

Bijlage 1 - Programma van eisen

Aanvullend begrip

Melding: (Storings-) meldingen, wijzigingsverzoeken, restoreverzoeken, gebruikersverzoeken en informatievragen, klachten, Incidenten

Nr	Algemene eisen
1.	Leverancier levert alle gevraagde diensten die nodig zijn om de scope zoals beschreven in hoofdstuk 1.3.3. te kunnen leveren.
2.	Leverancier en zijn dienstverlening dienen in opzet, bestaan en werking, te voldoen aan deel 2 van de Baseline Informatiebeveiliging Overheid (BIO2) en de Inkoop-eisen Cybersecurity Overheid (bijlage 12). Leverancier toont jaarlijks aan, middels onafhankelijke onderzoeken dat hieraan wordt voldaan conform eis 56.
3.	Leverancier levert een adequaat beveiligde dienstverlening, waarbij de informatiebeveiligingsprocessen zodanig ingericht is, dat opdrachtgever hiermee aan alle huidige en toekomstige reeds aangekondigde relevante wet- en regelgeving (zoals BIO2, NIS2/ cyberbeveiligingswet en daaruit volgende besluiten etc.) voldoet en blijft voldoen.
4.	De eisen gelden ook voor eventuele onderaannemers die door Leverancier in de toeleveringsketen worden ingezet.
5.	Leverancier geeft inzicht in de keten van toeleveranciers inclusief eventuele risico's die in de keten kunnen ontstaan. Tevens maakt leverancier inzichtelijk hoe deze risico's worden beheer(s)d en welke rol bij de beheersing van opdrachtgever wordt verwacht.
6.	Gedurende de looptijd van de overeenkomst geeft Leverancier veranderingen in de keten van toeleveranciers door, inclusief risico's. Dit omvat minimaal kwetsbaarheden, en informatiebeveiligingsincidenten die de dienstverlening kunnen raken.
Servicedesk	
7.	Alle meldingen van eindgebruikers van opdrachtgever worden via het vaste aanspreekpunt van opdrachtgever (op dit moment Hoofd ICT) of zijn vervanger (warm) doorgezet aan de servicedesk van de Leverancier. Terugkoppeling van de melding verloopt via het vaste aanspreekpunt van opdrachtgever. Eindgebruikers kunnen alleen rechtstreeks contact opnemen bij urgente storingen of security incidenten als het vaste aanspreekpunt van opdrachtgever niet bereikbaar is.
8.	Om (proactief) regie te voeren op de meldingen, heeft het vaste aanspreekpunt van opdrachtgever of zijn vervanger via een portaal van Leverancier inzicht in de voortgang, status en afhandeling van alle meldingen.
9.	De 1e lijns Service Desk van Leverancier is een skilled Service Desk, die voor de facilitaire service desk van opdrachtgever en eindgebruikers het eerste contactpunt is voor vragen, (wijzigings-) verzoeken en meldingen voor alle diensten ook van derden. Die voldoet aan de volgende eisen:

	a) Nederlandstalige skilled Service Desk; b) Single point of contact; c) Alle meldingen dienen geregistreerd en ter afhandeling gerouteerd te worden. Ook dient de voortgang van de afhandeling van de meldingen bewaakt en teruggekoppeld te worden; d) De Service Desk van Leverancier behandelt (storings-) meldingen, wijzigingsverzoeken en informatievragen met betrekking tot de door Leverancier geleverde dienstverlening; e) De servicedesk is via telefoon en e-mail bereikbaar voor vragen en meldingen; f) Meldingen kunnen middels een selfservice portaal van Leverancier door worden gegeven en is via Single Sign On (SSO) te benaderen en bereikbaar; g) Meldingen worden voorzien van een nummer die teruggekoppeld wordt per email aan de gebruiker.
10.	Naast meldingen van gebruikers, worden ook geautomatiseerde meldingen, vanuit monitoringssystemen en statusmeldingen door de Servicedesk geregistreerd en afgehandeld.
11.	De 1 ^e lijns service desk lost meldingen zoveel mogelijk direct of na het eerste contactmoment op.
12.	Indien de melding niet direct kan worden opgelost, wordt deze doorgezet naar de 2 ^e lijns helpdesk/3 ^e lijns helpdesk en/of oplosgroep van Leverancier en/of doorgezet naar een andere externe partij.
13.	Leverancier is verantwoordelijk voor het opvolgen van meldingen aan externe partijen. De externe partij blijft verantwoordelijk voor het oplossen van de melding.
14.	De 1 ^e lijns servicedesk is bereikbaar via telefoon en e-mail van maandag tot en met vrijdag van 8:00 uur tot 17:00 uur.
15.	De servicedesk is, voor het melden van urgente en kritische incidenten (ernstige verstoring, hack etc.) 24 uur per dag, 7 dagen per week, inclusief feestdagen, telefonisch en per e-mail bereikbaar. Leverancier start direct na de melding met passende herstelwerkzaamheden en zet, indien nodig, escalatieprocedures en/of een workaround in.
16.	Het is mogelijk om de werkplek van een gebruiker remote over te nemen door de servicedesk (1 ^e lijns/2 ^e lijns) na akkoord van de gebruiker.
17.	Indien een melding niet direct kan worden opgelost is de maximale oplostijd 3 werkdagen.
Service levels	
18.	Leverancier hanteert voor incidentmanagement minimaal de volgende niveaus van dienstverlening. Prio 1 Kritisch incident: Reactietijd <1 uur, Oplostijd <4 uur. Opdrachtgever verstaat onder een kritisch incident het niet beschikbaar zijn van functionaliteit wat effect heeft op de gehele organisatie of een groot deel hiervan (b.v. één van de twee hoofdlocaties). Het niet kunnen beschikken over deze functionaliteit heeft direct substantiële gevolgen voor de financiële positie van de

	opdrachtgever of haar medewerkers, het kunnen voldoen aan wet- en regelgeving (b.v. informatiebeveiliging), de te leveren kwaliteit (zoals productieverstoring) door de opdrachtgever en/of de klanttevredenheid van één of meer klanten van de opdrachtgever. De overige niveaus voor incidentmanagement maken onderdeel uit van de gunningscriteria.
19.	Voor Changes (wijzigingsverzoeken) gelden de volgende doorlooptijden: • Standaard changes: < binnen twee (2) werkdagen; • Niet standaard changes: Binnen twee (2) werkdagen analyse van de impact en doorlooptijd; • Emergency changes: Direct handelen na vaststelling van urgentie door beide partijen.
20.	Standaard changes kunnen niet in rekening worden gebracht en zijn in de prijs van de servicedesk inbegrepen (zie prijzenblad). De meeste standaard changes worden door opdrachtgever zelf uitgevoerd. Leverancier stelt opdrachtgever in staat om de volgende standaard changes zelf uit te kunnen voeren. Standaard changes die opdrachtgever uitvoert: • Gebruikers(rechten) aanmaken, wijzigen, verwijderen en/of wachtwoord reset uitvoeren; • Rechten toekennen binnen applicaties voor uitbreiding van reeds aanwezige functionaliteit bij bestaande gebruikers; • Toekennen van rechten op gebruik van applicaties die door Leverancier worden beheerd; • Uitrollen van beschikbare images op werkplekken of mobile devices die al eerder succesvol uitgerold zijn geweest; • Restore-verzoeken van bestanden en mail vanuit de back-up; • Applicaties toevoegen aan mobiele apparaten. Standaard changes die door Leverancier worden uitgevoerd: • Aanpassingen in de Firewall. In het geval van afwezigheid, van het vaste aanspreekpunt van opdrachtgever, kan Leverancier worden verzocht om alle standaard changes uit deze eis uit te voeren, zodat de continuïteit van changes is geborgd. Voor Niet standaard en Emergency changes geldt dat hiervoor een request for change en nadere offerte wordt opgesteld. De offerte is gebaseerd op de uurtarieven in het prijzenblad en worden P&Q afgerekend.
Managen van de werkplek	
21.	Leverancier is verantwoordelijk voor het op afstand (kunnen) beheren van endpoints (Windows/MAC OS apparaten en mobiele telefoons) van opdrachtgever.

