

Bijlage 4: Programma van Eisen

A: Organisatie		
A01	De ICT-Prestatie functioneert voor wat betreft aspecten van beveiliging en privacy volledig in overeenstemming met alle betreffende wet- en regelgeving (AVG, WPG ¹ en CBW ²) en andere van toepassing zijnde wetgeving c.q. normen zoals de Baseline Informatiebeveiliging Overheid 2.0 (BIO 2).	
A02	Alle door de Opdrachtnemer geleverde diensten zijn zodanig blijvend geconfigureerd dat deze voldoen aan de BIO 2 en de daaropvolgende versies. Opdrachtnemer implementeert de van toepassing zijnde verplichte overheidsmaatregelen en legt deze vast in een door Opdrachtgever vast te stellen Verklaring van Toepasselijkheid. Tevens ondersteunt Opdrachtnemer Opdrachtgever om compliant te zijn en te blijven aan de BIO-vereisten.	
A03	Opdrachtnemer beschikt over een geldig ISO 27001-certificaat voor de gehele looptijd van de Overeenkomst. Daarnaast toont Opdrachtnemer jaarlijks de werking van onderstaande beheerprocessen aan via een onafhankelijke assurance-rapportage, bijvoorbeeld een ISAE 3402 type II: - Service Level Management; - Leveranciers Management; - Security Management; - Toegang- en identiteitsbeheer; - Wijzigingsbeheer; - Continuïteitsbeheer, waaronder: Monitoring, Patch Management, Backup Management & Fail-over Management; - Incidentenbeheer; - Privacy Management.	
A04	Opdrachtnemer beheert alle licenties voor en namens Opdrachtgever behorende bij de gevraagde dienstverlening, zoals Microsoft365, Windows servers, anti-virus, etc. De licenties komen op naam van Opdrachtgever en zijn overdraagbaar bij einde Overeenkomst. De bijbehorende licentie-, onderhouds- en beheerkosten zijn integraal onderdeel van de aanbidding.	
A05	Opdrachtnemer stelt het ontwerp en de bijbehorende documentatie van haar de ICT-omgeving op verzoek van Opdrachtgever en bij de exit-procedure beschikbaar.	
A06	De Opdrachtnemer gaat akkoord met de 'Gemeentelijke Inkoop bij IT' versie 2023 (GIBIT 2023 (zie bijlage 6a). Leveranciers- of verkoopvoorwaarden worden expliciet van de hand gewezen.	
A07	Opdrachtnemer conformeert zich aan de GIBIT gerelateerde 'Gemeentelijke ICT kwaliteitsnormen' (versie 2024-1) (zie bijlage 6b). Hierin worden kwaliteitsnormen beschreven die van toepassing zijn op de te leveren dienst zoals: architectuur, interoperabiliteit, informatiebeveiliging en privacy, data-portabiliteit, infrastructuur, documentatie en e-facturering.	
A08	Opdrachtnemer verplicht zich om de 'pas toe of leg uit' vereisten voor veilig internet van het forum standaardisatie toe te passen. https://www.forumstandaardisatie.nl/open-standaarden/verplicht?domein=125 Als maatregelen niet worden toegepast, worden deze voorgelegd aan Opdrachtgever. Opdrachtnemer is verplicht om de toepasselijke infrastructuur op basis van deze vereisten te onderhouden. Minimaal jaarlijks toetst Opdrachtnemer of de infrastructuur nog aan de vereisten voldoet en rapporteert hierover aan Opdrachtgever. Opdrachtnemer voldoet ten minste aan de hier genoemde verplichte standaarden gedurende de gehele looptijd. Indien deze verplichte standaarden wijzigen zal Opdrachtnemer binnen 12 maanden voldoen aan de nieuwe standaard en de oude standaard gedurende deze zelfde periode van 12 maanden ondersteunen.	

¹ WPG: Wet PolitieGegevens

² CBW: Cyber BeveiligingsWet

A09	Het Forum Standaardisatie hanteert een aanbevolen doch niet verplichte set aan standaardisatieadviezen. Opdrachtnemer verplicht zich om de toepasselijkheid per standaard te beoordelen en indien toepasselijk toe te passen. https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen?domein=125	
A10	Opdrachtnemer levert alle gevraagde diensten (incl. data) aan Opdrachtgever vanuit aantoonbaar in de EER (Europese Economische Ruimte) gevestigd datacenter.	
A11	Assistentie DPIA (kosteloos en redelijk): - Opdrachtnemer verleent, zonder afzonderlijke vergoeding, redelijke en tijdige medewerking aan de uitvoering van een Data Protection Impact Assessment (art. 35 AVG) en – waar van toepassing – voorafgaande raadpleging (art. 36 AVG) voor zover deze van toepassing is op de door Opdrachtnemer te leveren/te beheren ICT-Prestatie. Deze medewerking omvat ten minste het beschikbaar stellen van actuele en volledige documentatie (architectuur, gegevensstromen, beveiligingsmaatregelen, subverwerkerslijst en verwerkerslocaties), het invullen van DPIA-vragenlijsten, deelname aan interviews/workshops en het leveren van een voorstel voor passende maatregelen. Acceptatiecriterium: - De DPIA-rapportage en een geaccordeerd maatregelenplan maken onderdeel uit van de acceptatie. Acceptatie vindt uitsluitend plaats indien geen 'hoog' rest-risico resteert dat aan Opdrachtnemer toerekenbaar is, of indien Opdrachtgever dit rest-risico expliciet besluit te accepteren. Toerekenbaarheid & scope: - Risico's die (geheel of gedeeltelijk) voortkomen uit inrichting, processen of systemen buiten de invloedssfeer van Opdrachtnemer worden door Opdrachtnemer voorzien van een schriftelijk mitigatie-advies; - De besluitvorming en uitvoering daarvan liggen bij Opdrachtgever. Meerwerksgrens (proportionaliteit): - Indien mitigerende maatregelen leiden tot scope-uitbreiding of structurele aanvullende werkzaamheden die redelijkerwijs buiten de overeengekomen ICT-Prestatie vallen, worden deze uitgevoerd volgens het wijzigingsmechanisme tegen de overeengekomen tarieven, tenzij de noodzaak is veroorzaakt door een toerekenbaar tekortschieten van Opdrachtnemer.	
A12	Beschikbaarheid Servicedesk: - Tijdens kantooruren: maandag t/m vrijdag van 07:30 tot 17:30 uur; - Tijdens avondopenstelling van Publiekszaken op donderdagavond van 17:30 tot 20:00 uur; - 24/7 Nederlandstalige wachtdienst beschikbaar. Bereikbaarheid Servicedesk: - Via telefoon, e-mail en serviceportaal; - Telefonische oproepen worden in 95% van de gevallen binnen 3 minuten beantwoord door een Servicedeskmedewerker van Opdrachtnemer. Kwaliteit van dienstverlening: - De Servicedesk is 'skilled' en oplossingsgericht; - Wordt uitgevoerd vanaf een locatie in Nederland; - Registratie en rapportage vinden plaats in de Nederlandse taal; - De registraties van meldingen zijn in sync met de registraties in het ticketsysteem van Opdrachtgever (in NeoForce). Taken van de Servicedesk: - Registratie, beantwoording en oplossing van incidenten, problemen en vragen volgens ITIL; - Herstel van verstoringen op een effectieve en efficiënte manier binnen afgesproken servicelevels; - Afhandeling van incidenten, problemen, wijzigingen en verzoeken in overleg met het meldpunt van de Opdrachtgever; - Opbouwen van een kennisbank als een centrale, georganiseerde opslagplaats van informatie, zoals handleidingen, oplossingsgidsen en veelgestelde vragen.	

