Bijlage 5; Programma van eisen (ICT)

1.1 Techniek

1.1.1 Algemeen

E1.	De aangeboden oplossing die door Inschrijver wordt geleverd als een Software as a Service (SaaS) omgeving (vanaf nu '*de SaaS-applicatie*'), een gehoste cloudoplossing waarbij technisch beheer door de leverancier (Opdrachtnemer) uitgevoerd wordt.
E2.	De SaaS-applicatie beschikt over een webbased of over een remote desktop userinterface. Deze is zonder beperking van functionaliteit benaderbaar met de twee (2) laatste major versies van de meest gangbare browsers waaronder in ieder geval Google Chrome en Mozilla Firefox. Er zal geen gebruik worden gemaakt van plug-ins. Er zijn ook geen verdere instellingen of installaties (op het client device en/of in de webbrowser) benodigd, met uitzondering van acceptatie van client certificaten. Inschrijver levert bij zijn Inschrijving een bijlage met architectuurplaat hoe zij Opdrachtgever toegang biedt tot de oplossing, Wij zullen de bijlage toetsen op ons informatieveiligheidsbeleid en op het beheer.
E3.	De aangeboden SaaS-applicatie bevat geen maatwerkfunctionaliteiten. Mocht het toch voorkomen dat maatwerk wordt toegepast, dan is de werking hiervan blijvend gegarandeerd in nieuwe releases.
E4.	De aangeboden SaaS-applicatie is direct leverbaar en de levering van alle in de offerte opgenomen onderdelen zijn gedekt in het Inschrijvingsbiljet en toonbaar tijdens de Videodemonstratie.
E5.	De opslag van data vindt plaats binnen de Europese Economische Ruimte (EER) en bij een hosting partij/datacenter die geen vestiging heeft in de Verenigde Staten, dit in verband met de USA Freedom Act. In de Overeenkomst zal worden beschreven op welke fysieke locaties de data van Opdrachtgever wordt/is ondergebracht.
E6.	De volgende risicovolle situaties zijn niet toegestaan zonder expliciete goedkeuring van Opdrachtgever: • Gebruik maken van een back-up dienst (al dan niet van derden) waarbij niet 100% zeker is dat de data binnen de EER blijft. • Gebruik maken van beheerdiensten van partijen gevestigd buiten de EER. • Gebruik maken van ontwikkeldiensten van partijen gevestigd buiten de EER. • Opslag van gemeentelijke data buiten de beveiligde omgeving, bijvoorbeeld op laptops van medewerkers om 'even' wat te testen, fouten te zoeken etc. Op voorhand zal Opdrachtgever geen toestemming geven voor deze situaties. Indien één van bovenstaande situaties zich voordoet bij de inschrijver, dient hij dit kenbaar te maken via de Nota van inlichtingen.
E7.	De Opdrachtnemer zorgt voor een redundant uitgevoerde SaaS-applicatie verdeeld over meerdere geografisch gescheiden datacenters.
E8.	Er wordt minimaal een acceptatie- en productieomgeving beschikbaar gesteld, beiden inclusief alle in dit Programma van Eisen en wensen geëiste en later toegevoegde koppelingen. De acceptatieomgeving (in gebruik als testomgeving) geeft te allen tijde een representatie van de productieomgeving en dient continu beschikbaar te zijn.
E9.	De test- en productieomgeving zijn gescheiden omgevingen en hebben gescheiden datasets (lees databases). Opdrachtgever moet zelf kunnen beslissen wanneer productiedata wordt gekopieerd naar de testomgeving. Deze datamigratie kan door de functioneel beheerder van Opdrachtgever worden uitgevoerd en is zonder meerkosten. Of kan op verzoek van Opdrachtgever door Opdrachtnemer worden uitgevoerd, zonder meerkosten.
E10.	De testomgeving werkt geïsoleerd en is niet gekoppeld aan de productieomgeving. De testomgeving is benodigd voor o.a. uitproberen van een nieuwe inrichting.

