

Integratieplatform Programma van Eisen				
Id	Onderwerp	Beschrijving	Prio	Fase
1	Architectuur	De geboden oplossing bestaat uit "Bewezen Technologie"; alleen hard- en software wordt ingezet waar binnen de markt (aantoonbaar) goede ervaringen mee behaald zijn.	Must	2
2	Architectuur	Er wordt minimaal een test-, acceptatie- en productieomgeving beschikbaar gesteld. De acceptatie-omgeving dient te allen tijde gelijk te zijn aan de productieomgeving (geanonimiseerd). In de implementatie fase wordt op verzoek en zonder kosten een opleidingsomgeving geleverd.	Must	2
3	Architectuur	Het moet voor de Provincie ten alle tijden duidelijk zijn welke nieuwe, gewijzigde of verwijderde functionaliteit in een update zit.	Must	2
4	Architectuur	De leverancier heeft een roll-back scenario, dat garandeert dat de situatie van vóór het doorvoeren van de update hersteld kan worden. Er dient specifiek aandacht te zijn voor contentmutaties.	Could	2
5	Architectuur	De Provincie moet kunnen beschikken over alle nieuwe functionaliteit die het platform van de leverancier biedt, maar de Provincie moet zelf in staat zijn de keuze te maken of zij de nieuwe functionaliteit wil activeren binnen het platform zoals de Provincie dat gebruikt.	Could	2
6	Architectuur	De leverancier dient back-ups van de gegevens te maken en te beheren conform de retentie-eisen van de Provincie, of beter. De minimale eisen zijn: - Retentieperiode: 12 maanden, tenzij wet- of regelgeving anders voorschrijft. - Beschikbaarheid: Back-ups moeten op verzoek van de Provincie unencrypted beschikbaar worden gesteld. - Herstelbaarheid: Gegevens dienen hersteld te kunnen worden in geval van dataverlies. Indien de leverancier geen adequate retentie garandeert, moet het technisch in staat zijn aan te sluiten op het back-upsysteem (Commvault) van de Provincie. Aanvullend moet de leverancier in gezamenlijkheid met de Provincie ook twee keer per jaar testen of de restores goed zijn v.w.b. herstelbaarheid	Must	2
7	Architectuur	Wanneer een van de componenten in een SaaS-omgeving draait dient de leverancier te borgen dat back-ups geografisch gescheiden van productiedata worden opgeslagen (offsite) binnen de EER, zodat een storing of calamiteit op de primaire locatie niet leidt tot gelijktijdig verlies van productie- en back-updata.	Must	1
8	Architectuur	Het platform biedt standaard mogelijkheden voor integratie met architectuurtooling ten behoeve van het vastleggen, hergebruiken en beheren van architectuurartefacten, afhankelijkheden en impactanalyses.	Should	2
9	Architectuur	Het platform dient te kunnen integreren met de CMDB-oplossing van de Provincie (ServiceNow) waarbij de CMDB van de Provincie leidend is.	Should	2
10	Architectuur	Er dient volledig getest te kunnen worden zonder de productieomgeving te raken. Daarvoor kan het nodig zijn dat er minimaal een A(acceptatie)-omgeving beschikbaar is, waarop getest kan worden. Als hiervoor gekozen is dan moet de acceptatie omgeving van de het platform tenminste kunnen koppelingen met de Acceptatie omgeving van het zaakstelsel en zo mogelijk nog andere gekoppelde back-end systemen (o.a. SAP en externe systemen zoals Belastingdienst). Als de leverancier een andere optie heeft dan staat de Provincie hier ook voor open om dit in gezamenlijkheid te onderzoeken.	Must	2
11	Architectuur	De Provincie moet zelfstandig of met behulp van de leverancier koppelingen kunnen toevoegen, wijzigen of verwijderen in de A(acceptatie) (bijvoorbeeld ten behoeve van regressietests).	Must	2
12	Architectuur	Updates worden voorafgaand aan productie getest en door de Provincie geaccordeerd. Dit geldt niet voor updates van onderliggende platformdiensten waarop de leverancier geen invloed heeft.	Must	2
13	Architectuur	De leverancier moet wijzigingen en vernieuwingen bij integraties kortcyclisch en beheerst doorvoeren, bijvoorbeeld volgens Continuous Delivery of vergelijkbare werkwijzen, met behoud van stabiliteit en beheersbaarheid van de productieomgeving.	Must	1
14	Architectuur	De inrichting kan omgaan met zowel verwachte als onverwachte intensivering of extensivering (horizontaal en verticaal schalen).	Must	2
15	Architectuur	Deployments van het integratieplatform in het vertrouwde provinciale netwerk of door de Provincie aangewezen cloudomgeving wordt als IaC (Infrastructure as Code) uitgerold.	Must	2
16	Architectuur	Het platform moet beschikken over een centrale, doorzoekbare servicecatalogus of developer portal waarin alle via het platform aangeboden integratiediensten vindbaar zijn. De catalogus moet zowel voor bevoegde gebruikers als via een machineleesbare interface toegankelijk zijn.	Must	1
17	Architectuur	Gegevens over het ontstaan, de beveiliging, de beschikbaarheid, het gebruik, het beheer, wijziging en de verwijdering van informatie moeten worden vastgelegd in logbestanden. Het platform moet hiervoor ingericht zijn. De bewaartermijn hiervan is 12 maanden.	Must	2
18	Architectuur	Het platform moet gegevensuitwisseling tussen (web)applicaties ondersteunen via gedocumenteerde API's op basis van REST, conform de NLGov REST API Design Rules, SOAP, met formele specificaties zoals OpenAPI en XML Schema Definition (XSD).	Must	2
