



Programma van eisen

“API Gateway en ESB”

Naam aanbesteding: API Gateway en ESB
Corsanummer: D26-00447
Datum: 16 juli 2026

Inhoud

1.	Inleiding	3
2.	Huidige situatie	3
3.	Gewenste situatie	3
3.1	Integratieoplossingen	3
3.2	Migratie	4
4.	Programma van Eisen	5
4.1	Algemeen	5
4.1.1	Architectuur en standaarden	5
4.1.2	Common ground	6
4.1.3	Continuïteit en Exit strategie	6
4.2	Functionaliteiten	7
4.3	Techniek	7
4.3.1	Technische eisen	7
4.3.2	Privacy en Beveiliging	8
4.4	Dienstverlening	10
4.4.1	Implementatie Migratie	10
4.4.2	Beheer	10
4.4.3	Consultancy	12
4.4.4	Service level agreement	12

1. Inleiding

In dit document vindt u het Programma van Eisen. De eisen zijn uitsluitende criteria; het niet onvoorwaardelijk voldoen aan deze eisen uit dit document heeft uitsluiting van verdere deelname aan deze aanbestedingsprocedure tot gevolg.

De gemeente Lansingerland omarmt de principes van Common Ground. Doel is om een nieuwe architectuur binnen het applicatielandschap te implementeren, waarbij data wordt losgekoppeld van werkprocessen en applicaties. Dubbel opslaan van informatie is uit den boze, en meervoudig gebruik wordt gestimuleerd. Een goede integratieoplossing is daarvoor onontbeerlijk. De integratieoplossing is een servicelaag die informatiesystemen, zowel on premises als in de cloud, op een veilige manier met elkaar verbindt voor het uitwisselen van data.

De gemeente Lansingerland wil middels een Europese aanbesteding overgaan tot inkoop een integratieoplossing (Enterprise Service Bus en API Gateway). Deze nieuw aan te bieden Oplossing komt in de plaats van de huidige oplossing en moet als een SaaS-Oplossing te worden aangeboden. Naast technisch beheer moet ook functioneel beheer worden uitgevoerd door Opdrachtnemer conform dit Programma van Eisen. Vanuit de gemeente Lansingerland is de technisch beheerder het vaste aanspreekpunt.

2. Huidige situatie

Op dit moment beschikt gemeente Lansingerland over een on premises versie van Enable2Secure, Enable2Orchestrate (Adeptia) en VLTrader (Digikoppeling). Om diverse redenen moet deze applicatie vervangen worden door een nieuw aan te schaffen Oplossing.

3. Gewenste situatie

3.1 Integratieoplossingen

Als het gaat om de aan te bieden integratie-Oplossing, dan moet deze Oplossing in elk geval te voldoen aan de volgende belangrijkste eisen:

De aan te bieden Oplossing wordt volledig als een veilige SaaS-Oplossing aangeboden. Enkel een cloud connector in het DMZ mag nog in het DMZ van gemeente Lansingerland worden geplaatst om aan te kunnen sluiten op de on premises informatiesystemen bij gemeente Lansingerland;

1. De integratie-Oplossing zorgt voor optimale connectiviteit en integratie via beveiligde verbindingen tussen overheidspartijen, landelijke voorzieningen, applicaties in de cloud en applicaties on-premises;
2. De integratie-Oplossing biedt een Digikoppelingsadapter en een API Gateway;
3. De integratie-Oplossing biedt orchestratie-, validatie-, routeer- en transformatiefunctiealliteit voor een zo volledig mogelijke integratie van systemen;
4. De integratie-Oplossing ondersteunt tenminste de standaard koppelvlakken volgens de open standaarden van het Forum Standaardisatie en de standaarden uit de GEMMA;
5. De integratie-Oplossing ondersteunt het inrichten van maatwerkkoppelingen;

6. De integratie-Oplossing bestaat uit een productie en een testomgeving. Het verschil tussen beide omgevingen moet duidelijk zichtbaar zijn (bijv. door een andere kleurstelling);
7. De integratie-Oplossing zet maximaal in op het hergebruiken van services en configuraties, wat niet alleen de snelheid van het realiseren van nieuwe koppelingen gunstig beïnvloedt, maar ook de ontwikkelkosten minimaliseert;
8. De aan te bieden Oplossing voorziet in de logging van het dataverkeer en in de technische logging van verbindingen en infrastructuur;
9. Het functioneel-, applicatie- en technisch beheer van servers, dataverkeer, certificaten en infrastructuur wordt door Opdrachtnemer uitgevoerd.