1.1.2 Beveiliging

E11.	De SaaS-applicatie ondersteunt Domain Name System Security Extensions (DNSSEC) voor de webservices.
E12.	De fysieke locaties van waar de SaaS-applicatie wordt gehost is beveiligd tegen toegang door onbevoegden. De locaties zijn adequaat – minimaal naar marktstandaarden - beveiligd tegen onheil van buitenaf, waaronder in ieder geval weersomstandigheden en vandalisme.
E13.	Authenticatie voor medewerkers van de Opdrachtgever dient te verlopen met behulp van Two Factor Authentication (2FA).
E14.	Indien gebruik wordt gemaakt van de e-mailvoorziening binnen de SaaS-applicatie i.p.v. via de mailserver van de Opdrachtgever, wordt bij het sturen en ontvangen van e-mail standaard gebruik gemaakt van ten minste TLS 1.3 (Transport Layer Security). Er is een mogelijkheid tot het gebruik van een DKIM-sleutel (DomainKeys Identified Mail) waarmee de afzender kan worden geverifieerd door de ontvanger. De mail is hierbij herkenbaar als e-mail van de Opdrachtgever.
E15.	De integriteit van data blijft gewaarborgd door data van Opdrachtgever aantoonbaar te scheiden van andere klanten.
E16.	De Opdrachtnemer zorgt ervoor dat Opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten van Opdrachtnemer (bijv. spamming vanuit eenzelfde IP-adres).
E17.	De Opdrachtnemer zorgt er voor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten van Opdrachtnemer die actief zijn binnen de systeemomgeving van Opdrachtnemer.
E18.	De Opdrachtnemer voorkomt dat gebruik van gedeelde infrastructuurcomponenten door andere klanten van Opdrachtnemer de performance bij Opdrachtgever bedreigen.
E19.	De SaaS-applicatie voldoet aan de voorwaarden genoemd in de Algemene verordening Gegevensbescherming (AVG). De software mag geen persoonsgegevens vergaren zonder doelbinding.
E20.	De opdrachtnemer voldoet aan ISO 27001. De opdrachtnemer toont het aan met een TPM-verklaring.
E21.	Het BOR-beheersysteem past binnen Baseline Informatiebeveiliging Overheid (BIO).
E22.	Inschrijver dient, indien hiertoe een verzoek wordt gedaan, op eigen kosten jaarlijks een verklaring van getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij, om aan te tonen dat zij als Contractant veilig omgaat met vertrouwelijke informatie.
E23.	De Opdrachtnemer dient gebruik te maken van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen (Hardenen van systemen bestaat uit verschillende stappen om een gelaagde bescherming te bieden. Met behulp van antivirus, -spyware, -spam en -phishing software, regelmatig installeren van de laatste patches van de Opdrachtnemer, het uitschakelen van onnodige software en diensten leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillende is te misbruiken).
E24.	Gegevens die van en naar de SaaS-applicatie getransporteerd worden, in welke vorm dan ook, dienen beveiligd te worden door middel van encryptie. Hierbij dient gebruik te worden gemaakt van het TLS-protocol op basis van TLS 1.3 of beter.
E25.	Penetratietests dienen periodiek uitgevoerd te worden (minimaal een (1) maal per jaar). Het resultaat dient beschikbaar gesteld te worden aan de opdrachtgever.
E26.	Vulnerability assessments (security scans) dienen periodiek uitgevoerd te worden (minimaal één (1) maal per Jaar).
E27.	Beveiligingsincidenten waarbij meer dan normale kwetsbaarheden of risico's aanwezig zijn, dienen onmiddellijk gemeld te worden aan en besproken met de Opdrachtgever.
E28.	Opdrachtnemer dient actief kwetsbaarheden te volgen die gepubliceerd worden (via www.cvedetails.com bijvoorbeeld). Opdrachtnemer dient bij een beveiligingsincident noodzakelijke maatregelen te nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. Het beveiligingsincident, alsmede alle getroffen maatregelen, worden aan de Opdrachtgever gerapporteerd.
E29.	Alle communicatie met de applicatie geschiedt o.a. o.b.v. HTTPS. De securitylagen van de verbindingen mogen maximaal 1 versie achterlopen (N-1) van wat als de securitystandaard wordt beschouwd.
E30.	Communicatie voor het HTTPS protocol dient plaats te vinden over poort 443.

E31.	De SaaS-applicatie kent veilige verbindingen. Alle communicatie tussen de applicatie en clients is adequaat beschermd tegen afluisteren en manipulatie middels versleuteling. Voorkeur protocollen van Opdrachtgever hiervoor zijn HTTPS (IPv4 & IPv6), DANE, VPN, SFTP. Deze dienen allemaal ondersteund te worden. (TLS 1.3, HSTS of gelijkwaardig).
E32.	De actieve gebruikerssessies met de applicatie zijn adequaat beveiligd tegen overname en manipulatie.
E33.	Medewerkers van leverancier mogen niet zonder voorafgaande toestemming van opdrachtgever de gegevens van opdrachtgever in de database benaderen.
E34.	IP-filtering Om onbevoegd toegang tot de Oplossing tegen te gaan is het een eis dat we kunnen “whitelisten” via de IP-adressen.