19	Architectuur	Het platform moet dataformaat- en protocoltransformaties ondersteunen, minimaal voor XML, JSON en tekstformaten, zodat verschillende systemen veilig en eenduidig kunnen communiceren.	Must	2
20	Architectuur	Het platform moet out-of-the-box connectoren bieden voor ten minste databases (SQL, MySQL), SOAP, REST, bestanden, FTP, SFTP en JMS.	Must	2
21	Architectuur	Bij oplevering van het platform wordt door de leverancier een functionele beschrijving meegeleverd bijvoorbeeld in de vorm van een handleiding.	Must	2
22	Architectuur	De door de Provincie gevraagde functionaliteiten moet geleverd kunnen worden door standaard software en direct leverbaar te zijn bij start implementatie. Daarmee wordt bedoeld dat de Provincie alleen standaard software wil en dat daar slechts in uitzonderingssituaties van kan worden afgeweken. Nieuw te ontwikkelen functionaliteit en / of maatwerk dient zo dicht mogelijk op de Core van het platform te zitten.	Must	2
23	Architectuur	Het integratieplatform dient een hybride implementatiemodel te ondersteunen waarbij integratiediensten kunnen worden uitgevoerd en beheerd vanuit zowel SaaS-omgevingen als vanuit het vertrouwde provinciale netwerk of door de provincie aangewezen cloudomgeving. Het platform moet de mogelijkheid bieden om integratiecomponenten, runtimes en connectiviteitsvoorzieningen binnen het vertrouwde provinciale netwerk of een door de provincie aangewezen cloudomgeving te plaatsen. Oplossingen die uitsluitend als SaaS-dienst beschikbaar zijn en geen hybride implementatie ondersteunen, voldoen niet aan deze eis.	Must	1
24	Architectuur	Self-service automation moet via het Service Management Tooling van de Provincie lopen (huidig: ServiceNow).	Must	2
25	Architectuur	Beleid leveranciersbeveiliging De leverancier heeft een formeel beleid opgesteld voor de beveiliging van leveranciersrelaties. Dit beleid is gedocumenteerd, actueel en aantoonbaar in gebruik binnen de organisatie.	Must	2
26	Architectuur	Voor elke inkoopopdracht van de Provincie wordt er een Business Impact Analyse (BIA) of risicoanalyse door de Provincie uitgevoerd, zodat op basis hiervan de passende beveiligingsmaatregelen kunnen worden bepaald. Leverancier dient hieraan mee te werken.	Must	2
27	Architectuur	Leverancier is verplicht om minimaal jaarlijks via een onafhankelijke derde (bijv. auditrapport) aan te tonen dat hij voldoet aan de beveiligingseisen, inclusief de volledige keten van toeleveranciers. Wijzigingen die leiden tot een verandering in het auditrapport dienen zo spoedig mogelijk bij de Provincie, in de persoon van de contractmanager, te worden aangegeven.	Must	1
28	Architectuur	Indien, naar oordeel van de Provincie, aanvullend onderzoek noodzakelijk is, naar aanleiding van aangeleverde stukken, is leverancier verplicht hier aan mee te werken.	Must	2
29	Architectuur	Transparantie over incidenten en kwetsbaarheden Leverancier is verplicht is om (potentiele) beveiligingsincidenten en (potentiele) kwetsbaarheden (inclusief datalekken) binnen 4 uren te melden.	Must	2
30	Architectuur	Inzicht in toeleveranciersketen Leverancier verschaft vooraf inzicht in de keten van onderaannemers, zodat de Provincie de eventuele risico's kan beoordelen zodat mogelijk mitigerende maatregelen ten behoeve van risico's worden genomen.	Must	2
31	Architectuur	Beveiliging in de keten borgen De vastgestelde beveiligingseisen gelden voor de gehele keten van toeleveranciers. Eventuele uitzonderingen moeten expliciet worden onderbouwd en goedgekeurd op het juiste niveau binnen de Provincie.	Must	2
32	Architectuur	De Provincie beoordeelt jaarlijks of de leverancier nog voldoet aan de door haar gestelde eisen, identificeert eventuele risico's en neemt beslissingen over eventueel aanvullende maatregelen. Leverancier dient hieraan mee te werken.	Must	2
33	Architectuur	Leverancier houdt een actueel overzicht bij van alle relevante leveranciers en de bijbehorende contracten.	Must	2

Integratieplatform Programma van Eisen				
Id	Onderwerp	Beschrijving	Prio	Fase
34	Architectuur	Leverancier heeft een beleid voor het selecteren, beoordelen en beheren van cloudproviders. Dit beleid wordt minimaal elke drie jaar herzien en bevat duidelijke ontbindingscriteria.	Must	2
35	Architectuur	Beoordeling ISMS-beleid leverancier. De leverancier geeft inzicht in zijn informatiebeveiligingsbeleid, inclusief rollen, incidentmanagement, awareness en continuïteitsmaatregelen zodat dit kan worden beoordeeld.	Must	2
36	Architectuur	De leverancier overlegt jaarlijks een geaccrediteerd ISO 27001 certificaat met Verklaring van Toepasselijkheid (VvT), waarvan de scope de relevante dienst daadwerkelijk afdekt.	Must	1
37	Architectuur	De leverancier heeft een gedocumenteerd en aantoonbaar werkend proces voor het identificeren en oplossen van kwetsbaarheden (ontdekking, registratie, beoordeling, herstel en termijnen).	Must	2
38	Architectuur	Medewerkers van de leverancier of onderaannemers met toegang tot de systemen en/of data worden gescreend volgens passende normen (VOG profielen 11,12 of 13, te bepalen door de Provincie).	Must	2
39	Architectuur	Business Continuity Plan (BCP) De leverancier beschikt over een getest continuïteitsplan voor de dienst, inclusief vastgelegde hersteldoelstellingen (RTO/RPO).	Must	2