	Inzage voor Opdrachtgever: - Volledige inzage in de registratie en afhandeling van incidenten, problemen, wijzigingen en serviceverzoeken; - Inzage in de kennisbank.	
A13	De in het Programma van Eisen opgenomen functionele en niet-functionele eisen vormen gezamenlijk het uitgangspunt voor de gevraagde dienstverlening. Tijdens de implementatie kunnen technische, organisatorische of operationele inzichten ontstaan die invloed hebben op de haalbaarheid van (delen van) de eisen. Als blijkt dat bepaalde eisen niet volledig of gelijktijdig gerealiseerd kunnen worden, wordt dit tijdig en transparant besproken tussen Opdrachtgever en Opdrachtnemer. Opdrachtnemer stelt zich proactief op in het signaleren van mogelijke conflicten of beperkingen en doet voorstellen voor alternatieve oplossingen die zoveel mogelijk recht doen aan de oorspronkelijke doelstellingen. Afwijkingen van de eisen worden uitsluitend doorgevoerd na schriftelijke instemming van de Opdrachtgever, waarbij de impact op functionaliteit, kwaliteit, planning en kosten wordt onderbouwd.	
A14	Opdrachtgever heeft het recht om, in overleg met Opdrachtnemer, een onafhankelijke security-audit, scan of pentest te laten uitvoeren. Opdrachtnemer verleent hieraan volledige medewerking. Als uit deze toetsing gebreken blijken die aantoonbaar binnen de verantwoordelijkheid van Opdrachtnemer vallen en niet eerder door Opdrachtgever expliciet als afwijkingen zijn geaccepteerd, worden deze kosteloos door Opdrachtnemer hersteld. Frequentie, scope en timing van dergelijke toetsingen worden vooraf afgestemd.	
A15	Opdrachtgever heeft en behoudt het eigendom op alle door en voor Opdrachtgever opgeslagen data. Opdrachtnemer garandeert en waarborgt de geheimhouding van de inhoud van de data van Opdrachtgever en garandeert de bescherming van de (persoons)gegevens die worden verwerkt en houdt daarbij de richtlijnen van de AVG in acht.	
A16	Opdrachtnemer tekent de verwerkingsovereenkomst van Opdrachtgever. Opdrachtnemer voldoet aan de Meldplicht Datalekken, welke is vastgelegd in de verwerkingsovereenkomst van Opdrachtgever.	
A17	Opdrachtnemer verplicht zich tot het direct informeren van Opdrachtgever over alle situaties waar data op basis van wettelijke eisen door niet-Nederlands en/of Nederlands bevoegd gezag wordt gevorderd en zal deze niet zonder toestemming van Opdrachtgever leveren.	
A18	Opdrachtgever verwacht van Opdrachtnemer de rol van een ICT-partner die: - Meedenkt vanuit het bedrijfsbelang van Opdrachtgever, zoals ICT-vraagstukken en innovaties; - Zich gedraagt als onderdeel van het interne team Informatisering en Automatisering; - Meehelpt met het stellen van kaders voor inpasbaarheid van systemen en software in de ICT-infrastructuur.	
A19	Opdrachtgever is nadrukkelijk op zoek naar een partner die niet alleen uitvoering geeft aan de dagelijkse (beheer)activiteiten, maar die ook een proactieve rol neemt in het realiseren van verbeteringen/vernieuwingen. Een partner die tijdig nieuwe IT-ontwikkelingen signaleert en veranderende inzichten op de IT-markt toepast in (upgrades van) haar aanbod en hierover periodiek met Opdrachtgever overleg voert. Een partner die over voldoende kennis beschikt om voor specifieke ICT-vraagstukken als vraagbaak te functioneren. Opdrachtgever verwacht dat de partner continu, gevraagd en ongevraagd, haar kennis en kunde inbrengt om te komen tot de voor Opdrachtgever best passende ICT-inrichting.	
A20	Voor uitvoering van werkzaamheden dient een vast team van medewerkers bij Opdrachtnemer beschikbaar te zijn dat deskundig is voor wat betreft de ICT-omgeving van Opdrachtgever, welke allen gedurende de looptijd van de Overeenkomst een geldige verklaring omtrent het gedrag hebben (VOG). De Inschrijver dient zelf voor de aanvraag en instandhouding van de VOG zorg te dragen.	

