

Bijlage E: Programma van Eisen

Europese aanbesteding openbare procedure betreffende Partner voor Integratie Services

Inhoudsopgave

Inhoudsopgave	2
1. Inleiding	3
1.1 Algemeen	3
1.2 Relatie tot Beschrijvend document	3
1.3 Definities	3
2. Generiek eisen	4
3. Aanvullend eisen per sub-dienst	8
4. Niet functionele eisen (security)	9

1. Inleiding

1.1 Algemeen

Dit document beschrijft de eisen van Opdrachtgever ten aanzien van de te bieden Oplossing, zijnde Dienstverlening in de vorm van Integratie Services en heeft betrekking op de Dienstverlening zoals beschreven in Beschrijvend document. Voor een duidelijker beeld van de context waarin onderstaande eisen en Diensten passen, wordt verwezen naar de Beschrijving van de Opdracht in Beschrijvend document.

De eisen zijn van toepassing op alle diensten die geleverd worden door Wederpartij, zoals beschreven in het Beschrijvend document. De eisen zijn bindend en vormen een integraal onderdeel van de overeenkomst tussen Opdrachtgever en Wederpartij. Wederpartij is verplicht om te voldoen aan alle specificaties, eisen en voorwaarden zoals uiteengezet in dit Programma van Eisen, ongeacht de categorie van de geleverde dienst.

Inschrijver dient bijlage A 'Inschrijfformulier' rechtsgeldig te ondertekenen en aan de Inschrijving toe te voegen *en te uploaden in Source to Contract* om hiermee te verklaren dat Opdrachtnemer akkoord gaat met en voldoet aan de in het Programma van Eisen gestelde eisen en deze zal naleven gedurende uitvoering van de Opdracht.

Het niet voldoen aan één of meerdere eisen zal voor Aanbestedende dienst aanleiding zijn de Inschrijving uit te sluiten van verdere beoordeling.

1.2 Relatie tot Beschrijvend document

Deze Bijlage is onderdeel van Beschrijvend document Openbare procedure betreffende Partner voor Integratie Services.

1.3 Definities

De opgenomen begrippen en afkortingen in Beschrijvend document zijn onverkort van toepassing op deze Bijlage.