22.	Leverancier controleert en signaleert of de endpoints van opdrachtgever altijd zijn voorzien van de laatste Windows updates, Microsoft 365 versies en security patches (Defender). Indien dit niet het geval is dan zorgt Leverancier dat deze zo spoedig mogelijk binnen de ingestelde update-ringen op het endpoint worden geïnstalleerd. Indien een update niet is uitgevoerd omdat dit te wijten is aan een eindgebruiker meldt Leverancier dit aan het vaste aanspreekpunt van opdrachtgever.
23.	Opdrachtgever zorgt dat op Windows gebaseerde apparaten worden geregistreerd in Windows Autopilot.
24.	Opdrachtgever is verantwoordelijk voor de aanwezigheid van de benodigde licenties.
25.	Leverancier maakt het mogelijk dat opdrachtgever zelfstandig de remote uitrol van werkplekken op basis van beschikbare image (Intune) kan uitvoeren. De images met standaard functionaliteiten en applicaties worden in overleg tussen Leverancier en opdrachtgever bepaald.
26.	Op verzoek van opdrachtgever worden door Leverancier additionele applicaties toegevoegd en uitgerold aan gebruikers.
27.	Het is mogelijk om te allen tijde gegevens en data op afstand te wissen van mobiele apparaten (smartphone, tablet).
28.	Indien een apparaat niet veilig is zal de gebruiker hierover per mail worden geïnformeerd. Na negentig (90) dagen zal de toegang tot op zekere hoogte worden geblokkeerd. Indien er sprake is van een zeer hoog risico zal er direct een blokkade plaats vinden. Na gunning zal deze eis nader met opdrachtgever worden afgestemd.
Beheren en managen van Microsoft 365 Tenant	
29.	Leverancier voert ten minste éénmaal per maand een health check uit op de Microsoft 365 tenant van opdrachtgever. De resultaten worden vastgelegd in een rapport met aanbevelingen en besproken in een overleg met opdrachtgever.
30.	Leverancier maakt het mogelijk dat opdrachtgever zelfstandig het identiteits- en toegangsbeheer van de Azure Active Directory kan inrichten en beheren. Dit betreft het: a) Beheer van gebruikers- en groepstoegang; b) Configuratie van multi-factor authenticatie (MFA); c) Beheer van gastgebruikers (guest acces); d) Toepassen van rolgebaseerde toegangsrechten conform autorisatiematrix van opdrachtgever.
31.	Leverancier past beschikbare beveiligingsmaatregelen toe binnen de Microsoft 365 tenant op basis van de aanwezige licenties, waaronder: a) Beheer van Microsoft Defender instellingen; b) Toepassen van Data Loss Prevention (DLP) policies (nader te bepalen met Leverancier) bijvoorbeeld via een oplossing als Purview. c) Beheer van Conditional Access policies; d) Beheren van sensitieve gegevens (oa voor inzet AI/CoPilot); e) Monitoring op verdachte inlogpogingen of datalekken.
32.	Leverancier monitort en detecteert risicovolle gebruikers en onderscheidt: a) Anoniem IP-gebruik;

