Bijlage 4 Programma van Eisen '' Europese aanbesteding volgens de openbare procedure voor het beheer en de optimalisatie van de IT-werkomgeving t.b.v. Stichting WIJeindhoven"

Doel van dit document: het Programma van Eisen legt alle vereisten vast met betrekking tot de gewenste dienstverlening, zoals bepaald door de stakeholders. Het Programma van Eisen vormt de basis voor de uitvoering van de overeenkomst en dient tevens als input voor de management gesprekken over de geleverde prestaties.

Servicemanagement

IS	Inrichting servicemanagement
IS1	De opdrachtnemer levert maandelijkse inzet voor samenwerking en beheer (zoals wijzigings- en herstelbeheer, beheer en monitoring, en advies).
IS2	De aanbestedende dienst en de opdrachtnemer stemmen bij aanvang van de samenwerking de verdeling van de vaste maandelijkse inzet per hoofdactiviteit (zoals wijzigings- en herstelbeheer, beheer en monitoring, en advies) gezamenlijk af op basis van een indicatief urenkader.
IS3	De verdeling dient als uitgangspunt voor sturing, monitoring en evaluatie. De opdrachtnemer rapporteert maandelijks op de inzet per domein, inclusief een overzicht van opgebouwde en bestede uren.
IS4	Niet-benutte uren binnen de reguliere maandelijkse inzet worden doorgeschoven naar een latere maand binnen hetzelfde kalenderjaar. Deze opgebouwde capaciteit kan worden ingezet voor piekbelasting of grotere wijzigingen.
IS5	Aan het einde van het kalenderjaar vervallen niet-benutte uren, tenzij schriftelijk anders overeengekomen.
IS6	De indicatieve verdeling van de vaste maandelijkse inzet over de domeinen wordt jaarlijks geëvalueerd en bijgesteld op basis van realisatie, ervaren knelpunten en veranderende behoeften van de aanbestedende dienst.
IS7	Opschaling van inzet buiten de reguliere capaciteit vindt alleen plaats na schriftelijke goedkeuring door de aanbestedende dienst.
IS8	Projectmatige ondersteuning (meerwerk) valt binnen de scope van de overeenkomst maar buiten de scope van de basisinzet en dienen afzonderlijk te worden geoffreerd. Uitvoering vindt uitsluitend plaats na schriftelijke goedkeuring door de aanbestedende dienst.
IS9	De opdrachtnemer stelt een servicemanager of coördinator aan als vast aanspreekpunt.
IS10	De opdrachtnemer adviseert de aanbestedende dienst proactief over optimalisaties, risico's, trends en kansen op het gebied van beheer, beveiliging en functioneel gebruik van de IT-omgeving.
IS11	De opdrachtnemer volgt actief relevante ontwikkelingen binnen het Microsoft-platform (zoals wijzigingen in licentievoorwaarden, beheerfunctionaliteit of beveiligingsinstellingen) en informeert de aanbestedende dienst tijdig over impactvolle updates of beleidswijzigingen.
OS	Overleg & sturing
OS1	De opdrachtgever en opdrachtnemer hanteren een vaste overlegstructuur, die bij aanvang van de samenwerking gezamenlijk wordt vastgesteld. Standaard wordt uitgegaan van een maandelijks operationeel overleg en een kwartaalgesprek op tactisch of strategisch niveau, tenzij anders overeengekomen.
OS2	De opdrachtnemer maakt tijdens het overleg notulen en levert deze binnen drie werkdagen aan bij de ICT-coördinator van de opdrachtgever.
OS3	De opdrachtnemer levert voorafgaand aan het operationele overleg een gestructureerde rapportage aan over prestaties, knelpunten, voortgang en ureninzet.
OS4	De opdrachtnemer initieert structureel verbeteracties op basis van analyses en trends.
OS5	De opdrachtnemer werkt samen volgens het principe "voordoen – samen doen – zelf doen".
RE	Regie & escalatie