2. Generiek eisen

#	Onderwerp	Eis									
1	Algemeen	<p>Wederpartij is verantwoordelijk voor de volledige initiële implementatie van de projectactiviteiten, conform de scope zoals beschreven in het Beschrijvend Document (fase A en B), bijbehorende subonderdelen en de bijbehorende eisen uit het Programma van Eisen. De implementatie dient uiterlijk te starten binnen één maand na formele contractering en uiterlijk te worden afgerond binnen zes maanden na contractering, tenzij hierover expliciet andere afspraken zijn gemaakt met de Opdrachtgever.</p> <p>De Wederpartij dient hiervoor een Plan van Aanpak op te stellen en als onderdeel van de Inschrijving in te dienen.</p>									
2	Algemeen	De Wederpartij is in staat gedurende de projectactiviteiten op te schalen voor aanvullende verzoeken, zoals beschreven in fase D (proactieve dienstverlening) van het Beschrijvend Document, met betrekking tot het ontwikkelen van integraties die niet tot de initiële scope van de projectactiviteiten behoren.									
3	Algemeen	Na acceptatie van de projectactiviteiten (diensten A en B, zie het Beschrijvend Document) start de Wederpartij met het beheer en de supportdienstverlening, zoals beschreven in diensten C en D, zie het Beschrijvend Document).									
4	Algemeen	Wederpartij realiseert het integratieplatform uitsluitend binnen de Azure-tenant van de Opdrachtgever en maakt daarbij gebruik van de reeds ingerichte Azure Landing Zone.									
5	Algemeen	Wederpartij dient zowel infrastructuurcomponenten als integratiecomponenten in Azure in te richten en te wijzigen conform de principes van Infrastructure as Code (IaC), middels ARM/BICEP templates en Azure DevOps voor CI/CD pipelines.									
6	Algemeen	Wederpartij dient te beschikken over een actueel en gedocumenteerd rollbackbeleid waarin wordt vastgelegd op welke wijze wijzigingen, implementaties en configuraties teruggedraaid kunnen worden bij verstoringen of fouten.									
7	Algemeen	De wederpartij dient de rollbackprocedures minimaal éénmaal per jaar aantoonbaar te testen in een representatieve test- of acceptatieomgeving.									
8	Algemeen	Wederpartij dient CI/CD pipelines te voorzien van logging en auditing, waarbij alle uitgevoerde acties herleidbaar zijn tot individuele gebruikers.									
9	Algemeen	Wederpartij dient bij de realisatie en het beheer van integraties uitsluitend gebruik te maken van de in Microsoft Azure beschikbare Integratie Services, tenzij anders overeengekomen met de Opdrachtgever.									
10	Algemeen	Wederpartij dient volledige overdraagbaarheid van de IaC- en CI/CD-opzet te garanderen zodat Opdrachtgever of een opvolgende leverancier deze zonder belemmeringen kan beheren.									
11	Algemeen	De inrichting en werking van de Azure Cloud omgeving van de Opdrachtgever wordt niet afhankelijk gemaakt van de dienstverlening en services van de Wederpartij. Bij beëindiging van de Overeenkomst dient de Opdrachtgever de Cloud omgeving zelfstandig te kunnen blijven functioneren nadat eventuele koppelingen met de omgeving van de Wederpartij zijn verwijderd.									
12	Algemeen	Alle intellectuele eigendomsrechten op de door Wederpartij ingerichte of aangepaste Cloud infrastructuur, CI/CD-pipelines, Infrastructure-as-Code-scripts, configuraties, templates en aanverwante automatiseringsvoorzieningen berusten bij de Opdrachtgever. Deze voorzieningen worden volledig binnen de Azure-omgeving van de Opdrachtgever ontwikkeld, opgeslagen en beheerd, en verlaten deze omgeving niet zonder voorafgaande schriftelijke toestemming van de Opdrachtgever.									
13	Algemeen	Wederpartij dient de uitvoering van de werkzaamheden uitsluitend te laten verrichten door medewerkers die fysiek werkzaam zijn vanuit Nederland. Offshoring of nearshoring van werkzaamheden buiten het Nederlandse grondgebied is niet toegestaan									
14	Algemeen	<p>NWO streeft een samenwerkingsvorm na waarin NWO functioneel regie voert over de oplossing (het integratieplatform en de koppelingen tussen applicaties, via het integratieplatform). Wederpartij is daarbij verantwoordelijk voor de technische uitvoering. De roldemarcatie is globaal als volgt:</p> <table border="1"> <thead> <tr> <th>Taak</th><th>NWO</th><th>Wederpartij</th></tr> </thead> <tbody> <tr> <td>Vaststellen functionele behoefte</td><td> <ul style="list-style-type: none"> - Het functioneel vaststellen wat de vereisten zijn van gebruikers of relevante stakeholders binnen NWO. - Het functioneel goedkeuren van het functioneel ontwerp. </td><td> <ul style="list-style-type: none"> - Meedenken over technische haalbaarheid van de door NWO geïdentificeerde behoeftestelling - Vertalen van de functionele eisen naar functionele en technische ontwerpen. </td></tr> <tr> <td>Impactanalyse</td><td>- Goedkeuren van de impactanalyse uitgevoerd</td><td>- Analyseren van de impact van de voorgestelde wijziging of</td></tr> </tbody> </table>	Taak	NWO	Wederpartij	Vaststellen functionele behoefte	<ul style="list-style-type: none"> - Het functioneel vaststellen wat de vereisten zijn van gebruikers of relevante stakeholders binnen NWO. - Het functioneel goedkeuren van het functioneel ontwerp. 	<ul style="list-style-type: none"> - Meedenken over technische haalbaarheid van de door NWO geïdentificeerde behoeftestelling - Vertalen van de functionele eisen naar functionele en technische ontwerpen. 	Impactanalyse	- Goedkeuren van de impactanalyse uitgevoerd	- Analyseren van de impact van de voorgestelde wijziging of
Taak	NWO	Wederpartij									
Vaststellen functionele behoefte	<ul style="list-style-type: none"> - Het functioneel vaststellen wat de vereisten zijn van gebruikers of relevante stakeholders binnen NWO. - Het functioneel goedkeuren van het functioneel ontwerp. 	<ul style="list-style-type: none"> - Meedenken over technische haalbaarheid van de door NWO geïdentificeerde behoeftestelling - Vertalen van de functionele eisen naar functionele en technische ontwerpen. 									
Impactanalyse	- Goedkeuren van de impactanalyse uitgevoerd	- Analyseren van de impact van de voorgestelde wijziging of									