3.2 Migratie

De migratie van de huidige omgeving naar de nieuwe maakt onderdeel uit van deze opdracht. De migratie van de huidige omgeving naar de nieuwe omgeving moet voor onze klanten ‘geruisloos’ geschieden, zonder downtime (hooguit een kort overschakelmoment van zo’n 15 minuten buiten kantoor tijd). Bestaande functionaliteit aan koppelingen en beveiligde toegang moet één op één worden gemigreerd volgens een nader af te spreken detailplanning.

Maar met de Oplossing alleen zal het gewenste resultaat niet optimaal zijn. De organisatie die deze Oplossing ‘bespeelt’ en beheert is daarin net zo belangrijk. We zoeken dan ook een organisatie die ons als gemeente Lansingerland op het gebied van integraties faciliteert:

1. Door een heldere en duidelijke communicatie met de technisch beheerder, applicatie- en systeembeheerders en andere relevante functies binnen Lansingerland;
2. Voor de technisch beheerder wordt een dashboard aangeboden om zo inzicht te krijgen in de status van alle koppelingen;
3. Tevens krijgt gemeente Lansingerland op een gebruiksvriendelijk manier toegang tot logging-informatie voor informatiebeveiligingsdoeleinden;
4. Opdrachtnemer levert kundige medewerkers die de aangeboden Oplossing implementeren en onderhouden (zowel technisch als functioneel);
5. Opdrachtnemer levert consultants om nieuw te realiseren koppelingen uit te schrijven in een functioneel- en technisch ontwerp, waarna Opdrachtnemer overgaat tot het implementeren van de nieuwe koppeling.

4. Programma van Eisen

4.1 Algemeen

4.1.1 Architectuur en standaarden

Nr	Omschrijving
AES01	De Inschrijver garandeert dat de Oplossing voldoet aan geldende nationale- en internationale wet- en regelgeving, standaarden (koppelingen) en afspraken (zie ook het katern Gemma Verbinden: https://www.gemmaonline.nl/index.php/KV2_Referentiecomponenten).
AES02	De volledige Oplossing en ondersteunende tools wordt geleverd als Software as a Service, in de cloud gehost, inclusief beveiligde verbindingen. Enige uitzondering hierop is, indien nodig, een, als onderdeel van de Inschrijving, in het DMZ van gemeente Lansingerland (ook deze Gateway wordt volledig beheerd door Opdrachtnemer). De volledige Oplossing en ondersteunende tools wordt geleverd als Software as a Service, in de cloud gehost, inclusief beveiligde verbindingen. De enige uitzondering is wanneer er een gateway en/of cloudconnector in het DMZ van het gemeentelijke netwerk geplaatst moet worden om de verbindingen met lokale interne systemen op een veilige en transparante wijze te laten verlopen.
AES03	De Opdrachtnemer levert na definitieve gunning, en voor het implementatietraject, een informatiearchitectuur voor de nieuwe situatie waarin de voorzieningen, alle koppelingen en afhankelijkheden met andere informatievoorzieningen in kaart zijn gebracht en beschreven.
AES04	De Opdrachtnemer waarborgt dat de aangeboden Oplossing niet meer dan één major versie achterloopt ('neerwaartse comptabiliteit') op de open standaarden van het Forum Standaardisatie en op de standaarden uit GEMMA die voor de Oplossing relevant zijn. Aanpassingen in de hierboven genoemde standaarden worden binnen 6 maanden door de Leverancier verwerkt nadat de aanpassingen als nieuwe standaard zijn gepubliceerd op genoemd forum of Gemma online. De vorige versie wordt nog minimaal 12 maanden ondersteund.
AES05	Indien de Oplossing gebruik maakt van email servers (e-mailen vanuit de Oplossing) dan geldt onderstaande eis: De gemeente Lansingerland heeft de mogelijkheid om de instellingen van striktheidsvormen in te stellen zonder dat de maildienst verstoord wordt. Dit is van toepassing voor de (verplichte) open standaarden SPF, DKIM en DMARC en het betreft het maildomein Lansingerland.nl.
AES06	De Oplossing moet gegevens uit kunnen uitwisselen via standaard koppelingen (gebaseerd op GEMMA) met andere systemen/applicaties, ook als deze binnen de gemeentelijke infrastructuur staan en/of van een andere leverancier zijn. Hieronder vallen o.a. het