A21	De prijs kan gedurende de looptijd van de Overeenkomst jaarlijks worden geïndexeerd conform GIBIT-voorwaarden 2023. Deze indexatie kan voor het eerst worden toegepast op 1 januari 2027.	
A22	Opdrachtnemer draagt de zorg dat de dienstverlening aan Opdrachtgever en alle benodigde onderdelen daarvoor en de van dienstverlening afhankelijke interne processen van Opdrachtgever te allen tijde aan van toepassing zijnde Nederlandse en Europese wet- en regelgeving voldoet.	
A23	Opdrachtnemer zorgt voor de back-up van de gehele omgeving, zoals de Microsoft 365, de servers in het datacenter en evt. servers in Azure. Binnen de scope van de dienstverlening dienen de back-ups versleuteld te zijn, dienen periodieke (preventieve) restore-tests te worden uitgevoerd, evenals ook expliciete restore-verzoeken vanuit Opdrachtgever.	
A24	Opdrachtgever beschikt over een 'Reisdocumenten Aanvraag- en Archiefstation' (RAAS) server. Deze blijft op locatie van opdrachtgever. Opdrachtgever blijft zelf verantwoordelijk voor het beheer en de back-up van deze server.	
A25	Opdrachtnemer meldt significante cybersecurity-incidenten onverwijld, uiterlijk binnen 24 uur na ontdekking, aan Opdrachtgever. Boetes of sancties door te late melding zijn volledig voor rekening van Opdrachtnemer	
B: Connectiviteit		
B01	Onderdeel van de ICT-Prestatie is dat Opdrachtnemer de performance en beschikbaarheid van de dienstverlening van de WAN-leverancier dient te monitoren. Daarmee wordt bedoeld: het proactief benaderen van de WAN-leverancier wanneer de dienstverlening is verstoord, om een toelichting te krijgen op de geconstateerde storing. Rapportage over deze monitoring maakt deel uit van de maandelijkse rapportage.	
B02	Onderdeel van de ICT-Prestatie is dat Opdrachtnemer de coördinatie op zich neemt wanneer er een storing is geconstateerd waar zowel de WAN-leverancier als ander partijen bij betrokken zijn. Opdrachtnemer houdt Opdrachtgever gedurende de storingsafhandeling op de hoogte van de voortgang.	
B03	Onderdeel van de ICT-Prestatie is dat Opdrachtnemer het LAN- en Wifi-netwerk van Opdrachtgever beheert (accesspunten, switches, routers etc. exclusief bekabeling). Dit is inclusief het up-to-date houden van c.q. vervangen van alle componenten en besturingssystemen gedurende de looptijd van de Overeenkomst als onderdeel van de ICT-Prestatie. Na afloop van de Overeenkomst worden deze componenten en besturingssystemen om niet overgedragen aan Opdrachtgever.	
B04	Opdrachtgever maakt gebruik van GovRoam (landelijk netwerk voor ambtenaren). Opdrachtnemer ondersteunt deze mogelijkheid en beheert het deel dat relevant is voor Opdrachtgever. De hiervoor benodigde RADIUS-server mag niet als Public-Cloud-oplossing worden aangeboden.	
B05	De geboden Oplossing biedt ondersteuning voor IPv4 en IPv6. Intern wordt beperkt tot IPv4.	
B06	Van Opdrachtnemer wordt geëist dat zij als onderdeel van ICT-Prestatie het netwerk op basis van een nog te ontwikkelen segmentatie ontwerp zo geconfigureerd dat er verschillende segmenten ontstaan; zogenoemde Virtual Local Area Networks (VLAN's). Het verkeer tussen de verschillende segmenten dient gereguleerd en/of geblokkeerd te worden via een beveiligd koppelvlak. Computers kunnen worden geïdentificeerd, gecontroleerd en automatisch in het juiste segment geplaatst op basis van Network Access Control (NAC).	
B07	Opdrachtnemer verleent medewerking om tot een actieplan te komen zodat Zero Trust kan worden toegepast bij toekomstige vervangings- of uitbreidingsinvesteringen. Het actieplan maakt duidelijk in welke tijdspanne veranderingen mogelijk zijn en hoeveel werk/investeringen ervoor nodig is. Opdrachtnemer en Opdrachtgever hanteren de Zero-trust beveiligings-uitgangspunten. Ofwel: never trust, always verify. Dit geldt o.a. voor authenticatie en autorisatie (MFA en blokkeren onbekende apparatuur) als ook voor het realiseren van netwerksegmentatie binnen de beheerde infrastructuur en het actief monitoren van apparaten, gebruikers en services.	

B08	Opdrachtnemer is in staat om een Digikoppeling, Gemnet en koppelingen via het GGI-netwerk te ontsluiten om te kunnen integreren en koppelen met overheidsdiensten en -voorzieningen.	
B09	Daar waar server/applicaties die worden gehost via en/of bij Opdrachtnemer connectiviteit benodigen naar landelijke voorzieningen via Gemnet en/of DigiNetwerk voorziet Opdrachtnemer voor Opdrachtgever in deze connectiviteit.	
B10	Opdrachtnemer migreert en beheert de servers voor het netwerkbeheer (o.a. DHCP en interne DNS services).	
B11	De e-mailberichten moeten voordat ze de organisatie van Opdrachtgever binnenkomen of verlaten gecontroleerd zijn op spam en virussen. Bij (netwerk)problemen dienen e-mails van en aan Opdrachtgever gebufferd te worden, zodat deze na het oplossen van de storing alsnog bezorgd kunnen worden.	
B12	De infrastructuur van Opdrachtgever dient optimaal beveiligd te zijn tegen kwaadaardige programmatuur zoals bijvoorbeeld virussen en malware. Opdrachtnemer moet ervoor zorgen dat de beveiliging voldoende is, volgens de meest recente BIO 2 normen en richtlijnen. De kosten hiervoor maken integraal onderdeel uit van deze Opdracht en dienen in het maandbedrag opgenomen te zijn.	
B13	Gemeentelijke softwareleveranciers moeten de beschikking kunnen krijgen over een terdege beveiligde VPN-verbinding waarmee zij toegang verkrijgen tot de (server)omgeving van Opdrachtgever. Opdrachtnemer dient de tijdelijke toegang gecontroleerd toe te staan. Dergelijke verzoeken worden gelogd. Sterke authenticatie: - Toegang via VPN is uitsluitend toegestaan met Multi-Factor Authenticatie (MFA), gekoppeld aan Microsoft Entra ID of een gelijkwaardig IdP. Autorisatieproces: - Elke toegang wordt vooraf schriftelijk of via een geautomatiseerd goedkeuringsproces door Opdrachtgever geautoriseerd; - Toegang is tijdgebonden (maximaal 1 dag) en vervalt automatisch na afloop. Logging en monitoring: - Alle toegangsverzoeken en sessies worden volledig gelogd (inclusief datum/tijd, gebruiker, IP-adres, uitgevoerde acties); - Logbestanden worden minimaal 12 maanden bewaard en zijn op verzoek van Opdrachtgever beschikbaar. Beveiligingsstandaarden: - VPN-verbinding maakt gebruik van versleuteling volgens actuele NCSC-richtlijnen (bijv. TLS 1.3 of IPsec met AES-256); - Alleen apparaten die voldoen aan vooraf gedefinieerde beveiligingscriteria (bijv. up-to-date OS, antivirus) krijgen toegang. Segmentatie en least privilege: - Leveranciers krijgen uitsluitend toegang tot de strikt noodzakelijke systemen of segmenten (principle of least privilege); - Toegang tot productieomgevingen is alleen toegestaan na expliciete goedkeuring van Opdrachtgever en onder toezicht van Opdrachtnemer. Incidentrespons: - Onregelmatigheden of misbruik worden direct gemeld aan Opdrachtgever conform het security-incidentproces.	
B14	De Opdrachtnemer zorgt ervoor dat alle diensten die via internet toegankelijk zijn en door de Opdrachtnemer worden geleverd, een score van 100% behalen op internet.nl. Dit geldt eveneens voor de aangeboden e-mailfunctionaliteiten.	
B15	Opdrachtnemer draagt zorg voor de traceerbaarheid van eventuele incidenten die voortkomen uit connectiviteit via logging.	
C: Werkplek		
C01	Uitgangspunt voor het (technisch) beheer van de werkplek oplossing is de huidige werkplek oplossing (moderne werkplekconcept van Microsoft in combinatie met Liquit).	