40	Architectuur	De leverancier maakt inzichtelijk welke derden data verwerken en informeert de provincie tijdig over eventuele wijzigingen.	Must	2
41	Architectuur	De leverancier toont aan dat hij bij maatwerkontwikkeling veilige ontwikkelmethoden toepast, zoals in de relevante richtlijnen op developer.overheid.nl.waaronder secure Software Development Life Cycle (SDLC), code reviews en beheer van afhankelijkheden.	Must	2
42	Architectuur	De leverancier wijst binnen zijn organisatie een vaste contactpersoon (en vervanger) aan voor communicatie betreffende informatiebeveiliging.	Must	2
43	Architectuur	De leverancier moet kosteloos meewerken indien de de Provincie audits wil laten uitvoeren.	Must	2
44	Architectuur	Ketenbeveiliging: Indien de leverancier gebruik maakt van onderaannemer(s) dan worden de beveiligingseisen een-op-een doorgelegd naar de onderaannemers.	Must	2
45	Architectuur	Producten en diensten worden geleverd met een veilige standaardconfiguratie (hardening). Systemen voldoen aan standaarden zoals die van het Center for Internet Security (CIS), indien afgeweken dient dit gemotiveerd te worden.	Must	2
46	Architectuur	Er is een actief patch- en updatebeleid waarin beveiligingsupdates worden geprioriteerd. Er zijn vaste termijnen voor het installeren van updates en beveiligingspatches. De Provincie hanteert hierbij de NCSC richtlijnen: Kritiek / actief misbruikt: binnen 24-72 uur High risk: binnen 7-14 dagen Medium: binnen 30 dagen Low: binnen 90 dagen	Must	2
47	Architectuur	Indien er actief misbruikte kwetsbaarheden worden gedetecteerd moeten deze gemeld worden conform de EU Cyber Resilience Act (CRA) verplichtingen.	Must	2
48	Architectuur	Alle door leverancier geleverde services en producten voldoen aan EU Cyber Resilience Act (CRA)-eisen en zijn voorzien van CE-markering daar waar verplicht.	Must	2
49	Functioneel	Uptime en beschikbaarheid (beschreven in de SLA) Er zijn afspraken over beschikbaarheid (SLA) met meetbare uptimepercentages en financiële consequenties bij niet-naleving. Tijdens service window 07:00-22:00 >= 99,8% gemeten per kalendermaand Daarbuiten >= 99,5% gemeten per kalendermaand Bij herhaald niet halen van een SLA KPI, presenteert de directie van de Leverancier een verbeterplan bij de Provincie.	Must	2
50	Architectuur	De Provincie heeft toegang tot logs van gebruik en beheer. Deze zijn exporteerbaar en leesbaar en worden 12 maanden bewaard en daarna vernietigd door leverancier tenzij anders wettelijk bepaald.	Must	2
51	Architectuur	Beveiligingsmonitoring op SaaS dienstverlening is beschikbaar bij de leverancier en er wordt actief gemonitord op de dienstverlening aan de provincie.	Must	2
52	Architectuur	Dataportabiliteit. Data kan worden geëxporteerd in een open en gestandaardiseerd formaat; bijvoorbeeld CSV.	Must	2
53	Architectuur	Encryptie in transit. Alle communicatie is versleuteld met TLS 1.3, met fall back naar TLS 1.2, of hoger en zwakke protocollen zijn uitgeschakeld, conform forum voor standaardisatie. Er dient blijvend te worden voldaan aan forum voor standaardisatie.	Must	2
54	Architectuur	Encryptie at rest. Opgeslagen data is versleuteld om bescherming te bieden bij datalekken of opslagincidenten. Versleuteling dient te worden gedaan met een door de Provincie verstrekte sleutel naar aanleiding van een BIA.	Must	2
55	Architectuur	De leverancier levert alle benodigde informatie om een Data Protection Impact Assessment (DPIA) te kunnen uitvoeren.	Must	2
56	Architectuur	Tenant-segmentatie. Gegevens van verschillende klanten zijn logisch gescheiden. De leverancier toont periodiek bewijs van deze tenant-scheiding.	Must	2
57	Architectuur	De beheeromgeving van de leverancier is gescheiden van de dienstomgeving. Toegang wordt beperkt en gelogd.	Must	2
58	Architectuur	Wijzigingsbeheer (changemanagement). Belangrijke wijzigingen in de dienst worden vooraf aangekondigd (minimaal 30 dagen) en beheerst uitgevoerd conform DAP en SLA.	Must	2
59	Architectuur	Monitoring en SIEM-koppeling De bij de leverancier aanwezige beveiligingsmonitoring incl logging van de geleverde dienst, wordt (near) real-time geïntegreerd met de SIEM van de SOC leverancier van de Provincie.	Must	2
60	Functioneel	Samenwerking met andere partners van de provincie in de keten is onderdeel van de diensverlening van de leverancier.	Must	2
61	Architectuur	Het High Level Design (HLD) en Low Level Design (LLD) dient door de leverancier te worden beschreven en onderhouden gedurende de looptijd van het contract waarbij de aangeboden oplossing overeenkomt met de wensen, eisen en doelstellingen uit dit PVE. De Provincie wil en kan dienen als partner zodat de leverancier hier op de juiste en volledige wijze invulling aan kan geven.	Must	2
62	Functioneel	De leverancier neemt deel aan de relevante strategische, tactische, roadmap, architectuur en operationele, Financial Operations, Change Advisory Board overleggen als onderdeel van de dienstverlening. De relevantie wordt door de Provincie aangegeven	Must	2