	datadistributiesysteem, Zaaksysteem/DMS, maar ook bestandsdeling via bijvoorbeeld FTP.
AES07	De Oplossing moet gegevens uit kunnen uitwisselen via maatwerk koppelingen met andere systemen/applicaties, ook als deze binnen de gemeentelijke infrastructuur staan en/of van een andere leverancier zijn.
AES08	De Oplossing moet modulaair opgebouwd zijn, zodanig dat functionele componenten logisch gescheiden zijn en afzonderlijk te autoriseren.
AES09	De Oplossing moet voldoen aan de architectuur-principes van GEMMA: https://www.gemmaonline.nl/wiki/Wat_is_de_basisarchitectuur
AES10	De architectuur moet een logische scheiding hebben tussen: • gebruikersschermen, technische interfaces en web services; • proceslogica en informatieverwerking en • gegevensopslag en databases.
AES11	De Inschrijving mag niet uitgaan van al in gebruik zijnde producten en/of diensten bij/voor/van de gemeente Lansingerland, behalve voor daaruit te migreren content en/of daarmee te realiseren koppelingen, zoals deze zijn aangegeven in de Opdrachtscope van deze aanbesteding.

4.1.2 Common ground

Nr	Omschrijving
COG01	De inschrijver heeft het groeipact Common Ground van VNG ondertekend.
COG02	Indien nodig moet de leverancier gebruik maken van de API's waarvoor geldt 'verplicht deze standaard toe te passen' en de 'pas toe of leg uit' maatregel geldt. Zie https://www.gemmaonline.nl/index.php/API-standaarden .

4.1.3 Continuïteit en Exit strategie

Nr	Omschrijving
ESX01	Op basis van het afgesloten contract garandeert de Opdrachtnemer dat de Oplossing, gedurende de contractperiode, doorontwikkeld wordt zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief, ook verstaan dat de Oplossing adaptief onderhoud wordt uitgevoerd om als gemeente Lansingerland te blijven voldoen aan in de contractperiode geldende wet- en regelgeving. Daarbij speelt de Oplossing in op de ontwikkelingen op de markt.
ESX02	Bij beëindiging van de overeenkomst draagt Opdrachtnemer kosteloos de actuele functionele en technische ontwerpen en overige relevante documentatie van alle in het kader van de overeenkomst gerealiseerde koppelingen over aan de gemeente Lansingerland of een door Opdrachtgever aangewezen derde. Opdrachtnemer verleent daarbij alle redelijke medewerking die noodzakelijk is voor een volledige en ononderbroken overdracht.
ESX03	De Opdrachtnemer levert daarna ook een bewijs aan van vernietiging van de data op hun servers. Het bewijsdocument dient digitaal per e-mail te worden gedeeld met de in de DAP geregistreerd contactpersoon van de gemeente Lansingerland.
ESX04	Geheimhouding blijft van kracht ná het overdragen of beëindigen van de dienst.

ESX05	De Opdrachtnemer heeft maatregelen getroffen dat de gegevens/ data van de gemeente Lansingerland niet in handen van derden komen (bijvoorbeeld bij ontbinding/ faillissement/ doorverkoop), en maakt de maatregelen inzichtelijk.
ESX06	Gemeente Lansingerland is en blijft eigenaar van de gegevens/ data, en heeft daar te allen tijde de zeggenschap over. Gemeente Lansingerland stelt als uitgangspunt dat het proces van contractbeëindiging, migratie en beschikbaarheid van gegevens in het contract is geregeld en schriftelijk wordt vastgelegd.
ESX07	Opdrachtnemer levert na gunning, uiterlijk bij oplevering van de aangeboden Oplossing een Exitplan. Het Exitplan beschrijft een plan van aanpak voor het overdragen van de relevante diensten en de daarbij eventueel behorende over te dragen gegevens uit de ICT Prestatie. In het Exitplan worden de wederzijdse verplichtingen uiteengezet om een optimale overgang terug naar de gemeente Lansingerland of een opvolgend leverancier te ondersteunen bij het einde van de betreffende dienstverlening.

4.2 Functionaliteiten

Nr	Omschrijving
EIV01	De aangeboden Oplossing biedt een Graphical User Interface (GUI) voor de technisch beheerder van de gemeente Lansingerland. Hiermee beschikt de technisch beheerder over monitoring en logging van alle koppelingen. Het gaat hierbij om: - Inzage in de status van koppelingen (koppelingen die in gebruik zijn of zijn gedeactiveerd); - Inzage status van de actieve koppelingen; - Connectiviteit en verstoringen; - Inzage dataverkeer en onderliggende logging en validatiefouten.
EIV02	De Oplossing biedt functionaliteit voor orchestratie, transformatie en validatie.
EIV03	De Oplossing voorziet tenminste ook in een Digikoppeling adapter en API Gateway, die al bij meerdere klant(en) in productie zijn.

