

Aanbestedingsdocument

Europese openbare aanbesteding

Microsoft 365 en Azure Cloud beheerdiensten



Opgesteld door : André van der Zanden en Maïke van Elzaker
Datum : 31 oktober 2024 versie 1.0 publicatie
Projectnummer : P24-0068
TenderNed nr : TN493811
CPV-code : 72000000-5 IT-diensten: adviezen, softwareontwikkeling,
internet en ondersteuning

Over ons

Wij zijn Veiligheidsregio Midden- en West-Brabant (VRMWB). ‘Samen maken we de regio veiliger’ is onze missie. Wij werken hecht samen met hulpverleners, bestuurders, ondernemers en inwoners aan een veilige en veerkrachtige samenleving.

VRMWB is een krachtige en gerespecteerde hulpdienst. Met onze brandweer-, crisisteams en centralisten staan we 24/7 klaar om hulp te bieden bij incidenten, rampen en crises. Dit doen we met ca. 1.800 medewerkers, waarvan ca. 1350 vrijwilligers bij de brandweer, verspreid over 70 kazernes, een oefencentrum Safety Village en de Risk Factory.

Meer informatie over de Veiligheidsregio Midden- en West-Brabant vindt u op onze website www.vrmwb.nl

Wat verwachten wij van u?

1 De opdracht: Microsoft 365 en Microsoft Azure Cloud beheerdiensten

Veiligheidsregio Midden-West-Brabant (hierna te noemen Opdrachtgever of VRMWB) beschikt over een wendbare en schaalbare technische infrastructuur met een Cloud- en Soursingsstrategie gericht op ‘SaaS, tenzij’ en ‘Microsoft, tenzij’. VRMWB is de afgelopen jaren volledig aangesloten op de Cloud beweging, het applicatielandschap is volledig verSaaS en VRMWB is eigenaar van de Microsoft Azure Cloud omgeving.

Door bovenstaande doorontwikkeling van de Cloud IT-omgeving van VRMWB is er behoefte om de huidige IT-dienstverlening te herijken. Omdat de huidige overeenkomst tussen de Veiligheidsregio Midden-West-Brabant en leverancier Dustin per 1 juli 2025 eindigt, is de aanbestedende dienst begonnen met de voorbereidingen voor een nieuwe aanbesteding. Opdrachtgever is voornemens een leverancier te selecteren, waarmee één overeenkomst wordt gesloten voor het leveren van diensten voor het beheer, onderhoud, ondersteuning en ontwikkeling van de in de aanbestedingsdocumenten beschreven Microsoft

365 en Microsoft Azure Cloud omgeving van de Opdrachtgever, uitgevoerd door de Opdrachtnemer of in samenwerking met de Opdrachtgever.

1.1 ICT-sourcingstrategie

Opdrachtgever heeft onlangs een uitgebreide ICT-sourcingstrategie opgesteld, wat een belangrijke mijlpaal is voor de organisatie. De strategie helpt Opdrachtgever om kosten te beheersen door onverwachte uitgaven zoveel mogelijk te vermijden en de kosten te optimaliseren. Bovendien verbetert het de kwaliteit van de ICT-diensten door toegang te bieden tot de beste technologieën en diensten. Dankzij deze strategie kan Opdrachtgever potentiële risico's beter identificeren en beheeren, waardoor de continuïteit van de ICT-diensten gewaarborgd blijft. De strategie maakt het ook mogelijk om snel in te spelen op veranderingen in de markt en de behoeften van de organisatie, wat zorgt voor meer flexibiliteit en schaalbaarheid. Tot slot stelt de ICT-sourcingstrategie Opdrachtgever in staat om zich de komende jaren nog beter te concentreren op haar kernactiviteiten en strategische doelen door ICT-diensten strategisch uit te besteden.

De ICT-Sourcingstrategie van Opdrachtgever is gebaseerd op drie belangrijke aspecten:

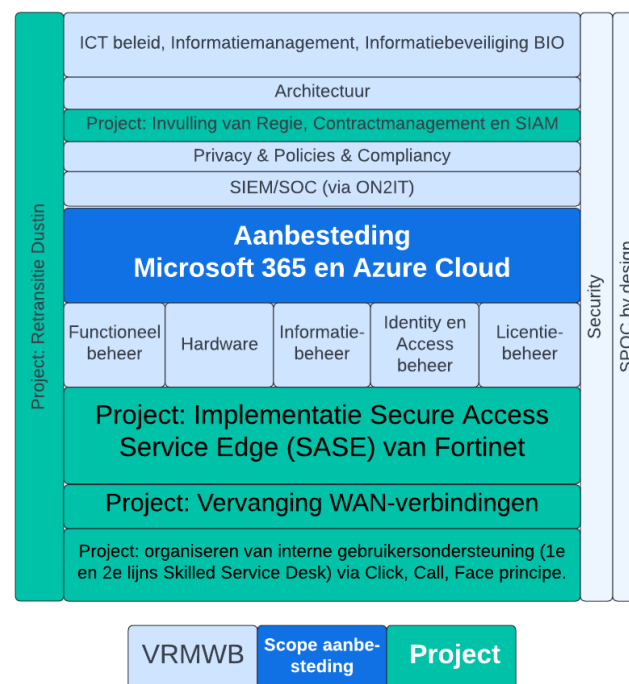
1. Gebruiksvriendelijkheid: Het streven naar een IT-omgeving die gemakkelijk te gebruiken en toegankelijk is voor eindgebruikers.
2. Wendbaarheid en schaalbaarheid: Het vermogen enerzijds de bedrijfscontinuïteit te borgen en anderzijds snel te reageren op veranderingen en de capaciteit om mee te groeien met de behoeften van de organisatie.
3. Informatiebeveiliging: Het waarborgen van de veiligheid en vertrouwelijkheid van gegevens en systemen.

1.2 Doelstelling aanbesteding

De doelstelling van deze aanbesteding, "Microsoft 365 en Microsoft Azure Cloud beheerdiensten", is het sluiten van een overeenkomst met één opdrachtnemer voor het leveren van ICT-diensten voor de bestaande Microsoft 365 en Microsoft Azure Cloud-omgeving van de opdrachtgever. De overeenkomst moet waarborgen dat de opdrachtgever een wendbare en

schaalbare ICT-omgeving behoudt of verbetert, met een hoge gebruikerstevredenheid. Het uitgangspunt is doorontwikkeling, met ondersteuning van de opdrachtnemer, naar een ICT-omgeving die blijft voldoen aan de geldende normen voor informatiebeveiliging en toekomstbestendig is voor de groei naar een vitale infrastructuur.

Opdrachtnemer heeft besloten om bepaalde delen van de ICT-omgeving zelf te gaan beheren, en daarbij als dienstverlener voor de organisatie op te treden. Om ervoor te zorgen dat Opdrachtgever gedurende de overeenkomst goed opdrachtgeverschap kan tonen, terwijl de Opdrachtnemer de afgesproken dienstverlening en de bijbehorende kwaliteit en continuïteit levert, is er een demarcatie opgesteld (zie afbeelding hieronder).



In de demarcatie is aangegeven welke ICT-diensten intern worden georganiseerd, welke worden uitbesteed en op welke ICT-diensten outsourcing (meerdere leveranciers en intern beheer) van toepassing is. Het overzicht legt vast dat security en een single point of contact (SPOC) op alle ICT-diensten van toepassing zijn. Dit betekent dat voor security het informatiebeveiligingsbeleid van Opdrachtgever en de opvolging van de Baseline Informatiebeveiliging Overheid (BIO) leidend zijn.

Deze aanbesteding "Microsoft 365 en Microsoft Azure Cloud beheerdiensten" maakt onderdeel uit van vier andere projecten die momenteel in scope zijn bij Opdrachtgever. De onderstaande drie projecten maken géén onderdeel uit van de scope van deze aanbesteding, maar worden vanwege de samenhang wel genoemd:

1. Implementatie Secure Access Service Edge (SASE) van Fortinet en vervanging van de huidige WAN-verbindingen van Dustin (via NG-BLU) naar WAN-verbindingen via GT vast;
2. Gebruikersondersteuning/ Servicedesk 1e en 2e lijn intern positioneren;
3. Invulling van de regieorganisatie, contractmanagement en service integratie;

Van Opdrachtnemer wordt verwacht dat zij deelneemt aan het vierde project waarbij de overdracht van de latende naar de nieuwe leverancier/ Opdrachtnemer wordt uitgevoerd:

4. Retransitie Dustin

1.3 Projectcapaciteit

Onderdeel van de Overeenkomst is het op afroep en in overleg leveren van projectcapaciteit met de juiste kennis en ervaring. Opdrachtnemer moet hier op afroep voldoende specialisten met ervaring kunnen leveren in de rol/functie van projectleider, engineers/consultants en architecten.

Er zijn 3 type projecten waarvoor Opdrachtnemer op aanvraag van Opdrachtgever, capaciteit, met juiste kennis en voldoende ervaring, zal aanleveren:

1. Projecten met betrekking tot de Microsoft 365 omgeving van Opdrachtgever.
2. Projecten waarbij bestaande Azure omgeving wordt voorzien van patches, updates en upgrades; Denk aan bestaande (SaaS)-applicaties en/of (Cloud) diensten of systemen.
3. Projecten waarbij nieuwe functionaliteiten aan de bestaande Azure omgeving wordt toegevoegd. Denk aan nieuwe (SaaS)-applicaties of (Cloud) diensten en of systemen.

Wanneer projecten zijn afgerond en door Opdrachtnemer in beheer worden genomen dient Opdrachtnemer als volgt te handelen:

1. *Type 1 projecten* die niet binnen de afgesproken dienstverlening als onderdeel van de Overeenkomst vallen. Voor deze projecten wordt door Opdrachtnemer een offerte aangeboden aan Opdrachtgever waarin de kosten voor het uitvoeren van het project zijn opgenomen.
2. *Type 2 projecten* de afgesproken dienstverlening als onderdeel van de Overeenkomst te leveren. Er worden geen meerkosten doorbelast aan Opdrachtgever.
3. *Type 3 projecten* de afgesproken dienstverlening te leveren nadat ze is opgenomen in de Overeenkomst/DAP. Voor deze projecten wordt door Opdrachtnemer een offerte aangeboden aan Opdrachtgever waarin de kosten voor het uitvoeren van het project en de kosten voor de beheerfase zijn opgenomen.

1.4 Informatiebeveiliging

Opdrachtgever streeft naar een veilige en betrouwbare digitale werkomgeving die processen ondersteunt en beschermt. Met de keuze voor het Cloud platform Microsoft Azure en Microsoft 365, wil de Opdrachtgever haar digitale samenwerking en gegevensbeheer optimaliseren. Tegelijkertijd blijft informatiebeveiliging een prioriteit, waarbij de bescherming van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens centraal staat.

Aan Opdrachtgever worden strikte eisen gesteld aan de naleving van de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Deze wet- en regelgeving stelt duidelijke eisen

aan de manier waarop gevoelige informatie wordt beschermd, privacy wordt gewaarborgd en de continuïteit van bedrijfsprocessen wordt gegarandeerd.

In de toekomst zal Opdrachtgever (VRMWB) naar verwachting ook worden aangemerkt als onderdeel van de vitale infrastructuur. Dit betekent dat er extra aandacht komt voor informatiebeveiliging, waarbij de eisen uit de BIO worden aangevuld met richtlijnen die voortvloeien uit de Europese NIS2-richtlijn. Hierdoor zullen aanvullende normenkaders van toepassing zijn op het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie, met bijzondere aandacht voor het voorkomen van verstoringen die een bedreiging vormen voor essentiële diensten en nationale veiligheid.

De ontwikkeling van informatiebeveiliging bij Opdrachtgever wordt geregistreerd vanuit het team informatieveiligheid. Dit team heeft als focus het bewaken van de BIV-criteria (Beschikbaarheid, Integriteit en Vertrouwelijkheid). Dit betekent dat er risico gebaseerd wordt gekeken naar de volledige informatievoorziening, op basis hiervan wordt onder andere de continuïteit van de informatievoorziening gewaarborgd. Naast het analyseren van de omgeving valt hier ook het CSIRT onder, dit is de cyber incident response organisatie bij Opdrachtgever. Het CSIRT wordt continu doorontwikkeld.

Maatregelen rondom beveiliging binnen de Microsoft 365/Microsoft Azure omgeving van de Opdrachtgever zijn risico gebaseerd. Alle informatie verwerkende systemen worden met een business impactanalyse geclassificeerd. Op basis van deze classificatie, het basisbeveiligingsniveau, worden een aantal standaard maatregelen afgedwongen en in bepaalde gevallen worden hier maatwerk maatregelen aan toegevoegd. Risico's worden hiermee gemonitord en zoveel mogelijk gemitigeerd. Van de Opdrachtnemer wordt verwacht dat zij ondersteund bij het implementeren van mitigerende maatregelen.

