uitsluitend via deze bijlage geborgd. De SLA legt vast:

- dat meldingen, vragen, wensen en verbetervoorstellen van de opdrachtgever en de Deelnemende Organisaties centraal worden geregistreerd en zichtbaar zijn voor de opdrachtgever;
- de wijze waarop en de criteria waarmee wensen worden geprioriteerd, en de rol die de opdrachtgever daarbij heeft;
- dat op iedere wens binnen 20 werkdagen inhoudelijk wordt teruggekoppeld, met een gemotiveerd besluit en, bij honorering, een indicatie van de release waarin realisatie plaatsvindt;
- dat ook expliciet wordt teruggekoppeld over wensen die niet of niet op korte termijn worden gerealiseerd, met opgave van de reden;
- de wijze waarop de opdrachtgever invloed heeft op de productroadmap en hoe regionale wensen daarin worden gewogen;
- de wijze waarop de opdrachtnemer de opdrachtgever ten minste jaarlijks informeert over de roadmap en de doorontwikkeling van de oplossing.

12. Beheer en autorisaties

De SLA legt ten minste vast:

- de taakverdeling tussen de centrale beheerder van Flex West-Brabant, de lokale beheerders van de Deelnemende Organisaties en de opdrachtnemer, vastgelegd in een verantwoordelijkhedenmatrix die aansluit op het Shared Responsibility Model;
- welke beheerhandelingen de opdrachtgever zelfstandig kan uitvoeren en welke uitsluitend door de opdrachtnemer worden verricht, met de bijbehorende doorlooptijden;
- de ondersteuning van key users en de frequentie van gebruikersoverleggen;
- de periodieke review van autorisaties en de rapportages en exports die de opdrachtnemer daarvoor levert;
- de wijze waarop de opdrachtnemer verhoogde rechten van eigen medewerkers op de omgeving van de opdrachtgever toekent, logt, periodiek beoordeelt en intrekt.

13. Rapportage en overleg

13.1 Rapportage

De opdrachtnemer stelt maandelijks een geautomatiseerd dashboard of managementrapportage beschikbaar in de applicatie, waarin ten minste wordt gerapporteerd over de gerealiseerde beschikbaarheid, de API-performance en de doorlooptijd van P1- en P2-incidenten. De rapportage is beschikbaar voor de aangewezen beheer- of servicemanagementrol en bevat tevens het aantal meldingen per prioriteitsklasse, de mate waarin de normen zijn gehaald, de openstaande meldingen en wensen en de status van beveiligingsmaatregelen.

13.2 Overleg

Overleg	Frequentie	Onderwerpen
Operationeel overleg	Maandelijks	Openstaande meldingen, incidenten, releases en planning, gerealiseerde serviceniveaus.
Overleg informatiebeveiliging	Halfjaarlijks	Beveiligingsincidenten, kwetsbaarheden, risico's, audits, patchstatus, verbetermaatregelen en verwerking van persoonsgegevens.

Overleg	Frequentie	Onderwerpen
Tactisch overleg	Per kwartaal	Trends in de dienstverlening, wensen en roadmap, capaciteit, verbeterplannen.
Strategisch overleg	Jaarlijks	Ontwikkeling van de dienstverlening, marktontwikkelingen, meerjarenplanning.
Contractevaluatie	Ten minste tweemaal per jaar	Evaluatie aan de hand van de prestatie-indicatoren, als bedoeld in paragraaf 3.1.3 van het beschrijvend document.

14. Kritische prestatie-indicatoren

De SLA neemt ten minste de volgende prestatie-indicatoren op, met de daarbij vermelde norm, meetmethode en rapportagefrequentie. De opdrachtnemer mag scherpere normen aanbieden; ruimere normen zijn niet toegestaan. Aan de prestatie-indicator gebruikerstevredenheid is geen boete verbonden; bij overschrijding geldt uitsluitend het verbetertraject.