			door Wederpartij.	(nieuw)bouw werkzaamheden.	
		Uitvoering & realisatie	- Functionele acceptatietest.	- Uitvoeren van alle werkzaamheden met betrekking tot het bouwen, wijzigen, testen, technisch accepteren en in productie nemen van de oplossing.	
		Regulier beheer & onderhoud en doorontwikkeling	- Functionele in gebruik name van de oplossing.	- Regulier beheer, onderhoud en doorontwikkeling conform onderling afgesproken service management processen en service levels.	
15		<p>Werkzaamheden die niet behoren tot het reguliere beheer of de reguliere support, worden door Wederpartij uitgevoerd conform de Agile Way of Working (Agile WoW) principes, waaronder ten minste de volgende voorwaarden van kracht zijn:</p> <ul style="list-style-type: none"> • Het opleveren van werkende en geteste functionaliteiten in iteratieve sprints; • Het hanteren van een vooraf met de Opdrachtgever afgestemde sprintritme en planningsproces; • Transparant rapporteren over voortgang, impediments en gerealiseerde waarde per sprint; • Het betrekken van de Opdrachtgever bij prioritering en refinement van de werkzaamheden. 			
16	Algemeen	<p>De door Wederpartij ingezette medewerkers beschikken over aantoonbare ervaring met Azure Integration Services (waaronder ten minste één of meer van de volgende componenten: Azure API Management, Azure Service Bus, Azure Event Grid, Azure Logic Apps, Azure Functions en Azure Key Vault). NWO maakt daarbij onderscheid tussen verschillende senioriteitsniveaus op basis van ervaringsjaren.</p> <ul style="list-style-type: none"> • Junior: 1 tot 3 ervaringsjaren; • Medior: 3 tot 6 ervaringsjaren; • Senior: 6+ ervaringsjaren. 			
17	Algemeen	Alle data die wordt ingevoerd in de oplossing, of door de oplossing wordt gegenereerd, bewerkt, verwerkt of uitgevoerd, blijft te allen tijde eigendom en onder regie van NWO.			
18	Algemeen	De oplossing moet geïmplementeerd zijn op een (server)infrastructuur welke zich bevindt binnen de Europese Economische Ruimte (EER) en volledig valt onder Europese wetgeving, inclusief de Algemene Verordening Gegevensbescherming (AVG/GDPR) in geval van persoonsgegevens.			
19	Algemeen	De architectuur van de Oplossing dient schaalbaar te zijn, zodat piekbelastingen efficiënt kunnen worden opgevangen zonder onderbreking van de dienstverlening.			
20	Algemeen	De wederpartij werkt mee aan het opstellen van een DPIA, indien het opstellen van een DPIA nodig is			
21	Security	De Wederpartij waarborgt dat alle informatiebeveiligingseisen, welke onderdeel zijn van deze uitvraag, zoals beschreven in bijlage I van het Beschrijvend document, worden nageleefd en zijn geïmplementeerd.			
22	Security	Toegang tot de oplossing in de kantoren van NWO in Den Haag en Utrecht gebeurt via Single Sign-On (SSO) authenticatie en Entra-ID. Entra-ID authenticatie via NWO zorgt voor de 2-factor-oplossing.			
23	Security	De securityvereisten worden tijdens de implementatiefase, in afstemming met de securityafdeling van NWO vastgesteld en geïmplementeerd.			
24	Security	De oplossing wordt, bij native-ondersteuning door de gebruikte oplossing, aangesloten op het bestaande SOC/SIEM van NWO.			
25	Security	De Wederpartij waarborgt dat alle informatiebeveiligingseisen, welke onderdeel zijn van deze uitvraag, zoals beschreven in bijlage I van het Beschrijvend document, worden nageleefd en zijn geïmplementeerd.			
26	Wet-regelgeving & audit	De oplossing voldoet bij oplevering en gedurende de volledige looptijd van het contract aan de dan geldende Baseline Informatiebeveiliging Overheid (BIO) plus aanverwante richtlijnen uit de ISO 27001 informatiebeveiligingsstandaarden.			
27	Wet-regelgeving & audit	De oplossing voldoet bij oplevering en gedurende de volledige looptijd van het contract aan de Cyberbeveiligingswet (NIS2).			
28	Wet-regelgeving & audit	Alle back-ups moeten worden opgeslagen op een externe locatie binnen de EU, in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG/GDPR) en relevante wetgeving. Wederpartij is verantwoordelijk voor naleving en moet aantonen dat gegevensopslag en back-upbeheer voldoen aan de geldende regelgeving en dataveiligheidseisen.			
29	Wet-regelgeving & audit	De oplossing faciliteert implementatie van wijzigingen voortkomend uit nieuwe of aangepaste wet- en regelgeving.			
30	Beheer	<p>Als onderdeel van de dienstverlening levert de Wederpartij ondersteuning bij beheer- en ontwikkelprocessen op basis van het IT4IT-raamwerk. Dit omvat ten minste de volgende processen:</p> <ul style="list-style-type: none"> • Incidentmanagement; 			