2. IST-situatie Microsoft 365

Opdrachtgever biedt een moderne digitale werkplek waar medewerkers flexibel kunnen werken, ongeacht tijd en locatie. De moderne digitale werkplek omvat Microsoft 365 apps, toegang tot SaaS-applicaties, beveiligde

netwerkinfrastructuur en Windows omgeving. Medewerkers kunnen voor ondersteuning terecht bij de Skilled Servicedesk. Alle beheerde apparaten, hybride vergaderruimten en digitale platformen vallen onder de digitale werkplek. Opdrachtgever biedt verschillende werkplek-typen en mobiele apparaten aan voor diverse doelgroepen en werkzaamheden. Vergaderruimten zijn uitgerust met Microsoft Teams Rooms voor hybride vergaderingen. Het intranet is ingericht met SharePoint-communicatiesites. Onderstaande is een weergave van de huidige Microsoft 365 functionaliteiten.

2.1 Entra ID

Opdrachtgever gebruikt Entra ID voor het automatiseren van de in-, door- en uitstroom van medewerkers. Voor identiteitsbeheer is HelloID Provisioning gekoppeld aan zowel het HR-systeem ADP als Entra ID. Daarnaast wordt HelloID Provisioning ingezet voor het automatiseren van TOPdesk-taken en het toevoegen van medewerkers aan het toegangscontrolesysteem Paxton.

2.2 Microsoft Teams

Microsoft Teams is uitgebreid uitgerold binnen de organisatie en dient als samenwerkingsplatform voor zowel projectmanagement als afdelingsteams. Gebruikers kunnen via een third-party provisioning applicatie (One for Teams van Ilionx) in Teams geautomatiseerd teams aanvragen. Deze oplossing wordt geleverd door Ilionx en beheerd door Opdrachtgever. Voor hybride vergaderingen worden Microsoft Teams Rooms installaties gebruikt.

2.3 SharePoint en OneDrive

Opdrachtgever gebruikt SharePoint als Document Management Systeem en voegt metadatering toe aan documenten en processen voor records management. Voor het intranet en persoonlijke zakelijke opslag worden zowel SharePoint als OneDrive ingezet. Het SharePoint-intranet wordt aangevuld met diverse third-party webparts voor functionaliteiten die niet standaard beschikbaar zijn in SharePoint. Deze third-party oplossing wordt beheerd door de leverancier Ilionx.

2.4 Intune

De werkplek apparaten van Opdrachtgever, zoals laptops, desktops, iPhones en iPads, worden beheerd met Windows Autopilot en Microsoft Intune,

inclusief applicatie distributie. Naast 650 beheerde werkplekken heeft Opdrachtgever ook BYOD-apparaten. 1350 brandweervrijwilligers beschikken *niet* over een door Opdrachtgever beheerd apparaat, maar gebruiken hun privé telefoon, tablet of PC in combinatie met een Office F3-licentie. Voor de gehele omgeving inclusief alle apparaten en applicaties, zijn compliance- en configuratiebeleid ingesteld. Daaronder vallen ook de standaard werkplek-, kiosk- en gedeelde apparaat profielen.

2.5 Microsoft Defender

Opdrachtgever beschermt identiteiten, apparaten en applicaties met behulp van de functionaliteiten van Microsoft Defender. Deze bescherming wordt verder uitgebreid met Security Information and Event Management (SIEM) en Security Operations Center (SOC) diensten. Door deze gecombineerde aanpak, die zowel Microsoft Defender als SIEM/SOC-functionaliteiten omvat, zorgt Opdrachtgever voor een robuuste beveiligingsstrategie die de integriteit en veiligheid van de ICT-omgeving waarborgt.

2.6 Microsoft Purview

Onlangs is Opdrachtgever begonnen met de implementatie van verschillende onderdelen van Microsoft Purview. Deze onderdelen omvatten onder andere compliance beheer, eDiscovery, informatiebeveiliging, gegevensverliespreventie en cyclusbeheer. Met de inzet van Purview worden geavanceerde tools en technologieën gebruikt om te voldoen aan wettelijke en interne compliance-eisen. Het eDiscovery-proces wordt geoptimaliseerd om efficiënt juridische en regelgevende onderzoeken te ondersteunen. Informatiebeveiliging wordt versterkt door middel van geavanceerde beveiligingsmaatregelen en gegevensverliespreventie, die ervoor zorgen dat gevoelige informatie beschermd blijft tegen ongeautoriseerde toegang en verlies. Daarnaast helpt cyclusbeheer bij het beheren van de levenscyclus van gegevens, van creatie tot archivering en verwijdering, waardoor de integriteit en beschikbaarheid van gegevens gewaarborgd blijven. Deze uitgebreide aanpak met Microsoft Purview stelt Opdrachtgever in staat om een robuust en geïntegreerd beheer van compliance en beveiliging te realiseren.

2.7 Microsoft Exchange

Elke medewerker beschikt over een persoonlijke mailbox, waarmee zij efficiënt kunnen communiceren en hun dagelijkse werkzaamheden kunnen uitvoeren. Naast deze persoonlijke mailboxen heeft Opdrachtgever ook functionele en gedeelde mailboxen ingericht. Deze mailboxen zijn bedoeld voor algemene functies en groepen binnen de organisatie, zoals afdelingen, projectteams en specifieke bedrijfsfuncties. Functionele mailboxen zorgen ervoor dat communicatie naar een bepaalde functie of rol binnen de organisatie gestroomlijnd wordt, terwijl gedeelde mailboxen samenwerking binnen teams en groepen bevorderen. Door het gebruik van zowel persoonlijke als functionele /gedeelde mailboxen, wordt de communicatie binnen de organisatie geoptimaliseerd en kunnen medewerkers effectiever samenwerken en informatie delen.

2.8 Software en licenties

Applicaties voor vakinhoudelijke werkzaamheden van de verschillende afdelingen worden voor 80% geautomatiseerd gedistribueerd via Intune en de Company Portal. Naast diverse SaaS-applicaties beschikt Opdrachtgever over enkele legacy- en organisatie-specifieke applicaties die handmatig worden geïnstalleerd.

- De gebruikte software en systemen omvatten:
- Besturingssysteem: Windows 10 en 11;
- KA-applicaties: Microsoft 365 apps (Office), Microsoft Visio, Projects, Power BI;
- Bedrijfsspecifieke SaaS-applicaties: AFAS, ADP en TOPdesk;
- Beveiligingssoftware: Defender en FortiClient.

Microsoft-licenties worden via een raamovereenkomst met Bechtle ingekocht. Opdrachtgever maakt gebruik van vijf verschillende licentietypen:

- Office F3: Voor vrijwilligers/manschappen (1350 licenties);
- Microsoft E5: Voor kantoormedewerkers (620 licenties);
- Enterprise Mobility + Security E3: Voor mobiele apparaten (210 licenties);
- Exchange Online Plan 1 (8 licenties);

- Microsoft Teams Rooms Pro: Voor hybride vergaderen (19 licenties).

Deze aanpak zorgt ervoor dat de benodigde software bij Opdrachtgever efficiënt en effectief wordt gedistribueerd en beheerd, terwijl de verschillende licentietypen aansluiten bij de specifieke behoeften van de diverse gebruikersgroepen binnen de organisatie.

2.9 Back-up Microsoft 365

Voor de back-up van Microsoft 365 data (Exchange, OneDrive, SharePoint en Teams) maakt Opdrachtgever gebruik van een Cloud back-up dienst Cove Microsoft 365 Back-up van N-Able.

De huidige back-up parameters zijn als volgt, naast de standaard mogelijkheden van Microsoft 365 voor het terughalen van verwijderde of kwijtgeraakte gegevens:

- Back-up van Exchange Online en Teams: 6 keer per dag;
- Back-up van SharePoint en OneDrive: 4 keer per dag;
- Retentie M365: 7 jaar.

Deze back-up parameters zorgen ervoor dat gegevens regelmatig worden geback-up't en gedurende de vastgestelde retentieperioden beschikbaar blijven voor herstel, wat bijdraagt aan de continuïteit en veiligheid.

2.10 Hardware

Opdrachtgever is eigenaar van alle apparaten en heeft alle apparaten in eigen beheer. De hardware wordt aangeschaft via een raamovereenkomst met leverancier Dustin (via het NIPV). De distributie, reparatie en vervanging van apparaten wordt intern afgehandeld.

Opdrachtgever maakt gebruik van de volgende typen apparaten.

- 140x Dell desktop;
- 660x Dell laptop;
- 1x Dell docking station per werkplek;
- 5x Microsoft Laptop;
- 70x Microsoft Surface Pro;
- 500x iPhone;
- 420x iPad 420;

- 19x Logitech Teams Rooms systemen (Android).

Naast deze apparaten zijn ook meerdere organisatie specifieke apparaten die door derde partijen worden beheerd denk hierbij aan test-pc (Windows) voor brandweer apparatuur.

Voor de verschillende apparaten en hun functie zijn Intune configuratie profielen in gebruik:

- Standaard werkplek;
- Kiosk;
- Shared device.

2.11 SIEM/SOC

De opdrachtgever heeft momenteel een contract met ON2IT voor SIEM/SOC-dienstverlening. ON2IT monitort 24/7 de firewalls en endpoints van de opdrachtgever. Met een "break glass"-account kan ON2IT, na goedkeuring van de opdrachtgever, ingrijpen bij beveiligingsdreigingen. Het SIEM-systeem verzamelt en analyseert beveiligingsgegevens uit diverse bronnen om potentiële bedreigingen te identificeren en te mitigeren. Het SOC-team monitort continu de beveiligingsstatus van de organisatie, reageert op incidenten en voert proactieve maatregelen uit om de beveiliging te verbeteren.

2.12 Skilled servicedesk

De huidige leverancier verzorgt uitgebreide ondersteuning op alle onderdelen van Microsoft 365 en werkplekbeheer, zowel remote als on-site. Dit omvat de volgende beheertaken:

- Eerste lijn Servicedesk medewerker: Deze medewerker is het eerste aanspreekpunt voor gebruikers die technische ondersteuning nodig hebben. De medewerker lost eenvoudige problemen op en escaleert complexere problemen naar de 2^{de} lijn.
- Tweede lijn Functioneel Beheer Microsoft 365/ Modern Workplace Engineer: Deze specialisten zijn verantwoordelijk voor het oplossen van complexe technische problemen, het functioneel beheer, het

beheer van gebruikersaccounts en het optimaliseren van de werkplekervaring voor de gebruikers.

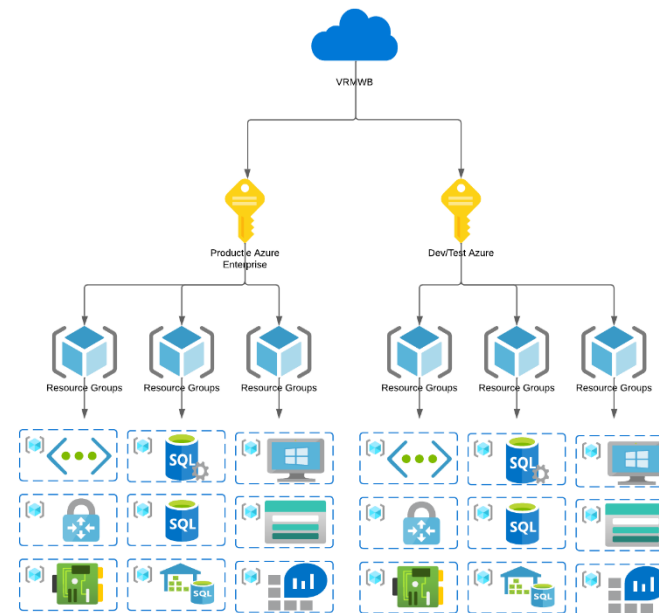
- Software updates: De huidige leverancier zorgt ervoor dat alle software up-to-date blijft door regelmatig patches en updates uit te voeren. Hiermee worden de beveiligingsrisico's geminimaliseerd en worden de prestaties van de werkplek en systemen verbeterd.
- Onderhoud en beheer van applicaties (via Intune gemanaged): Met behulp van Intune worden applicaties en mobiele apparaten beheerd. De huidige leverancier is verantwoordelijk voor de installatie, configuratie, doorontwikkeling en het onderhoud. Hiermee waarborgt ze het optimaal functioneren.