RE1	De aanbestedende dienst behoudt altijd de regie over eigenaarschap, prioriteiten en goedkeuring.
RE2	De opdrachtnemer werkt met een helder escalatiemodel bij afwijkingen of verstoringen.
RE3	Alle afspraken over samenwerking, regie, escalaties, rapportages, responstijden, oplossnelheid en beschikbaarheid worden, na definitieve gunning, binnen drie maanden na start van de overeenkomst vastgelegd in de SLA. Deze SLA wordt vervolgens jaarlijks geëvalueerd en waar nodig geactualiseerd.
RE4	Voor urgente meldingen met prioriteit P1 geldt dat de opdrachtnemer binnen 1 uur telefonisch contact opneemt, ook buiten kantooruren indien hierover expliciete afspraken zijn gemaakt in de SLA.
BS	Buiten scope
BS1	Meldingen of wijzigingsverzoeken die niet binnen de overeengekomen scope vallen, worden door de opdrachtnemer binnen één werkdag gemeld aan de aanbestedende dienst met een beknopte motivering.
BS2	Verdere behandeling van deze meldingen vindt uitsluitend plaats na expliciete goedkeuring van de aanbestedende dienst.

Wijzigings- en herstelbeheer

AS	Afhandeling & samenwerking
AS1	Meldingen worden alleen geëscaleerd via het afgesproken kanaal als de eigen interne IT-afdeling van de aanbestedende dienst het incident zelf niet kan oplossen; eindgebruikers hebben geen direct contact met de opdrachtnemer.
AS2	Herstel- en wijzigingsverzoeken worden geclassificeerd op basis van urgentie, impact en complexiteit (bijv. P1–P3 voor urgentie, standaard/significant/hoog risico voor wijzigingen), zoals verder uitgewerkt in de SLA voor het sluiten van de overeenkomst.
AS3	De opdrachtnemer levert passende expertise, ondersteuning en coördinatie, afhankelijk van de aard en complexiteit van de melding of wijziging.
AS4	De opdrachtnemer levert op afroep een consultant voor werkzaamheden op locatie bij de opdrachtgever, indien fysieke aanwezigheid noodzakelijk is voor uitvoering van wijzigings- of herstelverzoeken.
AS5	De inzet van een consultant (projectmatige ondersteuning) op locatie wordt separaat geoffreerd en valt buiten de vaste maandelijkse inzet. Uitvoering vindt uitsluitend plaats na voorafgaand schriftelijk akkoord van opdrachtgever.
AS6	De ingezette consultant beschikt aantoonbaar over relevante kennis, certificering en ervaring passend bij de aard van de wijziging of het incident. De aanbestedende dienst behoudt zich het recht voor een consultant te weigeren bij onvoldoende aansluiting op de opdracht.
AS7	Herstelverzoeken en changes worden vooraf afgestemd en uitgevoerd volgens het principe "voordoen – samen doen – zelf doen".
AS8	De opdrachtnemer werkt samen met de aanbestedende dienst aan voorbereiding, uitvoering en documentatie van changes en herstelacties.
AS9	De opdrachtnemer registreert alle incidenten, acties en doorlooptijden in een gedeeld ticketsysteem en/of changeboard met relevante metadata.
AS10	De opdrachtnemer bevestigt elke melding na ontvangst en sluit deze pas af na expliciete goedkeuring van de aanbestedende dienst.
AS11	Bij risicovolle wijzigingen geldt het vier-ogenprincipe: opdrachtnemer en de aanbestedende dienst stemmen vooraf af en controleren elkaars inzichten en acties.
AS12	Herstelverzoeken en changes met impact op gebruikers worden tijdig afgestemd en gecommuniceerd via de aanbestedende dienst, zodanig dat eindgebruikers minimaal twee (2) werkdagen voorafgaand aan de uitvoering geïnformeerd kunnen worden.
AS13	De opdrachtnemer voert acties bij voorkeur buiten kantooruren uit bij potentiële impact op continuïteit.