1.1.3 Back-up en restore

E35.	Er wordt een toereikend recovery proces ingericht waar back-up en restore onderdeel van uit maken.
E36.	In het geval een restore van data nodig is, kan de afgesproken dienstverlening binnen 24 uur worden gecontinueerd. Er mag sprake zijn van maximaalvierentwintig (24) uur dataverlies. Back-ups worden gemaakt terwijl de volledige SaaS-applicatie ‘online’ is.
E37.	In geval van corrupte data kan een herstel/rollback worden uitgevoerd om een eerdere (consistente) staat van de SaaS-applicatie te herstellen. Het herstel-/rollbackmechanisme van de SaaS-applicatie is zodanig dat het mogelijk is om de volledige SaaS-applicatie vanaf een bepaalde transactie te herstellen.
E38.	De Opdrachtnemer levert een uitwijkomgeving waardoor real-time uitgeweken kan worden naar een andere locatie.

1.1.4 Data, datamodel en database

E39.	De administratieve en geometrische gegevens zijn geïntegreerd en relationeel opgeslagen, waarbij de geometrische en administratieve gegevens in onderlinge samenhang kunnen worden beheerd en onderhouden.
E40.	Leverancier geeft inzage in het datamodel van de database, indien gewenst onder non-disclosure agreement. In de applicatie moet van ieder schermveld eenvoudig te achterhalen zijn wat de naam van het veld in de database is en in welke tabellen dit veld voorkomt.
E41.	Leverancier garandeert dat toevoegingen aan en veranderingen van het datamodel van de applicatie mogelijk zijn en blijven en zorgt ervoor dat de bijbehorende functionaliteiten beschikbaar blijven in latere versies van de SaaS-applicatie.
E42.	Leverancier biedt Opdrachtgever te allen tijde, uiteraard m.u.v. de afgesproken servicewindows, toegang tot de database met BOR-gegevens voor bevraging (bijvoorbeeld via ETL) bijvoorbeeld d.m.v. leesrechten op (views op) de database en/of webservices en/of API.
E43.	Leverancier voert alleen met toestemming van Opdrachtgever wijzigingen door in de database van de applicatie. Dit geldt zowel voor individuele wijzigingen, als voor massale wijzigingen al dan niet via de applicatie of rechtstreeks in de database.

1.1.5 Hosting

E44.	De SaaS-applicatie draait als cloud-oplossing, waarbij de verantwoordelijkheid voor de Hosting bij leverancier ligt. Onder de betreffende verantwoordelijkheid van leverancier vallen o.a. maar niet uitsluitend het in een fysiek en logisch voldoende beveiligde omgeving – bestaande uit alle daartoe benodigde software (zoals besturingssystemen, firewalls, technische beheertooling, virtualisatiesoftware, etc.) en hardware (zoals servers, opslag, back-up, netwerken, etc.) – beschikbaar stellen van de applicatie, incl. back-up, recovery en uitwijk(test).

1.2 Gebruiksvriendelijkheid

E45.	De SaaS-applicatie is geschikt voor verschillende soorten apparaten (laptop, tablet, smartphone etc.) en schaalt, met uitzondering van beheerfuncties, mee met de afmetingen van een scherm van mobile devices tot tabletniveau, zonder in te leveren op leesbaarheid van tekst of bruikbaarheid van de gebruikersinterface (responsive design).
E46.	Binnen de verschillende onderdelen van de SaaS-applicatie dienen op alle niveaus gegevens toegevoegd, opgevraagd en uitgeprint te kunnen worden (bijv. rapportage, kaart materiaal etc.).

