Formulier 1 Programma van Eisen Microsoft 365 en Microsoft Azure Cloud beheerdiensten

Behorende bij de aanbesteding “Microsoft 365 en Azure Cloud beheerdiensten met kenmerk P24-0068”

Door voor deze aanbesteding een Inschrijving in te dienen, verklaart Inschrijver zich onvoorwaardelijk en volledig akkoord met onderstaande eisen. Eventuele voortvloeiende kosten uit onderstaande eisen dient Inschrijver te verwerken in de prijsopgave op het Prijzenblad. Onderstaande eisen kunnen dus niet leiden tot extra kosten, tenzij in de eis expliciet aangegeven.

De inhoud van de aanbesteding op hoofdlijnen

Het leveren van ICT-diensten voor de bestaande Microsoft 365 en Microsoft Azure Cloud-omgeving.

De opdracht bestaat uit de volgende onderdelen:

- Implementatie/transitieperiode
- Microsoft 365 technisch support (IT-ondersteuning complexe vraagstukken)
- Beheer Azure Cloud
- Projectcapaciteit

Eis	Algemene eisen	Voldoet Ja/Nee
1.	Opdrachtnemer heeft kennis van, en past Microsoft frameworks (Cloud Adoption Framework, en Well Architected Framework) en Microsoft 365/ Microsoft Azure best practices toe.	
2.	Opdrachtnemer moet gedurende de Overeenkomst, voldoen aan voor Opdrachtgever relevante wet- en regelgeving.	
3.	De Opdrachtnemer communiceert in de Nederlandse taal (zowel woord als geschrift) met de Opdrachtgever.	
4.	Licenties en abonnementen die tijdens de looptijd in opdracht van de Opdrachtnemer worden afgesloten, worden op naam van de Opdrachtgever geregistreerd.	
Eis	**Implementatie**	**Voldoet Ja/Nee**
Eis 5 vervalt. Algemene informatie m.b.t. implementatie: Vanuit de Opdrachtgever wordt er capaciteit vrijgemaakt voor de transitiefase, in de vorm van 2 solution architecten Microsoft Azure en Microsoft 365 en een projectleider. Ook vanuit de latende partij is er capaciteit vrijgemaakt voor de begeleiding van de re-transitie.		
6.	De Overeenkomst met de Opdrachtnemer dient op 1 juli 2025 in te gaan.	
7.	De Opdrachtnemer mag 4 tot 6 weken voor de ingangsdatum van het contract starten met de voorbereidende transitie werkzaamheden, zoals bijvoorbeeld het maken van een technische scan van de omgeving. De voorbereidende transitie werkzaamheden maken onderdeel uit van de eenmalige kosten.	
Eis	**Technische eisen Microsoft 365**	**Voldoet Ja/Nee**
8.	Als de interne gebruikersondersteuning van de Opdrachtgever, zélf ondersteuning nodig heeft voor technisch complexe vraagstukken, wil de interne gebruikersondersteuning, bestaande uit 7 functionarissen, contact op kunnen nemen met Opdrachtnemer voor geavanceerde IT-ondersteuning voor functionele en technische complexe vraagstukken met betrekking tot de Microsoft 365 omgeving van Opdrachtgever. Opdrachtnemer beschikt over voldoende specialistische functionele en technische kennis/expertise én ervaring om door Opdrachtgever aangemelde incidenten op te lossen. Opdrachtnemer biedt gedurende en als onderdeel van de Overeenkomst alle diensten die nodig zijn de continuïteit en optimale werking van de omgevingen van Opdrachtgever te waarborgen.	