	Opdrachtnemer is als onderdeel van de ICT-Prestatie verantwoordelijk is voor het (technisch) beheer van de werkplekoplossing van Opdrachtgever. Hieronder valt, is echter niet beperkt tot: - Beheer identiteit en toegang (incl. aanmaken, wijzigen, verwijderen van accounts en rechten) - Microsoft 365 tenants (gemeente Meerssen en Raad Meerssen) - Microsoft 365 services en applicaties (o.a. Teams, SharePoint, OneDrive, Exchange online) - Entra ID, Entra Connect, MFA, Conditional Access, etc. - Endpoint management (o.a. Intune / MDM / MAM) - Lijst - Werkplek-images/profielen Alle licenties die nodig zijn c.q. aangeschaft moeten worden voor de ICT-Prestatie aan Opdrachtgever dienen kosteloos overdraagbaar te zijn aan Opdrachtgever bij het eind van de Overeenkomst.	
C02	Opdrachtgever maakt gebruik van Zivver als applicatie voor het veilig verzenden van (privacy)gevoelige informatie per mail. Deze applicatie is volledig geïntegreerd in de Outlook mail client. Deze functionaliteit moet ook in de aangeboden ICT-oplossing standaard aanwezig zijn voor alle gebruikers. De licenties voor Zivver worden geregeld en beschikbaar gesteld door Opdrachtgever. Opdrachtnemer zorgt voor het technisch (applicatie)beheer van Zivver.	
C03	Opdrachtnemer beheert de applicatie-ontsluiting (incl. koppelingen / autorisaties / rolebased / etc.) binnen de Microsoft 365 / Azure Tenant van Opdrachtgever. Beschikbaarheid en toegang naar de werkplek vindt plaats op basis van vastgelegde autorisaties en informatie in de tenant van de Opdrachtgever.	
C04	Inloggen in de ICT-omgeving van Opdrachtgever gebeurt altijd op basis van twee-factorauthenticatie (2FA) of multifactorauthenticatie (MFA) bij: - Accounts die vanaf het internet tot toegang verzoeken; - Functioneel beheeraccounts tijdens toegang tot specifieke essentiële systemen (ongeacht locatie); - Systeem- en/of netwerkbeheer accounts (administrator) (ongeacht locatie).	
C05	Toegangsrechten op serviceaccounts worden verleend op basis van de laagst mogelijke rechten. Het gebruik van Admin-rechten voor service-accounts dient te worden verklaard.	
C06	Opdrachtnemer is verantwoordelijk voor het beheren en monitoren conform de eisen uit de BIO2, AVG en andere wet- en regelgeving en voor het verantwoorden van de afgesproken servicelevels. Alle hieruit voortvloeiende kosten maken onderdeel uit van afgesproken prijs.	
C07	De aangeboden Oplossing dient selfservice voor eindgebruikers maximaal te ondersteunen (bijv. password-reset, onboarding), zodat eindgebruikers optimaal worden gefaciliteerd en leidinggevenden en/of het team Informatisering & Automatisering worden ontlast.	
C08	Voor de inrichting van de applicatie-omgeving (zie ook bijlage 9) kan Opdrachtnemer terugvallen op de leveranciers van de applicaties. Opdrachtnemer krijgt na gunning een volmacht van Opdrachtgever om de leveranciers te benaderen zodat Opdrachtnemer in staat is een optimale inrichting voor de applicaties te realiseren. De kosten voor het beheer van de applicaties zijn integraal onderdeel van de aangeboden dienstverlening.	
C09	Opdrachtnemer maakt gebruik van datacenters die zich bevinden in de EER en minimaal van het niveau Tier 3 of gelijkwaardig zijn. Deze datacenters zijn redundant verbonden met het WAN van Opdrachtgever. Het gebruik van een datacenter van niveau Tier 3 of gelijkwaardig is aantoonbaar door middel van een geldig certificaat of een onafhankelijke third-party assurance. De Opdrachtnemer dient op verzoek van Opdrachtgever bewijs te leveren van deze certificering of assurance, inclusief de scope, geldigheidsduur en betrokken auditinstantie. De Opdrachtgever behoudt het recht om audits uit te voeren of te laten uitvoeren door een onafhankelijke partij, met als doel de naleving van de overeengekomen	

	kwaliteits- en beveiligingsnormen te verifiëren. De Opdrachtnemer is verplicht volledige medewerking te verlenen aan dergelijke audits, waaronder toegang tot relevante documentatie, systemen en personeel. Indien uit een audit blijkt dat de Opdrachtnemer niet voldoet aan de gestelde eisen van 'Tier 3 of gelijkwaardig', behoudt de Opdrachtgever zich het recht voor om corrigerende maatregelen te eisen. Bij herhaalde en ernstige tekortkomingen kunnen contractuele sancties worden opgelegd, waaronder financiële boetes, opschorting van dienstverlening of ontbinding van de Overeenkomst.	
C10	Alle benodigde hardware, software, licenties, ondersteunende applicaties/componenten, onderhoudscontracten en/of anderszins, waaronder die in het datacenter en/of Microsoft Tenant in Azure zijn onderdeel van de offerte en dienstverlening. Opdrachtgever wil op dat gebied volledig ontzorgd worden.	
C11	Aan de back-up worden de volgende minimale eisen gesteld: - Opdrachtnemer stelt dagelijks alle voor de dienstverlening benodigde informatie en systemen via een back-up veilig. Dat is inclusief alle data in de Microsoft-cloud. - Instellingen van o.a. actieve netwerkcomponenten worden periodiek veiliggesteld; - Recovery Point Objective (RPO): maximaal 4 uur - Recovery Time Objective (RTO): maximaal 24 uur - Alle benodigde netwerkvoorzieningen zijn binnen de RTO periode van 24 uur operationeel - Opdrachtnemer controleert dagelijks de kwaliteit en bruikbaarheid van de back-up. - Opdrachtnemer is verantwoordelijk voor het inrichten en beheren van een back-up die bestendig is tegen cyberdreigingen (ransomware en/of andere security issues) en calamiteiten zoals brand. - Er zijn 0 (nul) fouten in de back-up- en herstelprocessen toegestaan. - De back-up retentie periode is 1 jaar. Na de retentieperiode worden verjaarde back-ups vernietigd.	
C12	Tussen de primaire en secundaire (back-up) locatie zitten meerdere kilometers afstand in vogelvlucht.	
C13	Opdrachtnemer moet periodiek (per kwartaal) een restore test uitvoeren en het resultaat van de test rapporteren aan Opdrachtgever als onderdeel van de servicelevel rapportage. Hierbij is het niet noodzakelijk dat alle servers/omgevingen tegelijkertijd onderdeel zijn van de restore test. Opdrachtnemer doet een voorstel, op basis van zijn best practices, hoe deze restore testen worden uitgevoerd. Jaarlijks moet de gehele omgeving een keer onderdeel zijn geweest van de periodieke restore testen. Integraal onderdeel van de restoretest is ook het testen van de werking van alle noodzakelijke verbindingen. Opdrachtgever is verantwoordelijk voor het testen van de uitwijkvoorziening.	
C14	Opdrachtnemer beheert de centrale configuratie van de werkplekken (zoals bijvoorbeeld Intune en Ligit).	
C15	Opdrachtnemer zorgt ervoor dat de werkplek van de gebruiker in de thuiswerkomgeving (laptop van Opdrachtgever) via een beveiligde omgeving met een VPN-connectie (incl. 2FA/MFA) verbonden wordt met de infrastructuur van Opdrachtgever.	
C16	Opdrachtnemer is verantwoordelijk voor de volledige inrichting van Endpoint management voor de werkplekken.	
C17	Opdrachtnemer voorziet in een continue Monitoring en Response oplossing (SIEM/SOC) die van toepassing is op de gehele infrastructuur. Vanuit deze voorziening vindt monitoring, detectie en alarmering van verdachte gebeurtenissen plaats richting de Opdrachtnemer en Opdrachtgever. Opdrachtgever moet vanuit haar verantwoordelijkheden regie kunnen voeren op de responseactiviteiten die door opdrachtnemer worden uitgevoerd. Als monitoringbron komen de volgende items (niet limitatief) in aanmerking: - Gebruikers-, admin- en systeemaccounts; - Servers, switches, routers, firewalls, wifi access points en -controllers;	