E47.	De teksten (incl. helpfunctie en foutmeldingen) in de SaaS-applicatie zijn makkelijk te begrijpen (taalniveau B1).
E48.	Er dient een digitale helpfunctie op te roepen te zijn.
E49.	De SaaS-applicatie dient zowel met de muis als met toetsenbordcombinaties te bedienen te zijn.
E50.	Voor alle onderdelen in de SaaS-applicatie dienen eenduidige procedures, schermen, menuopbouw en toetscombinaties te zijn.
E51.	de SaaS-applicatie dient te signaleren wanneer bij de invoer van gegevens velden niet of verkeerd zijn ingevuld (waarschuwing bij evidente fouten).
E52.	Fouten in de keten worden duidelijk en niet cryptisch omschreven.

1.3 Logging

E53.	De logging biedt voldoende inzicht in de bijhouding, uitwisseling, en selecties van gegevens om het gebruik van een gegeven door een applicatie te kunnen achterhalen en hierop te signaleren of acteren.
E54.	Logging en alle gegevens vallen onder de verwerkersovereenkomst. In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, etc.). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van de Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts).
E55.	De Opdrachtnemer voert actief controles uit op logging.
E56.	De logging dient niet te worden verwijderd en zal beschikbaar blijven binnen de SaaS-applicatie.
E57.	De logging dient read-only te zijn. Het muteren en verwijderen van log-records is niet toegestaan, uitgezonderd verwijdering o.b.v. de AVG.
E58.	Er dient een totaaloverzicht beschikbaar te zijn van autorisaties van zowel Opdrachtnemer als Opdrachtgever.
E59.	De logging dient alleen beschikbaar te zijn voor daartoe geautoriseerde medewerkers. Deze autorisaties zijn via de SaaS-applicatie inregelbaar door Opdrachtgever.
E60.	Opdrachtnemer dient medewerking te verlenen aan het uitoefenen van controle door of namens Opdrachtgever op bewaring en gebruik van data, en naleving van procedures.
E61.	De logging dient geen performanceverlies ten aanzien van de in deze aanbesteding gestelde eisen aan de SaaS-applicatie te veroorzaken.
E62.	Opdrachtnemer beschikt over een monitoringsysteem om de beschikbaarheid en performance van de aangeboden diensten te monitoren, zodat de beheersorganisatie direct gealarmeerd wordt bij onder andere, maar niet uitputtend: uitval, performanceproblemen, (D)DOS-aanvallen, onverklaarbare toename in verkeer naar internet, verlopen van beveiligingscertificaten, ongeautoriseerde wijzigingen aan configuratiebestanden, ongeautoriseerde wijzigingen aan systeembestanden etc.

1.4 Implementatie

E63.	De SaaS-applicatie moet in overeenstemming met de planning van de Aanbestedingsleidraad operationeel zijn. De Opdrachtnemer gaat akkoord met de planning om dit te realiseren.
E64.	De Implementatie wordt afgesloten met een Acceptatieprocedure conform GIBIT art 7.2 t/m 7.10. Er is alleen sprake van Acceptatie bij een wederzijdse akkoordverklaring, welke schriftelijk wordt geformaliseerd door zowel opdrachtgever als leverancier.
E65.	De Opdrachtnemer levert een projectleider die verantwoordelijk is voor de implementatie en inrichting van de SaaS-applicatie. De projectleider van Opdrachtnemer beheert tijd en risico's, reageert proactief en signaleert problemen; hierbij communiceert hij/zij veelvuldig met de projectleider van opdrachtgever. De projectleider van Opdrachtnemer dient over de nodige ervaring te beschikken, de Nederlandse taal te beheersen en dit alles aan te tonen in het implementatieplan,
E66.	De Opdrachtnemer is verantwoordelijk voor het aanleveren van een plan van aanpak zoals opgenomen in de aanbestedingsleidraad.
E67.	U levert een vast team van medewerkers voor de uitvoering van uw werkzaamheden tijdens de implementatie van de BOR-oplossing.
E68.	Alle aan leverancier gerelateerde personen die rechtstreeks contact hebben met opdrachtgever, dienen Nederlands te spreken en te schrijven op ten minste taalniveau B1.
E69.	Op het moment van tussentijdse oplevering, dienen alle “standaard” wachtwoorden (waaronder administrator) aangepast te worden.