AS14	Ad-hoc verzoeken zonder impact of risico worden afgehandeld als standaard service requests.
AS15	Bij significante of risicovolle wijzigingen wordt de inzet van een medior of senior consultant geborgd. De aanbestedende dienst behoudt zich het recht voor een consultant te weigeren bij onvoldoende expertise of ervaring.
CRE	Capaciteit, rapportage & evaluatie
CRE1	De opdrachtnemer bewaakt actief de inzet en capaciteit en meldt structurele overschrijdingen tijdig.
CRE2	De opdrachtnemer levert maandelijks een overzicht van uitgevoerde en geplande herstelverzoeken en wijzigingen.
CRE3	De aanbestedende dienst en opdrachtnemer bespreken structureel de voortgang, knelpunten en verbetervoorstellen binnen de overlegstructuur uit servicemanagement.
CRE4	Terugkerende of foutgevoelige meldingen worden geëvalueerd; waar mogelijk wordt geautomatiseerd.
CRE5	Bij herhaalde of kritieke meldingen wordt een root cause analysis (RCA) opgesteld.
CRE6	Het proces voor wijzigings- en herstelbeheer wordt jaarlijks geëvalueerd en bijgesteld op basis van ervaringen en veranderende omstandigheden.
SLA	SLA-koppeling
SLA1	De afspraken over prioritering, responstijden, beschikbaarheid, planning en escalaties worden vastgelegd in de SLA voor sluiten van de overeenkomst.
SLA2	De SLA wordt jaarlijks geëvalueerd en bijgesteld op basis van realisatie, trends en veranderende behoeften.

Projectmanagement

PS	Projectaanpak & samenwerking
PS1	De aanbestedende dienst en de opdrachtnemer hanteren een gestandaardiseerde projectaanpak voor initiatieven op het gebied van innovatie, beveiliging, automatisering en modernisering van de Microsoft 365- en Azure-omgeving.
PS2	Projectenvoorstellen kunnen door zowel de aanbestedende dienst als de opdrachtnemer worden aangedragen.
PS3	Uitvoering van een project vindt alleen plaats na schriftelijk akkoord van tekenbevoegde van de aanbestedende dienst.
PS4	De opdrachtnemer levert per projectvoorstel ten minste: een heldere afbakening van de scope; beoogde doelstellingen; globale planning met mijlpalen; verwachte inzet en benodigde expertise; afhankelijkheden en risico's; verwachte beheerimpact.
PS5	Projecten worden afgestemd en bewaakt binnen de tactische overlegstructuur, en waar nodig aangevuld met een specifiek projectoverleg.
PS6	Tijdens de uitvoering zorgt de opdrachtnemer voor actieve afstemming met een vaste contactpersoon van de aanbestedende dienst (bijv. ICT coördinator).
PS7	De projectmatige inzet valt buiten de reguliere inzet en wordt separaat geoffreerd, tenzij expliciet anders overeengekomen.
RIE	Rollen, inzet & expertise
RIE1	De opdrachtnemer kan op verzoek projectrollen invullen zoals projectmanager, lead consultant of solution architect met de uurtarieven conform prijzenblad.
RIE2	De opdrachtnemer borgt dat consultants over aantoonbare expertise beschikken die aansluit op de scope van het project.
RIE3	Bij kritieke of complexe trajecten kan de aanbestedende dienst vooraf goedkeuring vragen op inzet van specifieke medewerkers.
RIE4	De opdrachtnemer past het principe *voordoen – samen doen – zelf doen* toe, met als doel overdracht van kennis en eigenaarschap naar de interne IT-afdeling van de aanbestedende dienst.

KA	Kennisoverdracht & afronding
KA1	Bij afronding van elk project levert de opdrachtnemer: een overdrachtsdocument met technische inrichting, beheerafspraken en documentatie; aanbevelingen voor borging in beheer; een korte evaluatie van leerpunten, kansen en mogelijke vervolgacties.
KA2	Waar relevant zorgt de opdrachtnemer voor oplevering in lijn met wijzigings- en herstelbeheer, inclusief registratie in het ticketsysteem of changeboard.
KA3	Een project wordt pas als formeel opgeleverd beschouwd na expliciete goedkeuring ("sign-off") door beide partijen. Deze sign-off omvat een akkoord op de opgeleverde documentatie, uitvoering conform afspraken, en eventuele overdracht aan beheer. Zonder gezamenlijke goedkeuring geldt het project als niet afgerond.
SI	Strategische verkenning & innovatie
SI1	De opdrachtnemer initieert ten minste jaarlijks een strategisch gesprek met de aanbestedende dienst om relevante technologische ontwikkelingen te bespreken (bijv. AI, governance, compliance, modern device management).
SI2	Voorgestelde innovaties worden beoordeeld op relevantie, haalbaarheid, beheerimpact en bijdrage aan doelstellingen van de aanbestedende dienst (zoals efficiëntie, beveiliging, gebruiksgemak).
SI3	Op basis van dit overleg kunnen verkenningen of proof-of-concepts worden voorgesteld, die bij geschiktheid via het projectproces worden uitgewerkt.