	b) Atypisch reizen; c) Aanmelden vanaf een geïnfecteerd apparaat; d) Aanmelden vanaf IP-adressen met verdachte activiteit; e) Aanmelden vanaf onbekende locaties; f) Gelekte inloggegevens.
33.	Leverancier zorgt dat alle gebruikers gebruik moeten maken van multi-factor authenticatie (MFA).
34.	Leverancier borgt de werking van koppelingen tussen de databases en de huidige applicaties (Exact, COMPAS Core).
Back-up	
35.	Leverancier levert een managed back-updienst die dagelijks een back-up maakt van alle data vanuit Microsoft 365. Dit betreft onder andere, maar niet uitsluitend: a) Exchange Online: mailboxen, archieven, mappen, agenda's, contacten, berichten, machtigingen; b) SharePoint: site collecties of granulaire sites, lijsten, bibliotheken, bestanden, metadata, beveiligingsinstellingen en versiegeschiedenis; c) OneDrive: mappen, bestanden, metadata, beveiligingsinstellingen en versiegeschiedenis; d) Teams: Team Channels, privé Channels, gesprekken, vergader- en werkbestanden; e) Microsoft 365 Groepen: bestanden, gesprekken, notities, sites; f) Openbare mappen: mailboxen, berichten, contacten, formulieren en posts. g) Relevant geachte Loggegevens.
36.	De back-updata wordt uitsluitend opgeslagen in een datacenter in Europa en is end-to-end versleuteld (encrypted), zowel tijdens transport als in rust.
35.	Leverancier zorg dat de back-updata op alternatieve wijze wordt opgeslagen buiten de Microsoft omgeving, zodat deze te allen tijde overdraagbaar is en zonder het bestaan van Microsoft teruggehaald kan worden. Dit in het geval van een mogelijke (plotselinge) exit strategie.
36.	Leverancier voert minimaal dagelijks een back-up uit op een vast tijdstip. Het maximaal toegestane Recovery Point Objective (RPO) bedraagt 24 uur.
37.	De retentie van back-updata is beperkt tot maximaal zeven jaar.
38.	Leverancier voert dagelijks een controle uit op volledigheid van de back-up.
39.	De data van uitdienst getreden medewerkers van opdrachtgever worden niet verwijderd uit de backupdata.
40.	Leverancier zorgt voor een gedocumenteerd, getest en periodiek geverifieerd back-up- en herstelplan, inclusief toegang tot en eigenaarschap van de back-updata door opdrachtgever. In het plan en de uitvoering is rekening gehouden met immutable-backups, air-gaps of andere strategieën.
Managed services	
41.	Leverancier zorgt voor het waarborgen van de veiligheid, betrouwbaarheid en prestaties van de Microsoft Azure Cloud infrastructuur van opdrachtgever. Leverancier verricht alle noodzakelijke activiteiten die nodig zijn om dit te

	borgen. Hieronder vallen, maar niet uitsluitend, activiteiten zoals het bewaken van kosten (beheer subscription), toegang (rechten), beveiliging en gebruik van resources.
42.	Leverancier monitort en beheert de virtuele servers binnen de Azure tenant van opdrachtgever. Hieronder vallen, maar niet uitsluitend, activiteiten zoals monitoring van beschikbaarheid en capaciteit, beheren van besturingssystemen (patches en updates), ondersteuning systeemsoftware en beheren van datalocaties.
43.	Leverancier bewaakt de kwaliteit en inrichting van Azure services. Dit betreft het bewaken en doorvoeren van wijzigingen en innovaties binnen het Azure Cloud Platform.
44.	Leverancier beheert de netwerkconnectiviteit binnen de Azure Publice Cloud. Hieronder vallen, maar niet uitsluitend, activiteiten zoals monitoren van de beschikbaarheid en veiligheid van de componenten en het beheer hiervan (patches, updaten, configuratie veiligstellen, doorvoeren best practices) .
45.	Leverancier borgt en levert Workspacemanagement. Hieronder valt het beheer van de Azure virtual Desktops en cloud PC's.
46.	Managed services kunnen gedurende de looptijd worden aangepast door het doorvoeren van standaard changes en niet standaard changes.
Implementatie en beheer overeenkomst	
47.	Leverancier levert na gunning een implementatieplan die voldoet aan de criteria van artikel 6.3 van de GIBIT-voorwaarden
48.	Bij inschrijving levert Leverancier zijn concept SLA aan. De minimale uitgangspunten waaraan de SLA moet voldoen is opgenomen in bijlage 3 en voorwaarden zoals opgenomen in het PVE. De definitieve inhoud van de SLA wordt na gunning in overleg met opdrachtgever afgestemd.
49.	Bij inschrijving worden de volgende documenten door Leverancier opgeleverd: • Concept Dossier Afspraken en Procedures (DAP); • Concept Producten diensten catalogus (PDC) waarin minimaal de diensten zijn beschreven die in scope zijn van deze opdracht. Dit mag een uitgeklete versie zijn maar ook een volledige PDC van Leverancier. De definitieve inhoud van deze documenten wordt na gunning in overleg met opdrachtgever afgestemd.
50.	De implementatie van de ICT-prestatie is uiterlijk 30 juni 2026 afgerond. Op deze datum is de ICT-prestatie door opdrachtgever geaccepteerd en kan de ICT-prestatie per 1 juli 2026 in gebruik worden genomen.
51.	Jaarlijks vindt er tussen opdrachtgever en Leverancier een evaluatie over de geleverde dienstverlening plaats. Tijdens het overleg komen o.a. de volgende onderwerpen aan de orde: • Tevredenheid van opdrachtgever en gebruikerservaring; • Evaluatie contractuele afspraken; • Managementrapportages en toelichting; • Klachtenregistratie en behandeling; • Kwaliteit van de geleverde dienstverlening. Leverancier zorgt dat deze gesprekken worden ingepland.