63	Functioneel	In de overbruggingsperiode, zolang als de de Provincie nog geen functioneel beheer heeft ingericht is leverancier verantwoordelijk voor het functioneel beheer voor een periode van maximaal één jaar. Daarna heeft de leverancier een flexibele schil die op verzoek van de provincie wordt ingezet.	Must	2
64	Functioneel	Het integratieplatform stelt zowel de provincie als de leverancier in staat om koppelingen te ontwikkelen en te configureren. De verantwoordelijkheid voor het bouwen en configureren van een koppeling wordt per koppeling bepaald. Het bouwen van koppelingen door de provincie leidt niet tot een verantwoordelijkheid van de leverancier voor de betreffende koppeling.	Must	2
65	Functioneel	Het platform moet versiebeheer van integraties ondersteunen, inclusief beheer van wijzigingen en gecontroleerde uitfasering van versies, zodat continuïteit van gekoppelde systemen behouden blijft.	Must	2
66	Functioneel	Het platform moet end-to-end monitoring en tracing ondersteunen, zodat transacties over de volledige keten inzichtelijk, herleidbaar en actief bewaakbaar zijn.	Must	2
67	Functioneel	De online help faciliteit wordt bij iedere nieuwe release door de leverancier op actualiteit en wettelijke voorschriften aangepast.	Must	2
68	Functioneel	Leverancier dient minimaal maandelijks standaard servicelevel reporting en performance reporting te leveren. Daarnaast dient management informatie beschikbaar te zijn. De managementinformatie dient conform de SLR en SLA te zijn. Gedurende de samenwerking kan de behoefte aan managementinformatie variëren, leverancier is verplicht hier op aan te passen.	Must	2
69	Functioneel	Het platform moet koppelingen met andere systemen ondersteunen via gedocumenteerde, beveiligde API's en gangbare uitwisselstandaarden, zodat gegevens en functionaliteit uitwisselbaar zijn zonder maatwerk in het platform. De Provincie hanteert de standaarden van Forum Standaardisatie.	Must	1

Integratieplatform Programma van Eisen				
Id	Onderwerp	Beschrijving	Prio	Fase
70	Functioneel	Het platform moet business events en wijzigingen in realtime kunnen publiceren en, waar nodig, consumeren via een event- of berichtgebaseerde integratievoorziening.	Must	1
71	Functioneel	Het platform moet bulk data-ingestie kunnen ondersteunen voor grote datasets, zodat gegevens efficiënt en gecontroleerd kunnen worden ingeladen vanuit meerdere bronnen	Must	2
72	Functioneel	Het platform moet synchrone en asynchrone communicatie ondersteunen via gestandaardiseerde integratie-interfaces, zodat processen zowel direct als ontkoppeld kunnen communiceren.	Must	2
73	Functioneel	Het platform moet batch- en near-real-time data-integratie ondersteunen, zodat per gegevensstroom de passende verwerkingssnelheid en actualiteit kan worden gekozen.	Must	2
74	Functioneel	Het platform moet event-gedreven integratie ondersteunen, inclusief publiceren en consumeren van berichten, zodat wijzigingen en gebeurtenissen realtime door de keten kunnen worden verwerkt.	Must	2
75	Functioneel	Het platform moet schema-mapping en datatransformaties ondersteunen tussen bron- en doelmodellen, zodat gegevens uit verschillende systemen uniform en bruikbaar worden gemaakt.	Must	2
76	Functioneel	Het platform moet procesorkestratie en choreografie ondersteunen, inclusief routing en volgordebepaling van integratiestappen, zodat ketenprocessen beheerst en reproduceerbaar kunnen worden uitgevoerd.	Must	2
77	Functioneel	Het platform moet herstartbare en fouttolerante dataverwerking ondersteunen, zodat onderbroken of mislukte loads gecontroleerd hervat kunnen worden zonder dataverlies of dubbeltellingen.	Must	2
78	Functioneel	Het platform moet bericht- en datatransformatie ondersteunen, inclusief mapping en validatie tussen bron- en doelschema's, zodat systemen met verschillende datamodellen veilig kunnen koppelen.	Must	2
79	Functioneel	Het platform moet data-integriteitscontroles ondersteunen, waaronder validatie op volledigheid, formaat en consistentie, zodat dataintegriteit aantoonbaar kan worden bewaakt.	Must	2
80	Functioneel	Het platform moet mechanismen bieden voor foutafhandeling, retries, idempotente verwerking en compensatie, zodat integratieprocessen robuust blijven bij verstoringen.	Must	2
81	Functioneel	Het platform moet integratie met AI-platformen en LLM-diensten ondersteunen via gangbare AI-koppelingen en documentatie, zodat AI-functionaliteit kan worden toegevoegd zonder aanpassing van het platform.	Must	2
82	Functioneel	Het Nederlands (minimaal CERF B2 niveau) is de standaardtaal in woord en geschrift voor alle door de de Provincie gebruikte onderdelen van het platform. Dit omvat ten minste: - de gebruikersinterface; - beheer- en operationele dashboards; - standaardmeldingen, foutmeldingen en rapportages; - functionele en beheerdocumentatie; - supportcommunicatie.	Must	1
83	Functioneel	Trainingsmateriaal wordt in het Nederlands aangeboden. Indien dit niet mogelijk is, mag Engels worden gebruikt, mits het trainingsmateriaal voorzien kan worden van Nederlandse ondertiteling.	Should	2
84	Functioneel	De oplossing is voorzien van de huisstijl van de Provincie.	Should	2
85	Functioneel	De oplossing wordt aangeboden als open source software.	Should	2
86	Functioneel	Indien open source software wordt aangeboden is de European Union Public Licence (EUPL) licentie of EUPL compatible licentie van toepassing.	Should	2