9.	De Opdrachtnemer voert als onderdeel van de Overeenkomst tenminste 2x per jaar health checks uit op Microsoft 365. Acties en aanbevelingen die hieruit voortkomen, worden in principe door Opdrachtgever zelf of in opdracht samen met de Opdrachtnemer opgepakt.	
10.	De Opdrachtnemer ondersteunt Opdrachtgever bij Microsoft 365 gerelateerde (security) incidenten.	
11.	De Opdrachtnemer levert op verzoek van Opdrachtgever technische expertise en/of projectcapaciteit voor Microsoft 365 gerelateerde projecten.	
12.	De Opdrachtnemer geeft gedurende de Overeenkomst minimaal 2x per jaar gevraagd en ongevraagd aanbevelingen/adviezen over de Microsoft 365 omgeving, zoals compliancy, monitoring, resourcegebruik, security en de manier waarop oplossingen ingezet worden	Eis
Eis	**Technische eisen Microsoft Azure Cloud**	**Voldoet Ja/Nee**
13.	De Azure Cloud omgeving wordt op 1 juli 2025 door de Opdrachtnemer “as-is” in beheer genomen.	
14.	De Opdrachtnemer levert tijdens de looptijd van het contract als onderdeel van de Overeenkomst alle diensten (zoals configuratie, installatie, beheer, onderhoud en beveiliging, die benodigd zijn om de Azure Cloud omgeving te continueren en te waarborgen zoals Opdrachtnemer die op het moment van het in beheer nemen van de ICT-omgeving heeft geaccepteerd.	
15.	De Opdrachtnemer richt vanaf 01 juli 2025 de Azure Cloud omgeving van VRMWB in volgens het Well-Architected Framework en Cloud Adoption Framework op basis van Infra as Code. Hierbij zijn de foundation basiscomponenten ingericht zoals een Azure firewall, VPN-verbindingen, ExpressRoute, Identities en back-up. Dit op basis van een hub en spoke netwerk topologie, foundation en landing zones. De workloads worden ondergebracht in landing zones.	
16.	De Opdrachtnemer is verantwoordelijk voor resourcebeheer, dat bestaat uit het aanmaken en configureren van Azure resources, het beheren van resource groepen en subscriptions en het rapporteren en verwijderen van ongebruikte resources.	
17.	De Opdrachtnemer is verantwoordelijk voor virtuele netwerkbeheer in Azure, met daarin het configureren van netwerken, beheer van netwerkbeveiligingsgroepen en Azure Firewall en het configureren van VPN-gateways en verbindingen.	
18.	De Opdrachtnemer is verantwoordelijk voor Identiteit- en Toegangsbeheer voor administratieve accounts, zoals de configuratie van rol gebaseerde toegangscontrole tot landingzones/ workloads. De Opdrachtnemer adviseert over het beheer van Entra ID.	
19.	De Opdrachtnemer is verantwoordelijk voor beveiliging en compliance, implementeert beveiligingsmaatregelen, monitort beveiligingsincidenten en beheert en rapporteert over compliance policies binnen de Azure omgeving.	
20.	De Opdrachtnemer is verantwoordelijk voor monitoring en rapportage, en zorgt voor configuratie van Azure Monitor en Log Analytics, monitort resourcegebruik en prestaties en rapporteert over gebruik en kosten. Opdrachtgever gaat akkoord met een eigen monitoring oplossing mits functionarissen van Opdrachtgever toegang krijgen tot een dashboard.	
21.	De Opdrachtnemer zal, waar mogelijk, de Azure-consumptie minimaliseren. Opdrachtnemer monitort en adviseert de Opdrachtnemer maandelijks over de mogelijkheden om dit te bereiken.	
22.	De Opdrachtnemer is verantwoordelijk voor de monitoring, het rapporteren, beheren en herstellen (restore) van de Azure back-up.	
23.	De Opdrachtnemer ondersteunt Opdrachtgever bij Azure gerelateerde incidenten.	
24.	De Opdrachtnemer is verantwoordelijk voor de implementatie van updates en patches (update plans, type resource).	
25.	De Opdrachtnemer is verantwoordelijk voor het beheren en beschikbaar stellen van de meest recente documentatie met betrekking tot de inrichting en configuratie van de Azure-omgeving van de Opdrachtgever.	
26.	De Opdrachtnemer is voor het onderdeel DevOps verantwoordelijk voor de configuratie van CI/CD pipelines en het beheer van Infrastructure as Code (Platform & LZ Resources).	