Beheer en monitoring

LB	Licentiebeheer
LB1	De opdrachtnemer verzorgt het inkoopproces van licenties op verzoek van de aanbestedende dienst en sluit geen overeenkomsten af zonder voorafgaand schriftelijk akkoord, conform de afspraken vastgelegd in de SLA.
LB2	De opdrachtnemer monitort en beheert licentie-instellingen in Microsoft 365 Admin Center, met gedeelde toegang voor de aanbestedende dienst.
LB3	De aanbestedende dienst behoudt zelf het recht en de regie om licenties toe te wijzen aan gebruikers.
LB4	De opdrachtnemer levert rapportage over het actuele licentiegebruik en de kosten per licentietype volgens servicemanagement.
LB5	Licentiebeheer is onderdeel van de vaste overlegstructuur volgens servicemanagement.
LB6	De opdrachtnemer signaleert proactief onevenwichtigheden in het licentiegebruik, zoals onder- of over-gebruik, en stelt ten minste eenmaal per jaar een concreet voorstel op ter optimalisatie op basis van gebruik, functionaliteit en kostenefficiëntie.
LB7	De opdrachtnemer ondersteunt bij het uitvragen van Microsoft-licentiekortingen of het benutten van bestaande partnerprogramma's en benut waar mogelijk Non-Profit licentiemodellen of andere voordelige regelingen die passen bij het profiel van de aanbestedende dienst.
LB8	De opdrachtnemer volgt actief wijzigingen in het licentiebeleid van Microsoft en informeert aanbestedende dienst tijdig over relevante ontwikkelingen, inclusief alternatieven of migratieadviezen.
LB9	De opdrachtnemer houdt rekening met de verhouding van circa 85% jaarlicenties en 15% maandlicenties.
LB10	De opdrachtnemer houdt bij het overnemen van bestaande contracten rekening met resterende looptijden en voorkomt waar mogelijk dubbele kosten.

Back-up & disaster recovery

BD	Back-up & disaster recovery
BD1	De opdrachtnemer is verantwoordelijk voor het beheer van back-upvoorzieningen binnen de Azure- en Microsoft 365-omgeving.

BD2	De opdrachtnemer is verantwoordelijk voor het dagelijks uitvoeren en beheren van back-ups binnen de volledige Microsoft 365- en Azure-omgeving van de aanbestedende dienst, met als doel volledige herstelbaarheid van kritieke data en diensten in geval van incidenten zoals hacking, ransomware, of grootschalig dataverlies.
BD3	De back-upvoorzieningen dekken ten minste de volgende onderdelen: • Microsoft SharePoint Online • Microsoft Teams (inclusief gedeelde bestanden en gesprekken waar mogelijk) • Microsoft OneDrive for Business • Microsoft Exchange Online (e-mail, agenda, contactpersonen) • Configuratiegegevens binnen Microsoft 365 en Intune • Virtuele machines, SQL-databases en andere bedrijfskritieke componenten binnen Azure
BD4	Back-ups moeten versleuteld worden opgeslagen (bijv. AES-256) zowel tijdens overdracht als in rust.
BD5	Herstelpunten zijn minimaal 180 dagen beschikbaar, tenzij anders overeengekomen.
BD6	De opdrachtnemer controleert actief de uitvoer en integriteit van back-ups en lost storingen hierin zelfstandig op.
BD7	Conform de rapportageafspraken in het kader van Servicemanagement levert de opdrachtnemer maandelijks een overzicht van de dagelijkse back-up slagingspercentages zoals vastgelegd in de SLA.
BD8	De opdrachtnemer stelt een concreet disaster recoveryplan (DR-plan) op voor de omgeving van de aanbestedende dienst.
BD9	De opdrachtnemer voert één keer per maand een recoverytest uit.
BD10	Bij uitval of gegevensverlies is de opdrachtnemer verantwoordelijk voor een volledige en gecontroleerde restore.
BD11	De opdrachtnemer signaleert proactief verbetermogelijkheden in het back-up- en DR-beleid en worden conform afspraken in het kader van Servicemanagement voorgelegd in het strategische overleg.
BD12	Bij wijzigingen in de omgeving (bijv. nieuwe VM's, databases) past de opdrachtnemer het back-upbeleid aan en informeert de aanbestedende dienst.