3 IST-situatie Microsoft Azure Cloud Infrastructuur

De huidige Microsoft Azure infrastructuur bestaat uit één tenant met daarin twee subscriptions:

1. Dev/Test Azure;
2. Productie Azure Enterprise.

Binnen deze subscriptions zijn in totaal 151 resourcegroepen actief, die kunnen worden beschouwd als workloads. Er zijn geen managementgroepen actief binnen de tenant.



Om de Microsoft Azure-omgeving van de Opdrachtgever goed te kunnen beheren, onderhouden, troubleshooten en door te ontwikkelen, heeft de Opdrachtnemer specialistische expertise en ervaring nodig.

Hieronder volgt een overzicht van de huidige opbouw van de Microsoft Azure-omgeving:

- 79x App Services;
- 99x Application Insights;
- 1x ExpressRoute;
- 2x Azure Databases for PostgreSQL Flexible Server;
- 3x Azure Databases for PostgreSQL Single Server;
- 1x DevOps organisatie;
- 24x Function Apps;
- 29x Key Vaults;

- 20x Log Analytics Workspaces;
- 65x SQL Databases;
- 10x SQL Servers;
- 102x storage accounts;
- 15x virtual machines;
- 1x Backup vault;
- 1x Data factory;
- 1x Entra Domain Services.

3.1 Virtuele netwerken

Opdrachtgever beschikt over een ExpressRoute-verbinding met het Microsoft Azure datacenter. Daarnaast zijn er momenteel vijf virtuele netwerken geconfigureerd en verspreid over de subscriptions:

1. VN-API;
2. VN-VRMWB;
3. VN-VRMWB-ER;
4. RSD-ITM-POC;
5. AZ-GEOVPN.

3.2 Data factory

De Azure Data Factory (ADF) omgeving is een beheerd cloudserviceplatform dat data-integratie mogelijk maakt via onder andere pipelines en dataflows. Momenteel worden er meer dan 30 linked services gebruikt die verwijzen naar een API-endpoint, blob storage of een Azure SQL-database. De pipelines worden automatisch getriggerd en zijn bedoeld om data te extraheren, te laden, op te schonen of te transformeren richting het Data Warehouse van Opdrachtgever. Alle rapportages zijn gebaseerd op data uit dit Data Warehouse. In ADF wordt de uitvoering van de pipelines gemonitord en de prestaties geanalyseerd. Daarnaast beheert Opdrachtgever in ADF de rollen en permissies.

3.3 Interne softwareontwikkeling

Opdrachtgever beschikt over een intern ontwikkelteam dat verantwoordelijk is voor het koppelen van verschillende applicaties, het ontwikkelen van eigen software en het leveren van data aan het Azure Data warehouse. De

ontwikkelaars zijn full stack, en houden zich momenteel ook bezig met het opzetten van omgevingen in Microsoft Azure, waarbij ze onder andere gebruik maken van Bicep.

3.4 Crisiswebsite VRMWB

Een cruciaal platform voor Opdrachtgever is de crisiswebsite <https://www.vrmwb.nl>. Deze website draait op Microsoft Azure en wordt via Cloudflare CDN ontsloten aan de buitenwereld, zodat incidentele grote aantallen bezoekers kunnen worden opgevangen en cyberaanvallen kunnen worden afgeslagen.

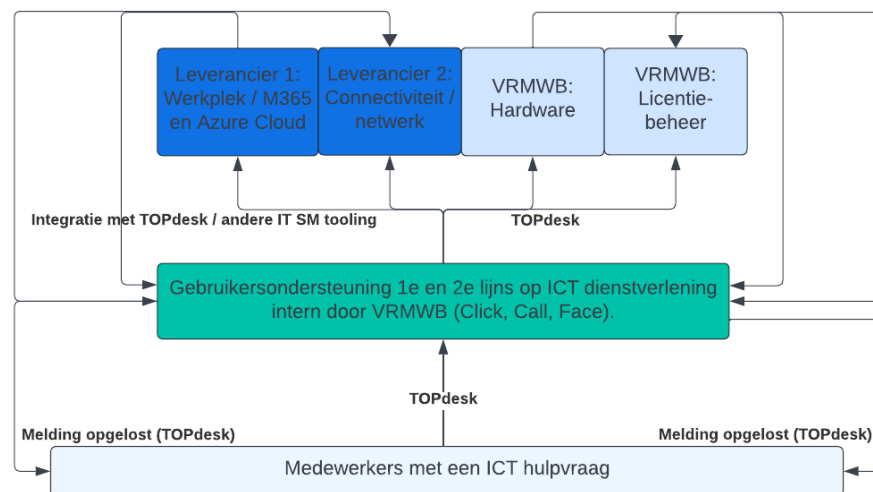
4 Soll Situatie Microsoft 365

4.1 Gebruikersondersteuning en servicelevels Microsoft 365

De Opdrachtgever heeft de gebruikersondersteuning voor Microsoft 365 intern georganiseerd. Alle medewerkers van Opdrachtgever melden hun ICT-gerelateerde incidenten met behulp van TOPdesk via het Click-Call-Face principe, waarna de interne 1^e lijn servicedesk (bekwame servicedeskmedewerkers) start met de afhandeling van de melding. Indien nodig wordt de melding intern 2^e lijn (Modern Workplace-engineers en Functioneel Beheer M365) doorgezet. Bij complexe vraagstukken worden ook de Solution Architect Microsoft 365 en/of de Solution Architect Microsoft Azure van Opdrachtgever betrokken. De verantwoordelijkheid voor het beheer en onderhoud van Microsoft 365 ligt bij de Opdrachtgever en wordt in de dagelijkse praktijk door de Opdrachtgever zelf uitgevoerd.

Indien bovengenoemde interne gebruikersondersteuning, zélf ondersteuning nodig heeft voor technisch complexe vraagstukken, wil de interne gebruikersondersteuning, bestaande uit 7 functionarissen, bij voorkeur via de eigen TOPdesk omgeving van Opdrachtgever contact op kunnen nemen met Opdrachtnemer voor geavanceerde IT-ondersteuning voor technische complexe vraagstukken met betrekking tot Microsoft 365 omgeving van Opdrachtgever. Dit vereist van Opdrachtnemer dat ze beschikt over voldoende specialistische functionele en technische kennis/expertise en ervaring om (complexe) 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.



In onderstaande tabel staan de oplostijden voor de incidenten, vanaf het moment dat deze gemeld zijn bij Opdrachtnemer:

Type incident	Oplostijd	Norm
Prio 1 (P1) – Hoog Hoge urgentie, Hoge Impact	4 uur	Per maand wordt 95% van het aantal incidenten binnen de oplostijd opgelost.
Prio 2 (P2) – Midden Medium urgentie, Medium impact	12 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.

Het is van groot belang dat de ICT-omgeving van Opdrachtgever up-to-date blijven met de laatste ontwikkelingen, en dat de omgeving zo ingericht is dat functionele vragen vanuit de organisatie snel en goed kunnen worden gerealiseerd, indien noodzakelijk op locatie. Opdrachtgever wil Microsoft 365 omgeving continu kunnen verbeteren. Deze verbeteringen zijn cruciaal voor de organisatie van de Opdrachtgever, omdat ze bijdragen aan een veilige, efficiëntere en effectievere werkomgeving voor de medewerkers. Opdrachtnemer zal als onderdeel van de Overeenkomst tenminste 2x per jaar health checks uitvoeren waarmee de kwaliteit van de Microsoft 365 omgeving wordt gewaarborgd. Acties en aanbevelingen die hieruit voortkomen, worden in principe door Opdrachtgever zelf of in samenwerking met Opdrachtnemer in een project opgepakt.

4.2 Projecten Microsoft 365

De projecten die de komende jaren op Microsoft 365 geïnitieerd kunnen worden hebben als gezamenlijk doel de optimalisatie van de inrichting. Voor deze beoogde projecten vraagt Opdrachtgever technische expertise en capaciteit van de Opdrachtnemer. Daarnaast is het van belang dat gedurende de looptijd van de Overeenkomst de Opdrachtnemer op verzoek van Opdrachtgever voldoende capaciteit, met de juiste kennis en voldoende ervaring, beschikbaar stelt voor projecten die momenteel nog niet in scope zijn:

- De evaluatie en optimalisatie van de inrichting van de Intune werkplek**
Het evalueren en verbeteren van de huidige werkplek inrichting door het toepassen van Microsoft standaarden en best practices, gericht op Intune inrichting;
- De evaluatie en optimalisatie van de inrichting van Defender**
Het evalueren en verbeteren van de huidige security inrichting door het toepassen van Microsoft standaarden en best practices, gericht op Microsoft Defender;
- Het optimaliseren van de Entra ID inrichting**
Het evalueren van de huidige inrichting en een voorstel doen voor verbeteringen door het toepassen van Microsoft standaarden en best practices;

4 **Het leveren van SIEM/SOC dienstverlening op de Microsoft Infrastructuur (Azure & M365).**

De Opdrachtgever heeft hierbij een groeipad voor ogen, waarbij SIEM/SOC dienstverlening op de Microsoft omgeving ná oplevering project WAF/CAF als eerste onderdeel opgepakt wordt;

5 **Het (her)inrichten van Compliance**

Het adviseren over generieke inrichting van compliance op o.a. Purview, Data Loss Prevention en Compliance Manager;

6 **Het opzetten van Device Lifecycle Management**

Het adviseren over vervangingsinvesteringen van hardware vanuit device lifecycle management;

7 **Het Power Platform**

Opdrachtgever onderzoekt de mogelijkheden van het Power Platform. Hierbij kan gedacht worden aan:

- a. De inrichting van OTAP-straat op het Power Platform;
- b. De ontwikkeling van Power Apps en Power Automate om apps te ontwikkelen en veel voorkomende taken te automatiseren;
- c. De integratie van AI in Microsoft 365.

8 **De migratie naar Microsoft Fabric;**

9 **De doorontwikkeling van Microsoft 365.**

Opdrachtgever heeft haar gebruikersondersteuning voor Microsoft 365 intern georganiseerd met Skilled servicedesk medewerkers (1^{ste} lijn) én modern workplace engineers (2^{de} lijn). 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.

Van een Opdrachtnemer wordt 3^e lijns technische support en expertise verwacht. Deze support richt zich op het beantwoorden van technische vragen op alle onderdelen van Microsoft 365 zoals Exchange, OneDrive, SharePoint, Microsoft 365 apps, Intune, Entra ID en Windows 11.

Om Microsoft 365 continue te verbeteren wil Opdrachtgever door de Opdrachtnemer tenminste tweemaal per jaar health check(s) laten uitvoeren om zo de kwaliteit van de werkplek en inrichting daarvan te waarborgen. Eventuele acties die hieruit komen worden door Opdrachtgever zelf uitgevoerd of samen met de Opdrachtnemer in een project opgepakt.

4.3 Soll Situatie Beheer Microsoft Azure infrastructuur

Opdrachtgever heeft als doel om de bestaande Microsoft Azure infrastructuur as-is in beheer te laten nemen door de nieuwe Opdrachtnemer. De nieuwe Opdrachtnemer is verantwoordelijk voor het beheer en onderhoud van de Microsoft Azure Cloud omgeving op het gebied van Resourcesbeheer, Netwerkbeheer, Identiteit en toegangsbeheer, Beveiliging en Compliance, Monitoring en Rapportage, Incidentbeheer, Updates en onderhoud, DevOps en Automatisering en Documentatie.

Na de transitie van de nieuwe Opdrachtnemer wordt meteen (vanaf 01-07-2025) een project gestart waarbij de Opdrachtnemer samen met Opdrachtgever een “Redesign” op gebied van Microsoft Azure uitvoert volgens de methode “Well-Architected Framework (WAF)” en “Cloud Adoption Framework (CAF)” met als uitgangspunt “Infra as Code”. De scope betreft het inrichten van de foundation en migratie van bestaande resourcegroepen naar workloads vóór eind december 2025.

Hiermee wil Opdrachtgever kunnen voldoen aan de huidige en toekomstige behoeften van de organisatie, klanten en technologische ontwikkelingen. Opdrachtgever streeft naar een efficiënte, flexibele en veilige infrastructuur, zodat nieuwe technologieën en diensten geïmplementeerd kunnen worden.

De gewenste situatie heeft de volgende kenmerken:

- Cloud-first strategie met het uitgangspunt Microsoft tenzij;
- Infrastructuur op basis van Infrastructure as Code (IaC) met Azure DevOps;
- Infrastructuur volgens Well-Architected Framework (WAF) en Cloud Adoption Framework (CAF).