27.	De Opdrachtgever is eigenaar van de Infrastructure as Code (IaC) welke door de Opdrachtnemer wordt ontwikkeld, onderhouden en toegepast op de Azure Cloud omgeving van Opdrachtgever.	
28.	De Opdrachtnemer levert op verzoek van Opdrachtgever technische expertise en/of projectcapaciteit voor Azure gerelateerde projecten.	
29.	De Opdrachtnemer verstrekt gedurende de Overeenkomst minimaal twee keer per jaar, zowel op verzoek als ongevraagd, aanbevelingen en adviezen over het gehele Azure-platform. Dit omvat aspecten zoals compliance, monitoring, resourcegebruik en de inzet van oplossingen.	
Eis	**Bescherming persoonsgegevens**	**Voldoet Ja/Nee**
30.	Opdrachtnemer verwerkt de persoonsgegevens van de VRMWB in overeenstemming met de bepalingen zoals opgenomen binnen de AVG.	
31.	Door ondertekening van de verwerkersovereenkomst gaat de opdrachtnemer akkoord met de hierin opgenomen voorwaarden over de bescherming van persoonsgegevens. De verwerkersovereenkomst zal na ondertekening als bijlage bij de overeenkomst worden opgenomen. Inschrijver zal dan ook met eventuele in te zetten onderaannemers, eenzelfde verwerkersovereenkomst dienen af te sluiten. VRMWB hanteert hiervoor de handreiking Standaard Verwerkersovereenkomst Gemeenten. Deze treft u aan als bijlage in het Aanbestedingsdocument. De Aanbestedende Dienst beschikt over een procedure meldplicht datalekken. Opdrachtnemers van de Aanbestedende Dienst dienen kennis te nemen van deze procedure en hieraan actief hun medewerking te verlenen.	
Eis	**Informatiebeveiliging**	**Voldoet Ja/Nee**
Op de aan te besteden opdracht is de GIBIT 2023 van toepassing. VRMWB heeft aanvullend op de GIBIT 2023 onderstaande eisen op het gebied van informatiebeveiliging opgenomen.		
32.	Opdrachtnemer dient het principe van de minste bevoegdheden toe te passen, waarbij medewerkers van de Opdrachtnemer alleen toegang krijgen tot de gegevens en systemen die zij strikt noodzakelijk hebben.	
33.	De Opdrachtnemer conformeert zich aan de eisen van Opdrachtgever op het gebied van MFA i.c.m. toegang tot de Azure-omgeving.	
34.	Opdrachtnemer moet gebruik maken van RBAC om de toegang tot resources binnen de Azure-omgeving te beheren.	
35.	Opdrachtgever houdt logs bij van alle activiteiten binnen de Azure-omgeving, inclusief toegangspogingen en configuratiewijzigingen. Deze logs worden veilig opgeslagen en periodiek door Opdrachtnemer worden geaudit. Opdrachtnemer draagt zorg voor het beschikbaar stellen van de logging op moment dat Opdrachtgever daarom vraagt.	
36.	Opdrachtnemer dient monitoring te implementeren voor dreigingsdetectie en moet in staat zijn om snel te reageren op beveiligingsincidenten in de Azure omgeving.	
37.	Opdrachtgever ontvangt iedere 2 maanden een rapportage waar aangegeven is welke High risk kwetsbaarheden geconstateerd zijn en welke acties hierop genomen zijn. ~~Opdrachtnemer laat wekelijks kwetsbaarheidsscans uitvoeren op de Azure omgeving van Opdrachtgever en lost geconstateerde kwetsbaarheden op.~~	
38.	Opdrachtnemer beschikt, voor de ICT-omgeving van Opdrachtnemer, over een getest disaster recovery plan, waarin duidelijk wordt aangegeven hoe snel systemen kunnen worden hersteld na een incident (RTO/RPO).	
39.	De Opdrachtgever heeft voor beveiligingsincidenten een 24/7 procedure, waarbij een CSIRT wordt opgestart. Opdrachtnemer is verplicht om beveiligingsincidenten direct te melden, inclusief de aard van het incident en de genomen stappen.	
40.	De opdrachtnemer werkt actief mee aan onderzoeken naar beveiligingsincidenten en ondersteunt bij het uitvoeren van audits	
41.	Er worden door Opdrachtgever jaarlijks periodieke evaluaties uitgevoerd van de beveiligingsmaatregelen van de opdrachtnemer, mogelijk door externe auditors. Opdrachtnemer stelt om niet capaciteit beschikbaar voor deze audits.	

<table>
<tr><th>Eis</th><th>Exit strategie</th><th>Voldoet Ja/Nee</th></tr>
<tr><td>42.</td><td>Bij elke samenwerking kunnen omstandigheden optreden waardoor een Re-transitie noodzakelijk is. De omstandigheden kunnen van positieve als van negatieve aard zijn. Met het overeenkomen van de Re-transitie als onderdeel van de Overeenkomst is het vanaf het begin helder dat aan de dienstverlening een einde komt. Op deze manier wordt een zakelijke en respectvolle manier van afscheid geborgd.

Opdrachtnemer stelt het Re-transitieplan in de Transitieperiode op en kent een aantal principes welke bij het uitvoeren van de Re-transitie door Opdrachtnemer t.z.t. als Latende Leverancier worden gehanteerd:
• Bij een Re-transitie levert Opdrachtnemer als Latende leverancier binnen vier (4) weken na verzoek van Opdrachtnemer een actueel Re-transitieplan op, met een compleet overzicht van High Level Design (HLD), Infrastructure as code (IaC), configuratie, architectuur, data;
• Opdrachtgever dient zo min mogelijk hinder te ervaren door contract beëindiging en de overdracht van de dienstverlening van Opdrachtnemer naar Opdrachtgever of een eventuele derde partij;
• Alle betrokken partijen committeren zich aan een constructieve samenwerking gedurende
het Re-transitie proces;
• Opdrachtnemer biedt volledige transparantie over de uit te voeren werkzaamheden, de te
besteden tijd en de opgebouwde kennis;
• Het Re-transitieplan wordt door Opdrachtnemer geactualiseerd en onderhouden. Elk jaar wordt het Re-transitieplan ter goedkeuring voorgelegd aan Opdrachtgever.</td><td></td></tr>
<tr><th>Eis</th><th>SLA</th><th>Voldoet Ja/Nee</th></tr>
<tr><td>43.</td><td>De Opdrachtnemer stelt, in afstemming met Opdrachtgever, een SLA en DAP op. In de SLA wordt tenminste de scope van de diensten, de behaalde servicelevels, de overlegmomenten en de wijze van escalatie beschreven.</td><td></td></tr>
<tr><td>44.</td><td>Tijdens kantoortijden is de Opdrachtnemer telefonisch tussen 08.00 en 18.00 bereikbaar voor de interne gebruikersondersteuning (7 functionarissen) van de Opdrachtgever.</td><td></td></tr>
<tr><td>45.</td><td>Over de overeengekomen KPI’s in de SLA wordt tenminste 1x per maand gerapporteerd door Opdrachtnemer. Deze documenten worden alleen gewijzigd in overleg met en na goedkeuring van Opdrachtgever. De documenten worden tenminste één (1) maal per half (1/2) jaar met Opdrachtgever doorgenomen en geactualiseerd.</td><td></td></tr>
<tr><td>46.</td><td>De Opdrachtnemer conformeert zich aan de oplostijden voor de Azure incidenten, vanaf het moment dat deze gemeld zijn bij Opdrachtnemer.