	- Het Intrusion Detection System/Intrusion Prevention System (IDS/IPS), de proxyserver - De Domain-controller; - Werkplekken (antivirus); - Backup en storage; - Toekomstige in overleg te bepalen bronnen. De bewaartermijn van de data die gebruikt wordt binnen de SIEM-omgeving is: - Zes maanden voor logging waar geen events, fraude, crisissituaties etc. uit voortvloeien; - Overige logging zo lang bewaren als noodzakelijk is voor de afhandeling van het betreffende incident, alsmede de afhandeling van eventuele claims in vervolg op het incident. De kosten voor de logging (genereren en verwerken) en de dataopslag maken integraal onderdeel uit van deze Opdracht en dienen in het maandbedrag opgenomen te zijn.	
C18	Opdrachtgever verwacht een proactieve houding van Opdrachtnemer in het uitvoeren van patchmanagement. Het patchmanagement moet voor Opdrachtgever te allen tijde inzichtelijk zijn.	
C19	Opdrachtnemer draagt zorg voor de inrichting van een testomgeving/testimage/testgebruikers voor de werkplek zodat uitbreiding of aanpassing van applicaties en/of functionaliteit getest kan worden voordat deze wordt uitgerold bij de medewerkers conform BIO2.	
D: Governance		
D1	Opdrachtgever is voor alle gebruikersvragen Single Point of Contact (SPoC) gedurende kantoor tijden (zie Eis A12). Opdrachtnemer is voor alle in de scope gedefinieerde werkzaamheden, voor alle leveranciers SPoC, zowel binnen als buiten kantooruren.	
D2	Opdrachtgever is de eigenaar van het ontwerp en de volledige documentatie van haar ICT-omgeving, inclusief configuratie instellingen. Volledige en technische (low-level) documentatie van de gerealiseerde oplossing wordt door Opdrachtnemer na implementatie aan Opdrachtgever bezorgd. Architectuurplaten dienen in Archi/Archimate en/of Visio formaat te zijn. Het bijhouden van deze documentatie maakt deel uit van de opdracht. Dit geldt voor alle onderdelen van de ICT-omgeving die Opdrachtnemer in beheer krijgt.	
D3	Opdrachtgever maakt gebruik van NeoForce als servicemanagementsysteem voor de afhandeling van incidenten en wijzigingen. Het doorzetten van en het verder afhandelen van meldingen bij Opdrachtnemer moet geautomatiseerd kunnen plaats vinden tussen het servicemanagementsysteem van Opdrachtgever (NeoForce) en het servicemanagementsysteem van Opdrachtnemer. In het servicemanagementsysteem van Opdrachtnemer moet de registratie en afhandeling van incidenten, problemen, wijzigingen en serviceverzoeken volledig inzichtelijk, traceerbaar en auditeerbaar zijn voor opdracht.	
D4	De volgende beheerprocessen vallen binnen de scope van de dienstverlening van de Opdrachtnemer: - Alle ICT-beheerprocessen die voor betrouwbare levering van de dienst zijn vereist. - De leverancier voorziet in opzet, bestaan en werking van alle op de dienst van toepassing zijnde beheerprocessen en toont de werking jaarlijks aan via een onafhankelijke assurance-rapportage, bijvoorbeeld een ISAE 3402 type II. Deze assurance rapportage bevat minimaal de volgende beheerprocessen; - o Service Level Management; - o Leveranciers Management; - o Security Management; - o Toegang- en identiteitsbeheer; - o Wijzigingsbeheer;	

	○ Continuïteitsbeheer, waaronder: Monitoring, Patch Management, Backup Management & Fail-over Management; ○ Incidentenbeheer; ○ Privacy Management. - Licentiebeheer (o.a. Microsoft 365, Azure Entra-ID) De volgende beheerprocessen vallen buiten de scope van de dienstverlening van de Opdrachtnemer: - De organisatorische, procedurele en fysieke BIO 2 beveiligingsmaatregelen die door Opdrachtgever opgepakt moeten worden; - Kabelmanagement eindgebruikers (werkplekken, printers, etc.); - Functioneel applicatiebeheer en functioneel relatiemanagement; - Beheer van de MFP's; - Beheer van de GEMNET-verbinding; - Beheer van de bedrijfsspecifieke licenties.	
D5	De Servicedesk van Opdrachtgever is verantwoordelijk voor de 1^{ste} lijns gebruikersondersteuning van de medewerkers en is voor de gebruikers SPoC voor gebruikersvragen, -ondersteuning en afhandeling meldingen. De Servicedesk van de Opdrachtgever verzorgt de eerste classificatie en prioriteitsstelling van de melding en bewaakt de verdere afhandeling van de melding. Opdrachtnemer biedt een centrale Nederlandstalige Servicedesk voor de 2^{de} en 3^{de} lijns ondersteuning en vormt het aanspreekpunt voor medewerkers van het team I&A van Opdrachtgever tijdens kantooruren. Bereikbaarheid via telefoon, email en serviceportaal is minimaal vereist.	
D6	Opdrachtnemer biedt buiten kantooruren een 24x7 calamiteitendienst/dekking in geval van storingen.	
D7	Opdrachtgever verlangt heldere vastlegging van servicelevels met bijbehorende KPI's. Het betreft minimaal (lees: is niet beperkt tot): - Support venster (reguliere kantoor tijden) - Standby venster (buiten kantoor tijden en/of feestdagen) - Service venster (ICT-omgeving) - Onderhoudsvenster (incl. communicatie procedure) - Beschikbaarheidspercentage (ICT-omgeving) - Performance garanties (incl. kwaliteit) En aangaande storingsopheffingen (minimaal) het volgende: - Categorieën (incl. omschrijving classificatie) - Reactietijden (i.r.t. categorie/classificatie) - Hersteltijden (i.r.t. categorie/classificatie) - Status updates (en/of communicatie)	
D8	Opdrachtnemer voert het technisch beheer uit over de gehele ICT-infrastructuur van Opdrachtgever, bestaande uit (maar niet uitputtend): - Servers (fysiek en virtueel) - Storage - Backup (3-2-1-1-0 strategie³) - Connectivity ○ Verbinding met Heuvelland glasvezelring van Eurofiber (Solido) ○ LAN, Wifi en WLAN-verbindingen ○ Firewall - Virtualisatie - Intune / Autopilot - Lijkt of vergelijkbaar - Antivirus - Anti-spam - Security Information and Event Management (SIEM) (zie ook Eis C17)	
D9	De navolgende diensten en producten maken onderdeel uit van de aan te bieden oplossing door Opdrachtnemer:	