87	Functioneel	Indien open source software wordt toegepast, mogen de licentievoorwaarden de Provincie niet verplichten afgeleide werken, maatwerk, configuraties of integraties openbaar te maken.	Must	2
88	Functioneel	Het integratieplatform faciliteert losgekoppelde (loosely coupled) integraties, zodat wijzigingen in één applicatie minimale impact hebben op andere applicaties.	Must	1
89	Functioneel	Het integratieplatform ondersteunt het ontsluiten en distribueren van stamgegevens ten behoeve van hergebruik binnen de provincie, zonder dat eigenaarschap van deze gegevens wordt overgenomen door het platform.	Must	1
90	Functioneel	Bronapplicaties blijven de authentieke bron van stamdata en operationele gegevens. Het integratieplatform faciliteert uitsluitend gegevensuitwisseling en neemt het bronhouderschap niet over.	Must	1
91	Functioneel	Gegevens afkomstig uit bronapplicaties mogen het vertrouwde provinciale netwerk of door de provincie aangewezen cloudomgeving niet verlaten, tenzij hiervoor expliciete toestemming is verleend door de Provincie.	Must	1
92	Architectuur	De leverancier is BIO2 compliant voor de dienst die hij aan de Provincie levert.	Must	1
93	Architectuur	De leverancier zorgt dat IPv6 wordt ondersteund daar waar componenten extern ontsloten worden.	Must	1
94	Architectuur	Koppelingen met (back-end)systemen moeten mogelijk zijn via API-calls.	Must	2
95	Architectuur	Data opslag, data verwerking en syste(e)m(en) bevinden zich binnen de grenzen van de EER (Europese Economische Ruimte).	Must	1
96	Architectuur	Specifiek voor IaaS: De leverancier zorgt dat het N, N-1 beleid actief wordt ingevuld. Dit houdt in dat, aangezien de Provincie een "actieve volger" is, de softwareversies op versie N zijn (= door de leverancier geadviseerde productversie van de software), en alleen bij uitzondering (tijdelijk) N-1 mag zijn. Daarbij worden (ook) alle applicaties, die worden aangeboden vanuit de Microsoft Store, automatisch bijgewerkt zodra er een update beschikbaar komt. De configuratie moet dusdanig zijn, dat de eindgebruiker hier niet/minimaal door wordt lastig gevallen, waarbij het werk wordt onderbroken.	Must	1
97	Architectuur	Het platform moet authenticatie laten verlopen via de Identity Provider van de Provincie (Microsoft Entra ID), zodat centrale identiteit- en toegangscontrole kan worden afgedwongen.	Must	2
98	Architectuur	Het platform moet Single Sign-On (SSO) met Microsoft Entra ID ondersteunen in combinatie met Multi Factor Authenticatie (MFA) voor toegang en autorisatie tot gebruikers- en beheerfuncties.	Must	2
99	Architectuur	Indien afgeweken wordt van wijzigingen in toegangsrechten en het deactiveren of verwijderen van accounts conform Entra ID dient dit gemotiveerd te worden door leverancier.	Must	2
100	Architectuur	De leverancier monitort (pro)actief op processen die bij de leverancier zijn belegd en waarover afspraken zijn gemaakt welke zijn opgenomen in de SLA.	Must	1
101	Architectuur	Het platform moet securitylogging bieden die volledig, integer en tenant-gescheiden beschikbaar is voor de Provincie, inclusief exportmogelijkheden voor auditdoeleinden.	Must	2
102	Architectuur	Het platform moet forwarding van securitylogs naar de SOC SIEM-oplossing van de Provincie ondersteunen via een beveiligde en beheersbare koppeling.	Must	2
103	Architectuur	Leverancier meldt datalekken (inbreuken op persoonsgegevens) binnen 4 uur aan de Security Officer van de Provincie, zodat de Provincie het datalek binnen 72 uur kan melden bij de Autoriteit Persoonsgegevens (AVG art. 33).	Must	1
104	Architectuur	Het platform en alle gerelateerde dienstverlening dienen te voldoen aan de Cyberbeveiligingswet/NIS2 verplichtingen. Dus niet alleen de software zelf, maar ook de gehele keten, inclusief aanverwante diensten gerelateerd aan het platform dient Cbw/NIS2 compliant te zijn (aantoonbaarheidplicht) en zodra mogelijk NIS2 gecertificeerd te worden.	Must	1
105	Architectuur	Sub-contractors moeten aan dezelfde eisen voldoen als de leverancier. Behuizing, datacenters door hostingpartners zijn gecertificeerd met de ISO 27001 normering, of gelijkwaardige norm. De datacenters moeten redundant zijn uitgevoerd.	Must	1
106	Architectuur	De inrichting van het platform dient te voldoen aan de geldende overheidsstandaarden, zoals vastgesteld in de Wet digitale overheid (Wdo) en de door Forum Standaardisatie voorgeschreven standaarden. De Provincie hanteert hierbij tevens de richtlijnen en principes zoals gepubliceerd op developer.overheid.nl.	Must	2
107	Architectuur	Alle communicatie van en naar het vertrouwde provinciale netwerk of door de provincie aangewezen cloudomgeving vindt plaats over beveiligde verbindingen, zoals HTTPS en sFTP met onderliggend certificaat.	Must	2
108	Architectuur	Leverancier levert jaarlijks (de eerste voor Acceptatie van de oplossing) een verklaring van getrouwheid (of vergelijkbaar) op te verkrijgen via een onafhankelijke derde partij, om aan te tonen dat zij als leverancier veilig omgaat met vertrouwelijke informatie.	Must	1