4.3 Techniek

4.3.1 Technische eisen

Nr	Omschrijving
ETE01	De aangeboden Oplossing moet volledig aansluiten met de aanwezige applicaties binnen het applicatielandschap zoals deze bij gemeente Lansingerland aanwezig is. Zie hiervoor ook Bijlage 1 - Overzicht huidige koppelingen.
ETE02	Opdrachtnemer geeft na definitieve gunning aan middels een technisch/functioneel ontwerp welke minimale vereisten nodig zijn aan de kant van de gemeente Lansingerland voor de toegang tot de Oplossing (de bandbreedte internetsnelheid, poorten, firewalls, systeemeisen van de eventuele Gateway, etc.).
ETE03	De Oplossing kent geen beperkingen met betrekking tot aantallen van gebruikers en/of te koppelen informatiesystemen en hoeveelheden data.

ETE04	De Opdrachtnemer draagt zorg voor het maken van back-ups waarbij de maximale RPO (Recovery Point Objective) 4 uur bedraagt. De maximale RTO (Recovery Time Objective) is 4 uur.
ETE05	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest. (gemeente Lansingerland ontvangt hierover een terugkoppeling).
ETE06	De aangeboden Oplossing voorkomt ongeautoriseerde toegang door middel van context based access control.
ETE07	De userinterface die beschikbaar wordt gesteld voor de technisch beheerder is toegankelijk via actuele en voorgaande (n-1) versies van gangbare internet browsers (Microsoft Edge, Mozilla Firefox, Apple Safari, Google Chrome) zonder gebruik te maken van plug-ins (zoals bijvoorbeeld Flash, Silverlight, ActiveX).
ETE08	De aangeboden Oplossing biedt mogelijkheden tot error handling.
ETE09	De aangeboden Oplossing biedt API Management en Ontwikkeling.
ETE10	De aangeboden Oplossing ondersteunt minimaal de volgende technische logging en opties: • Logging naar meerdere log hosts; • Logging kan niet (handmatig) worden aangepast; • Logging filters, welke event wel/ niet, IP Address exclusion; • Rate limiting; • Secure logging (signing); • Onderscheid tussen accounting, analyse en compliancy.
ETE11	De aangeboden Oplossing moet relevante logs, waaronder audit-, beveiligings- en systeemlogs, gedurende minimaal 13 maanden veilig en onveranderbaar op te slaan en beschikbaar te houden voor inzage en export.
ETE12	De user interface voor externe dienstverlening moet voldoen aan de eisen uit de Web Content Accessibility Guidelines (WCAG) toegankelijkheidsnorm: WCAG, niveau A + AA.
ETE13	De Oplossing beschikt over loggingsfunctionaliteit in het kader van de diverse audits, en om ook de inwoners en ondernemers te kunnen garanderen dat op een veilige manier met hun persoonlijke gegevens wordt omgegaan. Daarnaast maakt het inzichtelijk welke gegevens met wie worden gedeeld en waarom.
ETE14	Indien de Oplossing beschikt over debug logging-functionaliteit (waarbij gedetailleerde logs worden gegenereerd), dan mag dat niet onnodig aanstaan. Dit om te voorkomen dat er gegevens ten onrechte bewaard worden. Standaard staat deze functionaliteit uit en wordt geactiveerd voor diepgaande onderzoeksdoeleinden waarna de logs bij deactiveren/uitschakelen van de debug functionaliteit worden verwijderd.

4.3.2 Privacy en Beveiliging

Nr	Omschrijving
EIN01	Opdrachtnemer beschikt over een overeengekomen norm voor informatiebeveiliging zoals een ISO-27001:2015 ISO/IEC 27001:2022 of door Opdrachtnemer aan te tonen gelijkwaardig, waarbij dan de volgende voorwaarden van kracht zijn: a. De opdrachtnemer levert een afschrift van het certificaat.