Intune beheer

IB	Intune beheer
IB1	De opdrachtnemer is verantwoordelijk voor het tijdig en foutloos uitrollen van beveiligingsupdates en patches via Microsoft Intune op alle beheerde Windows-, iOS- en android-apparaten. De termijnen voor het uitrollen van de updates worden in samenspraak bepaald en vervolgens vastgelegd in de SLA.
IB2	De opdrachtnemer voert wekelijks een controle uit op de update-status via Intune en gebruikt hierbij logging en rapportages om de compliancegraad (minimaal 95%) aan te tonen. Conform rapportageafspraken in het kader van Servicemanagement, rapporteert de opdrachtnemer maandelijks aan de aanbestedende dienst over: het aantal uitgerolde updates; eventuele fouten of installatiemislukkingen; afwijkingen van de planning met oorzaak en oplossing
IB3	De opdrachtnemer is verantwoordelijk voor het beheer van de installatie, configuratie en het lifecyclebeheer van software en applicaties op alle door de aanbestedende dienst beheerde werkplekken, met behulp van Microsoft Intune. Dit betreft zowel: standaardapplicaties (zoals Microsoft 365, browsers, antivirus, etc.); organisatie-specifieke software (zoals intern ontwikkelde of ingekochte applicaties), waarbij ook de certificaten up-to-date gehouden worden door de opdrachtnemer.
IB4	De opdrachtnemer zorgt ervoor dat nieuwe of aangepaste applicaties binnen tien (10) werkdagen gebruiksklaar via Intune worden gesteld.
IB5	De opdrachtnemer zorgt ervoor dat updates of versies van bestaande applicaties eerst in een testgroep worden uitgerold, waarna gefaseerde uitrol volgt (tenzij anders afgesproken).

IB6	De opdrachtnemer adviseert over installatie- en configuratie instellingen voordat een nieuwe applicatie wordt ingericht. Na schriftelijke goedkeuring van de aanbestedende dienst wordt dit doorgevoerd.
IB7	De opdrachtnemer levert maandelijks een rapportage aan met daarin: het overzicht van geïnstalleerde en geüpdatete software; eventuele incidenten tijdens distributie; status van uitgevoerde updates per applicatie.
IB8	De opdrachtnemer is verantwoordelijk voor het opstellen, beheren en up-to-date houden van configuratieprofielen en beleidsinstellingen binnen Microsoft Intune, ten behoeve van Windows laptops en mobiele apparaten (iOS/Android) in gebruik bij de aanbestedende dienst. Dit omvat onder meer, maar is niet beperkt tot: compliance policies (bijvoorbeeld versleuteling, antivirus, wachtwoordbeleid); beveiligingsinstellingen (zoals BitLocker, Defender, firewall-instellingen, conditional access); applicatieconfiguraties (standaardinstellingen, toewijzing van apps); device configuration profiles (wifi, VPN, printerinstellingen, etc.).
IB9	De opdrachtnemer stelt minimaal elk kwartaal de beleidsinstellingen en configuraties opnieuw ter review voor, of vaker indien technologische of beleidsmatige ontwikkelingen dit vereisen.
IB10	De opdrachtnemer voert wijzigingen uitsluitend uit na voorafgaande schriftelijke goedkeuring van de aanbestedende dienst.
IB11	De opdrachtnemer documenteert alle significante en hoog-risico wijzigingen conform het wijzigingsbeheerproces van de aanbestedende dienst. De wijze van documentatie, het gebruik van versiebeheer en de gedeelde opslaglocatie worden bij aanvang van de overeenkomst in overleg vastgesteld.
IB12	De opdrachtnemer zorgt dat configuraties en policies voldoen aan de geldende wet- en regelgeving (zoals AVG) én aan het beleid van de aanbestedende dienst.