Het technisch beheer van de geoptimaliseerde Azure Cloud omgeving wordt door de Opdrachtnemer uitgevoerd. Dit gaat dan om policies, foundation, managementgroepen, subscriptions, connectiviteit, kosten. Daarnaast vraagt Opdrachtgever een dienst voor het klaarzetten van een nieuwe workloads (Subscription, Managementgroep, DevOps project en eventuele standaard resources).

Zoals eerder genoemd ziet Opdrachtgever verschillende varianten van landing zones voor zich. Belangrijk om te noemen is dat op alle varianten er inzet wordt verwacht van de leverancier.

4.3.1 Managed landing zone

De managed spoke is, waar mogelijk, volledig uitgerold via Infra as Code en onder beheer bij de Opdrachtnemer. Deze spoke maakt het mogelijk om connectie te maken met andere resources middels VNET peering met de HUB. Binnen deze spoke zijn een aantal onderdelen standaard aanwezig zoals;

- Azure Key Vault
- Azure Recovery Vault
- Virtual Network

4.3.2 Light managed landing zone

De light managed landing zone is bedoeld voor 3^e partijen die een dienstverlening levert via de Opdrachtgever-tenant. Denk hierbij aan toegangscontrole systeem waarvoor Azure resources nodig zijn. Van de Opdrachtnemer wordt verwacht de landing zone weg te zetten via Infra as Code met gelijke dienstverlening als de managed landing zone. Waar nodig worden ook standaard resources klaargezet zoals een Virtuele Machine. De 3^e partij doet zelf de verder inrichting, al dan niet via infra as code, van de resource en onderhoudt deze. Via VNET peering wordt het mogelijk gemaakt om via de foundation andere resources te benaderen. De light managed landing zone bevat minimaal het volgende:

- Azure Key Vault
- Azure Recovery Vault
- Virtual Network

Daarnaast wordt de dienst geleverd door partner door toe te zien op security & compliance, controle van Azure Monitor, Back-up enz.

4.3.3. Internet only Landing zone

De Internet only landing zone maakt het mogelijk om gebruik te maken van Azure resources binnen kaders van Opdrachtgever. Binnen deze type landing zone is het niet mogelijk om connectie te maken met resources in andere subscriptions. Daarnaast wordt de dienst geleverd door partner door toe te zien op security & compliance, controle van Azure Monitor, Back-up.

4.4 Lokale Connectiviteit

Lokale connectiviteit (LAN, WLAN, WAN) maakt geen onderdeel uit van de scope van deze aanbesteding. Uiteraard is het voor Opdrachtgever noodzakelijk dat deze partners met elkaar samenwerken om Azure beschikbaar te maken in de lokale netwerkinfrastructuur. Dit kan zijn op het gebied van een ExpressRoute, VPN-verbinding maar ook het vormgeven van de IP-Plannen. Het nieuwe netwerkdesign wordt 1^e kwartaal 2025 geïmplementeerd. Het design is gebaseerd op Fortinet en ziet er globaal als volgt uit:

Underlay: Dit is het fysieke deel van het netwerk op alle locaties. Denk hierbij aan firewalls, switches, WiFi, etc. De underlay voorziet in connectiviteit voor gebouw gebonden apparatuur zaken zoals IOT, camera's, gebouwbeheerssystemen, etc.

Overlay: Dit deel van het ontwerp voorziet in logische connectiviteit voor o.a. laptops. De overlay zorgt ervoor dat de laptops zich overal kunnen bevinden, waarbij veiligheid, inzicht en controle ten alle tijden gewaarborgd blijft. Hierbij kan worden gedacht aan een "agent-based" oplossing en valt onder het SASE/SSE architectuurmodel. Deze oplossing wordt gekoppeld aan de Azure Firewall voor ontsluiting van applicaties.

Soc as a Service

Opdrachtgever implementeert een modern op Fortinet gebaseerd SASE-netwerk, dat op 01-07-2025 beschikbaar is. Het netwerk wordt 24/7 gemanaged door Fortinet en bestaat uit functionaliteiten en diensten voor:

- Endpoint Protection;

- Endpoint Detection and Response;
- Application Protection;
- Secure Access en Managed Firewalls;
- Managed FortiClient ZTNA and EPP;
- Managed FortiGate Service;
- SOC-as-a-Service for FortiGate.

Opdrachtgever maakt tot 01-07-2026 gebruik van bestaande SIEM/SOC dienstverlening van ON2IT op onderdelen Microsoft Defender for O365 & Entra Protection.

Omvang van de opdracht

De opdracht bestaat uit de volgende onderdelen:

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

Procedure

Voor de aanbesteding van deze opdracht hanteren wij de Europese openbare aanbestedingsprocedure. Deze aanbesteding verloopt volledig via TenderNed. Dit houdt in dat de Aanbestedingsstukken door de VRMWB worden geplaatst op TenderNed en alle informatie tussen de VRMWB en de Inschrijvers wordt uitgewisseld via TenderNed.

Voor het gebruik van TenderNed verwijzen wij naar de gebruikershandleiding voor ondernemers en de gebruiksvoorwaarden van TenderNed.

Percelen of clustering

De Aanbesteding is niet onderverdeeld in meerdere percelen, omdat er sprake is van een technisch-functionele eenheid van de totale opdracht. Het is daarom

niet gewenst dat de opdracht door verschillende leveranciers geleverd c.q. uitgevoerd wordt. Er is evenmin sprake van een samenvoeging van meerdere opdrachten.

De overeenkomst

De Overeenkomst gaat in op 1 juli 2025 en heeft een initiële looptijd van vier (4) jaar. De initiële looptijd van deze Overeenkomst eindigt op 30 juni 2029.

Na afloop van de initiële looptijd wordt de Overeenkomst automatisch verlengd met twee (2) keer twee (2) jaar, tenzij de Opdrachtgever de overeenkomst schriftelijk opzegt met een opzegtermijn van drie (3) maanden voor het einde van de lopende termijn.



De Opdrachtnemer zal voorafgaande aan de ingangsdatum van de Overeenkomst voorbereidende werkzaamheden uitvoeren voor het goed doorlopen van de transitieperiode.

Mogelijkheden om in te schrijven

U kunt uitsluitend inschrijven op de hele opdracht. Als u alleen (als één bedrijf) inschrijft en uw bedrijf aan de eisen voldoet, dan kunt u zelfstandig inschrijven. Als zelfstandig Inschrijver voegt u hiervoor bij Inschrijving (onder meer) het UEA, volledig, juist, onvoorwaardelijk en zonder enig voorbehoud ingevuld en rechtsgeldig ondertekend toe.

Als dit niet het is geval, dan kunt u overwegen om als 'combinatie' in te schrijven of gebruik te maken van (een) derde(n) om gezamenlijk de opdracht uit te voeren.

In 'combinatie' is er altijd één vast contact als Inschrijver/opdrachtnemer. De Inschrijver (hoofdaannemer) is en blijft hoofdelijk aansprakelijk voor het nakomen van de Overeenkomst als de aanbidding wordt geaccepteerd. Als

samenwerkingsverband voegt u bij Inschrijving van iedere afzonderlijke deelnemende onderneming het UEA, volledig, juist, onvoorwaardelijk en zonder enig voorbehoud in te vullen en rechtsgeldig ondertekend toe.

Het is toegestaan om voor de uitvoering van de opdracht een of meerdere onderaannemers in te schakelen. Deze onderaannemers vermeldt u in het UEA bij Deel II Onderaannemers. Deze genoemde onderaannemers worden ook daadwerkelijk te ingezet bij de uitvoering van de opdracht. Bij een wijziging moet u toestemming krijgen van de VRMWB. De Inschrijver is en blijft de hoofdaannemer en aanspreekpunt voor de VRMWB tijdens de aanbestedingsprocedure en de uitvoering van de opdracht.

U krijgt voor uw Inschrijving geen vergoeding en uw Inschrijving moet minimaal 60 dagen geldig zijn.

Waar moet u aan voldoen?

Als overheid kunnen we niet zomaar met elke leverancier in zee gaan. Er zijn een aantal uitsluitingsgronden vastgesteld. Deze uitsluitingsgronden zijn benoemd in het Uniform Europees Aanbestedingsdocument (UEA). Dit document is bij de aanbesteding toegevoegd op TenderNed. Het UEA moet ingevuld en ondertekend worden en voegt u toe bij uw Inschrijving. Als er een uitsluitingsgrond op u van toepassing is, dan mogen wij uw Inschrijving niet beoordelen.

De volgende geschiktheidseisen zijn van toepassing op de opdracht.

Beroepsbekwaamheid - Inschrijving in Handelsregister

U staat ingeschreven in een handelsregister (in Nederland bij de Kamer van Koophandel).

Financiële en economische draagkracht – Verzekering

U heeft een adequate verzekering tegen bedrijfsaansprakelijkheid. In de inkoopvoorwaarden GIBIT 2023 - Artikel 16 is deze aansprakelijkheid geregeld. De aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade, is beperkt tot een bedrag van € 1.250.000,- per gebeurtenis.

Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis. De aansprakelijkheid voor overige schade is beperkt tot twee maal de Jaarvergoeding per gebeurtenis. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan vier maal de Jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

Beschikt u op het moment van Inschrijving niet over een verzekeringscertificaat? Dan mag u ook een door uw verzekeringsmaatschappij afgelegde verklaring aanleveren. In deze verklaring moet deze maatschappij verklaren dat zij met u een verzekering tegen bedrijfsaansprakelijkheid zal afsluiten (volgens de genoemde dekking) als de opdracht aan u gegund wordt. Deze verzekering moet u wel van af de ingangsdatum van de Overeenkomst afsluiten. U voldoet gedurende de gehele contractperiode aan deze verzekeringseis.

Technische- en beroepsbekwaamheid (kerncompetentie)

Het is voor ons belangrijk dat u ervaring heeft met het leveren van het door ons gevraagde product of dienst. U toont dit aan door op het referentieformulier (formulier 2) één referentie (kerncompetentie) op te geven waarbij u in periode van 3 jaar een soortgelijke opdracht heeft uitgevoerd.

Kerncompetentie 1:

U heeft aantoonbare ervaring met het implementeren van het Well-Architected Framework (WAF) en Cloud Adoption Framework (CAF). Deze ervaring moet blijken uit een eerder project waarin u verantwoordelijk was voor de migratie, optimalisatie en beheer van cloudomgevingen en best practices van M365 en Azure hebt toegepast.

Kwaliteitsmanagementsysteem

U beschikt over een kwaliteitsmanagementsysteem ISO 27001-certificering of een door de Opdrachtnemer aantoonbare gelijkwaardige norm voor informatiebeveiliging. De Opdrachtgever verstaat onder een gelijkwaardige norm voor informatiebeveiliging: NEN 7510, SOC 2, ISO 27701, C5 (Cloud Computing Compliance Controls Catalogue), Cyber Essentials (Plus) of het NIST Cybersecurity Framework.

Certificering Microsoft Solutions Partner Modern Work

U beschikt over het Microsoft Solutions Partner Modern Work certificaat. Dit certificaat moet geldig zijn op het moment van inschrijving en gedurende de gehele looptijd van de opdracht.

Certificering Microsoft Solutions Partner Infrastructure Azure

U beschikt over het Microsoft Solutions Partner Infrastructure Azure certificaat. Dit certificaat moet geldig zijn op het moment van inschrijving en gedurende de gehele looptijd van de opdracht.

U toont bovenstaande geschiktheidseisen aan door op formulier 3 Kwaliteitsmanagementsysteem en certificaten in te vullen.

De Inschrijver die als winnaar uit de aanbestedingsprocedure komt, dient binnen 14 dagen na voorlopige gunning de benodigde bewijsmiddelen aan te leveren. De VRMWB behoudt zich het recht voor om aanvullende bewijsmiddelen te vragen.

Akkoordverklaring met de documenten (minimumeisen)

Wij kunnen alleen zakendoen met u als u akkoord gaat met onze minimumeisen. Als Inschrijver gaat u akkoord met onderstaande documenten:

- Programma van eisen/ minimumeisen (formulier 1)
- Inkoopvoorwaarden GIBIT 2023
- Conceptovereenkomst (toegevoegd aan dit aanbestedingsdocument)
- Verwerkersovereenkomst (toegevoegd aan dit aanbestedingsdocument)

Wij beoordelen op prijs en kwaliteit

Wij gunnen de opdracht aan de Inschrijver die de Economisch Meest Voordelige Inschrijving op basis van beste prijs-kwaliteitverhouding (BPKV) heeft gedaan.

Prijs: Door het invullen van uw prijsopgave(n) in formulier 4 ontstaat er een totaalprijs (de inschrijfsom) waarvoor u het geheel levert en uitvoert. Naast de

aangeboden prijs mogen er geen aanvullende kosten worden gefactureerd. De prijs is dus inclusief reis en leveringskosten. U vult de tarieven in **excl. BTW**.