	b. Het certificaat is geldig én niet ouder dan 3 jaar en afgegeven onder accreditatie van de RVA. c. De opdrachtnemer levert de bijbehorende statement of applicability (SOA) (ook wel: verklaring van toepasselijkheid). d. De scope (certificering) en de verklaring (SOA) passen voor of bij de onderhavige opdracht. (als er een ISO-certificaat is dat gaat over "het keukenkastje" dan past dat natuurlijk niet bij de onderhavige opdracht) (als de SOA heel mager is, dan past hij ook niet echt bij de BIO (waarschijnlijk)) e. De opdrachtnemer laat jaarlijks zien dat het verschil tussen de ISO-27001-ISO/IEC 27001:2022 / ISAE3000 certificering en de in de BIO genoemde overeenkomstige harde maatregelen (passend op de SOA) is opgelost dan wel geïmplementeerd door middel van het afgeven van een Statement of Compliance (zie ook BIO 4.4 laatste paragraaf) (het verschil tussen de ISO en de BIO is dat de ISO implementatie voorbeelden kent en de BIO kent harde verplichte maatregelen)
EIN02	De Oplossing is ontwikkeld volgens het security en privacy by design-principe, en garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en cryptografische technieken. Waaronder: • Wachtwoorden worden eenrichting-versleuteld (hash en salt) opgeslagen • Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie.
EIN03	Opdrachtnemer sluit aan bij de informatiebeveiligingsdienst (IBD) https://www.informatiebeveiligingsdienst.nl/leveranciers/. De Leverancier moet een ICT-foto inleveren van de gebruikte componenten van de SaaS-dienst en ontvangt hiermee kwetsbaarheidswaarschuwingen. De Leverancier richt een intern proces in voor het ontvangen en verwerken van de kwetsbaarheidswaarschuwingen in het interne problem- en changeproces.
EIN04	Opdrachtnemer stelt jaarlijks een Third Party Mededeling (TPM-verklaring) op conform de eisen vanuit ISO/IEC 27001:2015 en BIO(2.0). De jaarlijkse TPM moet tenminste inzicht geven in hoeverre onderstaande procedures worden toegepast op basis van opzet, bestaan en werking: • Vermogensbeheer (apparaten); • Back-up en Restore; • Business Continuïteitsbeheer; • Risicobeheer; • Wijzigingsbeheer; • Autorisatie en toegangsprocedure; • Logging en Monitoring; • Incidentbeheer; • Malware, patching, hardening, versleuteling procedures; • Penetratietesten.
EIN05	Opdrachtnemer voldoet aan de eisen vanuit de NIS2/Cyberbeveiligingswet en beschrijft in het implementatieplan hoe hieraan voldaan gaat worden.
EIN06	Opdrachtnemer voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties.
EIN07	De ICT Prestatie voldoet aan de meest actuele OWASP richtlijnen. In het bijzonder de meest actuele OWASP Top 10 (voor webapplicaties en API's) en de OWASP Application

	Security Verification Standard (ASVS). De aangeboden software en koppelvlakken dienen aantoonbaar bestand te zijn tegen de daarin beschreven beveiligingsrisico's.
EIN08	De Opdrachtnemer hanteert het principe van minimale toegangsverlening ("least privilege") en verleent uitsluitend toegang aan bevoegde personen die deze toegang aantoonbaar nodig hebben voor de uitvoering van de overeengekomen dienstverlening.
EIN09	De Opdrachtnemer blijft volledig verantwoordelijk voor het waarborgen van het overeengekomen niveau van informatiebeveiliging, ook wanneer gebruik wordt gemaakt van toeleveranciers of onderaannemers. De Opdrachtnemer dient contractueel te borgen dat deze partijen dezelfde informatiebeveiligingseisen of gelijkwaardige maatregelen toepassen als overeengekomen tussen Opdrachtgever en Opdrachtnemer.
EIN10	De Opdrachtnemer dient functiescheiding toe te passen en te voorkomen dat één persoon onverenigbare rollen of verantwoordelijkheden binnen de dienstverlening combineert. Indien volledige functiescheiding niet mogelijk is, dient de Opdrachtnemer mitigerende maatregelen te treffen en deze aantoonbaar vast te leggen.

4.4 Dienstverlening

4.4.1 Implementatie Migratie

Nr	Omschrijving
IM01	Opdrachtnemer garandeert dat de migratie van de huidige omgeving (zie bijlage B1 - Koppelingen.png en B2 - Koppelingen.docx naar de nieuwe omgeving voor onze klanten zo 'geruisloos' mogelijk wordt uitgevoerd, met minimale downtime.
IM02	Opdrachtnemer levert een gedetailleerd migratieplan aan bij de technisch beheerder (waarin minimaal de specificaties volgens gunningscriteria G2 zijn uitgewerkt). Pas nadat het plan akkoord is bevonden door gemeente Lansingerland kan er worden overgegaan tot realisatie. De implementatie moet z.s.m. na gunning te starten en uiterlijk 31-12-2026 woensdag 30 juni 2027 te zijn afgerond (dan stopt de ondersteuning van de huidige oplossing).

