Bijlage 3 Beschrijving van de Opdracht

1. Algemene beschrijving van de Opdracht

Deze bijlage bevat een beschrijving van de Opdracht.

Opdrachtnemer dient de volgende werkzaamheden uit te voeren:

- Beheer van de netwerkinfrastructuur (LAN, WLAN, Firewalls)
- Beheer van de werkplekken (desktops, laptops, smartphones, tablets)
- Beheer van Microsoft Endpoint Manager (Intune)
- Beheer Digitale werkomgeving
- Beheer van Microsoft 365 tenant
- Beheer van de servers
- Beheer van de domain controller (Entra ID)
- Beheer Exchange omgeving inclusief e-mail security welke qua functionaliteiten gelijkaardig is als in de huidige situatie
- Beheer van digitale werkplekken, met onder andere SharePoint/ OneDrive/Teams
- Beheer MFA/SSO
- Managed dienstverlening voor proactieve bewaking, beveiliging en advisering van de algehele security aspecten binnen de ICT omgeving van Opdrachtgever
- Technisch Applicatiebeheer
- Helpdesk diensten op basis van tweede- en derdelijns ondersteuning
- Voorzien van Office 365 back-up waarbij de back-up opslag niet in een Microsoft Cloud omgeving plaatsvindt
- Levering en beheer van verbindingen vanuit een Cloud omgeving
- Levering van de benodigde licenties/resources ten behoeve van de beheerde onderdelen

In beheer name alsmede eventuele migratie van onderdelen die noodzakelijk zijn om de Opdracht uit te kunnen voeren, dienen onderdeel uit te maken van de Inschrijving. Licenties en onderdelen die noodzakelijk zijn om de werkzaamheden uit te kunnen voeren, dienen eveneens onderdeel uit te maken van de Inschrijving.

2. Buiten scope

Buiten de scope van de Opdracht vallen:

- De gebouw gebonden infrastructuur (netwerkbekabeling)
- Verbindingen op de locaties van Opdrachtgever
- Vervanging van werkplekken, smartphones of tablets
- Eerstelijns support inclusief inname en uitgifte apparatuur
- Lyfecycle management
- Printerbeheer inclusief tonermanagement
- Vervanging van printers
- Telefonie en/of vast mobile integratie

3. Nadere uitwerking van de Opdracht

a. <u>Centrale ICT-omgeving</u>

De toekomst van beheer, security en compliance verschuift van datacenter-gericht naar devices en Cloud. Opdrachtgever gaat in deze beweging mee en heeft daarom gekozen voor een Cloud opzet waarbij mede gebruik wordt gemaakt van onder andere een Virtual Private Cloud (VPC) en Microsoft 365 omgeving.

Opdrachtgever zoekt een strategisch partner die verder gaat dan enkel het uitvoeren van beheeractiviteiten. De ideale opdrachtnemer denkt actief mee over de dagelijkse beheerprocessen en beveiliging van de ICT-omgeving, neemt hierin een proactieve rol en richt zich op de toekomst door Opdrachtgever te adviseren en ondersteunen bij verwachte ontwikkelingen en innovaties binnen de markt.

Opdrachtnemer fungeert als vraagbaak voor een breed scala aan ICT-vraagstukken en brengt relevante kennis en expertise in. Het doel is om te komen tot een ICT-inrichting die optimaal aansluit bij de behoeften en doelen van Opdrachtgever. In dat kader dient Opdrachtnemer zorg te dragen voor een betrouwbare, veilige en efficiënt beheerde ICT-omgeving van Opdrachtgever, waarbij Opdrachtnemer dient te voldoen aan geldende en toekomstige wet- en regelgeving, zoals NIS2.

Bij de overgang naar de nieuwe Opdrachtnemer is Opdrachtnemer verplicht om de continuïteit van de centrale ICT-omgeving van Opdrachtgever te waarborgen. Gebruikers dienen ongestoord te kunnen doorwerken, waarbij de overhang naar de nieuwe Opdrachtnemer zo minimaal mogelijk merkbaar is.

Opdrachtgever volgt de volgende ICT-richtlijnen:

- Microsoft, tenzij
- Cloud, tenzij

b. <u>Persona</u>

Opdrachtgever heeft als doel om de veiligheid van haar ICT-omgeving naar een zo hoog mogelijk niveau te tillen, volledig in lijn met het BIO-beveiligingsbeleid (Baseline Informatiebeveiliging Overheid). Een belangrijk onderdeel hiervan is het reguleren van de toegang tot data en systemen. Dit geldt ook voor het beheer, waarbij het Role-Based Access Control (RBAC)-model verder wordt geïmplementeerd en geoptimaliseerd. Het RBAC-model wordt ingezet om redenen die cruciaal zijn voor de efficiëntie, veiligheid en schaalbaarheid van de organisatie.