		<ul style="list-style-type: none"> • Release & Deployment management; • Monitoring en alerting van de Azure componenten; • Change management; • Security management; • Continuity management; • Service request management; • Configuration management; • Cloud cost management.
31	Beheer	De exacte invulling en uitvoering van deze processen worden na contractering door de Wederpartij in onderling overleg afgestemd en vastgelegd in een Dossier Afspraken en Procedures (DAP). Dit document bevat afspraken over werkwijzen, serviceniveaus en escalatieprocedures. Daarbij verbindt de Wederpartij zich om na contracteren een DAP met Opdrachtgever overeen te komen.
32	Beheer	De oplossing moet beschikken over een gescheiden OTAP-omgeving, waarbij Ontwikkel, Test, Acceptatie en Productie duidelijk van elkaar gescheiden zijn. de oplossing ondersteunt binnen de OTAP-omgeving gelijktijdig gebruik van de afgezonderde omgevingen door verschillende geautoriseerde interne gebruikers. De Acceptatie-omgeving moet qua configuratie en performance representatief zijn voor de productieomgeving.
33	Beheer	<p>Opdrachtgever wenst zoveel mogelijk aan te sluiten op de standaard servicelevels van de Wederpartij, echter dienen deze minimaal op de door Opdrachtgever gevraagde niveau te liggen. Dit betreft:</p> <p>De leverancier hanteert de volgende responstijden en oplostijden per incidentcategorie:</p> <p>P1 – Kritiek (systeem onbeschikbaar / bedrijfskritisch)</p> <ul style="list-style-type: none"> • Responstijd: binnen 1 uur na melding bevestigen en starten met analyse. • Oplostijd: binnen 4 uur of er moet een tijdelijke workaround beschikbaar zijn die de bedrijfscontinuïteit waarborgt. <p>P2 – Hoog (ernstige verstoring, workaround mogelijk)</p> <ul style="list-style-type: none"> • Responstijd: binnen 2 uur na melding • Oplostijd: binnen 8 werkuren (maandag t/m vrijdag, 08:00–19:00 uur). <p>P3 – Middel (verstoring niet-kritieke functie)</p> <ul style="list-style-type: none"> • Responstijd: binnen 4 werkuren na melding (maandag t/m vrijdag, 08:00–19:00 uur). • Oplostijd: binnen 3 werkdagen <p>P4 – Laag (cosmetisch of wens)</p> <ul style="list-style-type: none"> • Responstijd: binnen 6 werkuren na melding (maandag t/m vrijdag, 08:00–19:00 uur). • Oplostijd: binnen 5 werkdagen
34	Beheer	De Opdrachtgever geeft bij het melden van een incident de prioriteit aan. De Wederpartij toetst deze prioriteit. Bij verschil van inzicht informeert de Wederpartij de Opdrachtgever hierover. Indien geen overeenstemming wordt bereikt, wordt de escalatieprocedure gestart.
35	Beheer	Wederpartij is in staat om de Azure omgeving (integratieplatform en de koppelingen tussen systemen) continu (24/7) te monitoren op beschikbaarheid, prestaties, en beveiliging. Dit omvat het gebruik van de standaard Azure monitoringsoplossingen, dashboarding en het delen van rapportages aan de Opdrachtgever.
36	Service management	<p>Wederpartij is verantwoordelijk voor het opstellen van Service Level Agreement (SLA) die volledig in lijn zijn met de eisen en uitgangspunten van de Opdrachtgever. De SLA moeten minimaal de volgende aspecten omvatten:</p> <ul style="list-style-type: none"> • Overlegstructuur, inclusief frequentie, inhoud en de betrokken rollen en personen; • Rapportages over de voortgang en prestaties van de dienstverlening; • Beschrijving van de geleverde diensten, inclusief de te behalen serviceniveaus en KPI's; • Duidelijke escalatieprocedure voor incidenten en problemen; • Reactie- en oplostijden voor incidenten, problemen en wijzigingen voor elk niveau; • De procedures voor escalatie, evaluatie, bijstelling en herziening van de inhoud van de SLA en DAP.
37	Service management	<p>Wederpartij hanteert een overlegstructuur op operationeel, tactisch en strategisch niveau. Wederpartij is verantwoordelijk voor het organiseren van deze overleggen, het documenteren en het opvolgen van de afspraken die daaruit voortvloeien. Opdrachtgever verwacht minimaal de volgende overlegfrequentie:</p> <ul style="list-style-type: none"> • Operationeel overleg: minimaal één (1) keer per maand; • Tactisch overleg: minimaal één (1) keer per vier (4) maanden; • Strategisch overleg: minimaal één (1) per twaalf (12) maanden.
38	Service management	Wederpartij wijst één (1) contactpersoon aan die verantwoordelijk is voor de afhandeling van onderwerpen op tactisch niveau. Deze contactpersoon dient als het centrale aanspreekpunt voor de Opdrachtgever betreffende de door de Wederpartij geleverde diensten en neemt deel aan het tactische overleg.