Voor deze aanbesteding gelden de volgende plafondbedragen (excl. BTW):

Beheerdiensten	
M365 technical support en Azure Cloud beheer	€ 350.000,- per jaar
Projectcapaciteit	
Inhuur Projectleider	€ 135,- per uur
Inhuur Architect	€ 135,- per uur
Inhuur Engineer/consultant	€ 100,- per uur
Implementatiekosten (eenmalige kosten)	
Implementatiekosten Microsoft 365, Azure Cloud en implementatie WAF/CAF	€ 80.000,- totaal

Als u hoger inschrijft dan de genoemde plafondbedragen, dan is dit een ongeldige inschrijving.

Kwaliteit: De eisen aan kwaliteit zijn benoemd in formulier 1. Daarnaast wordt uw Inschrijving beoordeeld aan de hand van onderstaande gunningscriteria.

Gunningscriteria	Maximaal aantal pagina's*	Fictieve korting
1 Implementatie WAF/CAF	4 pagina's	€ 500.000,-
2 "As is" situatie beheren	4 pagina's	€ 300.000,-
3 Borging kennis voor beheer	4 pagina's	€ 300.000,-
4 TopDesk koppeling	n.v.t.	€ 100.000,-

*Alle pagina's boven het aangegeven maximum nemen wij niet mee in de beoordeling.

Gunningscriterium 1 Implementatie WAF/CAF

Van de Opdrachtgever wordt verwacht dat zij aantoonbare ervaring heeft met de implementatie van het Well-Architected Framework (WAF) en Cloud

Adoption Framework (CAF). Dit gunningscriterium is bedoeld om de expertise en het succes van de inschrijver in vergelijkbare projecten te beoordelen.

Beschrijf hoe u uw ervaring met de implementatie van het Well-Architected Framework (WAF) en/of Cloud Adoption Framework (CAF) in deze opdracht gaat toepassen. Onderbouw uw antwoord met concrete voorbeelden van eerdere projecten, inclusief de resultaten en de impact op onze organisatie.

Beoordelingscriteria:

- a. Implementatiestrategie: Beschrijf uw aanpak, doorlooptijd, benodigde capaciteit en planning voor de implementatie van WAF/CAF.
- b. Hoe wordt de Infrastructure as Code onderhouden bij het beheer van een Azure omgeving die via WAF/CAF is ingericht?

Gunningscriterium 2 “As is” situatie beheren

Van de Opdrachtnemer wordt verwacht dat zij de Microsoft Azure omgeving van de Opdrachtgever in de situatie van “As Is” (situatie van overdracht) in beheer neemt.

Omschrijf in een Plan van Aanpak op welke manier u zich gaat voorbereiden op de overname van het beheer in de huidige situatie.

Beoordelingscriteria:

Voorbereiding op de overname van het Beheer van de As Is situatie:

- a. Maak een risicoanalyse en beschrijf de mitigerende maatregelen voor de overname van het beheer.
- b. Maak een conceptplanning voor de verschillende fases: voorbereiden van transitie, in beheer name van de 'As Is' omgeving en uitvoering van de optimalisatieprojecten.

Gunningscriterium 3 Borging kennis voor het beheer

Opdrachtgever hecht veel waarde aan continuïteit en efficiëntie in het beheer van de Azure omgeving. Om dit te waarborgen, is het essentieel dat er een vast team beschikbaar is dat verantwoordelijk is voor het beheer. Dit team moet goed op elkaar ingespeeld zijn en beschikken over de benodigde kennis en ervaring om de Azure omgeving effectief te beheren.

Beoordelingscriteria:

Kennisoverdracht, documentatie en training

- a. Hoe zorgt u ervoor dat alle relevante informatie en documentatie up-to-date en toegankelijk is voor alle teamleden?
- b. Hoe zorgt u ervoor dat de teamleden continu worden bijgeschoold en op de hoogte blijven van de laatste ontwikkelingen m.b.t de te beheren omgeving?

Beschrijf op welke manier u ervoor gaat zorgen dat er een vast team beschikbaar is voor het beheer van de Azure omgeving van de Opdrachtgever. Onderbouw uw antwoord met concrete maatregelen die aantonen hoe u de continuïteit, efficiëntie en effectiviteit van het beheer waarborgt, en hoe u voorkomt dat er tijd en kennis verloren gaat door personeelwisselingen.

Gunningscriterium 4 TopDesk koppeling

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 de opdrachtnemer automatisch worden gesynchroniseerd, bij voorkeur via een API-koppeling. De opdrachtnemer biedt een API die volledig integreert met TOPdesk. U vult hiervoor op formulier 1 Programma van Eisen bij het onderdeel Wens of u hieraan voldoet JA of NEE in.

Doelstelling: Een efficiënte uitwisseling van gegevens en een gestroomlijnde samenwerking realiseren. De opdrachtgever verwacht met deze koppeling een snellere en betere incidentafhandeling 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.

Hoe vindt de beoordeling plaats?

U beschrijft uw aangeboden producten of diensten zo concreet en aantoonbaar mogelijk.

Wij beoordelen uw antwoorden onder andere op:

- Hoe goed uw antwoord aansluit op onze gewenste situatie;
- Hoe concreet/'SMART' uw antwoord is;
- In hoeverre uw antwoord meerwaarde voor ons biedt;

Dit vertalen wij in rapportcijfers volgens onderstaande tabel:

Kwalificatie	Uw beantwoording:	Rapport-cijfer
Uitstekend	De uitwerking van de aspecten overstijgt in onderlinge samenhang de gevraagde dienstverlening en de vraagstelling en biedt daardoor meerwaarde.	10
Goed	De uitwerking van de aspecten sluit in onderlinge samenhang goed aan bij de gevraagde dienstverlening en de vraagstelling.	8
Voldoende	De uitwerking van de aspecten sluit in onderlinge samenhang voldoende aan bij de gevraagde dienstverlening en de vraagstelling.	6
Onvoldoende	De uitwerking van de aspecten sluit in onderlinge samenhang onvoldoende aan bij de gevraagde dienstverlening en de vraagstelling. De Inschrijving geeft geen of irrelevante informatie en de beantwoording sluit niet aan bij de verwachtingen van de aanbestedende dienst.	4
Slecht	De uitwerking van de aspecten sluit in onderlinge samenhang slecht aan bij de gevraagde dienstverlening en de vraagstelling.	2
Geen beantwoording	De Inschrijver geeft geen beschrijving of een beschrijving waarin geen van de gevraagde elementen terugkomt. De Inschrijver geeft geen relevante informatie.	0

De Aanbestedende Dienst heeft voor deze aanbesteding een beoordelingsteam samengesteld bestaande uit vijf beoordelaars van verschillende disciplines. De beoordeling van de Inschrijvingen op de gunningscriteria vindt plaats in twee fasen:

Fase 1: beoordeling kwalitatieve gunningscriteria (GC-1, GC-2, GC-3, GC-4)

De Inschrijvingen worden door het beoordelingsteam allereerst beoordeeld op basis van de kwalitatieve gunningscriteria. De inschrijfprijzen zijn bij de beoordelaars op dat moment nog niet bekend.

De leden van het beoordelingsteam beoordelen individueel iedere Inschrijving per kwalitatief gunningscriterium en kennen per kwalitatief gunningscriterium (GC-1, GC-2 en GC-3) een rapportcijfer toe.

Na de individuele beoordeling van de Inschrijvingen op de kwalitatieve gunningscriteria vindt een plenaire bijeenkomst van het beoordelingsteam plaats. Tijdens deze bijeenkomst worden de individuele beoordelingsresultaten per kwalitatief gunningscriterium besproken. Per kwalitatief gunningscriterium bespreken de betrokken beoordelaars hun individuele beoordelingen en motiveren zij waarom zij tot een bepaalde beoordeling zijn gekomen. Hierna wordt door alle beoordelaars een beoordelingscijfer vastgesteld afgerond op één decimaal. Nadat de definitieve beoordeling per kwalitatief gunningscriterium is vastgesteld, wordt per kwalitatief gunningscriterium de fictieve korting bepaald.

Voorbeeld beoordelingsresultaat:

Beoordelaar 1	8
Beoordelaar 2	6
Beoordelaar 3	6
Beoordelaar 4	8
Beoordelaar 5	8
Gemiddeld rapportcijfer (beoordelingscijfer)	7,2 (36/5)

De fictieve korting berekenen wij als volgt:
Gemiddeld rapportcijfer x 10% x maximale fictieve korting.

Voorbeeld: $7,2 \times 10\% \times € 300.000,- = € 216.000,-$ fictieve korting

Als u voor een gunningcriterium (GC-1 of GC-2 of GC-3) een beoordelingscijfer van 5,9 of lager scoort dan valt u af voor verdere beoordeling en kunt u niet voor gunning in aanmerking komen.

Fase 2: beoordeling gunningscriterium Prijs

Nadat de beoordeling van de Inschrijvingen op basis van de kwalitatieve gunningscriteria heeft plaatsgevonden worden de fictieve kortingen in mindering gebracht op de inschrijfprijzen. De Inschrijver die de laagste fictieve inschrijfprijs heeft, heeft de Inschrijving met de beste prijs-kwaliteitverhouding (BPKV) ingediend. VRMWB is voornemens om de Opdracht aan deze Inschrijver te gunnen. Uiteraard blijft de inschrijfsom het bedrag wat u mag factureren.

Als twee of meer Inschrijvers gelijk eindigen wint de Inschrijver met de laagste prijs. Is ook deze hetzelfde dan beslist het lot. De desbetreffende Inschrijvers worden er tijdig van in kennis gesteld, dat een loting zal plaatsvinden en waar, wanneer en door wie de loting zal worden gehouden. Zij zijn bevoegd daarbij in persoon of bij gemachtigde aanwezig te zijn.

Planning

Datum	Actie
31 oktober 2024	Verzending aankondiging TenderNed
19 november 2024 uiterlijk 10.00 uur	Uiterste datum indienen vragen via de Vraag en Antwoord tool via TenderNed.
27 november 2024	Beantwoording van alle binnengekomen vragen. Deze antwoorden worden gedeeld met alle geïnteresseerde partijen via een Nota van Inlichtingen.
10 december 2024 uiterlijk 10.00 uur	Uiterste datum indienen vervolgvragen via de Vraag en Antwoord tool via TenderNed.
17 december 2024	Beantwoording van alle binnengekomen vragen. Deze antwoorden worden gedeeld met alle geïnteresseerde partijen via een Nota van Inlichtingen.
21 januari 2024 uiterlijk 10.00 uur	Sluitingstermijn Inschrijving
4 februari 2025	Verzending gunningsbeslissing
25 februari 2025	Definitieve gunning
Mei – juni	Transitieperiode
1 juli 2025	Ingangsdatum Overeenkomst

Heeft u interesse?

Leest u dit document met de bijlage goed door en beoordeel of u voldoet aan de gestelde eisen. Als u een goede aanbidding kunt doen dan kunt u inschrijven via TenderNed. Alle communicatie doen we in het Nederlands.

Tip: Zorg ervoor dat uw organisatie juist en volledig is geregistreerd bij TenderNed. De registratie van uw organisatie neemt enkele werkdagen in beslag, dus houdt u hier rekening mee. Voor meer informatie verwijzen wij u graag naar het document: “In 6 stappen digitaal inschrijven op TenderNed”, in te zien via: <https://www.TenderNed.nl/cms/voor-ondernemingen/6-stappen-digitaal-inschrijven> en www.TenderNed.nl. Voor eventuele technische vragen over TenderNed kunt u contact opnemen met de servicedesk, via <https://www.tenderned.nl/cms/nl/contact/mailen> of via 0800-8363376.

Inhoud Inschrijving

Uw Inschrijving bestaat uit de volgende documenten:

- UEA ingevuld en ondertekend
- Formulier 1 Programma van Eisen ingevuld en ondertekend
- Formulier 2 Referentie-eis/kerncompetentie ingevuld en ondertekend
- Formulier 3 Kwaliteitssysteem ingevuld en ondertekend
- Formulier 4 Prijsopgave ingevuld en ondertekend
- Uitwerking gunningscriteria GC-1, GC-2 en GC-3

Rechtsbescherming/klachten

Op deze aanbestedingsprocedure is de Aanbestedingswet 2012 van toepassing. Voor het overige is op de onderhavige procedure en de daar uitkomende Overeenkomst het Nederlands recht van toepassing, met uitsluiting van het Weens koopverdrag. In het bijzonder wordt gewezen op de uitsluiting van partijen die gerelateerd zijn aan en/of Russische partijen.