109	Architectuur	Door middel van een toegangslog worden de gebruikersaccounts en –identificaties vastgelegd en valt exact te achterhalen wie wat waar heeft ingevoerd dan wel gewijzigd, dan wel geraadpleegd.	Must	2
110	Architectuur	De oplossing maakt autorisatie op component niveau mogelijk. Daarnaast dient de oplossing toekomstbestendig te zijn om autorisaties op rol niveau te kunnen aanpassen.	Must	2
111	Architectuur	De leverancier werkt volgens de normen die worden gesteld in ISO 27001 t.b.v. informatiebeveiliging en ISO 20000 t.b.v. service management.	Must	1
112	Architectuur	In het kader van de in deze aanbesteding gevraagde dienst sluiten de leverancier en Provincie de verwerkersovereenkomst van de Provincie af.	Must	1

Integratieplatform Programma van Eisen				
Id	Onderwerp	Beschrijving	Prio	Fase
113	Functioneel	Verwerking, routing, buffering en opslag van berichten en gegevensstromen met stam- en/of brondata vindt plaats binnen het vertrouwde provinciale netwerk of door de provincie aangewezen cloudomgeving	Must	1
114	Leverancier	Leverancier levert jaarlijks een document op met betrekking tot hoe, voor deze opdracht, om wordt gegaan met de informatiebeveiliging tijdens de looptijd van de opdracht en in welke mate de oplossing, bij de aangegeven prijs, aansluit bij de visie op en principes ten aanzien van de digitale werkomgeving-diensten zoals beschreven in het visie document van de Provincie. Leverancier dient hiervoor een beschrijving te geven met de geïmplementeerde informatiebeveiliging met daarin minimaal een beschrijving van: 1.De wijze waarop u technisch, procesmatig en organisatorisch borgt dat systeem en/of data uitval en/of verlies door een beveiligingsincident wordt voorkomen en welke aanpak u hanteert ingeval dat er onverhoopt toch uitval en/of verlies optreden op welke wijze u hier de provincie over informeert. 2.Op welke wijze u als organisatie continu de laatste informatiebeveiligings-ontwikkelingen volgt en deze expertise en oplossingen inzet voor de provincie. 3.De wijze waarop de provincie periodiek wordt geïnformeerd over de actuele status van de informatiebeveiliging en beveiligingsrisico's en over door u uitgevoerde acties. De eerste beschrijving dient te worden opgeleverd binnen 1 maand na definitieve gunning van de opdracht.	Must	2
115	Functioneel	Het integratieplatform ondersteunt gecontroleerde ontsluiting van brondata en stamdata naar het provinciale dataplatform ten behoeve van analyse, rapportages, archivering, Woo-verzoeken, open data en andere hergebruiksscenario's.	Must	1
116	Functioneel	Het platform moet idempotente verwerking van device-opdrachten en events ondersteunen, zodat herhaalde berichten niet leiden tot dubbele of conflicterende acties.	Must	2
117	Functioneel	Het platform moet lage-latency verwerkingspaden ondersteunen voor tijdkritische IoT-interacties, zonder afhankelijkheid van zware orkestratie waar dit niet nodig is.	Must	2
118	Functioneel	Het platform moet streaming ingestie van telemetrie ondersteunen, zodat continue datastromen van devices direct verwerkt en beschikbaar gemaakt kunnen worden.	Must	2
119	Functioneel	Het platform moet scheiding van raw, enriched en aggregated data ondersteunen, zodat datastromen per verwerkingsfase beheerst, herleidbaar en herbruikbaar blijven.	Must	2
120	Functioneel	Het platform moet replay en herverwerking van events ondersteunen, zodat historische datastromen gecontroleerd opnieuw verwerkt kunnen worden na fouten of wijziging van verwerkingslogica.	Must	2
121	Functioneel	Het platform moet consistente, gedocumenteerde en semantisch eenduidige API's bieden voor AI-toepassingen, zodat AI-clients en agents voorspelbaar met functionaliteit en data kunnen interacteren.	Must	2
122	Functioneel	Het platform moet fijnmazige autorisatie ondersteunen op alle gerelateerde data en functies, zodat toegang per rol, context en gebruiksdoel kan worden afgedwongen.	Must	2
123	Functioneel	Het platform moet integraties beschikbaar stellen voor AI-gebruik in gestructureerde, semi-gestructureerde en ongestructureerde vormen, met eenduidige ontsluiting voor verwerking en retrieval.	Must	2
124	Functioneel	Het platform moet ondersteuning bieden voor (toekomstige) open standaarden voor AI-integratie. Minimaal wordt ondersteuning verwacht voor: - MCP (Model Context Protocol) - A2A (Agents-to-Agent Protocol)	Should	2
125	Functioneel	De componenten moeten ondersteuning bieden om rollen en gebruikers(groepen) te definiëren en gebruikers(accounts) te koppelen aan één of meerdere van deze groepen dan wel rollen.	Must	2
126	Functioneel	De componenten moeten ondersteuning bieden voor user provisioning. Het moet mogelijk zijn om autorisaties en sjablonen toe te kennen aan rollen. Als er qua autorisaties of anderszins een wijziging plaatvindt op een rol, dan heeft dat betrekking op alle gebruikers waar deze rol aan gekoppeld is.	Must	2
127	Functioneel	Alle content, navigatie en actie-knoppen moeten meertalig aangeboden kunnen worden.	Could	2
128	Functioneel	Het platform moet toegankelijk zijn conform EN 301 549 WCAG 2.1 AA	Must	1
129	Leverancier	De geboden oplossing heeft alle licenties voor de oplossing zelf. Eventueel gebruik van derden software is beschreven. Er kan gebruik gemaakt worden van software waarvoor de provincie al licenties heeft.	Must	2