39	Service management	<p>Eens per kwartaal wordt tijdens het tactisch overleg de volgende punten tezamen met de Opdrachtgever en Wederpartij besproken:</p> <ul style="list-style-type: none"> • De geleverde serviceniveaus ten behoeve van de diensten in scope van de Overeenkomst; • Terugblik op de samenwerking van de afgelopen vier (4) maanden, te weten, wat gaat er goed en wat zijn de verbeterpunten; • Vooruitblik aankomende vier (4) maanden, te weten, acties om de dienstverlening te verbeteren, verwachte (onderhouds-)activiteiten, verwachte veranderingen ten aanzien van de dienstverlening, etc.
40	Service management	<p>Wederpartij biedt Opdrachtgever voortdurend inzicht in de uitvoering en status van de servicemanagementprocessen door middel van maandelijkse servicemanagementrapportages. De maandelijkse servicemanagement rapportage bevat minimaal de volgende aspecten:</p> <ul style="list-style-type: none"> • Afhandeling van incidenten verdeeld naar prioriteit; • Afhandeling van problemen met een verwijzing naar de bijbehorende Root Cause Analysis, indien van toepassing; • Overzicht van uitgevoerde wijzigingen en standaard-wijzigingen; • Voortschrijdende (maand-over-maand) beoordeling van de SLA.
41	Service management	<p>Wederpartij dient een aanspreekpunt (Single Point Of Contact) aan te stellen die in staat is om (op afstand) te reageren op storings, incidenten, wensen, calamiteiten of andere soorten informatieverzoeken. Deze aanspreekpunt moet op werkdagen van 08:00-17:30 uur bereikbaar zijn via een vast mailadres en een vast telefoonnummer.</p> <p>Buiten deze tijden wordt een calamiteitenregeling door Wederpartij beschikbaar gesteld, van toepassing zijnde op incidenten met prioriteit.</p>
42	Service management	Alle vormen van communicatie tussen Opdrachtgever en Wederpartij gebeurt in het Nederlands.
43	Service management	De aan Opdrachtgever toegewezen aanspreekpunt vanuit de Wederpartij dient te beschikken over de vereiste (technische) kennis om vanuit het perspectief van Opdrachtgever adequaat support te bieden omtrent de dienstverlening.
44	Service management	Personen die door Opdrachtgever zijn geautoriseerd kunnen 24/7 digitaal (via e-mail of een portaal) incidenten, wijzigingen, etc. melden bij de Wederpartij.
45	Service management	Iedere melding wordt gekoppeld aan een door de Opdrachtgever uitgegeven referentienummer, hiermee kan de voortgang gevolgd worden of kan navraag gedaan worden bij Wederpartij over de status van het incident.
46	Service management	<p>Na iedere melding ontvangt Opdrachtgever digitaal een bevestiging met de volgende informatie:</p> <ul style="list-style-type: none"> • Referentienummer (door NWO uitgegeven); • Datum en tijd van aanmelden; • Omschrijving van de melding, de verwachte oplostijd/responsetijd, conform de Service Level Agreement (SLA).
47	Beschikbaarheid	Gegadigde zorgt voor backups waarbij de maximale RPO (recovery point objective) 2 uur bedraagt, de maximale RTO (recovery time objective) bedraagt 5 uur.
48	Beschikbaarheid	<p>De integratieservices worden gehost binnen Microsoft Azure en dienen in beginsel 24 uur per dag, 7 dagen per week beschikbaar en toegankelijk te zijn, onafhankelijk van tijd en locatie. Gedurende werkdagen van 08:00 tot 19:00 uur (lokale tijd) wordt voor de productieomgeving een minimale beschikbaarheid van 99,99% per kalendermaand nagestreefd. Deze beschikbaarheid is exclusief gepland onderhoud.</p> <p>Buiten de genoemde kantoortijden geldt een minimale beschikbaarheid van 99%, waarbij eveneens geen rekening wordt gehouden met gepland onderhoud of werkzaamheden op verzoek van de Opdrachtgever.</p>
49	Exit	Wederpartij dient volledig mee te werken aan een overdracht van de dienstverlening bij beëindiging of wijziging van de Overeenkomst, inclusief het beschikbaar stellen van alle relevante documentatie, configuraties, bronbestanden, scripts, licentiesleutels en toegangsinformatie aan de Opdrachtgever of een door deze aangewezen opvolgende leverancier
50	Exit	Wederpartij dient gedurende de exitperiode de continuïteit van de dienstverlening te waarborgen, waarbij kritieke processen, systemen en koppelingen ononderbroken operationeel blijven tot de overdracht aantoonbaar en succesvol is afgerond.
51	Exit	Wederpartij dient op verzoek van de Opdrachtgever medewerking te verlenen aan kennisoverdracht en instructie aan interne medewerkers of de opvolgende leverancier, inclusief het organiseren van technische sessies, het beantwoorden van vragen en het faciliteren van toegang tot de Azure omgeving.
52	Exit	Wederpartij garandeert dat een eventuele exit niet leidt tot onvoorspelbare en hoge kosten.
53	Overig	Wederpartij conformeert zich aan de aansluitvoorwaarden voor de Azure Landing Zone van NWO, zoals beschreven in bijlage N van het Beschrijvend Document.