1.5	Functioneel beheer
E70.	Dagelijkse functionele beheertaken kunnen worden uitgevoerd, zonder dat dit invloed heeft op de werking van de SaaS-applicatie voor de overige gebruikers en op andere ICT-oplossingen. Gebruikers kunnen ingelogd blijven en volledig gebruik blijven maken van de SaaS-applicatie tijdens dagelijkse functionele beheertaken.
E71.	Autorisaties dienen middels een beheerinterface gebruiksvriendelijk te kunnen worden geconfigureerd. Het hele rollen- en rechtenmodel van de SaaS-applicatie wordt op één plek geconfigureerd.
E72.	Het is mogelijk om configuraties in rollen en rechten te stapelen, in groepen toe te kennen, te overerven, te kopiëren en te delegeren.
E73.	Voor het uitvoeren van het functioneel beheer van de SaaS-applicatie is geen programmeerkennis nodig.
E74.	De functioneel beheerder dient: • zelf de logging en audit trail (rapportages) te kunnen benaderen zonder tussenkomst van de opdrachtnemer. • snel en flexibel in te kunnen spelen op wijzigingen in processen. Dit houdt in dat de functioneel beheerder workflows snel aan kan passen.
E75.	Voor het uitvoeren van functioneel beheer moet de functioneel beheerder zelf de autorisaties en stamtabellen kunnen inrichten en beheren met begin- en einddatum en gebruikmakend van logfiles. Voorbeelden daarvan zijn het aanmaken en wijzigen van gebruikers, functierollen, stuur- en stamgegevens.
E76.	In de SaaS-applicatie moet de beschikbaarheid en het gebruik van de licenties inzichtelijk zijn (indien er gebruik wordt gemaakt van licenties). In de applicatie zit ofwel een signaalfunctie of er is een jaarlijkse systeemmeting op basis waarvan het verschil in gebruik/licenties wordt bezien.
E77.	De SaaS-applicatie voorziet in een goede scheiding tussen systeembeheer, functioneel- en technisch- applicatiebeheer en gebruikers.
E78.	Data dient eenvoudig van de productie- naar de acceptatieomgeving gezet te kunnen worden. Dit mag niet leiden tot meerkosten.
1.6	**Technisch beheer**
E79.	Beheer en onderhoud van de SaaS-applicatie geschiedt in de Nederlandse taal.
E80.	De duurzaamheid van de SaaS-applicatie is binnen de contractperiode gegarandeerd indien de SaaS-applicatie niet langer ondersteund wordt door de Opdrachtnemer (bijvoorbeeld wanneer de mogelijkheid bestaat om het onderhoud en de ondersteuning voort te zetten bij een andere partij).
E81.	Het systeembeheer en het technisch-applicatiebeheer dient geheel verzorgd te worden door Opdrachtnemer. Opdrachtnemer voert Updates en Upgrades door in zowel de productie- en testomgeving. De applicatie dient correct en probleemloos te functioneren na het doorvoeren van de Updates en Upgrades.
E82.	Technisch-applicatiebeheer betreft de werkzaamheden die nodig zijn voor het waarborgen van de ononderbroken goede werking van de SaaS-applicatie.
E83.	Er dient op geen enkele wijze sprake te zijn van inlogmogelijkheden voor Opdrachtnemer of diens voor deze opdracht in te zetten derden (backdoor) waar Opdrachtgever niet van op de hoogte is. Toegang tot de omgeving gaat altijd na overleg vooraf.
E84.	De technische omgeving is schaalbaar: o.a. de server- en databasecapaciteit moeten zonder downtijd uitgebreid kunnen worden wanneer Opdrachtgever daarom vraagt.
1.7	**Helpdesk**
E85.	De Opdrachtnemer beschikt over een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning ter ondersteuning bij onderhavige opdracht. 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.
E86.	De helpdesk van de leverancier levert zowel telefonische ondersteuning als ondersteuning via e-mail en een web-portaal/kennisbank.

E87. De helpdesk dient op werkdagen telefonisch bereikbaar te zijn tussen 08.00 en 17.00 uur. Voor ondersteuning door de helpdesk van de Opdrachtnemer worden geen aanvullende kosten in rekening gebracht.

E88. De Opdrachtnemer geeft totaal overzicht in ingediende wijzigingsvoorstellen van alle klanten.

E89. De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de SaaS-applicatie volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De Opdrachtgever bepaalt prioriteit van incidenten. T.a.v. ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:

Nr.	Omschrijving
1	De SaaS-applicatie is volledig niet beschikbaar (naar mening van de Opdrachtgever een Critical Problem)
2	De SaaS-applicatie is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers (naar mening van de Opdrachtgever een Major Problem)
3	Kleine verstoringen (naar mening van de Opdrachtgever een Minor Problem)
4	Gebruikers/beheerdersvraag

De helpdesk draagt tevens zorg voor het relateren van incidenten aan reeds bekende problemen m.b.t. de SaaS-applicatie. De Opdrachtnemer maakt voor de Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.