Mocht de Inschrijver een klacht hebben over de aanbesteding of een onderdeel daarvan, dan kunt u deze klacht schriftelijk te melden bij het NIPV via klachtenmeldpunt.aanbestedingen@nipv.nl

Na de voorgenomen gunningsbeslissing geldt een opschortende termijn. Mocht u het niet eens zijn met de voorgenomen gunningsbeslissing, dan kunt binnen een termijn van 20 kalenderdagen een kort geding aanhangig maken bij de Rechtbank Zeeland-West-Brabant, locatie Breda. Na het verstrijken van deze termijn vervalt uw recht om bezwaar te maken tegen de voorgenomen gunningsbeslissing.

Overige voorwaarden

- Wij behouden ons het recht voor om niet te gunnen en/of de aanbesteding tussentijds te beëindigen.

- Ook behouden wij ons het recht voor om de aanbesteding aan te passen en/of wijzigingen aan te brengen, via een nota van inlichtingen.
- Het indienen van alternatieven en varianten is niet toegestaan.
- Wij kunnen u om extra informatie en/of een nadere toelichting vragen.
- Gedurende de aanbestedingsprocedure bent u verplicht alle informatie die u van ons heeft ontvangen geheim te houden en niet aan derden te verstrekken, voor zover deze informatie niet openbaar is.
- Uw Inschrijving mag geen leverings-, betalings- en/of andere (algemene) voorwaarden bevatten en worden uitdrukkelijk van de hand gewezen.
- Uw documenten zijn rechtsgeldig ondertekend door de daartoe bevoegde persoon.
- Wij wijzen iedere aansprakelijkheid voor een eventuele onjuistheid of onvolledigheid van de informatie zoals opgenomen in dit aanbestedingsdocument van de hand.
- Op die plaatsen in het aanbestedingsdocument waar gesproken wordt over merknamen, typen, fabricage, procedés, etc. en waarbij het wellicht handelt om een unieke zaak zal volgens het gestelde in artikel 2.76 lid 6 van de Aanbestedingswet van toepassing zijn op het bewuste tekstdeel. U kunt in een dit geval “of gelijkwaardig” lezen.
- In geval van tegenstrijdigheden tussen dit aanbestedingsdocument en de Inkoopvoorwaarden GIBIT 2023 prevaleert het aanbestedingsdocument. De wijzigen en aanvullingen kunnen door een Nota van Inlichtingen als aanvulling op het aanbestedingsdocument gedaan worden.
- De gestelde voorwaarden en eisen gelden voor de gehele contractperiode.
- VRMWB zal vertrouwelijk omgaan met bedrijfsgevoelige informatie.
- De in de Inschrijving aangeboden prijzen en kortingen zijn onvoorwaardelijk en tot 31-12-2025 vast en onveranderlijk. Na deze periode mogen jaarlijks per 1 januari kunnen de overeengekomen (jaar)tarieven en doorlopende vergoedingen 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 2015=100), althans de opvolger daarvan, voor groep J62, althans J6202, over het gehele jaar in vergelijking met het prijsindexcijfer van het jaar daarvoor van diezelfde index.

- Opdrachtnemer deelt zijn voorstel voor de nieuwe prijzen voor de dienstverlening steeds van het jaar voorafgaand aan het jaar dat de prijsaanpassing in zal gaan, mee aan Opdrachtgever. Na schriftelijk akkoord van Opdrachtgever kan de prijsaanpassing worden doorgevoerd met de overeengekomen datum van het opvolgende jaar.
- De eenmalige implementatie/transitiekosten worden via één factuur gefactureerd.
- De jaarlijkse beheerkosten gaan in na ingangsdatum Overeenkomst (01-07-2025).

Bijlagen

UEA

Formulier 1 Programma van Eisen

Formulier 2 Referentie eis/kerncompetentie

Formulier 3 Kwaliteitssysteem

Formulier 4 Prijsopgave

Inkoopvoorwaarden GIBIT 2023

Bijlage A: Conceptovereenkomst (toegevoegd in dit aanbestedingsdocument)

Bijlage B: Concept verwerkersovereenkomst (toegevoegd aan dit aanbestedingsdocument)

Bijlage A Conceptovereenkomst

Conceptovereenkomst Microsoft 365 en Azure Cloud beheerdiensten

CONCEPTOVEREENKOMST ten behoeve van Microsoft 365 en Azure Cloud beheerdiensten

REFERENTIE: P24-0068

Ondergetekenden

- De publiekrechtelijke rechtspersoon Veiligheidsregio Midden- en West-Brabant (VRMWB), te dezen rechtsgeldig vertegenwoordigd door Jolanda Trijselaar, Algemeen Directeur / Regionaal Commandant, hierna te noemen "**Opdrachtgever**";

en

- ("NAAM_HIER") met Kamer van Koophandel nummer ("KvK_Hier") gevestigd en kantoorhoudende te ("PLAATS_HIER") aan de ("ADRES_HIER") ("POSTCODE_HIER"), te dezen rechtsgeldig vertegenwoordigd door, hierna te noemen "**Leverancier**";

tezamen hierna verder aan te duiden als "partijen" dan wel afzonderlijk als "partij",

overwegende dat:

- Opdrachtgever in het kader van de uitoefening van zijn taak behoefte heeft aan het beoogde gebruik van de ICT Prestatie zoals ten tijde van het sluiten van de Overeenkomst voor Leverancier (al dan niet op basis van de offerteaanvraag of andere aan de Overeenkomst voorafgaande documenten) bekend was of op grond van artikel 3 GIBIT 2023 voor Leverancier bekend behoorde te zijn, een en ander voor zover dat gebruik in onderhavige Overeenkomst niet uitdrukkelijk is uitgesloten of beperkt;
- Opdrachtgever in verband met hetgeen hiervoor is overwogen, tot Europese aanbesteding van de ICT Prestatie is overgegaan;
- Partijen de uit het bovenstaande voortvloeiende rechtsverhouding schriftelijk wensen vast te leggen;

zijn als volgt overeengekomen:

Voorwerp van de Overeenkomst

Leverancier verplicht zich tot het leveren van de ICT Prestatie zoals beschreven in:

Het aanbestedingsdocument inclusief bijlagen

De in het eerste lid bedoelde activiteiten zullen plaatsvinden onder de voorwaarden als beschreven in het onderhavige document en de hierin genoemde bijlagen (hierna gezamenlijk: "de Overeenkomst");

Wijzigingen op de Overeenkomst zijn uitsluitend geldig indien Partijen deze schriftelijk zijn overeengekomen.

Specificaties

Tot het Overeengekomen gebruik behoort dat de ICT Prestatie voldoet aan hetgeen beschreven is in de in artikel 1.1. genoemde documenten.

Gemeentelijke ICT-Kwaliteitsnormen, Interoperabiliteitseisen, normen en standaarden

De ICT-Prestatie zal gedurende de looptijd van de Overeenkomst voor de volgende ICT-kwaliteitsgebieden blijven voldoen aan de Gemeentelijke ICT-Kwaliteitsnormen:

- Architectuur;
- Interoperabiliteit;
- Informatiebeveiliging en privacy;
- Dataportabiliteit;
- Toegankelijkheid;
- Infrastructuur;
- Documentatie;
- E-facturering.

Voor een specificatie van de Gemeentelijke ICT-Kwaliteitsnormen wordt verwezen naar: https://vng.nl/sites/default/files/2024-07/gemeentelijke_ict_kwaliteitsnormen_2024.pdf

Looptijd

De Overeenkomst treedt in werking op 1 juli 2025 en heeft een initiële looptijd van vier (4) jaar. De initiële looptijd van deze Overeenkomst eindigt op 30 juni 2029.

Na afloop van de initiële looptijd wordt de Overeenkomst automatisch verlengd met twee (2) keer twee (2) jaar, tenzij de Opdrachtgever de overeenkomst schriftelijk opzegt met een opzegtermijn van drie (3) maanden voor het einde van de lopende termijn.

De Opdrachtnemer zal voorafgaande aan de ingangsdatum van de Overeenkomst voorbereidende werkzaamheden uitvoeren voor het goed doorlopen van de transitieperiode.

De looptijd van de Gebruiksrechten is gelijk aan artikel 20.3 GIBIT 2023.

De looptijd van de Dienstverlening op Afstand is gelijk aan de looptijd van de Overeenkomst.

De volgende onderdelen van de ICT Prestatie worden voor wat betreft looptijd in ieder geval als afzonderlijke Overeenkomsten beschouwd in de zin van artikel 24.3 GIBIT 2023:

- Verwerkersovereenkomst.

Implementatie

De Implementatie geschiedt volgens een in nader overleg vast te stellen Implementatieplan.

De Implementatie dient uiterlijk op 30-06-2025 te zijn voltooid.

Onderhoud

Het Onderhoud is vastgesteld:

In een service level agreement. Artikel 10 GIBIT 2023 vormt voor onvoorziene omstandigheden het vangnet.

Gebruiksrechten

Leverancier levert Gebruiksrechten zoals gespecificeerd in de in artikel 1.1 genoemde documenten. **[Nader overeen te komen of Leverancier al dan niet Derdenprogrammatuur gebruikt en zo ja, waar dit beschreven wordt.]**

Dienstverlening op Afstand

Op de Dienstverlening op Afstand zijn de Service Levels van toepassing zoals omschreven in een service level agreement.

In navolging van artikel 35 GIBIT 2023 is de TPM-verklaring **[Nader overeen te komen op welke wijze verwezen wordt naar de TPM-verklaring art. 35 GIBIT 2023].**

Exit-plan

Leverancier verplicht zich reeds nu **uiterlijk binnen drie (3) maanden** een exit-plan als bedoeld in artikel 26 GIBIT 2023 op te stellen. Het exit-plan wordt nader uitgewerkt in bijlage "".

Verwerking van persoonsgegevens

Leverancier handelt als verwerker in de zin van de Algemene verordening gegevensbescherming.

De standaard Verwerkersovereenkomst is opgenomen in bijlage Bijlage verwerkersovereenkomst.

De Leverancier zal, behoudens op haar rustende wettelijke (archief)verplichtingen, alle persoonsgegevens na beëindiging van de overeenkomst, per ommegaande kosteloos retourneren aan de Opdrachtgever en, indien de Opdrachtgever daartoe opdracht heeft gegeven, wissen en uit haar systemen (incl. back-ups) verwijderen dan wel vernietigen op de wijze als door de Opdrachtgever bepaald. De vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

De Leverancier zal alle subverwerkers die betrokken zijn bij de verwerking van de persoonsgegevens op de hoogte stellen van de beëindiging van de overeenkomst en zal waarborgen dat alle subverwerkers de persoonsgegevens retourneren, verwijderen dan wel (laten) vernietigen, zoals in het vorige lid bepaald.

Vergoedingen

De vergoeding van het Onderhoud is nader gespecificeerd in de Inschrijving van Leverancier.

Na ingebruikname voor productieve doeleinden wordt van de vergoeding voor de Gebruiksrechten opeisbaar.

De vergoeding voor de Hosting-diensten is nader gespecificeerd in de Inschrijving van Leverancier.

De vergoeding voor de exit-plan is nader gespecificeerd in de Inschrijving van Leverancier. De vergoeding voor de Implementatie is nader gespecificeerd in de Inschrijving van Leverancier.

Leverancier verzendt de factuur met ordernummer aan Opdrachtgever elektronisch als PDF-bestand naar facturen@vrmwb.nl.

De in artikel 11.8 GIBIT 2023 benoemde index J62, althans sectie J6202, conform CPA 2008, van het Centraal Bureau voor de Statistiek, wordt opgevolgd door index J62, conform CPA 2015, van het Centraal Bureau voor de Statistiek.

Indexeringsaankondigingen dienen te worden gezonden aan de in lid 1 van het artikel 'Contactpersonen en bevoegdheden' van de Overeenkomst bedoelde contactpersonen.

Contactpersonen en bevoegdheden

Partijen wijzen de in een bijlage gespecificeerde personen aan als contactpersoon namens hun organisatie gedurende de looptijd van de Overeenkomst.

Tenzij vooraf door de ene partij uitdrukkelijk schriftelijk aan de andere partij van het tegendeel mededeling wordt gedaan, zijn de bedoelde contactpersonen bevoegd de partij die hen heeft aangewezen, in het kader van de uitvoering van deze Overeenkomst en de nadere overeenkomsten te vertegenwoordigen, en in dat kader aanvullende of afwijkende afspraken te maken.

Een partij mag haar contactpersonen wijzigen middels schriftelijke mededeling aan de andere partij. De wijziging zal minimaal een week van tevoren worden gemeld, behoudens in spoedgevallen.