4.4.2 Beheer

Nr	Omschrijving
EBE01	Opdrachtnemer voert het technisch beheer uit. De technisch beheerder is verantwoordelijk voor het functioneren en beheren van de server(s) en database, alsmede voor de noodzakelijke verbindingen en de beschikbaarheid van de applicatie: • Zorgdragen voor een dagelijkse back-up van de systeemprogrammatuur en databases; • Tijdig plaatsen van updates en serverpatches; • Technisch en functioneel onderhoud van de database; • Tijdig beschikbaar stellen van nieuwe en geüpdatet standaardkoppelvlakken; • Beheer van de infrastructuur (koppeling naar gemeente Lansingerland en ketenpartners); • De technisch beheerder van de Opdrachtnemer is bevoegd om direct maatregelen te treffen als de continuïteit van de applicatie of de in de database opgeslagen informatie acuut in het geding is en is verplicht om in dit

	geval achteraf ter zake te rapporteren aan de technisch beheerder van de gemeente Lansingerland. • Voorzien in de fysieke beveiliging van de applicatie.
EBE02	Opdrachtnemer voert het functioneel- en applicatiebeheer uit. Hieronder wordt o.a. verstaan: • Gebruikersbeheer; • Beschikbaarheid van de applicatie en monitor; • Inrichting en onderhoud van gewenste processen (workflow) • Onderhouden van (systeem)documentatie; • Pro-actief beheer op dataverkeer en koppelingen en zorgen voor een ongestoorde werking van het dataverkeer; • Beheer cpa's en certificaten. • Afhandelen van het berichtenverkeer en oplossen communicatieproblemen; • Zorgdragen voor een zo spoedig mogelijke oplossing in geval van storingen binnen de applicatie, zo nodig door inschakeling van de technisch beheerder; • Opschonen logging volgens vooraf afgesproken bewaartermijnen • Afstemming nieuwe of gewijzigde functionaliteit en verstoringen met de technisch beheerder.
EBE03	De beheeractiviteiten worden geregistreerd en bespreekt Opdrachtnemer periodiek met de technisch beheerder van gemeente Lansingerland en draagt verbetervoorstellen voor.
EBE04	Alle functionele beheertaken worden uitgevoerd, zonder dat dit invloed heeft op de werking van de Oplossing voor de overige gebruikers. Gebruikers kunnen ingelogd blijven en volledig gebruik maken van de Oplossing tijdens deze functionele beheertaken.
EBE05	Autorisatie/toegang wordt bepaald door gemeente Lansingerland. Eventuele wijzigingen in autorisatie/toegang worden in opdracht van gemeente Lansingerland door Opdrachtnemer uitgevoerd.
EBE06	De Opdrachtnemer voert eigen ontwikkel- en testactiviteiten uit op een eigen omgeving.
EBE07	Toegang van vooraf geselecteerde medewerkers van gemeente Lansingerland tot de Oplossing (voor dashboard-doeleinden), gaat via Microsoft EntraID. Mocht dit niet mogelijk zijn dan dwingt de Oplossing minimaal een 'sterk' wachtwoord af, dat ieder (half) jaar moet worden aangepast en waarbij inloggen plaatsvindt op basis van 2FA.
EBE08	De Oplossing wordt na een instelbaar aantal minuten ongebruikt te zijn automatisch vergrendeld, wat alleen door het invoeren van een wachtwoord opgeheven kan worden. Bewerkingen worden opgeslagen. Hiermee wordt bedoeld dat openstaand werk wel bewaard wordt en via een hersteloptie wordt aangeboden.
EBE09	Gebruikersaccounts worden geblokkeerd na een instelbaar aantal achtereenvolgende foutieve authenticatiepogingen binnen een instelbare periode.
EBE010	De Opdrachtnemer dient ervoor zorg te dragen dat alle gebruikers- en beheeraccounts binnen de aangeboden Oplossing persoonsgebonden zijn en uitsluitend worden verstrekt aan individuele geautoriseerde gebruikers. Accounts dienen zodanig te zijn ingericht dat handelingen binnen de Oplossing altijd tot een specifieke gebruiker kunnen worden herleid.
EBE11	Het moet mogelijk zijn om met verschillende rollen te werken (bijvoorbeeld: alleen lezen, lezen en schrijven).