3. Aanvullend eisen per sub-dienst

#	Onderwerp	Eis
54	A1. Design van het integratie-platform	<p>Wederpartij levert een Low Level Design (LLD) op voor het integratieplatform (inclusief aangesloten applicaties) waarin zowel de functionele als de technische aspecten van de oplossing zijn uitgewerkt. Het LLD dient als basis voor de realisatie en wordt afgestemd op de eisen en wensen van de interne stakeholders van NWO. Daarbij dienen minimaal de volgende aspecten te worden beschreven in het LLD:</p> <p>Functioneel:</p> <ul style="list-style-type: none"> • Een beschrijving van de functionaliteiten die door het integratieplatform worden geleverd (zoals berichtenuitwisseling, transformatie van berichtenverkeer, logging en foutafhandeling); • Een beschrijving van de functionele vereisten van de stakeholders van NWO; • Doelstelling van de koppeling(en); • Bron- en doelsysteem; • Berichtentype en format; • Frequentie van uitwisseling; • Triggers voor berichtenuitwisseling; • Logging en monitoring; • Transformatie van berichtenverkeer, indien van toepassing; • Toepassing van business rules (zoals validaties, filters of beslisregels), indien van toepassing; • Foutafhandeling; • Kwaliteitsvereisten (als voorbeeld, beschikbaarheid, performance, schaalbaarheid, security). <p>Aanvullend wenst NWO inzicht te verkrijgen in technische aspecten, waaronder, maar niet beperkt tot:</p> <ul style="list-style-type: none"> • Overzicht technische componenten van het platform (integratiebus, message brokers, API-gateways); • Specificatie van gebruikte standaarden, technieken en formats (als voorbeeld: JSON, REST, XML); • Security vereisten, waaronder, maar niet beperkt tot (authenticatie, autorisatie en versleuteling van gegevens); • Overzicht van de benodigde netwerkverbindingen en infrastructuur.
55	A1. Design van het integratie-platform	<p>Het LLD dient het ontwerp aantoonbaar in lijn te brengen met de voor NWO relevante standaarden, richtlijnen of wetgeving, te weten:</p> <ul style="list-style-type: none"> • Baseline Informatiebeveiliging Overheid (BIO); • NIS2; • Zero Trust; • GDPR.
56	A1. Design van het integratie-platform	Wederpartij dient het ontwerp (LLD) te laten goedkeuren door de Opdrachtgever binnen NWO voorafgaand aan realisatie.
57	A2. Realisatie van het integratie-platform	De realisatie van het integratieplatform vindt plaats op basis van het goedgekeurde Low Level Design (LLD) door de Opdrachtgever.
58	A2. Realisatie van het integratie-platform	<p>De acceptatie van het gerealiseerde integratieplatform vindt uitsluitend plaats nadat:</p> <ul style="list-style-type: none"> • Het platform volledig is gerealiseerd conform het door de Opdrachtgever goedgekeurde Low Level Design (LLD) • Alle overeengekomen testfases, zoals opgenomen in het LLD, zijn uitgevoerd en de resultaten door de Opdrachtgever zijn goedgekeurd. • Kritieke bevindingen, die naar voren zijn gekomen uit de testresultaten, zijn opgelost. <p>Technische- en beheerdocumentatie zijn opgeleverd en goedgekeurd door de Opdrachtgever.</p>
59	B1. Transitie van bestaande koppelingen	Als aanvulling op het Low Level Design (zie eis 51), dient wederpartij voor iedere koppeling een ontwerp op te stellen, inclusief een realisatieplan met planning, testaanpak en risicoanalyse. Dit ontwerp en plan worden ter goedkeuring aan Opdrachtgever voorgelegd voordat met de realisatie wordt begonnen.
60	B1. Transitie van bestaande koppelingen	Wederpartij realiseert iedere koppeling conform het goedgekeurde ontwerp en realisatieplan, voert de overeengekomen testfases uit (waaronder integratie-, functionele en performance-tests) en levert de koppeling op in de productieomgeving na schriftelijke acceptatie door de Opdrachtgever.
61	B1. Transitie van bestaande koppelingen	De transitie van een koppeling mag niet leiden tot regressie in functionaliteit of het verlies van bestaande functionaliteiten die aanwezig zijn in de huidige situatie, tenzij schriftelijk overeengekomen met de Opdrachtgever.
62	B1. Transitie van bestaande koppelingen	De transitie van een koppeling wordt zodanig uitgevoerd dat de impact op de bedrijfsvoering en eindgebruikers minimaal is, en waar mogelijk geen merkbare verstoring optreedt in de dienstverlening van de Opdrachtgever.