Evaluatie

Oprachtgever evalueert minimaal één (1) maal per jaar de uitvoering van de opdracht en het resultaat van de ICT Prestatie. De onderwerpen van evaluatie omvatten in ieder geval en indien van toepassing:

- de kwaliteit
- de prijs
- oplevering en levertijd
- service
- nazorg
- onderhoudstermijnen
- garantie

Verder worden de tussen Partijen gesloten contractbijlagen minimaal één (1) maal per half jaar, of op verzoek van de Partijen, geëvalueerd.

Partijen kunnen voorstellen doen om de betreffende overeenkomst aan te passen. Aanpassingen op de documenten worden door Leverancier verwerkt. Tijdens deze evaluatie wordt het document in ieder geval getoetst op de bruikbaarheid in achterliggende periode van het document, contactpersonen en hun functie, scope van de dienstverlening of de lopende procedures. Indien nodig, kunnen additionele onderwerpen voor de evaluatie uiterlijk één (1) week voor het evaluatieoverleg ingediend worden.

Voorwaarden en overige afspraken

Op deze Overeenkomst zijn de Inkoopvoorwaarden GIBIT 2023 van toepassing, zoals bijgesloten als bijlage. Leverancier verklaart een exemplaar van de GIBIT 2023 te hebben ontvangen.

Eventuele leveringsvoorwaarden van Leverancier zijn uitdrukkelijk niet van toepassing. De navolgende stukken vormen gezamenlijk de Overeenkomst. Voor zover deze stukken met elkaar in tegenspraak zijn, prevaleert het eerder genoemde stuk boven het later genoemde:

- Het onderhavige document;
- De verwerkersovereenkomst;

De in artikel 1.1. genoemde documenten (in de daar genoemde volgorde). In de Overeenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan is gegeven in de GIBIT 2023.

Aangezien dit een conceptovereenkomst betreft kan deze derhalve niet ondertekend worden.

- De Nota van Inlichtingen;
- Contactpersonen.

BIJLAGEN UITWERKING ASPECTEN ICT PRESTATIE

- ("NAAM/VERSIE/DATUM_BIJLAGE_EXITPLAN_HIER").

Bijlage contactpersonen

Opdrachtgever

Naam Telefoon E-mail	Rolbeschrijving
<i>Veiligheidsregio Midden- en West-Brabant Maike van Elzaker 06-42512959 inkoop@vrmwb.nl</i>	Inkoopadviseur Afdeling Inkoop & Contractmanagement

Opdrachtnemer/leverancier

Naam Telefoon E-mail	Rolbeschrijving
<i>nader te bepalen</i>	

Bijlage B Verwerkersovereenkomst

Verwerkersovereenkomst Microsoft 365 en Azure Cloud beheerdiensten

Verwerkersovereenkomst uitvoering Microsoft 365 en Azure Cloud beheerdiensten

Veiligheidsregio Midden- en West-Brabant, verder te noemen verwerkingsverantwoordelijke is, hierbij rechtsgeldig vertegenwoordigd door de heer Gerard Palma, afdelingshoofd Informatisering,

en

<Bedrijf>, gevestigd te <plaatsnaam>, KVK-nummer <nummer> verder te noemen Verwerker, hierbij rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam>, <functie>,

hierna afzonderlijk te noemen "Partij", of gezamenlijk "Partijen"

Overwegen het volgende:

- a) Partijen hebben op <datum> de <titel hoofdovereenkomst>, hierna Hoofdovereenkomst, afgesloten, op grond waarvan Verwerker de volgende dienst(en) levert aan de Verwerkingsverantwoordelijke: <specificatie dienst(en)>;
- b) Verwerker verwerkt voor de uitvoering van de Hoofdovereenkomst Persoonsgegevens voor Verwerkingsverantwoordelijke;
- c) Op de verwerking van Persoonsgegevens door Verwerker zijn de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) van toepassing;
- d) Partijen willen in aanvulling op de AVG en de UAVG de volgende afspraken over de verwerking van Persoonsgegevens vastleggen in deze verwerkersovereenkomst (hierna: de Verwerkersovereenkomst);

En komen het volgende overeen:

Artikel 1 Definities

- 1.1 Begrippen uit de AVG en de UAVG die in deze Verwerkersovereenkomst worden gebruikt, hebben dezelfde betekenis.
- 1.2 Bijlagen: aanhangsels bij deze Verwerkersovereenkomst, die onlosmakelijk deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2 Ingangsdatum en duur

- 2.1 Deze Verwerkersovereenkomst gaat in op het moment dat de Hoofdovereenkomst tot stand is gekomen, tenzij Partijen anders overeenkomen.

- 2.2 Deze Verwerkersovereenkomst eindigt op het moment dat Verwerker de verwerking van Persoonsgegevens op grond van de Hoofdovereenkomst heeft beëindigd en de afspraken over het teruggeven en/of wissen van Persoonsgegevens zijn nagekomen.
- 2.3 Wanneer Partijen een (nieuwe) Verwerkersovereenkomst overeenkomen, betekent dat dat de oude Verwerkersovereenkomst komt te vervallen.

Artikel 3 Onderwerp van deze Verwerkersovereenkomst

- 3.1 Verwerker verwerkt de door of via Verwerkingsverantwoordelijke ter beschikking gestelde Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke voor de uitvoering van de Hoofdovereenkomst en uitsluitend overeenkomstig schriftelijke instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke wettelijke bepaling hem tot verwerking verplicht. In dat geval zal Verwerker Verwerkingsverantwoordelijke, voorafgaand aan de verwerking, daarvan zonder onredelijke vertraging in kennis stellen, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
- 3.2 De door Verwerker uit te voeren verwerkingen staan beschreven in tabel 1 van Bijlage 1.

Artikel 4 Inhoudelijke afspraken

- 4.1 **Beveiligingsmaatregelen**
Verwerker zorgt voor passende technische en organisatorische maatregelen om de Persoonsgegevens goed te beveiligen, zoals bedoeld in artikel 32 AVG. De wijze waarop Verwerker de passende technische en organisatorische maatregelen aantoont, staat in Bijlage 2.
- 4.2 **Audits**
Verwerker verleent alle benodigde medewerking aan audits uitgevoerd door een gecertificeerde auditor over de nakoming van de afspraken binnen deze Verwerkersovereenkomst en Bijlagen, tenzij Verwerker door middel van een geldige certificering, die periodiek door een geaccrediteerde instelling wordt getoetst, heeft aangetoond dat Verwerker de gemaakte afspraken nakomt. De kosten van deze audit worden gedragen door Verwerkingsverantwoordelijke (zowel eigen kosten als kosten van Verwerker), tenzij de auditor één of meer tekortkomingen van niet ondergeschikte aard van Verwerker constateert die ten nadele zijn van Verwerkingsverantwoordelijke.
- 4.3 **Verwerking buiten de EER**
Verwerker mag Persoonsgegevens buiten de Europese Economische Ruimte (laten) verwerken wanneer is voldaan aan de voorwaarden van artikel 45 of 46 AVG. Wanneer er sprake is van een verwerking buiten de EER, dan stelt Verwerker Verwerkingsverantwoordelijke daarvan vooraf op de hoogte.
- 4.4 **Geheimhouding**
Personen die werken voor (sub)Verwerker en (sub)Verwerker zelf, moeten Persoonsgegevens waarmee zij werken geheimhouden. De personen die werken voor Verwerker en subverwerkers hebben daarom een geheimhoudingsverklaring getekend, of zich op een andere manier schriftelijk gebonden aan de geheimhouding.
- 4.5 **Subverwerkers**

- De ten tijde van het afsluiten van deze Verwerkersovereenkomst bekende subverwerkers vermeldt Verwerker in tabel 3 van Bijlage 1.
- Verwerkingsverantwoordelijke verleent hierbij algemene toestemming voor de inschakeling van subverwerkers. Verwerker houdt na de start van de werkzaamheden Verwerkingsverantwoordelijke op de hoogte van de beoogde inschakeling van nieuwe subverwerkers. Bij de inschakeling van subverwerkers blijven de artikelen 28.2 en 28.4 AVG onverkort van kracht.
- 4.6 **Rechten van betrokkenen**
- Als een betrokkene een beroep doet op zijn rechten zoals genoemd in artikel 12 t/m 22 AVG, helpt Verwerker Verwerkingsverantwoordelijke om daarop binnen de wettelijke termijnen een beslissing te nemen.
- 4.7 **Gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging**
- Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker altijd mee aan een gegevensbeschermingseffectbeoordeling (DPIA) en een voorafgaande raadpleging als bedoeld in artikel 35 en 36 AVG.

Artikel 5 Inbreuk in verband met Persoonsgegevens

- 5.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar uiterlijk binnen 24 uur, informeren na vaststelling van een (vermoedelijke) Inbreuk in verband met Persoonsgegevens. Verwerker vermeldt hierbij voor zover bekend de vermeende oorzaak van de (vermoedelijke) Inbreuk, de categorie persoonsgegevens, de categorie betrokkenen en het aantal betrokkenen.
- 5.2 In geval van een Inbreuk neemt Verwerker zonder onredelijke vertraging alle maatregelen om de Inbreuk te herstellen, de gevolgen daarvan te beperken en verdere Inbreuken te voorkomen en houdt de Verwerkingsverantwoordelijke hiervan voortdurend op de hoogte.
- 5.3 Verwerker heeft een gedetailleerd logboek van de Inbreuken en de maatregelen die op Inbreuken zijn genomen. Verwerkingsverantwoordelijke mag dat inzien, wanneer deze daarom vraagt.
- 5.4 Verwerkingsverantwoordelijke beslist of de Inbreuk moet worden gemeld bij de toezichthoudende autoriteit en/of Betrokkene. Verwerker ondersteunt de Verwerkingsverantwoordelijke waar nodig bij de melding aan de toezichthoudende autoriteit en/of Betrokkene.

Artikel 6 Aansprakelijkheid

- 6.1 Eventuele in de Hoofdovereenkomst overeengekomen beperkingen van de aansprakelijkheid hebben ook betrekking op de Verwerkersovereenkomst.

Artikel 7 Beëindigen verwerkersovereenkomst

- 7.1 Partijen moeten in de Hoofdovereenkomst afspraken maken over de beëindiging van de Hoofdovereenkomst en de daaruit voortvloeiende teruggave en wissing van Persoonsgegevens.
- 7.2 De geheimhouding geldt ook nog na beëindiging van deze Verwerkersovereenkomst.

Artikel 8 Overige bepalingen

- 8.1 Op deze overeenkomst is Nederlands recht van toepassing. Alle geschillen, ook als alleen één Partij vindt dat er een geschil is, zullen in eerste instantie worden voorgelegd aan dezelfde bevoegde rechter als genoemd in de Hoofdovereenkomst.

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend,

Ingangsdatum: <.....>

Veiligheidsregio Midden- en West-Brabant

<Naam organisatie>

namens deze: Gerard Palma, afdelingshoofd Informatisering

namens deze: <naam, functie>

plaats: <.....>

plaats: <.....>

datum: <.....>

datum: <.....>

Bijlage 1: Overzicht van te verwerken persoonsgegevens

1. Naam verwerking, doeleinden categorieën van betrokkenen, categorieën persoonsgegevens en eventuele doorgifte naar derde landen.

Naam verwerking	Verwerkingsdoeleinden	Categorieën van Betrokkenen	Categorieën Persoonsgegevens (waaronder bijzondere persoonsgegevens)	Verwerkingslocatie	Doorgifte-instrument (indien van toepassing)	Aanvullende maatregelen (indien van toepassing)

2. Contactgegevens

Contactpersoon Verwerkingsverantwoordelijke (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactpersoon Verwerkingsverantwoordelijke (NB: ook buiten kantooruren)	Naam: S. Huijbregts Contactgegevens: FG@vrmwb.nl - 0634459836

Contactpersoon Verwerker (NB: Ook buiten kantooruren)	Naam: Contactgegevens:
Contactgegevens IBD	telefoonnummer: 070-204 55 11 e-mailadres : privacy@vng.nl

*NB: Eventuele wijzigingen in bovenstaande tabellen geven partijen op korte termijn aan elkaar door.

3. Ingeschakelde subverwerkers

Naam en contactgegevens subverwerker	KvK-nummer	Uitbestede verwerkingen	Toepassing (geautomatiseerd systeem)	Verwerkingslocatie	Doorgifte-instrument	Aanvullende maatregelen (indien van toepassing)

Bijlage 2: Aantonen passend niveau van beveiliging

Normenstelsel

- ☐ De verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten: (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS) en is volgens deze norm wel/niet gecertificeerd.
- ☐ Datum laatste certificering:
- ☐ De verwerker werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:,
- ☐ De verwerker werkt volgens een andere norm, te weten:

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- Verwerker verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) genoemd in Bijlage 1.