EBE12	Meldingen en wijzigingsaanvragen kunnen telefonisch door de technisch beheerder op werkdagen tussen 8.00 en 18.00 uur worden gemeld; daarbuiten kunnen meldingen en wijzigingsaanvragen 24x7 uur digitaal worden ingediend. Dit gebeurt bij voorkeur via een meldingenportaal of anders via e-mail.
EBE13	Opdrachtnemer neemt binnen een half uur telefonisch contact op met de technisch beheerder als een ernstige verstoring is geconstateerd. Daarnaast volgt er nog een afschrift naar de servicedesk van ICT. Dit kan via een melding in onze TOPdesk, of als dit niet kan via een e-mail.
EBE14	Verstoringen worden aan de technisch beheerder als een melding geregistreerd met een e-mailnotificatie naar de technisch beheerder en de servicedesk ICT.
EBE15	De Opdrachtnemer moet voor het beheer en gebruik, relevante en actuele beschikbare documentatie over de functionele en technische werking van de actuele ICT Prestatie beschikbaar stellen aan de beheerders van de gemeente Lansingerland, zodat deze aansluit bij de laatste en dus gebruikte release. Alle documentatie is opgesteld in de Nederlandse taal.

4.4.3 Consultancy

Nr	Omschrijving
C001	Gemeente Lansingerland wil inzicht in de uurtarieven behorende bij de consultancydiensten. Inschrijver moet deze opnemen in het prijzenblad.
C002	Reiskosten mogen niet apart worden gefactureerd.
C003	Bij de realisatie van een nieuwe koppeling levert Opdrachtnemer de juiste kundige expertise voor het betreffende type koppeling.
C004	Bij de realisatie van een nieuwe koppeling wordt een functioneel ontwerp opgesteld, aangevuld met een volledig technisch ontwerp. Deze worden door de technisch beheerder van gemeente Lansingerland aan de RFC toegevoegd die is aangemaakt in het gemeentelijke service-managementsysteem, waarna pas tot uitvoering zal worden overgegaan na goedkeuring van de changemanager van gemeente Lansingerland.
C005	Na oplevering van een nieuwe koppeling wordt deze gedocumenteerd door de Opdrachtnemer, wordt de architectuur bijgewerkt door de Opdrachtnemer en toegevoegd aan de totale systeemdokumentatie door de gemeente Lansingerland.
C006	Gemeente Lansingerland heeft de voorkeur voor een vaste consultant en een vaste vervanger (zowel in de projectfase van de implementatie/migratie, als daarna). De beschikbaarheid van deze consultants is uiterlijk binnen 2 werkweken te garanderen na aanvraag van hun diensten.
C007	Een nieuw te realiseren koppeling kent een gemiddelde doorlooptijd van maximaal 2 maanden.
C008	Opdrachtnemer levert gedurende de implementatiefase een projectleider als primair aanspreekpunt voor de gemeente Lansingerland.

4.4.4 Service level agreement

Nr	Omschrijving
EL01	Opdrachtnemer biedt een SLA (Service Level Agreement) aan en levert actief periodiek een rapportage op. Wij ontvangen rapportages omtrent: • beschikbaarheid van de dienst (maandelijks); • onderhoudsrapportages/kalender (maandelijks); • beveiligingscontroles (jaarlijks); • wijzigingsaanvragen en de afhandeling daarvan (maandelijks); • klachtenrapportages.
EL02	Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken dienstenniveaus en het doorvoeren van veranderingen en verbeteringen is regelmatig overleg op diverse organisatieniveaus noodzakelijk. De periodieke rapportage(s) - zie EL01 - maken hier onderdeel van uit. Na definitieve gunning worden hierover met beoogd Opdrachtnemer nadere afspraken gemaakt.
EL03	Opdrachtnemer brengt geen kosten in rekening voor ondersteuning door de helpdesk van de leverancier en aangemelde, aan de applicatie gerelateerde incidenten. Dit moet in het contract afgedekt zijn.
EL04	Voorafgaande aan een update (releases en patches) wordt de technisch beheerder minimaal twee weken van tevoren op de hoogte gebracht van de te verwachte wijziging(en). Gelijktijdig hierbij worden ook de release notes vrijgegeven en actief bekend gemaakt aan beheerders
EL05	Patchmanagement is procesmatig en procedureel ingericht, zodanig dat de laatste (beveiligings)patches zo snel mogelijk zijn geïnstalleerd in de ICT-voorzieningen.
EL06	Opdrachtnemer verzorgt een deskundige Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning, beschikbaar via telefoon, via e-mail en/of een 24x7 uur toegankelijk webportaal. 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.
EL07	De gemeente Lansingerland kan zelf (gerubriceerd) meldingen aanmaken en het volledige afhandelingsproces volgen.
EL08	De gemeente Lansingerland geeft bij het melden de prioriteit aan, de uiteindelijke prioritering wordt in samenspraak met Opdrachtgever vastgesteld op basis van onderstaande prioriteitsbepaling. Bij verschil met de opgegeven Prioriteit informeert Opdrachtnemer de gemeente Lansingerland hierover. 1. De Oplossing is volledig niet beschikbaar (naar mening van gemeente Lansingerland een Critical Incident). 2. De Oplossing is deels niet beschikbaar of deels niet beschikbaar voor meer dan 10% van de gebruikers (naar mening van gemeente Lansingerland een Major Incident). 3. Kleine verstoringen (naar mening van gemeente Lansingerland een Minor Incident). 4. Gebruikers/ beheedersvraag. De helpdesk van Opdrachtnemer draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen met betrekking tot de Oplossing. Vervolgens wordt het incident met de vastgestelde Prioriteit afgehandeld. Indien geen overeenstemming wordt bereikt over de prioriteit treedt de escalatieprocedure in werking.