63	C2. Beheer & onderhoud van de integraties tussen systemen	Opdrachtgever beoogt in de toekomst zelfstandig integraties te beheren. Wederpartij stelt de Opdrachtgever in staat om deze beheeractiviteiten uit te voeren, door het overdragen van volledige beheerinstruaties, toegang tot beheerportalen en monitoringtools en door het inrichten van de beheeromgeving zodanig dat de Opdrachtgever zelfstandig incidenten, wijzigingen en verbeteringen kan doorvoeren. Het recht tot het zelf beheren van integraties is expliciet aan de Opdrachtgever voorbehouden.
64	C2. Beheer & onderhoud van de integraties tussen systemen	Het prijsmodel voor beheer is gebaseerd op een beheerprijs per koppeling. Een vermindering van het aantal koppelingen dat door Wederpartij wordt beheerd leidt tot een evenredige aanpassing van de beheervergoeding aan de Wederpartij, ingaande vanaf de maand volgend op de wijziging in het aantal koppelingen.
65	D1. Proactieve dienstverlening, advisering en consultancy	Wederpartij kan op verzoek van de Opdrachtgever nieuwe integraties realiseren. Deze werkzaamheden worden, tenzij anders overeengekomen, op korte termijn ingepland, doch uiterlijk binnen drie maanden na het verzoek van de Opdrachtgever.
66	D1. Proactieve dienstverlening, advisering en consultancy	Wederpartij zorgt voor voorspelbaarheid in de opleverplanning door te werken met vooraf overeengekomen integratietypen (bijvoorbeeld niet complex, complex, zeer complex), waarvan de exacte definities en doorlooptijden na contractering gezamenlijk worden vastgesteld.
67	D1. Proactieve dienstverlening, advisering en consultancy	De realisatie van nieuwe integraties vindt plaats conform een vast bouwproces, bestaande uit ten minste: <ul style="list-style-type: none"> • Inventarisatie en documentatie van functionele, technische en beveiligingsvereisten in samenwerking met de Opdrachtgever; • Opstellen en afstemmen van een ontwerp inclusief realisatieplan; • Ontwikkeling en configuratie van de integratie; • Uitvoering van overeengekomen testfases; • Oplevering (na acceptatie door Opdrachtgever) in de productieomgeving.
68	D1. Proactieve dienstverlening, advisering en consultancy	Elke opgeleverde integratie wordt voorzien van volledige documentatie en wordt aangesloten op de bestaande beheer- en supportprocessen (incl. monitoring) en voldoet aan de afspraken zoals vastgelegd in de geldende SLA tussen Opdrachtgever en Wederpartij.
69	D1. Proactieve dienstverlening, advisering en consultancy	Opdrachtgever beoogt in de toekomst zelfstandig nieuwe integraties te realiseren. Wederpartij stelt de Opdrachtgever in staat om deze activiteiten uit te voeren, door het beschikbaar stellen van alle benodigde documentatie, bouwstandaarden, sjablonen, ontwikkeltools en toegangsrechten binnen de omgeving van de Opdrachtgever. Het recht tot het zelf bouwen van integraties is expliciet aan de Opdrachtgever voorbehouden.
70	D1. Proactieve dienstverlening, advisering en consultancy	Wederpartij is in staat om op verzoek adviesdiensten te verlenen inzake de huidige en mogelijk toekomstige dienstverlening in scope van deze Overeenkomst. Dit omvat onder meer, maar niet beperkt tot: <ul style="list-style-type: none"> • Begeleiden van Opdrachtgever in het bevorderen van de integratie volwassen- en deskundigheid; • Adviseren van Opdrachtgever op het gebied van integratietechnologie, technologische kansen/ontwikkelingen, competentieontwikkeling, etc.

4. Niet functionele eisen (security)

#	Onderwerp	Eis
71	Wet- en regelgeving	Opdrachtnemer moet kunnen aantonen dat zij en haar producten en voldoen aan de Nederlandse en EU-wetgeving die op hun dienstverlening van toepassing is, zoals Wet Computercriminaliteit, Cyberbeveiligingswet (Cbw/NIS2), Algemene Verordening Gegevensbescherming (AVG) en Archiefwet.
72	Wet- en regelgeving	Opdrachtnemer en aangeboden oplossing voldoet bij oplevering en gedurende de volledige looptijd van het contract aan de genoemde wet- en regelgeving.
73	Standaarden	Opdrachtnemer moet gedurende de volledige doorlooptijd van het contract gecertificeerd zijn op het gebied van informatiebeveiliging (bijvoorbeeld ISO 27001 of gelijkwaardig).
74	Standaarden	Opdrachtnemer moet gedurende de volledige doorlooptijd van het contract voldoen aan de gestelde eisen vanuit de Baseline Informatiebeveiliging Overheid (BIO) 2.0.
75	Standaarden	Opdrachtnemer moet een erkend informatiebeveiligingsbeheersysteem (ISMS of gelijkwaardig) geïmplementeerd en in gebruik hebben.
76	ICO	Opdrachtnemer voldoet aan de gestelde eisen vanuit de ICO-wizard die van toepassing zijn op haar organisatie en dienstverlening zoals gesteld in Bijlage - ICO Wizard.xls.
77	Audit	Opdrachtnemer moet regelmatig (minimaal jaarlijks) een onafhankelijke audit van haar informatiebeveiligingspraktijken en pentest van haar aangeboden oplossing laten uitvoeren.

