

Programma van Eisen (PvE)

In dit Programma van Eisen (ook wel te noemen 'PvE') – dat integraal onderdeel uitmaakt van de aanbestedingsleidraad 'Ondersteuning ICT kantoorautomatisering' van 26-11-2025 – staan de uitvoeringseisen beschreven die van toepassing zijn voor de uitvoering van de werkzaamheden onder de overeenkomst.

Dit document is met grote zorgvuldigheid samengesteld. Mocht dit PvE desondanks onduidelijkheden, tegenstrijdigheden/fouten of zaken waar een partij het niet mee eens is of een alternatief voor wil voorstellen bevatten dan dient deze partij dit de aanbestedende dienst bij de inlichtingenrondes – vóór het indienen van een inschrijving – kenbaar te maken (zie ook paragraaf 3.3 van de aanbestedingsleidraad).

Een inschrijving dient – op straffe van uitsluiting van de aanbestedingsprocedure – zich onvoorwaardelijk en volledig aan het PvE te conformeren (zie ook

Betreft	Eis nr	Omschrijving
Personeel		
	1	Het personeel van de opdrachtnemer dat wordt ingezet voor de gevraagde dienstverlening beheerst de Nederlandse taal vloeiend in woord en geschrift.
	2	Personeel van de opdrachtnemer dat wordt ingezet voor de gevraagde dienstverlening dient in het bezit te zijn van een VOG-verklaring en een de opdrachtnemer zelf opgestelde geheimhoudingsverklaring te hebben ondertekend.
Beveiliging algemeen		
	3	Opdrachtnemer garandeert dat gegevens van opdrachtgever na beëindiging van de overeenkomst zijn te exporteren en daarna aantoonbaar door opdrachtnemer worden verwijderd en/of vernietigd.
	4	Opdrachtnemer is verantwoordelijk voor de beveiliging van de in beheer genomen informatie, waaronder (maar niet beperkt tot) persoonsgegevens in de zin van de AVG. Niets van deze informatie mag zonder toestemming van opdrachtgever aan derden ter beschikking worden gesteld.
Exit strategie		
	5	Opdrachtnemer dient, uiterlijk één (1) maand voor de beëindiging van de overeenkomst, een Exit strategie te beschrijven waarmee aan opdrachtgever garanties geboden worden dat bij het verstrijken van de overeenkomst de continuïteit en kwaliteit van de dienstverlening gedurende de transitie naar een derde partij gewaarborgd blijft.
	6	Opdrachtnemer onderbouwt deze strategie in een operationeel Exit plan opdat een naadloze overdracht van kennis, ervaring en informatie plaatsvindt.
	7	Opdrachtnemer verwoordt in het Exit plan welke taken en verantwoordelijkheden belegd zijn bij opdrachtnemer en welke bij opdrachtgever.
Beheer en ondersteuning		
	8	Opdrachtnemer zal 2e en 3e lijns werkzaamheden uitvoeren op gebied van Microsoft servers, werkplekken, Azure en Microsoft 365 zoals beschreven in paragraaf 2.5 van de Aanbestedingsleidraad.
	9	Opdrachtnemer zal het volledige beheer van de bestaande firewall (Sophos XGS2300) verzorgen: uitvoeren van (firmware) updates, het uitvoeren van aanpassingen en het leveren van de benodigde XGS 2300 Enhanced Support licentie.
	10	Opdrachtnemer zal een backup oplossing verzorgen en inrichten waarmee de volledige Microsoft 365 omgeving van de opdrachtgever kan worden gebackuped (Mailboxen, Teams/SharePoint, OneDrive). Dagelijks zal er een mailbericht naar de opdrachtgever worden verstuurd met daarin de status van de backups van de afgelopen 24 uur.
	11	Opdrachtgever zal de dagelijkse backup controle uitvoeren en eerstelijnsproblemen oplossen, opdrachtnemer zal op verzoek van de opdrachtgever tweede en derdelijnsproblemen behandelen.
	12	Opdrachtnemer zal de ICT-adviseur van de opdrachtgever periodiek (maar tenminste eens per kwartaal) voorlichten en adviseren op gebied van innovatie, beveiliging en ICT-strategie.
	13	Opdrachtnemer zal er zorg voor dragen dat alle laptops worden voorzien van anti-virus/anti-mallware software. Keuze van de betreffende oplossing zal in samenspraak met de opdrachtgever geschieden.
	14	Opdrachtgever heeft diverse ICT-diensten uitbesteed aan derde partijen (wifi, printers, mobiele telefonie etc.). Deze derde partijen zullen primair verantwoordelijk zijn voor het optimaal verlenen van hun diensten, maar zullen (deels) verbindingen hebben met Microsoft 365, Azure of andere diensten. Bij problemen zal opdrachtnemer op verzoek zijn volledige medewerking verlenen.
Vervanging systeembeheerder		
	15	Opdrachtnemer zal bij afwezigheid van de interne systeembeheerder van de opdrachtgever op verzoek remote eerstelijns-problemen aannemen en behandelen.
	16	Bij langdurige afwezigheid van de interne systeembeheerder van de opdrachtgever (bijvoorbeeld vakantie of ziekte) zal opdrachtnemer in overleg met opdrachtgever een medewerker op locatie van de opdrachtgever te Hilversum beschikbaar stellen voor het behandelen van eerste en tweedelijns incidenten. Opdrachtgever zal dit bij <i>geplande</i> afwezigheid van de interne systeembeheerder zo spoedig mogelijk melden bij de opdrachtnemer.
Support Desk		
	17	Medewerkers van de supportdesk spreken vloeiend Nederlands.