Prestatie-indicator	Norm	Meting	Frequentie
Beschikbaarheid applicatie	≥ 99,7% per maand	Onafhankelijke externe monitoring, exclusief aangekondigd onderhoud	Maandelijks
API-responstijd	< 800 ms voor 95% van de standaard CRUD-requests	Meting op het koppelvlak	Maandelijks
Reactietijd P1	≤ 1 uur 24/7 (VMS); binnen de diensttijd 1 uur en daarbuiten 4 uur bij volledige onbeschikbaarheid (ATS), en 1 uur bij een beveiligingsincident of datalek	Registratie in het ticketsysteem	Maandelijks
Structureel herstel P1	≤ 8 uur	Registratie in het ticketsysteem	Maandelijks
Structureel herstel P2	≤ 2 werkdagen	Registratie in het ticketsysteem	Maandelijks
Actualiteit en toetsing BCP en DRP	Jaarlijks geactualiseerd en getest	Testrapportage	Jaarlijks
Recovery Point Objective	≤ 24 uur	Back-upconfiguratie en jaarlijkse hersteltest	Jaarlijks
Recovery Time Objective	≤ 8 uur	Jaarlijkse hersteltest	Jaarlijks
Melding datalek of zwaar beveiligingsincident	≤ 24 uur na ontdekking	Incidentregistratie	Per incident
Herstel kritieke kwetsbaarheid	≤ 7 kalenderdagen; ≤ 48 uur bij actief misbruik	Kwetsbaarhedenrapportage	Maandelijks
Terugkoppeling op wensen	≤ 20 werkdagen	Registratie in het meldingensysteem	Per kwartaal
Tijdige aankondiging gepland onderhoud	≥ 5 werkdagen vooraf, 100% van de gevallen	Onderhoudskalender en statuspagina	Per kwartaal

Prestatie-indicator	Norm	Meting	Frequentie
Gebruikerstevredenheid	Ten minste een 7,0 op een tienpuntsschaal	Jaarlijkse meting onder key users, uitgevoerd door de opdrachtnemer	Jaarlijks

De SLA beschrijft het verbetertraject dat in werking treedt wanneer een norm in twee opeenvolgende maanden niet wordt gehaald: een schriftelijk verbeterplan binnen tien werkdagen, met maatregelen, verantwoordelijken en termijnen, en bespreking daarvan in het eerstvolgende overleg. Dit laat de toepassing van het boetebeding onverlet.

Boetegevoeligheid: uitsluitend de prestatie-indicatoren Beschikbaarheid applicatie, API-responstijd, Recovery Point Objective en Recovery Time Objective zijn boetegevoelig op grond van paragraaf 3.2.4 onder a van het beschrijvend document. Aan de overige negen prestatie-indicatoren in deze tabel is geen boete verbonden; overschrijding daarvan leidt tot het verbetertraject van deze paragraaf. Aan gebruikerstevredenheid is geen boete verbonden.

De Recovery Time Objective van acht uur geldt uitsluitend voor het calamiteitenscenario waarin de productieomgeving als geheel uitvalt en herstel op een uitwijklocatie nodig is. De termijn wordt gerekend vanaf het moment waarop de opdrachtnemer de calamiteit vaststelt volgens de calamiteitenprocedure in de SLA; die procedure legt vast dat de vaststelling plaatsvindt binnen ten hoogste één uur na de constatering van de verstoring. De naleving wordt getoetst via de jaarlijkse hersteltest en niet op basis van een werkelijke calamiteit alleen. Verstoringen binnen de productieomgeving vallen onder het P1-regime van paragraaf 5.

15. Exit en beëindiging

De SLA legt ten minste vast:

- dat de opdrachtgever gedurende de gehele looptijd zelfstandig, zonder tussenkomst van de opdrachtnemer en zonder aanvullende kosten, een volledige export van alle gegevens kan maken, inclusief documenten, bijlagen en metadata, in een gangbaar, gedocumenteerd en machineleesbaar formaat, met een actuele beschrijving van het datamodel; Een volledige export is binnen vijf (5) werkdagen beschikbaar.
- dat de benodigde integratie-API's bij beëindiging gedurende ten minste zes maanden in read-only modus beschikbaar blijven;
- dat de data-export, het datamodel en de bijbehorende documentatie kosteloos zijn en dat transitiebegeleiding, proefmigraties, projectondersteuning en het in read-only modus beschikbaar houden van de integratie-API's worden geleverd tegen de vaste prijs van regel 7 van het Prijzenblad, op basis van de uitgangspunten uit paragraaf 3.4 van het beschrijvend document, en dat werkzaamheden daarboven worden verrekend tegen het uurtarief van regel 6;
- de inhoud, de vaststelling en de jaarlijkse actualisatie van het exitplan, zoals bedoeld in paragraaf 3.4 van het beschrijvend document;
- de wijze en het moment van vernietiging van de gegevens na afloop van de transitie en de wijze waarop dit ketenbreed wordt aangetoond.

16. Wijziging van de SLA

De SLA wordt ten minste eenmaal per jaar geëvalueerd, gelijktijdig met de evaluatie van de dienstverlening. Wijziging van de SLA vindt uitsluitend plaats met voorafgaande schriftelijke instemming van beide partijen. Eenzijdige wijziging door de opdrachtnemer, ook via algemene

voorwaarden, productvoorwaarden of standaardmededelingen, heeft geen werking. Normen kunnen gedurende de looptijd niet worden verlaagd.

17. Invulinstructie voor de inschrijver

De concept-SLA die bij de inschrijving wordt ingediend, bevat alle in deze bijlage genoemde onderdelen. Gebruik onderstaande controlelijst; de aanbestedende dienst toetst hierop bij de beoordeling van de geldigheid van de inschrijving.