	Cat	Reactietijd	Oplossing binnen
	1	0-1/2 uur beantwoorden 0-1 uur doorzetten naar de backoffice	Workaround binnen 4 uur. Oplossing binnen 8 uur
	2	1 uur	Workaround binnen 8 uur. Oplossing binnen 48 uur.
	3	24 uur	Workaround binnen 2 dagen. Oplossing in volgende reguliere versie.
	4	24 uur	Workaround binnen 1 week, oplossing in samenspraak met opdrachtgever.
Categorie 1 (Kritieke verstoring / Prio 1 - uitval gehele platform/kernkoppeling): Hiervoor gelden de reactie- en responstijden 24/7 (365 dagen per jaar). Buiten kantooruren dient een bereikbaarheidsdienst beschikbaar te zijn. Categorie 2, 3 en 4 (Hoog, Medium, Laag / niet-kritieke verstoringen): Hiervoor gelden de reactie- en oplostijden gedurende kantooruren (werkdagen van 08:00 tot 18:00 uur).			
EL09	Wijzigingen en releases van de Oplossing zelf: Opdrachtnemer is verantwoordelijk voor de gehele afhandeling van wijzigingsvoorstellen met betrekking tot de Oplossing. Elk wijzigingsvoorstel ondergaat een intakeprocedure.		
EL10	De Opdrachtnemer verzorgt jaarlijks dat de releasementen worden vastgesteld voor het volgend jaar. Bij vrijkomen van een release worden de releasenotes opgeleverd. Het streven is om zoveel mogelijk wijzigingen 'releasegewijs' door te voeren. Releases kunnen de volgende soorten wijzigingen omvatten: • Nieuwe versies van de standaardsoftware(componenten); • Nieuwe versies van de configuratie van de Oplossing.		
EL11	Voor het oplossen van urgente productieverstoringen kunnen ad-hoc crashreleases worden ingepland; Gemeente Lansingerland (technisch beheerder) wordt hier zo snel mogelijk over geïnformeerd.		
EL12	Productie versturende werkzaamheden worden buiten kantooruren uitgevoerd, tenzij anders overeengekomen. De gemeente Lansingerland kent de volgende kantooruren: • Maandag, dinsdag, woensdag en vrijdag: van 08.00 tot 18.00 uur • Donderdag: van 08.00 tot 19.00 uur		
EL13	De beschikbaarheid van de Oplossing is op werkdagen van 06.00 - 24.00 uur voor minimaal 98% gegarandeerd.		
EL14	De Opdrachtnemer hanteert als uitgangspunt Handreiking-Service-Level-Agreement-v2.3.1 (Bijlage E - 201912-Handreiking-Service-Level-Agreement-v2.3.1) van informatiebeveiligingsdienst. Dit betreft een modelovereenkomst, die u niet 'letterlijk' hoeft te volgen, zolang uw eigen SLA maar qua inhoud dezelfde onderdelen beschrijft.		
EL15	De opslag van de applicatie en gegevens en overige onderdelen van de Oplossing vindt fysiek plaats binnen de Europese Economische Ruimte en bij een hosting partij/datacenter		

die geen vestiging heeft in de Verenigde Staten, dit in verband met de USA Freedom Act. Dan wel dat de Opdrachtnemer kan garanderen dat de data niet onder USA Freedom Act kan worden opgevraagd.

Let op, voor alle Bijlagen verwijzen we u naar TenderNed.