130	Leverancier	De leverancier levert zijn dienst overeenkomstig een Service Level Agreement (SLA). De Provincie werkt bij voorkeur met de SLA van de leverancier waarbij de bijgevoegde SLA kaderstellend is. De SLA wordt door leverancier als bijlage toegevoegd. Standaard changes zijn onderdeel van de SLA en worden niet apart gefactureerd. De Provincie verwacht dat standaard changes zijn geautomatiseerd	Must	2
131	Leverancier	De leverancier verzorgt vanuit de System Integrator rol voor de integraties waarvoor hij verantwoordelijk is, het end-to-end-beheer, specifiek voor de processen incident management, security management, problem management, configuratie management, change management en request fulfillment.	Must	2
132	Leverancier	De leverancier levert capaciteit met voldoende inhoudelijke deskundigheid, en zorgt voor beschikbaarheid hiervan, om te participeren in projecten. Dit geldt ook voor de delen die tijdens de implementatie in gebruik zijn genomen en waarvan de dienstverlening - vastgelegd in een Service Level Agreement (SLA) - op van toepassing is.	Must	2
133	Leverancier	De leverancier biedt ten behoeve van meldingen en vragen een deskundige servicedesk aan, dat wil zeggen 'een tweedelijns-ondersteuning', die als aanspreekpunt rechtstreeks in contact staat met beheer van de Provincie. De servicedesk communiceert in begrijpelijk Nederlands en is in Nederland gevestigd.	Must	2
134	Leverancier	Wanneer de leverancier gebruik wil maken van haar eigen helpdesksysteem, realiseert de leverancier een (near-)realtime koppeling tussen de helpdesksystemen van de Provincie en de leverancier. De realisatie, het beheer en het onderhoud van deze koppeling is tevens onderdeel van de verantwoordelijkheid van de leverancier. De Service Management Tool (huidig: ServiceNow) van de Provincie is ten alle tijden leidend	Must	2
135	Leverancier	Voor de oplossing wordt een acceptabele, goed werkbare performance gegarandeerd conform de SLA.	Should	2
136	Leverancier	De duurzaamheid van de oplossing is gegarandeerd binnen het contractstermijn. Als de oplossing niet langer ondersteund wordt door de leverancier dan wordt de broncode (open source, Escrow) beschikbaar gesteld of bestaat de mogelijkheid om het onderhoud en de ondersteuning voort te zetten bij een andere partij (exclusief de Leverancier en zuster- dochter en moedermaatschappijen).	Must	1
137	Leverancier	Bereikbaarheid helpdesk van leverancier is als volgt: Telefonisch 07:00 – 22:00 P1 t/m P4 Telefonisch 22:00 - 07:00 P1 Service management tool (huidig: ServiceNow) 24/7 P1 t/m P4 Voor ondersteuning door de helpdesk van de Leverancier worden geen aanvullende kosten in rekening gebracht. De diensverlening is 24x7.	Must	1
138	Leverancier	De helpdesk van leverancier is verantwoordelijk voor de gehele behandeling van meldingen, incidenten met betrekking tot de Oplossing volgens de procedure zoals vastgelegd in de SLA waarbij één centraal contactpunt wordt gehanteerd. De Provincie bepaalt de prioriteit van incidenten.	Must	1
139	Leverancier	De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De leverancier maakt voor de Provincie inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De leverancier is eindverantwoordelijk voor het beheren van incidenten.	Must	1
140	Leverancier	De leverancier is verantwoordelijk voor de gehele afhandeling van wijzigings-voorstellen m.b.t. de oplossing. De leverancier is verantwoordelijk voor het aanbieden van wijzigingsvoorstellen (met uitzondering van standaard changes) bij de change manager zodat deze aangeboden kunnen worden aan het Change Advisory Board (CAB) ten behoeve van het oplossen van reeds geïdentificeerde problemen en nieuwe aanvragen. Elk wijzigingsvoorstel ondergaat een intakeprocedure.	Must	1
141	Leverancier	De Provincie heeft de mogelijkheid om nieuwe releases tegen te houden, indien dit een risico vormt voor bedrijfskritische processen, in geval van laaS oplossing.	Should	2
142	Leverancier	De leverancier conformeert zich aan de inspanningsverplichting om nauw samen te werken met de Provincie tijdens de implementatiefase.	Must	2
143	Leverancier	Leverancier verzorgt (online) trainingen in het gebruik van (variabelen voor het platform) voor (groepen) gebruikers bij de Provincie.	Must	2
144	Leverancier	De leverancier leidt gebruikers en beheerders van de oplossing op. Hierbij worden zij voorzien van alle benodigde documentatie (incl. alle technische documenten) en eventuele hulpmiddelen zodat het beheer volledig zelfstandig kan plaatsvinden.	Must	2

Integratieplatform Programma van Eisen				
Id	Onderwerp	Beschrijving	Prio	Fase
145	Leverancier	Binnen twee weken na de gunning wordt door leverancier het Plan van Aanpak aangevuld in samenspraak met de Provincie. Hierbij wordt benoemd welke activiteiten door de leverancier en welke door de Provincie uitgevoerd dienen te worden.	Must	2
146	Leverancier	Er is alleen sprake van acceptatie van de oplossing (inclusief koppelingen) bij een wederzijdse akkoordverklaring, welke schriftelijk wordt geformaliseerd door beide partijen.	Must	1
147	Leverancier	Tijdens de test- en acceptatiefase werkt de leverancier mee aan mogelijk te houden stress- en ketentesten, ten einde de robuustheid en performance van de oplossing te testen.	Must	1