³ 3-2-1-1-0: Ten minste 3 kopieën van gegevens, Opslaan van kopieën op ten minste 2 verschillende media, Ten minste 1 kopie van de gegevens moet extern worden opgeslagen, Ten minste 1 kopie van de gegevens moet offline worden opgeslagen, 0 fouten in de back-up- en herstelprocessen

	- Housing en hosting - Monitoring en rapportage over o.a. - o Prestaties/capaciteit - o Security Information and Event Management (SIEM) (zie ook Eis C17) - o Back-ups - o Security threats - o Hardening en patchmanagement - o Licenties - Health en security checks - o Periodieke pen-testen - o Checks op beheersmaatregelen (onafhankelijke assurance-rapportage, zoals bijv. ISAE type 2) - Technisch applicatiebeheer - Continuïteit - o Back-up (waaronder immutable) - o Restore van backups - o Uitwijktests - Ketenverantwoordelijkheid - o Voor alle activiteiten in scope - o Voor third party leveranciers van Opdrachtnemer - o Alsmede regie op afstemming activiteiten met applicatieleveranciers - Security - o BIO 2.0 (of elke vigerende vervolgversie) - o ISO-27001	
D10	Opdrachtnemer is verantwoordelijk voor het up to date houden van de gehele ICT-infrastructuur die door Opdrachtnemer wordt aangeboden. Daarbij wordt verstaan: - Actueel houden van de systeemsoftware; - Actueel houden van alle componenten van de ICT-infrastructuur; - De omgeving voorzien van alle noodzakelijke updates om aan de afgesproken services en (beveiligings)eisen te kunnen voldoen; - Actueel houden van documentatie.	
D11	Integraal onderdeel van de dienstverlening (en de bijbehorende kosten) is het doorvoeren van standaard wijzigingen. Standaard wijzigingen dienen door Opdrachtnemer binnen de afgesproken servicenormen uitgevoerd en werkend opgeleverd te worden. Daaronder wordt (niet limitatief) verstaan: - Het doorvoeren van kleine wijzigingen in bedrijfsapplicaties (versieverhoging na de eerste 'punt'); - Het doorvoeren van urgente security patches; - DHCP-aanpassingen; - Interne DNS aanpassingen; - Aanpassen certificaten na beschikbaarstelling; - VPN-wijzigingen; - Wijzigen switchpoort op locatie Meerssen; - Aanpassing firewall; - Aanvraag (in-dienst) / verwijderen (uit-dienst) / wijzigen account (functie- of rolwijziging) doorvoeren; - Aanvraag / wijzigen / verwijderen (gedeelde) mailbox (Outlook) doorvoeren; - Aanvraag / wijzigen / verwijderen agenda (Outlook) doorvoeren; - Aanvraag / wijzigen / verwijderen distributielijst (Outlook) doorvoeren; - Wijzigen autorisaties MS365 applicaties (Outlook, Teams); - Wijzigen / resetten / unlock password gebruiker; - Restore mailbox van gebruiker; - Restore bestanden van gebruiker. Tijdens de implementatie wordt gezamenlijk een uitputtende, definitieve lijst opgesteld en vastgelegd in de DAP.	
D12	Voor de niet-standaard wijzigingen geldt dat er een gedegen wijzigingenmanagement procedure is ingeregeld. Opdrachtnemer moet in staat zijn om een ingediende wijziging te classificeren en een risicoanalyse voor de ICT-omgeving te kunnen maken. De wijziging moet gedocumenteerd worden en, na accordering door de	