Nr.	Onderdeel	Opgenomen in hoofdstuk
1	Definities, waaronder diensttijd, piekperiode, reactietijd, hersteltijd en beschikbaarheid	
2	Serviceorganisatie, meldkanalen, bereikbaarheid en escalatieladder	
3	Beschikbaarheidsnorm, meetmethode en statuspagina	
4	Onderhoudsvensters, aankondigingstermijn en piekperiodes. Voor perceel 1 wordt aan dit onderdeel voldaan met de vermelding van het onderhoudsvenster en de aankondigingstermijn en met de vaststelling dat voor het ATS geen piekperiodes gelden en dat uitval van de sollicitatiefunctie als P1 wordt behandeld	
5	Performancenormen en meetmethode	
6	Prioriteitsklassen met reactie-, workaround- en hersteltijden	
7	Terugkoppeling, sluiting van meldingen en evaluatie na P1 en P2	
8	Probleembeheer	
9	Back-up, RPO, RTO en jaarlijkse hersteltest	
10	Escrow- of continuïteitsvoorziening, uitwijk, BCP en DRP	
11	Kwetsbaarhedenbeheer, hersteltermijnen, pentest en SBOM	
12	Logging, logretentie en SIEM-export	
13	Datalekproces en meldtermijn van 24 uur	
14	Privacy in de uitvoering, bewaartermijnen en betrokkenenrechten	
15	Release-, wijzigings- en versiebeheer	
16	Behandeling van meldingen, vragen en wensen en invloed op de roadmap	
17	Beheer, autorisaties en verantwoordelijkhedenmatrix	
18	Rapportage en overlegstructuur	
19	Prestatie-indicatoren met normen	
20	Exit en beëindiging	
21	Wijzigingsprocedure van de SLA	

18. Herkomst van de normen

Onderstaande tabel geeft de herkomst weer van de normen in deze bijlage, ten behoeve van de traceerbaarheid naar het Programma van Eisen en het beschrijvend document.

Onderwerp	Bron
Beschikbaarheid 99,7% per maand, statuspagina, onderhoud buiten kantooruren	Programma van Eisen, onderdeel Architectuur

Onderwerp	Bron
met aankondiging van vijf werkdagen	
RPO 24 uur, RTO 8 uur, geteste herstelprocedures, geografisch gescheiden back-ups binnen de EER, actueel en getoetst BCP en DRP	Programma van Eisen, onderdeel Architectuur (GEN-B11, GEN-B12)
API-responstijd onder 800 ms (p95), API-gateway, gescheiden acceptatie- of sandboxomgeving	Programma van Eisen, onderdeel Integratie
Maandelijkse rapportage over uptime, API-performance en doorlooptijd P1 en P2	Programma van Eisen, onderdeel Integratie
Jaarlijkse penetratietest, kwetsbaarhedenbeheer, SBOM, halfjaarlijks overleg informatiebeveiliging	Programma van Eisen, onderdelen Architectuur en Integratie
Melding datalek binnen 24 uur aan het door de opdrachtgever aangewezen meldpunt, logretentie van 12 maanden, SIEM-export, PAM	Programma van Eisen, onderdeel Informatiebeveiliging
Verwerking en opslag uitsluitend binnen de EER, subverwerkers, DPIA, recht op vergetelheid	Programma van Eisen, onderdelen Informatiebeveiliging, Integratie en Privacy
Kosteloze updates, eerst op de acceptatieomgeving met een minimumtermijn van vijf werkdagen, uitstel van de uitrol bij een procesblokkerende bevinding	Perceel 2: Programma van Eisen, VMS-Y8 en VMS-Y9. Perceel 1: artikel 8.2 van de conceptovereenkomst (Bijlage 6); dit onderdeel berust voor perceel 1 niet op een VMS-eis
Release- en wijzigingsbeheer, releasenotes, centrale en lokale beheerfunctie, beheer als dienst	Programma van Eisen, onderdeel Beheer
Nederlandstalige documentatie en handleidingen op B1-niveau	Perceel 2: Programma van Eisen, VMS-V1, VMS-V5 en VMS-V6. Perceel 1: artikel 12.3 van de conceptovereenkomst (Bijlage 6); dit onderdeel berust voor perceel 1 niet op een VMS-eis
Exit: kosteloze export, read-only API's gedurende zes maanden, exitplan en actualisatie	Programma van Eisen, onderdeel Integratie, en paragraaf 3.4 van het beschrijvend document
Prioriteitsklassen, reactie- en hersteltijden, escalatie, overlegstructuur, gebruikerstevredenheid	Nader ingevuld door de aanbestedende dienst binnen de kaders van paragraaf 3.5 van het beschrijvend document