- Begrijpelijk toegangsbeheer
    - Door het gebruik van de bestaande Persona's bij het opstellen van een RBAC-configuratie, kan Opdrachtgever een begrijpelijke benadering van toegangsbeheer realiseren. Dit maakt het eenvoudiger om rechten en toegangen toe te wijzen op basis van de specifieke rollen en verantwoordelijkheden van medewerkers.
- Gericht toekennen van rechten
    - Het RBAC-model stelt Opdrachtgever in staat om een gerichte controle te doen op rechten en permissies die van toepassing moeten zijn. Opdrachtnemer helpt daarbij om deze toekenning op een gestructureerde en bij voorkeur automatische wijze om de toekenning te doen en biedt daarbij de middelen en rapportages zodat Opdrachtgever deze controle kan uitvoeren. Dit zorgt ervoor dat medewerkers alleen toegang hebben tot de systemen en gegevens die zij nodig hebben voor hun dagelijkse taken, wat de beveiliging versterkt.
- Ondersteuning van securitybeleid
    - Een goed ingericht RBAC-model ondersteunt de handhaving van het securitybeleid van Opdrachtgever. Door duidelijke rollen en toegangsrechten te definiëren, kan de organisatie beter voldoen aan beveiligingsnormen en -richtlijnen.
- Schaalbaarheid
    - Het RBAC-model biedt schaalbaarheid, wat betekent dat Persona's eenvoudig kunnen worden aangepast of uitgebreid naarmate de organisatie groeit of verandert. Dit maakt het mogelijk om snel te reageren op nieuwe behoeften zonder de hele toegangsstructuur opnieuw te moeten ontwerpen.
- Security awareness gebruikers
    - Een belangrijk onderdeel van security is dat gebruikers getraind worden op mogelijke beveiligingsaanvallen. Aangezien op basis van Persona's een RBAC-model wordt toegepast, kunnen naast de algemene awareness trainingen op bijvoorbeeld e-mail ook specifieke onderdelen getoetst worden.

c. Fysieke werkplekken

De fysieke werkplek is een belangrijk onderdeel voor de uitvoering van de dataverwerking door de gebruiker. Daarom dient de fysieke werkplek zodanig ingericht te zijn dat deze optimaal bijdraagt aan een efficiënte en veilige uitvoering van de dataverwerking. Opdrachtnemer is verantwoordelijk voor het rapporteren aan Opdrachtgever over de status en geschiktheid van de fysieke werkplekken. Waar nodig verstrekt Opdrachtnemer advies om ervoor te zorgen dat de fysieke werkplek blijft voldoen aan de eisen en inzetbaar blijft voor de beoogde werkzaamheden.

Voor toegang tot specifieke (beheer)onderdelen dient gebruik te worden gemaakt van een op de werkplek beschikbaar gestelde VPN verbinding naar het netwerk van Opdrachtgever. De VPN-verbinding moet rekening houden met Azure Entra ID voor de voorwaardelijke toegang (Conditional Access) en gebruik van Multi Factor Authenticatie (MFA).

Opdrachtgever maakt gebruik van een Choose Your Own Device (CYOD)-beleid, waarbij zowel gedeelde werkplekken (afdelingscomputers) als persoonlijke laptops in gebruik zijn. Opdrachtnemer dient rekening te houden met beide typen werkplekken en de vereisten die hieruit voortvloeien.

d. Werkplekbeheer

Het werkplekbeheer dient ingericht te blijven op basis van Microsoft Intune, bestaande uit onder andere:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Beveiliging en Compliance
- Toegangsbeheer
- Selfservice (onder andere wachtwoord resetten)

e. Microsoft 365

Opdrachtnemer dient bij het leveren en beheren van de juiste licenties uit te gaan van het volgende:

- Microsoft OneDrive voor Bedrijven blijft ingezet als persoonlijke opslag voor medewerkers
- Microsoft SharePoint blijft ingezet als gedeelde opslag voor medewerkers
- Microsoft Teams blijft ingezet voor Communicatie
- Microsoft Exchange Online blijft ingezet worden ten behoeve van e-mailservices
- Behouden van een security baseline die te minste bestaat uit:
    - Defender for Endpoint
    - Defender for Cloud
    - MFA/SSO
    - Bitlocker
- Inzet SharePoint, Teams en OneDrive
    - Alle persoonlijke documenten bevinden zich in OneDrive
    - De afdeling/samenwerk documenten bevinden zich in SharePoint
    - Teams gebruik voor communicatie. Daarnaast wordt Teams beperkt ingezet voor samenwerking in projecten
- Inzet van Exclaimer handtekening oplossing of vergelijkbaar

f. Applicatie landschap

Het huidige applicatie landschap blijft gelijk. Hierbij is wel het uitgangspunt dat de huidige Exact omgeving over twee (2) jaar is uitgefaseerd en vervangen door een andere (SaaS) oplossing. Inschrijver dient hiermee rekening te houden bij het indienen van de Inschrijving; Opdrachtnemer kan hiervoor dan ook geen extra kosten in rekening brengen. Alle applicaties zijn gekoppeld en ingericht met single sign on gekoppeld aan Entra ID.

g. Digitale werkplek

Ten aanzien van het beheer zijn de volgende onderdelen van de digitale werkplek van toepassing:

- Documentbeheer en samenwerking
  - Versiebeheer: mogelijkheid om verschillende versies van documenten bij te houden
  - Real-time samenwerking: meerdere gebruikers kunnen tegelijkertijd aan documenten werken
  - Toegangscontrole: beheer wie toegang heeft tot welke documenten en mappen
  - Communicatie -en informatievoorziening
  - Nieuws en mededelingen: een centrale plek voor bedrijfsnieuws en belangrijke mededelingen
  - Smoelenboek: een overzicht van medewerkers met contactinformatie en functies
  - Teamsites: specifieke sites voor verschillende teams of projecten om informatie te delen en samen te werken
- Behoud van integratie met andere Microsoft 365-applicaties
  - Microsoft Teams: naadloze integratie voor chat, vergaderingen en samenwerking
  - Microsoft Outlook: integratie voor e-mail en agenda's
  - Microsoft OneDrive: voor persoonlijke opslag en delen van bestanden
- Behoud van integratie met andere applicaties
  - Vanuit Exact wordt gebruik gemaakt van ODBC koppelingen waarbij de verwerking deels in Excel wordt uitgevoerd
- Zoekfunctionaliteit
  - Slimme zoekfunctie: snel en efficiënt zoeken naar documenten, personen en informatie binnen de organisatie
- Beveiliging en compliance
  - Gegevensbescherming: ingebouwde beveiligingsfuncties om gevoelige informatie te beschermen
  - Compliance-tools: hulpmiddelen om te voldoen aan wettelijke en bedrijfsvoorschriften
- Gebruiksvriendelijkheid en aanpasbaarheid
  - Templates en Thema's: mogelijkheid om de werkplek aan te passen aan de huisstijl van de organisatie
  - Toegang via mobiele apparaten: er dient voor gezorgd te worden dat medewerkers ook onderweg toegang hebben tot de digitale werkplek

h. E-mail security

De functionaliteiten zoals gebruikt worden in de Mimecast oplossing dienen in ieder geval behouden te blijven.

i. Back-up

Opdrachtnemer zorgt voor een back-up van de Cloud omgeving en de Microsoft 365 omgeving. In onderstaande tabel is het back-up schema van de Virtual Private Cloud/ Microsoft 365 te zien.

Job type	Schedule	Retentie
MS 365/ VM	Dagelijks	90 dagen
MS 365/ VM	Wekelijks	90 dagen
MS 365/ VM	Maandelijks	90 dagen

In de huidige omgeving is een SQL database structuur opgezet. Hiervan wordt gedurende de dag (per twee (2) uur) tussentijdse SQL back-ups gemaakt.

j. Beheer

Opdrachtgever levert zelf de eerstelijns helpdesk. Deze helpdesk is het centrale aanspreekpunt voor alle medewerkers van Opdrachtgever.

- Met betrekking tot de eerstelijns ondersteuning, beschikt Opdrachtgever zelf over een back-up oplossing bij vakantie of afwezigheid van de betreffende medewerker(s). Indien noodzakelijk, dient Opdrachtnemer de eerstelijns ondersteuning over te nemen
- De tweede- en derdelijns ondersteuning van de Opdrachtnemer werkt nauw samen met Opdrachtgever
- Opdrachtgever heeft een eigen incident managementsysteem (Topdesk) voor ICT -en functionele vragen/problemen. De Opdrachtnemer sluit hierop aan
- De dienstverlening is gebaseerd op 9x5
- Opdrachtnemer vervult een Single Point of Contact (SPoC) rol bij incidenten.