78	Audit	Opdrachtnemer verschaft inzicht aan Opdrachtgever in de aard en omvang van de uitgevoerde beveiligingstest(en) alsmede de resultaten ervan.
79	Audit	Opdrachtgever behoudt zich het recht om periodiek/jaarlijks (externe) audits uit te voeren op de gestelde eisen in dit document.
80	Informatiebeveiligingsbeleid	De opdrachtnemer is in bezit van een gedocumenteerd informatiebeveiligingsbeleid, onderhoudt dit en handhaaft het. Dit beleid is door het management goedgekeurd en aan al het personeel en relevante derden worden gecommuniceerd. Deze procedures ondersteunen een informatiebeveiligingsbeheersysteem (ISMS).
81	Organisatie van informatiebeveiliging	De opdrachtnemer definieert, documenteert en onderhoudt een organisatiestructuur voor informatiebeveiliging met duidelijk toegewezen rollen, verantwoordelijkheden en bevoegdheden.
82	Beveiliging van personeel	De opdrachtnemer implementeert gedocumenteerde informatiebeveiligingsprocedures voor de indiensttreding, functieveranderingen en uitdiensttreding van medewerkers. Het personeel wordt gedurende hun dienstverband op de hoogte gehouden van hun beveiligingsverantwoordelijkheden. De opdrachtnemer zorgt ervoor dat personeel met toegang tot informatieactiva onderworpen is aan passende antecedentenonderzoeken, trainingen in beveiligingsbewustzijn en contractuele geheimhoudingsverplichtingen gedurende hun dienstverband of opdracht.
83	Beheer van activa	De opdrachtnemer identificeert, classificeert, documenteert en houdt een nauwkeurige inventaris bij van informatieactiva, waaronder hardware, software en data, en implementeert beheersmaatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van deze activa te beschermen.
84	Toegangsbeheer	De opdrachtnemer implementeert toegangscontrolebeleid en -procedures die de toegang tot informatie en systemen beperken op basis van functies en bedrijfsbehoeften, met gedefinieerde processen voor goedkeuring, beoordeling en intrekking van toegang. De opdrachtnemer zorgt dat de toegang tot informatiesystemen en gegevens beperkt is tot geautoriseerde personen op basis van bedrijfsbehoeften en het principe van minimale bevoegdheden.
85	Cryptografie	De opdrachtnemer past passende cryptografische beheersmaatregelen toe om de vertrouwelijkheid, integriteit en authenticiteit van gevoelige informatie in rust en tijdens transport te beschermen, inclusief het gebruik van, in de branche erkende (bijv. NCSC), aanvaarde encryptiestandaarden, en documenteert hoe encryptie wordt geïmplementeerd in de relevante systemen.
86	Fysieke en omgevingsbeveiliging	De opdrachtnemer dient fysieke en omgevingsbeveiligingsmaatregelen te implementeren om faciliteiten, apparatuur en informatieactiva te beschermen tegen ongeautoriseerde toegang, schade of verstoring.
87	Operationele beveiliging	De opdrachtnemer dient operationele procedures en controles te implementeren en te handhaven om een veilige verwerking, opslag en overdracht van informatie te waarborgen, inclusief wijzigingsbeheer, logging, monitoring en bescherming tegen malware. Opdrachtnemer dient gedocumenteerde gegevensstromen en opslaglocaties vast te stellen.
88	Communicatiebeveiliging	De opdrachtnemer dient informatie die via netwerken wordt verzonden te beschermen door passende beveiligingsmaatregelen te implementeren voor communicatiesystemen, waaronder e-mail-, berichten- en videoconferentieplatformen om ongeautoriseerde toegang, onderschepping of wijziging van gegevens te voorkomen.
89	Systeemverwerving en -onderhoud	De opdrachtnemer dient ervoor te zorgen dat de informatiebeveiligingsvereisten gedurende de gehele levenscyclus van systemen worden nageleefd, inclusief verwerving, ontwikkeling, implementatie, onderhoud en uitfasering van informatiesystemen en -applicaties.
90	Relaties met leveranciers	De opdrachtnemer dient ervoor te zorgen dat informatiebeveiligingsrisico's die verband houden met onderopdrachtnemers en derden worden geïdentificeerd en beheerd, en dat contractuele overeenkomsten passende informatiebeveiligingsvereisten bevatten en de hierin gedefinieerde vereisten worden opgelegd en gehandhaafd.
91	Beheer van beveiligingsincidenten	De opdrachtnemer dient een incidentbeheerproces op te zetten en te handhaven voor de identificatie, rapportage, het beheer, het reageren op, herstellen en de tijdige melding van informatiebeveiligingsincidenten, inclusief incidenten die van invloed zijn op de informatie of diensten van de klant, inclusief gedocumenteerde rollen, escalatiepaden en reactieprocedures.
92	Bedrijfscontinuïteitsbeheer	De opdrachtnemer dient bedrijfscontinuïteits- en rampenherstelplannen te implementeren en te onderhouden die de informatiebeveiliging tijdens verstoringen waarborgen en de beschikbaarheid en continuïteit van kritieke diensten garanderen.
93	Naleving	De opdrachtnemer dient alle toepasselijke wettelijke, regelgevende en contractuele informatiebeveiligingsvereisten met betrekking tot de geleverde diensten te identificeren, te documenteren en na te leven en dient op verzoek bewijs van deze naleving te kunnen overleggen.
94	Sub-leveranciers & ketenbeheer	Partners van Opdrachtnemer en/of eventuele derde partijen die namens Opdrachtnemer werkzaamheden verrichten voor Opdrachtgever moeten voldoen aan alle gestelde eisen aan Opdrachtnemer.
95	Datalocatie	Alle data, logging en back-ups moeten worden opgeslagen op een externe locatie binnen de EU, in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG/GDPR) en relevante wetgeving. Opdrachtnemer is verantwoordelijk voor naleving en moet aantonen dat gegevensopslag en back-upbeheer voldoen aan de geldende regelgeving en dataveiligheidseisen.