148	Leverancier	Leverancier is verantwoordelijk voor het leveren van voldoende mankracht om aangegeven planning te realiseren. De leverancier zal zich schikken naar door de Provincie voorgestelde data (afspraken) en naar de voorgestelde planning. Mocht een datum vanwege overmacht niet passen dan komt de leverancier met minimaal drie opties die binnen de planning vallen.	Must	1
149	Leverancier	De leverancier levert een projectleider voor implementatie van de oplossing.	Must	1
150	Leverancier	De leverancier levert een projectteam met minimaal een consultant en architect voor de inrichting van de oplossing inclusief koppelingen.	Must	1
151	Leverancier	Het bijgevoegde exit- en retransitieplan is integraal van toepassing op de overeenkomst met de leverancier, inclusief rollen, verantwoordelijkheden, termijnen en overdrachtsactiviteiten bij beëindiging van het contract.	Must	2
152	Leverancier	De leverancier moet zich conformeren aan de gedragscode re-transitie van Sourcing Nederland (v1.2) en afwijkingen alleen na schriftelijke instemming van de Provincie toepassen.	Must	1
153	Leverancier	De leverancier biedt een zo eenvoudig en volledig mogelijke datamigratie aan bij contractbeëindiging. De data welke volgens (open) standaarden is vormgegeven en opgeslagen dient qua content te kunnen worden geëxporteerd conform een standaard format dat door een andere leverancier in een ander (vergelijkbaar) systeem kan worden ingelezen. Daarbij moet de structuur van de export dusdanig zijn dat het zonder datamodificatie, of zo min mogelijk datamodificatie, met de juiste structuur wordt weggeschreven zodat de data op een goede en volledige manier kan worden ingelezen in een nieuwe oplossing waarbij de data op de juiste plek land in de nieuwe omgeving. Na bevestiging van overdracht wordt alle data van de systemen van de leverancier vernietigt. De leverancier levert een verklaring van vernietiging (purge of destroy).	Must	1
154	Leverancier	De Oplossing wordt gedurende het contract doorontwikkeld en speelt in op ontwikkelingen in de markt.	Must	1
155	Leverancier	De Oplossing en alle dienstverlening vanuit leverancier dient te voldoen aan de relevante wet- en regelgeving en bij het inwerking treden van nieuwe relevante wet- en regelgeving aan die nieuwe wet- en regelgeving voldoen.	Must	1
156	leverancier	Er bestaat een organisatiebreed testbeleid dat vastlegt hoe de leverancier tegen testen aankijkt en welke uitgangspunten voor het testproces altijd gelden.	Must	2
157	Leverancier	Voor elk product, project of release bestaat een teststrategie. Deze moet minimaal beschrijven: 1. Testorganisatie waarin zowel testrollen (zoals tester, testmanager) als project / agile rollen (zoals projectmanager, Scrum Master, Product Owner) zijn vastgelegd; 2. Testsoorten (bijvoorbeeld systeemtest, functionele test, integratietest, acceptatietest) die worden gebruikt en toegepast; 3. Kwaliteitscriteria of minimale kwaliteitseisen (per testsoort) die gebruikt worden als basis voor GO / NOGO momenten; 4. Testbasis (op welke documentatie - bijvoorbeeld User Stories, acceptatiecriteria, requirements, technische / functionele ontwerpen - de testgevallen gebaseerd zijn.	Must	1
158	Leverancier	In de gehanteerde teststrategie (voor product, project of release) wordt door de leverancier beschreven: 1. Risico's (product, andere) welke prioriteit dienen te krijgen; 2. Test(ontwerp)technieken die gebruikt worden voor het bepalen van testgevallen; 3. Testdata en tools die nodig zijn bij het testen; 4. Omstandigheden waaronder er testen worden uitgevoerd.	should	2
159	Leverancier	Leverancier zorg ervoor dat testuitvoer en bevindingen reproduceerbaar en herhaalbaar zijn.	must	2
160	Leverancier	De leverancier hanteert een gestandaardiseerd testproces dat is gebaseerd op een algemeen erkende industriestandaard, zoals TMAP® of ISTQB. Minimaal één sleutelrol in het testproces (testcoördinator of testmanager) beschikt over een geldige TMAP- of ISTQB-certificering.	Should	2
161	Leverancier	Penetratietesten moeten worden uitgevoerd door de leverancier of de leverancier moet deze kunnen faciliteren.	Must	2
162	Architectuur	Het platform dient ondersteuning te bieden voor het ACME-protocol (RFC 8555), zodat certificaten voor beveiligde communicatie geautomatiseerd kunnen worden beheerd en vernieuwd zonder handmatige interventie.	Must	2
163	Architectuur	De Leverancier levert na definitieve gunning, en voor het implementatietraject, een informatiearchitectuur voor de nieuwe situatie waarin de voorzieningen, koppelingen en afhankelijkheden met andere informatievoorzieningen geïnventariseerd en beschreven zijn.	Must	2
164	Architectuur	De aangeboden oplossing biedt een User Interface voor de beheerder van de Provincie. Voor monitoring en logging van alle koppelingen. Het gaat daarbij om inzage in de status van koppelingen, connectiviteit, verstoringen, het dataverkeer, logging en validatiefouten.	Must	1
165	Architectuur	De oplossing voorziet in een Digikoppeling adapter en een Haal Centraal koppeling.	Must	1
166	Architectuur	De oplossing voorziet in een ZGW-API koppeling.	Should	2