	Change Advisory Board (CAB) van Opdrachtgever, voor Opdrachtgever in een test situatie worden aangeboden. Na een test en een akkoord door Opdrachtgever moet de wijziging binnen 2 werkdagen in productie worden gezet.																															
D13	Opdrachtnemer levert met de aanbidding gedurende de gehele contractperiode inzicht in haar dienstverlening en richt een overlegstructuur in om met de Opdrachtgever in overleg te gaan op de verschillende niveaus: - Operationeel niveau: maandelijks Er vindt maandelijks overleg plaats tussen de Opdrachtgever en de Opdrachtnemer. Dit overleg zal vooral gaan over operationele processen en lopende issues. Input voor dit overleg is de SLA rapportage en gegevens uit de servicemanagement software. - Tactisch niveau: 1x per kwartaal Er vindt periodiek overleg plaats tussen Opdrachtgever en de Servicemanager van Opdrachtnemer. Het overleg op Tactisch niveau gaat over de geleverde serviceniveaus, wijzigingen, evaluatie en bijstelling van servicelevels, facturatie, procedures, lopende projecten, samenwerking, innovatie, vernieuwing, etc.; - Strategisch niveau: minimaal 1x per jaar Er vindt jaarlijks afstemming plaats tussen Opdrachtgever en de Accountmanager en Servicemanager van Opdrachtnemer. Het overleg op Strategisch niveau gaat over de evaluatie van het contract, klanttevredenheid, strategische ontwikkelingen, verbeterprogramma's, uitbreiding van de dienstverlening, afstemming beleidsplannen, tarieven, etc.																															
D14	Incidenten worden als volgt gecategoriseerd: Impact: Per gemeld incident kan de impact op de volgende manier door de Opdrachtgever worden bepaald. <table><tr><th>Impact</th><th>Omschrijving</th></tr><tr><td>Impact 1</td><td>Zeer hoog - Raakt alle gebruikers, Algehele verstoring</td></tr><tr><td>Impact 2</td><td>Hoog - Raakt een overgroot gedeelte van de gebruikersorganisatie, Betreft een verstoring van een kritiek bedrijfsproces</td></tr><tr><td>Impact 3</td><td>Middel - Raakt een bepaalde gebruikersgroep, Het betreft een verstoring van een belangrijk bedrijfsproces</td></tr><tr><td>Impact 4</td><td>Laag - Raakt één gebruiker, Is hinderlijk voor meerdere gebruikers maar er kan via alternatieve oplossingen worden doorgewerkt</td></tr></table> Urgentie: De urgentie wordt bepaald door de Opdrachtgever. <table><tr><th>Urgentie</th><th>Omschrijving</th></tr><tr><td>Urgentie 1</td><td>Zeer hoog - Het oplossen van een incident is vitaal en kan geen uitstel verdragen.</td></tr><tr><td>Urgentie 2</td><td>Hoog - Het verhelpen van het incident is belangrijk en dient spoedig te worden uitgevoerd.</td></tr><tr><td>Urgentie 3</td><td>Middel - Het incident is vervelend maar een oplossing kan beperkt wachten.</td></tr><tr><td>Urgentie 4</td><td>Laag - Het is niet kritisch om het incident op korte termijn op te lossen.</td></tr></table> Prioriteit Op basis van de urgentie en de impact wordt de prioriteit van het incident bepaald. <table><tr><th>Prioriteit</th><th>Impact 1</th><th>Impact 2</th><th>Impact 3</th><th>Impact 4</th></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table>	Impact	Omschrijving	Impact 1	Zeer hoog - Raakt alle gebruikers, Algehele verstoring	Impact 2	Hoog - Raakt een overgroot gedeelte van de gebruikersorganisatie, Betreft een verstoring van een kritiek bedrijfsproces	Impact 3	Middel - Raakt een bepaalde gebruikersgroep, Het betreft een verstoring van een belangrijk bedrijfsproces	Impact 4	Laag - Raakt één gebruiker, Is hinderlijk voor meerdere gebruikers maar er kan via alternatieve oplossingen worden doorgewerkt	Urgentie	Omschrijving	Urgentie 1	Zeer hoog - Het oplossen van een incident is vitaal en kan geen uitstel verdragen.	Urgentie 2	Hoog - Het verhelpen van het incident is belangrijk en dient spoedig te worden uitgevoerd.	Urgentie 3	Middel - Het incident is vervelend maar een oplossing kan beperkt wachten.	Urgentie 4	Laag - Het is niet kritisch om het incident op korte termijn op te lossen.	Prioriteit	Impact 1	Impact 2	Impact 3	Impact 4						
Impact	Omschrijving																															
Impact 1	Zeer hoog - Raakt alle gebruikers, Algehele verstoring																															
Impact 2	Hoog - Raakt een overgroot gedeelte van de gebruikersorganisatie, Betreft een verstoring van een kritiek bedrijfsproces																															
Impact 3	Middel - Raakt een bepaalde gebruikersgroep, Het betreft een verstoring van een belangrijk bedrijfsproces																															
Impact 4	Laag - Raakt één gebruiker, Is hinderlijk voor meerdere gebruikers maar er kan via alternatieve oplossingen worden doorgewerkt																															
Urgentie	Omschrijving																															
Urgentie 1	Zeer hoog - Het oplossen van een incident is vitaal en kan geen uitstel verdragen.																															
Urgentie 2	Hoog - Het verhelpen van het incident is belangrijk en dient spoedig te worden uitgevoerd.																															
Urgentie 3	Middel - Het incident is vervelend maar een oplossing kan beperkt wachten.																															
Urgentie 4	Laag - Het is niet kritisch om het incident op korte termijn op te lossen.																															
Prioriteit	Impact 1	Impact 2	Impact 3	Impact 4																												

	Urgentie 1	Prio 1	Prio 1	Prio 2	Prio 2
	Urgentie 2	Prio 1	Prio 1	Prio 2	Prio 3
	Urgentie 3	Prio 2	Prio 2	Prio 3	Prio 3
	Urgentie 4	Prio 2	Prio 3	Prio 3	Prio 4
Prestaties					
	Prioriteit	Maximale reactietijd	Maximale oplostijd	Norm	
	Prio 1	Direct bij telefonisch contact	< 4 uur binnen supportvenster	90% / maand	
	Prio 2	Direct bij telefonisch contact	< 8 uur binnen supportvenster	90% / maand	
	Prio 3	< 4 uur	< 24 uur binnen supportvenster	90% / maand	
	Prio 4	< 8 uur	< 40 uur binnen supportvenster	90% / maand	
De volgende aanvullingen gelden hierbij:					
- Maximale oplostijd gerekend vanaf het moment van aanmelding; - De gegarandeerde oplostijden gelden alleen voor de in scope activiteiten. Door derden geleverde componenten en/of diensten die de oorzaak zijn van een verstoring vallen hierbuiten; - In geval van overmacht of bij afhankelijkheden van gebruikers, leveranciers of derden in welke vorm dan ook vervalt of verschuift de oplostijd; - Voor de ondersteuning door derden gelden afwijkende reactie- en oplostijden conform de afspraken in de separate SLA's of underpinning contracts met deze partijen; - Bij Prio 1 en Prio 2 incidenten zal Opdrachtnemer alles in werking stellen om het incident zo spoedig mogelijk op te lossen; - Bij het aanmelden via mail van Prio 1 en Prio 2 incidenten geldt een reactietijd van maximaal 4 uur; - Voor Prio 1 verstoringen geldt dat wordt doorgewerkt buiten het supportvenster.					
Deze afspraken worden vastgelegd in de SLA (Service Level Agreement). Afwijkingen en bijzonderheden worden vastgelegd in de DAP (Dossier Afspraken en Procedures).					
D15	Opdrachtgever beschouwt haar ICT-infrastructuur als bedrijfskritisch en wenst hiervoor de juiste servicemaatregelen te treffen. Opdrachtnemer dient te voldoen aan de volgende parameters / service levels: - De ICT-omgeving is 24x7 beschikbaar voor gebruik met uitzondering van het onderhoudsvenster; - Beschikbaarheid van de ICT-omgeving: 99,7% per maand exclusief geplande downtijd/gepland onderhoud (gemeten over een rollend gemiddelde in een periode van 3 maanden); - Onderhoudsvenster: buiten reguliere kantooruren. Bij grotere wijzigingen wordt dit in onderling overleg afgesproken. Communicatie dient minstens 2 weken van tevoren plaats te vinden.				
D16	Opdrachtnemer verplicht zich tot de installatie van security updates (patches) binnen 3 weken nadat deze door een leverancier (lees: fabrikant) beschikbaar zijn gesteld. Kritische updates/patches, zoals zero-day dienen binnen 72u in productie doorgevoerd te worden.				
D17	Opdrachtnemer draagt de zorg voor geharde systemen. Dit houdt onder meer in dat alle niet noodzakelijke functionaliteiten zijn verwijderd of uitgeschakeld en dat de toegang voor standaard Admin-accounts is geblokkeerd en als dat niet mogelijk is, de toegang van Admins wordt voorzien door zeer sterke authenticatie technieken (bv. FIDO2 passkey tokens).				