SQL-database- en VM-beheer

SDVB	SQL-database & VM-beheer
SDVB1	De opdrachtnemer is verantwoordelijk voor het technisch beheer van de SQL-databases en de virtuele machine in Azure. Dit omvat het uitvoeren van noodzakelijke updates, het tijdig toepassen van beveiligingspatches en het beschikbaar houden van back-ups.
SDVB2	De opdrachtnemer draagt zorg voor het correct functioneren van deze meldingen. De aanbestedende dienst ontvangt meldingen automatisch en kan op basis daarvan ondersteuning inroepen. De opdrachtnemer reageert hierop conform de afgesproken responstijden in het SLA.
SDVB3	Binnen 90 dagen na de start van de dienstverlening voert de opdrachtnemer een technische en financiële evaluatie uit van de huidige inrichting van de VM- en databasestructuur. Het schriftelijke adviesrapport bevat concrete aanbevelingen voor optimalisatie van kosten, schaalbaarheid, performance, beveiliging en opschoning.
SDVB4	De opdrachtnemer richt in overleg met de aanbestedende dienst automatische meldingen (alerts) in via beschikbare functionaliteiten in Azure (zoals Azure Monitor of Log Analytics). Deze meldingen dekken ten minste: • SQL-databases: beschikbaarheid, responstijden, deadlocks, opslagcapaciteit, CPU-belasting, IOPS, foutmeldingen, beveiligingsincidenten. • Virtuele machines: uptime, CPU-/geheugen-/schijfgebruik, netwerkprestaties, systeemfouten, patchstatus en back-upstatus.

Exchange beheer

EB	Exchange beheer
EB1	De opdrachtnemer stelt het spamfilter eenmalig goed af binnen 90 dagen na de start van de dienstverlening, op basis van analyse van e-mailverkeer en gebruikerservaring.
EB2	De opdrachtnemer is verantwoordelijk voor het onderhouden van anti-spam, anti-phishing en anti-malwarebeleid op basis van best practices en risicoprofiel van de aanbestedende dienst.

EB3	De opdrachtnemer draagt zorg voor een spamfilterconfiguratie die is gericht op het minimaliseren van false positives (legitieme e-mails die onterecht worden geblokkeerd) én false negatives (ongewenste e-mails die toch binnenkomen), met als doel de werkdruk voor interne ICT te verlagen.
EB4	De opdrachtnemer ondersteunt bij het aanmaken en onderhouden van allow- en blocklists in overleg met de aanbestedende dienst.
EB5	De opdrachtnemer voert elk kwartaal een evaluatie en optimalisatie uit van het spamfilter, waarbij wordt gekeken naar trends, incidenten en gebruikersmeldingen.
EB6	De opdrachtnemer levert hiervan een kort evaluatierapport met bevindingen, doorgevoerde wijzigingen en aanbevelingen.
EB7	Bovenstaande eisen worden binnen de mogelijkheden van Microsoft gerealiseerd.

Security & Compliance Monitoring

SCM	Security & Compliance Monitoring
SCM1	De aanbestedende dienst wenst de digitale veiligheid en wettelijke naleving structureel te monitoren, zonder gebruik te maken van kostbare enterprise-oplossingen zoals Microsoft Sentinel of aanvullende licentieproducten. De opdrachtnemer maakt bij voorkeur gebruik van de beschikbare monitoring- en rapportagemogelijkheden binnen Microsoft 365 E3 of vergelijkbare bestaande licentieconstructies.
SCM2	De opdrachtnemer bewaakt periodiek de Microsoft Secure Score en rapporteert per kwartaal over beveiligingsstatus, afwijkingen en mogelijke kostenefficiënte verbetermaatregelen.
SCM3	De opdrachtnemer stelt in overleg meldingen en waarschuwingen in via bestaande Microsoft-diensten (zoals Azure AD Sign-in logs, Defender for Office 365 en de M365 Security portal), zonder aanvullende licentiekosten.
SCM4	De opdrachtnemer ondersteunt op verzoek bij het inrichten van audit logging en basis-retentiebeleid binnen de mogelijkheden van het Microsoft 365-platform.
SCM5	De opdrachtnemer wijst de aanbestedende dienst proactief op relevante wettelijke of beleidsmatige aandachtspunten (zoals AVG of informatiebeveiliging), maar adviseert alleen over oplossingen die binnen bestaande licentie-inrichting toepasbaar zijn.
SCM6	De opdrachtnemer ondersteunt bij het periodiek controleren en optimaliseren van toegangsbeveiliging binnen Microsoft 365 en Azure AD, waaronder multi-factor authentication (MFA), Conditional Access en blokkade van verouderde protocollen. Hierbij wordt gestreefd naar een evenwicht tussen veiligheid en gebruikersgemak.
SCM7	De opdrachtnemer signaleert en adviseert proactief over risico's of afwijkingen in identiteits- en toegangsbeheer, inclusief afwijkende inlogpatronen, niet-afgedwongen MFA, gebruik van gedeelde accounts of accounts zonder rolgebaseerde rechtenstructuur.