Nr.	Reactietijd	Oplossing binnen
1	0.5 uur beantwoorden (Op werkdagen tussen 8.30 en 17.00 uur)	Work-around binnen 4 uur op werkdagen Oplossing binnen 8 uur op werkdagen
2	1 uur (Op werkdagen tussen 8.30 en 17.00 uur)	Work-around binnen 8 uur op werkdagen Oplossing binnen 2 werkdagen.
3	4 uur (Op werkdagen tussen 8.30 en 17.00 uur)	Work-around binnen 2 werkdagen Oplossing in volgende reguliere versie
4	1 werkdag (Op werkdagen tussen 8.30 en 17.00 uur)	Antwoord binnen 1 week Oplossing in volgende reguliere versie

1.8 Beschikbaarheid en onderhoud

E90. De beschikbaarheid van de SaaS-applicatie is voor minimaal 98% per maand gegarandeerd, berekend met 24 uur per dag en zeven (7) dagen per week. Er wordt uitgegaan van een beschikbaarheid van de verbinding vanuit de Opdrachtgever van 100%, waarbij gepland onderhoud niet wordt meegenomen.

De beschikbaarheid wordt op basis van de volgende formule bepaald:
*(([aantal dagen maand x] * 24 * 60 - [aantal minuten gepland onderhoud maand x]) – [aantal minuten downtime]) / ([aantal dagen maand x] * 24 * 60 - [aantal minuten gepland onderhoud maand x]) * 100 = beschikbaarheid maand x*

E91. Onderhoudstijden van Opdrachtnemer worden ingepland buiten werktijden. Gepland onderhoud vindt derhalve plaats op avonden, weekenden of op nationale feestdagen.

E92. Werkzaamheden door de Opdrachtnemer worden altijd minimaal veertien (14) kalenderdagen van tevoren gecommuniceerd.

E93. Een uitzondering op de vaste onderhoudstijden (inclusief communicatie) zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn en informatieveiligheidsincidenten.

E94. Leverancier levert een concept SLA. In detail wordt deze in overleg met opdrachtgever na gunning fijn geslepen. De volgende onderdelen komen in ieder geval terug in de concept SLA:
1 Inleiding
-1.1 Looptijd en duur SLA
2 Communicatie en voorwaarden
-2.1 Communicatie
-2.2 Betrokkenheid van Derden
-2.3 Voorwaarden
- 2.3.1 Functioneel Beheer Organisatie

	-2.4 Informatiebeveiliging -2.5 Data binnen de EER 3 Diensten -3.1 Gebruiksondersteuning. -3.2 Technisch beheer ○ 3.2.1 Remote Release management ○ 3.2.2 Remote beheer -3.6 Service Level Management 4 Service levels -4.1 Afhandelen Incidenten ○ 4.2.1 Technisch beheer - Remote Release management ○ 4.2.2 Technisch beheer - Remote beheer -4.3 Beschikbaarheidsbeheer -4.4 Wijzigingsbeheer inclusief Updates en releasemanagement -4.5 Beschikbaarheidsbeheer -4.6 Capaciteitsbeheer -4.7 Uitwijk en Continuïteitsbeheer 5 Communicatie en escalatie -5.1 Functies en rollen -5.2 Communicatieniveaus -5.3 Communicatie bij Incidenten met prioriteit 1 en 2 -5.4 Escalatie 6 Exit strategie -6.1 Beëindiging contract -6.2 Gegevensoverdracht in geval van outsourcing of nieuwe opdrachtnemer -6.3 Gegevensoverdracht in geval van faillissement of overname -6.4 Formaten en kosten in geval van gegevensoverdracht