18	Medewerkers van de opdrachtgever dienen - bij afwezigheid van de interne systeembeheerder - rechtstreeks contact op te kunnen nemen met een supportdesk. Medewerkers van deze supportdesk dienen eerstelijns problemen op te kunnen lossen en de laptop van de betreffende medewerker remote over te kunnen nemen.
19	Supportdesk medewerkers dienen de mogelijkheid te hebben om -na expliciete toestemming van de laptopgebruiker- de laptop op afstand te kunnen overnemen om problemen op te kunnen lossen.
20	De supportdesk dient tussen 08:00u - 18:00u bereikbaar te zijn via telefoon, e-mail en via een webportaal waarop medewerkers kunnen inloggen om de status van de door hun aangemelde problemen te zien. De ICT adviseur en interne systeembeheerder van de opdrachtgever hebben ook toegang tot dit webportaal en kunnen de status van alle medewerkers inzien en aanpassen.
21	Gebruik van een betaald servicenummer voor de toegang tot de supportdesk is niet toegestaan.
Monitoring en NOC	
22	Opdrachtnemer zal een monitoringsysteem leveren en onderhouden dat systemen (servers, laptops en infrastructuur hardware) monitort op prestatie en beveiligingsproblemen. Deze monitoring zal minimaal toezien op de status van de antivirusoplossing, de aanwezigheid of blokkade van malware, kritieke meldingen in logboeken (eventviewer) of mislukte Windows updates.
23	Opdrachtnemer zal bij geconstateerde problemen contact opnemen met de systeembeheerder van de opdrachtgever en op verzoek de systeembeheer ondersteunen bij het oplossen van de geconstateerde problemen.
24	De opdrachtnemer zal software leveren, installeren en onderhouden om laptops op afstand te kunnen overnemen. Het overnemen van laptops dient enkel te kunnen gebeuren na een akkoord van de betreffende laptop-gebruiker. De interne systeembeheerder van de opdrachtgever zal ook toegang krijgen tot dit systeem en de rechten krijgen om laptops op afstand over te nemen .
25	Opdrachtnemer zal de bestaande SIEM oplossing (XDR / Microsoft Sentinel) beheren, monitoren en met gepaste urgentie acteren op meldingen.
Licenties	
26	Opdrachtnemer verschaft een veilige en simpele methode waarmee de interne systeembeheerder van de opdrachtgever eenvoudig en snel Microsoft 365 licenties kan aanschaffen en beheren.
27	Aangeschafte licenties staan op naam van de opdrachtgever door middel van (bijvoorbeeld) het gebruik van een CSP-model.
28	Opdrachtnemer factureert de licenties maandelijks aan de opdrachtgever.
29	Opdrachtnemer heeft inhoudelijke kennis van Microsoft licenties en adviseert de ICT-adviseur van de opdrachtgever pro-actief over de verschillende mogelijkheden.
Overig	
30	De opdrachtnemer beschikt over een geldige SOC2 Type II of een ISAE Type II verklaring, of is binnen de periode van 9 maanden na de ingangsdatum van de overeenkomst in het bezit van deze verklaring. In geval van een samenwerkingsverband geldt dat de penvoerder dient te beschikken over deze verklaring.
31	De opdrachtnemer dient geregistreerd te zijn als trusted partner bij Microsoft. De opdrachtnemer voldoet minimaal de volgende Services expertises; Consulting, Custom Solution, Hardware, Licensing, Project management, System integration. De opdrachtnemer voldoet minimaal de volgende Solution expertises; Backup & Disaster Recovery, Cloud Database Migration, Cloud Migration, Cloud Voice, Security, Sharepoint on Azure, Threat Protection. De opdrachtnemer heeft volgens het trusted partner programma ervaring met Government (Industries expertise). De opdrachtnemer voldoet minimaal de volgende Products expertises; Azure, Enterprise Mobility & Security, Exchange, Microsoft en Office 365, Power BI, Project, SQL, SharePoint, Teams, Visio, Windows.