52.	Leverancier zorgt voor één aanspreekpunt voor opdrachtgever in de rol van een Service manager. Deze Service manager is het vaste contactpersoon voor opdrachtgever en draagt zorg voor het up-to-date houden van de dienstverlening, rapporteren over de geleverde prestaties en bewaakt de kwaliteit van de dienstverlening
53.	Als de overeenkomst eindigt wordt van Leverancier verwacht, dat deze bereidwillig en kosteloos meewerkt aan de overdracht van kennis en ervaring en transitie naar een andere externe partij. Leverancier verleent op eerste verzoek van Opdrachtgever tijdige en volledige medewerking aan het overleggen van relevante rapportages en (management)informatie, die opdrachtgever in het kader van de overdracht aan een externe partij en/of voorbereiding van een aanbestedingsprocedure nodig acht.
Rapportages en monitoring	
54.	Leverancier levert periodieke (kwartaal) rapportages aan opdrachtgever omtrent het gebruik van de ondersteuning en afhandeling van meldingen en de dienstverlening. Leverancier denkt proactief mee om mogelijke structurele incidenten te signaleren en in overleg met opdrachtgever oplossingen te bespreken.
Informatiebeveiliging & Data	
55.	De data die wordt verwerkt in de ICT-prestatie blijven altijd eigendom van opdrachtgever.
56.	Leverancier verleent zekerheid ('assurance') over de kwaliteit van de dienstverlening aan opdrachtgever, bij voorkeur door middel van het jaarlijks aanleveren van een ISAE3402 type II rapportage, ISAE3000 of een SOC2 type II verklaring, waarin de scope is bepaald door de ICT-prestatie die opdrachtgever afneemt. Indien Leverancier niet beschikt over een ISAE3402, ISAE3000 of SOC2 rapportage zal Leverancier de dienstverlening aan opdrachtgever jaarlijks laten auditen door een onafhankelijke auditor en hierover aan opdrachtgever rapporteren. De kosten van de genoemde assurance verklaringen zijn voor rekening van Leverancier.
57.	Na gunning wordt er met Leverancier een verwerkersovereenkomst (bijlage 11) afgesloten die integraal onderdeel uitmaakt van de hoofdovereenkomst. Leverancier gaat bij inschrijving akkoord met de inhoud van deze concept verwerkersovereenkomst.
58.	Leverancier rapporteert transparant over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Zowel bij Leverancier als in de toeleveringsketen
Facturatie & Administratie	
59.	Leverancier stuurt maandelijks een factuur voor de geleverde diensten. Facturen dienen te worden gemaild naar Opdrachtgever.
60.	Op de factuur wordt minimaal de volgende informatie vermeldt: • Naam en adres van de leverancier; • Naam en adres opdrachtgever; • Het btw-nummer van de leverancier; • Het KvK-nummer van de leverancier; • Datum van de factuur;