Aansluiting bij goedgekeurde gedragscode

- ☐ Verwerker is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten

Bijlage 3: Relevante GIBIT 2023 artikelen

Artikel 16. Aansprakelijkheid

- 16.1 De partij die toerekenbaar tekortschiet in de nakoming van zijn verplichtingen, of jegens de ander onrechtmatig handelt, is tegenover de andere partij aansprakelijk voor de door deze aldus geleden en/of te lijden schade.
- 16.2 Voor zover nakoming niet reeds blijvend onmogelijk is, of de verbintenis voortvloeit uit onrechtmatige daad of strekt tot schadevergoeding, vindt lid 1 slechts toepassing met inachtneming van het bepaalde in artikel 24.9 omtrent verzuim.
- 16.3 De in lid 1 bedoelde aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade, is beperkt tot een bedrag van € 1.250.000,- per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.
- 16.4 De aansprakelijkheid voor overige schade is beperkt tot twee maal de Jaarvergoeding per gebeurtenis. De totale aansprakelijkheid per jaar bedraagt evenwel nooit meer dan vier maal de Jaarvergoeding (ongeacht het aantal gebeurtenissen). Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.
- 16.5 De in dit artikel opgenomen beperkingen van aansprakelijkheid zijn niet van toepassing:
- i) in geval van aanspraken van derden op schadevergoeding ten gevolge van dood of letsel en/of;
 - ii) indien sprake is van opzet of grove schuld aan de zijde van de andere partij of diens Personeel; en/of
 - iii) in geval van schending van intellectuele eigendomsrechten als bedoeld in artikel 20;
 - iv) ten aanzien van door de toezichthoudende autoriteit opgelegde boetes:
 - 1. voor zover die boetes ook rechtstreeks aan de Leverancier hadden kunnen worden opgelegd, maar niet zijn opgelegd; en
 - 2. onder de voorwaarde dat Opdrachtgever Leverancier:
 - a. onverwijld schriftelijk informeert over een door een toezichthoudende autoriteit gestart onderzoek dat kan leiden tot een boete alsmede over en het bestaan en de inhoud van de opgelegde boete; en
 - b. Leverancier volledig betreft bij het voeren van verweer tegen die boete althans het aan Leverancier toe te rekenen deel van die boete.
- 16.6 Alle verplichtingen met betrekking tot Personeel van Leverancier krachtens de belasting-, zorgverzekerings- en sociale verzekeringswetgeving, komen ten laste van Leverancier. Leverancier vrijwaart Opdrachtgever tegen elke aansprakelijkheid die daarmee verband houdt. Op deze vrijwaring zijn de voorgaande beperkingen van aansprakelijkheid niet van toepassing.

Artikel 24. Opschorting, opzegging en ontbinding

Gevolgen van beëindiging

- 24.14 Onverminderd het bepaalde in artikel 26 (exit) retourneert of verwijdt Leverancier bij het, op welke grond dan ook, eindigen van de Overeenkomst(en) op het eerste verzoek en om niet alle hem door Opdrachtgever ter hand gestelde documenten, boeken,

bescheiden en andere zaken (waaronder begrepen gegevens- en informatiedragers). Bij vroegtijdige beëindiging geldt het voorgaande wederkerig.

Artikel 25. Controlerecht en medewerking audits bij Opdrachtgever

Controlerecht

- 25.1 Opdrachtgever is gerechtigd de naleving door Leverancier van de wezenlijke verplichtingen uit hoofde van de Overeenkomst, de Inkoopvoorwaarden en de daarmee samenhangende overeenkomsten (SLA, verwerkersovereenkomst, etc.), alsmede de juistheid van toegezonden facturen, binnen een redelijke termijn door een onafhankelijke ter zake deskundige aan geheimhouding gebonden derde te laten controleren.
- 25.2 Opdrachtgever zal alvorens een controle te doen verrichten eerst Leverancier om de op grond van het vorige lid noodzakelijke informatie vragen en daarbij de aanleiding voor het betreffende verzoek kenbaar maken, althans bij generieke Dienstverlening op Afstand eerst vragen om de in artikel 35 bedoelde verklaring.
- 25.3 De controle zal alleen plaatsvinden indien Opdrachtgever - ook na beantwoording van het in het vorige lid bedoelde verzoek om informatie - gerede twijfel heeft over de nakoming van de verplichtingen door Leverancier, of indien Opdrachtgever anderszins een gerechtvaardigd belang bij de controle heeft (o.m. wettelijke plicht, instructie toezichthouder). Opdrachtgever zal vooraf de aanleiding voor de controle kenbaar maken.
- 25.4 Leverancier zal alle redelijkerwijs te verwachten medewerking verlenen aan een dergelijke controle. Leverancier zal in dat kader ten minste inzage verlenen in alle relevante gegevens en achtergrondinformatie die relevant kan zijn in het kader van voornoemde controle. Ook zal Leverancier voor zover redelijkerwijs mogelijk toegang verlenen tot de locatie waar de diensten worden verleend.
- 25.5 Opdrachtgever staat er voor in dat de in het eerste lid bedoelde derde eventueel door Leverancier gehanteerde voorschriften zal opvolgen. Indien de controle niet (volledig) kan worden uitgevoerd vanwege voornoemde voorschriften, dan komt dit evenwel voor risico van Leverancier.
- 25.6 De kosten voor deze controle worden gedragen door Opdrachtgever (zowel eigen kosten als kosten van de Leverancier), tenzij de derde één of meer tekortkomingen van niet ondergeschikte aard van Leverancier constateert die ten nadele zijn van Opdrachtgever.

Medewerking audits bij Opdrachtgever

- 25.7 Voor zover Opdrachtgever afhankelijk is van Leverancier voor de uitvoering van (wettelijke verplichte) audits, zal Leverancier alle noodzakelijke medewerking verlenen aan de uitvoering van deze audits. De kosten voor deze medewerking worden gedragen door Opdrachtgever.

Artikel 26. Exit-plan, overstap, beperkte voortzetting, overdracht en verlengd gebruik

Exit-plan (algemeen)

- 26.1 Op eerste verzoek van Opdrachtgever zullen Partijen een exit-plan opstellen, dan wel een bestaand exit-plan bijwerken. In het exit-plan wordt vastgelegd wat er dient te

gebeuren ter voorbereiding op en uitvoering van de in dit artikel beschreven werkzaamheden. Artikel 6.2 en 6.3 zijn van overeenkomstige toepassing op het exit-plan.

- 26.2 De in dit artikel bedoelde werkzaamheden – te weten overstap (artikel 26.5 e.v.), beperkte voortzetting (artikel 26.8 e.v.), overdracht (artikel 26.10) en beperkte verlenging (artikel 26.11) – zullen worden verricht overeenkomstig het bepaalde in de volgende documenten bij tegenstrijdigheid prevaleert het document hoger in rangorde):
- i. het exit-plan (indien opgesteld); en
 - ii. de Overeenkomst (voor zover deze voorziet in de gevolgen van de beëindiging van de Overeenkomst); en
 - iii. de Algemene Voorwaarden.
- 26.3 Leverancier doet bij het, op welke grond ook beëindigen van de Overeenkomst(en), op eerste verzoek van Opdrachtgever datgene wat redelijkerwijs noodzakelijk is om er voor te zorgen dat een nieuwe leverancier of Opdrachtgever zelf zonder belemmeringen een soortgelijke ICT Prestatie ten behoeve van Opdrachtgever kan verrichten (zults met uitzondering van de afgifte van de broncode van de Programmatuur).
- 26.4 Opdrachtgever kan in het kader van de in het vorige lid bedoelde redelijke maatregelen in ieder geval de keuze maken uit (een en ander verder uit te werken in het exit-plan):
- i) het door Leverancier alsnog aan de verplichtingen uit artikel 21 voldoen;
 - ii) het door Leverancier vernietigen van de gegevens waarvoor Opdrachtgever verantwoordelijk is (tegen afgifte van bewijs van vernietiging);
 - iii) het door Leverancier technisch ontlechten en ontmantelen van (een deel van) de ICT Presentatie

Overstap naar soortgelijke ICT Prestatie

- 26.5 Leverancier doet bij het, op welke grond ook beëindigen van de Overeenkomst(en), op eerste verzoek van Opdrachtgever datgene wat redelijkerwijs noodzakelijk is om er voor te zorgen dat een nieuwe leverancier of Opdrachtgever zelf zonder belemmeringen een soortgelijke ICT Prestatie ten behoeve van Opdrachtgever kan verrichten (zults met uitzondering van de afgifte van de broncode van de Programmatuur).
- 26.6 Opdrachtgever kan in het kader van de in het vorige lid bedoelde redelijke maatregelen in ieder geval de keuze maken uit (een en ander verder uit te werken in het exit-plan):
- i) het door Leverancier alsnog aan de verplichtingen uit artikel 21 voldoen;
 - ii) het door Leverancier vernietigen van de gegevens waarvoor Opdrachtgever verantwoordelijk is (tegen afgifte van bewijs van vernietiging);
 - iii) het door Leverancier technisch ontlechten en ontmantelen van (een deel van) de ICT Presentatie
- 26.7 In afwijking van het bepaalde in lid 4 worden voornoemde diensten kosteloos verricht indien de Overeenkomst wordt beëindigd wegens toerekenbaar tekortschieten door Leverancier. De onder lid 6 sub ii) bedoelde werkzaamheden worden op verzoek hoe dan ook kosteloos verricht.

Beperkte voortzetting van ICT Prestatie

- 26.8 Leverancier verklaart zich reeds nu voor alsdan bereid bij beëindiging van de Overeenkomst(en) - op welke grond dan ook - op eerste verzoek van Opdrachtgever:

- i) een nieuwe ICT Prestatie of beperkte voortzetting van de bestaande ICT Prestatie te leveren waarmee Opdrachtgever in staat blijft de met de huidige ICT Prestatie opgeslagen gegevens te raadplegen; en
 - ii) een beperkte vorm van Onderhoud te (blijven) verlenen op de in het vorige lid bedoelde ICT Prestatie (namelijk binnen de kaders van de in het vorige lid bedoelde beperkte functionaliteit).
- 26.9 Voor de duur, kosten en voorwaarden voor de in het vorige lid bedoelde ICT Prestatie geldt dat:
- i) de duur ten minste een zodanige duur is dat Opdrachtgever aan de wettelijke administratieplichten kan voldoen;
 - ii) de kosten in redelijke verhouding staan tot de oorspronkelijke kosten voor de gehele ICT Prestatie (naar rato van de verminderde functionaliteit), met dien verstande dat noodzakelijke verlengingen van Derdenprogrammatuur volledig kunnen worden doorbelast;
 - iii) de voorwaarden behoudens het bepaalde in het vorige lid gelijk zijn aan die van de Overeenkomst.

Overdracht ICT Prestatie

- 26.10 Opdrachtgever is gerechtigd de ICT Prestatie geheel of gedeeltelijk, inclusief alle daarbij behorende Gebruiksrechten en alle aanspraken in het kader van Onderhoud, onder gelijkblijvende voorwaarden (waaronder begrepen gelijkblijvende omvang Gebruiksrechten) over te dragen aan een gemeenschappelijke regeling of andere entiteit met een publieke functie in het kader van een uitbesteding van een deel van de activiteiten van Opdrachtgever. Leverancier zal alle noodzakelijke medewerking verlenen aan voornoemde overdracht. Leverancier is niet gerechtigd voor de overgang als zodanig kosten in rekening te brengen, wel voor eventueel aanvullend te verrichten werkzaamheden. Derdenprogrammatuur is alleen overdraagbaar voor zover de wet of de toepasselijke licentievoorwaarden daaraan niet in de weg staan (vgl. artikel 22.5).

Verlengd gebruik

- 26.11 Leverancier verklaart zich voorts bereid om Opdrachtgever desgewenst toe te staan het gebruik van de ICT Prestatie na de beëindigingsdatum voor een redelijke periode te verlengen, indien de werkzaamheden overeenkomstig het Exit-plan niet tijdig zijn afgerond. Hiervoor zal een vergoeding in rekening worden gebracht naar rato van de laatst geldende gebruiksvergoedingen (waarbij noodzakelijke verlengingen van Derdenprogrammatuur volledig kunnen worden doorbelast), tenzij de niet-tijdige afronding van de Exit-werkzaamheden toerekenbaar is aan Leverancier (de verlenging is dan gratis).