1.9 Trainingen en opleidingen

E95.	De Opdrachtnemer leidt in overleg met de opdrachtgever groepen van eindgebruikers, trainers (t.b.v. eindgebruikers. train de trainer) en functioneel-applicatiebeheerders van de SaaS-applicatie op in de Nederlandse taal. Hierbij worden zij voorzien van alle benodigde documentatie in digitale vorm, in de Nederlandse taal (indicatie B1 niveau) (incl. handleidingen, instructies en alle technische documenten) en eventuele hulpmiddelen, zodat het beheer volledig zelfstandig kan plaatsvinden. Het uitgangspunt is dat de betrokkenen na de opleiding als onderdeel van de implementatie alle vaardigheden van het script “praktijkweergave en opleiding (scenario’s)” (toegevoegd als bijlage bij de aanbestedingsleidraad) zelfstandig kunnen uitvoeren. Inschrijver biedt opleidingen voor de betrokkenen ((eind-)gebruikers en functioneel-applicatiebeheerders) van het BOR-beheersysteem, zodat zij met het BOR-beheersysteem zelfstandig (zonder tussenkomst van de Opdrachtnemer) kunnen werken.
E96.	De Opdrachtnemer geeft minimaal eenmaal – gedurende de beginperiode van de Overeenkomst – een gebruikerstraining aan hier direct boven genoemde gebruikers, en zoveel vaker als Opdrachtgever dit van Opdrachtnemer verlangt zonder hiervoor meerkosten te berekenen.
E97.	Na de implementatie is het volgen van een opleiding van het BOR-beheersysteem is minimaal 2x per jaar mogelijk. Dit vindt dan niet alleen plaats voor de opdrachtgever, maar gecombineerd met andere gebruikers.
E98.	De inschrijver verzorgt de opleiding op locatie bij de opdrachtgever. De opdrachtgever faciliteert de inschrijver (leslokaal, beamer, werkplekken, teams).

1.10 Doorontwikkeling

1.10.1 Algemeen

E99.	Op basis van het afgesloten contract garandeert de Opdrachtnemer dat de SaaS-applicatie, gedurende de contractperiode zal worden doorontwikkeld. Hieronder wordt, naast correctief en preventief onderhoud, ook verstaan dat binnen de SaaS-applicatie innovatief onderhoud wordt uitgevoerd om te blijven voldoen aan geldende wet- en regelgeving. Zie artikel 8 e.v. van de GIBIT.

E100.	De Opdrachtnemer hanteert een degelijk patchschema om alle componenten (zoals firmware, operatingsystems, applicaties) van de gehoste SaaS-applicatie actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen.
E101.	De laatste (beveiligings)patches zijn geïnstalleerd en deze worden volgens een patchmanagementproces doorgevoerd.
E102.	Kritische beveiligingsupdates worden binnen 24 uur na uitgifte geïnstalleerd en beschikbaar gesteld in de SaaS-applicatie.
E103.	Systeemsoftware, inclusief software die niet vanaf het internet benaderbaar is, dient up-to-date te worden gehouden.
E104.	Alle wijzigingen worden door de leverancier altijd eerst getest en gecontroleerd (o.a. op mogelijke beveiligingsissues) voordat deze in productie worden genomen en worden via wijzigingsbeheer doorgevoerd.

1.11 Exit strategie

E105.	De Opdrachtnemer stelt als onderdeel van het contract samen met de opdrachtgever een exit-plan op voor de overdracht van de data bij beëindiging van de overeenkomst, conform artikel 22 van de GIBIT. In dit plan wordt ten minste beschreven: - Op welke wijze, bij (reguliere of onverwachte) beëindiging van het contract, de (meta-)data wordt overgedragen aan een andere partij (bijvoorbeeld de eerstvolgende partij bij de aanbesteding); - Op welke wijze de betreffende (meta)data vervolgens wordt verwijderd en vernietigd.
E106.	De Opdrachtnemer zegt haar volledige medewerking toe wanneer er, bijv. bij beëindiging van de overeenkomst, een conversie/migratie naar een andere oplossing plaats dient te vinden. De data, ingevoerd door onze functioneel beheerders en gebruikers, is en blijft eigendom van Opdrachtgever. De Opdrachtnemer stelt de data van de Opdrachtgever ter beschikking aan de Opdrachtgever in een met de Opdrachtgever overeengekomen formaat. De Opdrachtgever van leverancier krijgt kosteloos de beschikking over alle gegevens en configuratiebestanden met alle bijbehorende documentatie zodat opdrachtgever of een derde partij namens haar e.e.a. kan migreren. Bovendien zal leverancier hierbij desgevraagd aanvullende dienstverlening verzorgen zodanig dat de continuïteit van de bedrijfsvoering van opdrachtgever niet in gevaar komt. Deze medewerking vindt plaats o.b.v. een nadere offerteaanvraag, tegen maximaal de uurtarieven zoals aangeboden bij de inschrijving.