	• Een uniek factuurnummer; • Een gespecificeerde omschrijving van diensten, producten of projecten die zijn geleverd; • Het aantal geleverde diensten; • De datum waarop de diensten zijn geleverd, of de datum van een vooruitbetaling; • Bedragen, exclusief btw; • Het geldende btw-tarief; • Het btw-bedrag.
61.	De omschrijving van diensten, producten, projecten zijn dusdanig op de factuur vermeldt dat deze te allen tijde te herleiden zijn naar de in de overeenkomst overeengekomen diensten en prijzen.
62.	De door Leverancier opgegeven prijzen dekken alle in deze uitvraag opgenomen eisen en door inschrijver aangeboden invullingen van de gunningcriteria volledig. Dit betekent dat alle kosten (beheer en ontwikkeling van de producten, dienstensystemen, personele kosten, reiskosten, afleveringskosten, overhead, accountantsverklaring e.d.) in de door Leverancier aangeboden prijzen zijn verwerkt. Facturatie van extra kosten is dus niet mogelijk, tenzij door Opdrachtgever expliciet anders aangegeven.
63.	Aanvullende of variabele kosten zijn alleen te factureren indien deze vooraf zijn afgestemd en schriftelijk goedgekeurd door opdrachtgever.
64.	Het is mogelijk om delen van de dienstverlening op- en af te schalen middels P&Q conform de vereisten zoals vermeldt in het prijzenblad. Verder is het mogelijk dat gedurende de looptijd van de overeenkomst het mogelijk is om aanvullende opdrachten waaraan behoefte is en die nauw verband houden met de scope van deze opdracht aan Leverancier te verstrekken. Deze aanvullende opdrachten hebben uitsluitend betrekking op: • De uitbreiding van het aantal gebruikers of systemen binnen de bestaande dienstverlening; • Aanverwante beheer- en supportdiensten binnen de bestaande technische en functionele scope; • Het uitvoeren van gebruikersondersteuning en werkplekbeheer wat nu door opdrachtgever zelf wordt uitgevoerd. • Doorontwikkeling of optimalisatie van reeds geleverde ICT-diensten. De omvang van de aanvullende opdrachten is beperkt tot 50% van de geraamde jaarlijkse opdrachtwaarde.
65.	In afwijking van de GIBIT-voorwaarden kunnen de tarieven jaarlijks per 1 januari, maar voor het eerst per 1 januari 2028 , door Leverancier worden aangepast, mits deze aanpassing minimaal één maand voorafgaand is aangekondigd. Een stijging is gelimiteerd tot maximaal de (eventuele) stijging van het op het moment van aankondiging laatst door het Centraal Bureau voor de Statistiek (CBS) gepubliceerde definitieve prijsindexcijfer dienstenprijzen commerciële dienstverlening en transport (index 2021=100), of de opvolger daarvan, voor groep J62, althans J6202, over het gehele jaar in vergelijking met het prijsindexcijfer van het kwartaal van inschrijving van diezelfde index.

	Als voorbeeld: het indexcijfer in het kwartaal van inschrijving Q2 2026 is 105. Het jaar dat geïndexeerd gaat worden is 2028. Het indexcijfer van Q2 2027 is 108. De formule is als volgt: $108/105 \times 100\% = 2,85\%$. De prijzen mogen worden geïndexeerd met 2,85%. Leverancier heeft ingeschreven met een prijs van €1000,-. De nieuwe prijs wordt dan € 1028,50. In het jaar 2030 is de index Q1 2029 112. De formule is als volgt $112/105 \times 100\% = 6,67\%$. De nieuwe prijs voor 2030 wordt €1000,- + €66,70 = €1066,70
--	---