<table>
<tr><th>Type incident</th><th>Oplostijd</th><th>Norm</th></tr>
<tr><td>Prio 1 (P1) – Hoog
Hoge urgentie, Hoge Impact</td><td>4 uur</td><td>Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.</td></tr>
<tr><td>Prio 2 (P2) – Midden
Medium urgentie, Medium impact</td><td>12 uur</td><td>Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.</td></tr>
<tr><td>Prio 3 (P3) – Laag
Lage urgentie, Lage Impact</td><td>24 uur</td><td>Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.</td></tr>
</table></td><td></td></tr>
</table>

	Voor de Microsoft 365 incidenten gaat Opdrachtgever met Opdrachtnemer na gunning in dialoog om tot een voor beide partijen werkbare/acceptabele afspraak te komen die recht doet aan de intentie om de continuïteit optimaal te borgen. Opdrachtnemer levert hiervoor een maximale inspanningsverplichting. ~~De Opdrachtnemer conformeert zich aan de oplostijden voor de **M365 incidenten**, vanaf het moment dat deze gemeld zijn bij Opdrachtnemer.~~ ~~Type incident~~ / ~~Oplostijd~~ / ~~Norm~~ ~~Prio 1 (P1) – Hoog Hoge urgentie, Hoge Impact~~ / ~~8 uur~~ / ~~Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.~~ ~~Prio 2 (P2) – Midden Medium urgentie, Medium impact~~ / ~~16 uur~~ / ~~Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.~~ ~~Prio 3 (P3) – Laag Lage urgentie, Lage Impact~~ / ~~24 uur~~ / ~~Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.~~	
47.	~~De Opdrachtnemer is in staat om tijdens incidenten binnen de gestelde SLA tijden van Prioritering ondersteuning op locatie van Opdrachtgever aanwezig te zijn, indien dit nodig is.~~ De Opdrachtnemer is in staat om, in onderling overleg, tijdens incidenten op locatie van Opdrachtgever aanwezig te zijn	
48.	De Opdrachtnemer heeft 24/7 dienstverlening gegarandeerd voor het oplossen van P1 security- en bereikbaarheidsincidenten die een hoge impact op de bedrijfscontinuïteit van Opdrachtgever hebben.	

Wens	TOPdesk koppeling (Gunningscriterium 4)	Voldoet Ja/Nee
GC-4	Van de Opdrachtnemer wordt verwacht dat zij de ITIL-processen afstemt op die van de Opdrachtgever voor een soepele samenwerking. De Opdrachtgever gebruikt TOPdesk (SaaS) voor ITIL-processen en wil dat incidenten en wijzigingen voor de derde lijn tussen TOPdesk en het ITSM-systeem van Opdrachtnemer automatisch worden gesynchroniseerd. Bij voorkeur via een API-koppeling. De Opdrachtnemer biedt een API die volledig integreert met TOPdesk. Doelstelling is om een efficiënte uitwisseling van gegevens en een gestroomlijnde samenwerking te realiseren. Opdrachtgever verwacht met deze koppeling een snellere en betere incidentafhandeling te realiseren doordat incidenten direct naar de juiste teams worden doorgezet. Het changemanagement wordt efficiënter omdat wijzigingen automatisch worden gesynchroniseerd, wat handmatige invoer vermindert. Dit leidt tot een betere samenwerking dankzij de naadloze gegevensuitwisseling, wat de communicatie tussen teams verbetert. Bovendien verhoogt deze koppeling de productiviteit doordat de focus op kernactiviteiten ligt.	

Bedrijfsnaam	
Naam ondertekenaar	
Functie ondertekenaar	
Handtekening	
Plaats en datum	