Personeel

P	Personeelseisen
P1	Opdrachtnemer beschikt tijdens de uitvoering van de opdracht over een team met minimaal: 1x Microsoft Azure Administrator (AZ-104 of vergelijkbaar), 1x Microsoft 365 Administrator (MS-102 of vergelijkbaar), 1x Endpoint Administrator (MD-102 of vergelijkbaar), 1x Identity & Access Administrator (SC-300 of vergelijkbaar).
P2	Alle in te zetten medewerkers spreken en schrijven de Nederlandse taal op ten minste taalniveau B2 (CEFR).
P3	Beschikbaarheid: Tijdens de uitvoering is per expertisegebied minimaal één gecertificeerd medewerker beschikbaar tijdens werkdagen tussen 09:00 – 17:00 uur.
P4	Bij afwezigheid van een medewerker dient binnen 24 uur een gelijkwaardig gecertificeerde medewerker beschikbaar te zijn.
P5	De medewerkers worden gedurende de looptijd van de opdracht zoveel mogelijk continu ingezet (vaste teamstructuur).

P6	Indien opdrachtnemer van mening is dat gelijkwaardige certificeringen of rollen van toepassing zijn, dient dit gemotiveerd te worden aangetoond bij inschrijving. De aanbestedende dienst beoordeelt of de gelijkwaardigheid wordt aanvaard.

Privacy en Juridisch

PJ	Privacy en juridisch
PJ1	Indien en zodra aanbestedende dienst als verwerkingsverantwoordelijke vaststelt dat leverancier onder zijn verantwoordelijkheid handelt als verwerker van persoonsgegevens in de zin van de Algemene verordening gegevensbescherming, sluiten partijen een verwerkersovereenkomst conform bijlage 5.B behorende bij het beschrijvend document.
PJ2	Gegevens worden niet in zijn geheel of in delen voor ander doelen ingezet dan volgens de afspraken uit de op te stellen (verwerkers)overeenkomst.
PJ3	Medewerkers die werkzaam zijn voor de opdrachtnemer, moeten persoonsgegevens waarmee zij werken geheimhouden. De personen die werken ten behoeve van de opdrachtnemer hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.
PJ4	De aanbestedende dienst hanteert de geheimhoudingsverklaring uit de GIBIT 2023, opgenomen als bijlage 5.C bij het beschrijvend document.

Facturatie

F	Facturatie
F1	Opdrachtnemer moet digitaal factureren en de factuur aan de opdrachtnemer versturen. Opdrachtnemer richt alle facturen digitaal aan facturenwij@wijeindhoven.nl. Er wordt maandelijks achteraf, na akkoord van de opdrachtgever gefactureerd. De factuur dient gespecificeerd te zijn en tenminste staan daarop de volgende gegevens vermeld: • De betreffende periode; • Uitgevoerde werkzaamheden/licenties; • Eventuele uurtarief; • Kostenplaats; • Grootboekrekening; • Subtotaalbedrag excl. BTW; • BTW identificatienummer, BTW percentage en BTW bedrag; • Totaalbedrag incl. BTW; • Factuurnummer; • Datum factuur; • Inkooporder nummer.