D18	Opdrachtgever heeft het recht om bij calamiteiten via Service Level Rapportages van derden toegangscontrole en geleverde servicelevels van de Datacenters in te zien, die betrekking heeft op de ICT-dienst van Opdrachtgever.	
D19	Opdrachtgever ontvangt maandelijks een beveiligingsoverzicht van alle gebruikers (rechten, wachtwoordwissel of -methodiek). Dit is incl. de administraties en service-accounts. Opdrachtgever ontvangt maandelijks rapportages betreffende backup/restore, patching, etc. Bij voorkeur kan de opdrachtgever dit zelf raadplegen in een portaal.	
D20	Opdrachtgever en Opdrachtnemer hebben de plicht tot wederzijdse geheimhouding.	
D21	Alle data in de nieuwe ICT-omgeving dient ongeacht de wijze van hosting binnen het grondgebied waarop de Europese regelgeving van toepassing is opgeslagen te worden conform Nederlandse wetgeving.	
D22	Op regelmatige basis kan Opdrachtgever specifieke wensen en/of eisen t.a.v. security kenbaar maken bij Opdrachtnemer. Na overleg zullen deze worden opgenomen in het Dossier Afspraken en Procedures (DAP)	
D23	Leverancier verleent alle medewerking aan een door de Opdrachtgever geïnitieerde en gefinancierde audit. Opdrachtgever bepaalt het bereik van de audit. Eventuele geconstateerde gebreken ten aanzien van de afgesproken dienstverlening dient door Opdrachtnemer om niet te worden hersteld.	
D24	Per maand dient de Opdrachtnemer aan Opdrachtgever te rapporteren over de dienstverlening. De Opdrachtnemer levert daartoe maandelijks een overzicht van de service, de overeengekomen SLA en DAP en het behaalde niveau. De service rapportage bevat minimaal de volgende onderwerpen: - Aantal 2^{de} en 3^{de} lijns incidenten, problemen (vragen, storingsmeldingen, klachten) per kalendermaand; - Aantal afgesloten incidenten, problemen binnen/buiten de gesteld hersteltijd; - Aantal openstaande incidenten en problemen; - Aantal wijzigingen (uitgevoerd en openstaand); - Beschikbaarheid van de infrastructuur in de afgelopen periode (3 maanden); - Afwijkingen van het overeengekomen serviceniveau; - Lopende en komende ontwikkelingen (trends, belangrijke vervangingen, groot onderhoud, etc.); - Monitoring; - Patchmanagement; - Resultaat van de restoretests (per kwartaal); - Informatie m.b.t. schaalbaarheid (trends).	
D25	Bij het beëindigen van de Overeenkomst wordt van de Opdrachtnemer geëist dat deze meewerkt aan de transitie naar een nieuwe leverancier. De Opdrachtnemer levert hiervoor een exitplan aan uiterlijk 3 maanden na livegang. De kosten voor het maken en onderhouden van het exitplan zijn onderdeel van de inschrijfprijs. In dit exitplan beschrijft de Opdrachtnemer minimaal het volgende: - De aanpak van de transitie van de werkomgeving van de Opdrachtnemer naar de werkomgeving van de nieuwe leverancier (data, documenten en applicaties); - Welke projectorganisatie de Opdrachtnemer hierin voorziet; - Planning en (maximale) doorlooptijd; - Overdracht, vernietiging en verwijdering van de oude omgeving en bevestiging hiervan; - Randvoorwaarden; - Een kostenindicatie voor de uitvoering van het exitplan; - Overige punten die volgens de Opdrachtnemer relevant zijn voor het exitplan. Voor de uitvoering van het exitplan geldt artikel 26 van de GIBIT-voorwaarden.	
D26	Vanuit het perspectief van de Opdrachtnemer geldt als randvoorwaarde dat Opdrachtnemer een nieuwe leverancier voor IT-diensten voorafgaand aan het einde van de Overeenkomst toegang en beheerrechten geeft tot de Microsoft tenant van de Opdrachtgever. Hierbij faciliteert Opdrachtnemer de nieuwe leverancier maximaal in de door deze nieuwe leverancier uit te voeren migratiestappen.	

D27	Bij einde van de Overeenkomst stelt Opdrachtnemer gegevens van Opdrachtgever weer beschikbaar aan Opdrachtgever (in een door Opdrachtgever nader te bepalen de facto format) en verleent hieraan tijdig zijn volledige medewerking. Opdrachtnemer draagt vervolgens verder zorg voor de vernietiging van de gegevens van Opdrachtgever van zijn systemen.	
D28	Om te voorkomen dat Opdrachtgever na beëindiging van de Overeenkomst op enig moment zonder dienstverlening komt te zitten, verklaart Opdrachtnemer reeds dat Opdrachtgever en de nieuwe leverancier na expiratie van de Overeenkomst een periode wordt geboden van maximaal twee keer zes (6) maanden om de nieuwe dienstverlening te implementeren. Dit betekent dat de dienstverlening nog maximaal twaalf (12) maanden na contracttermijn kan doorlopen.	
D29	Bij beëindigen van de Overeenkomst overhandigt Opdrachtnemer aan Opdrachtgever en/of de nieuwe leverancier alle relevante configuratiegegevens, documentatie en wachtwoorden. Data in de service managementtool is eigendom van Opdrachtgever en dient overgedragen te worden aan Opdrachtgever in een nader af te spreken format.	

E: Optioneel: Beheer Oracle		
E01	Op dit moment maakt Opdrachtgever nog gebruik van een Oracle-database ten behoeve van één applicatie. De Opdrachtnemer neemt de huidige Oracle-databaseomgeving over en biedt een alternatieve omgeving aan die past binnen de overeengekomen dienstverlening. De Opdrachtgever is eigenaar van de bijbehorende Oracle-licenties en wenst dit ook te blijven. Van de Opdrachtnemer wordt verwacht dat deze Oracle als dienst aanbiedt, waarbij de volgende verantwoordelijkheden gelden: Technisch en functioneel beheer: - Zorgdragen voor de operationele continuïteit van de Oracle-databaseomgeving, inclusief monitoring, back-ups, herstelprocedures en performance-optimalisatie; - Uitvoeren van updates, patches en upgrades conform het Oracle-licentiebeleid en de beveiligingsrichtlijnen van de Opdrachtgever; - Implementeren van toegangsbeheer op basis van het principe van “least privilege” en gebruik van rolgebaseerde toegangscontrole (RBAC); - Bijhouden van auditlogs van alle systeemactiviteiten, inclusief toegangspogingen en configuratiewijzigingen, en zorgen voor veilige opslag en periodieke audits. Licentiebeheer en compliance: - De Opdrachtnemer is verantwoordelijk voor het correct toepassen van het Oracle-licentiebeleid binnen de aangeboden dienst; - Hoewel de Opdrachtgever eigenaar blijft van de licenties, dient de Opdrachtnemer te zorgen voor naleving van de licentievoorwaarden, inclusief rapportage over gebruik en compliance; - Indien aanvullende licenties nodig zijn voor de aangeboden dienst, dient de Opdrachtnemer dit tijdig te signaleren en af te stemmen met de Opdrachtgever. Beveiligingsincidenten dienen direct gemeld te worden, inclusief aard, impact en genomen maatregelen. - De Opdrachtnemer dient een getest disaster recovery plan te hanteren met de RTO/RPO-afspraken, die gelden voor de gehele ICT-dienst.	

F: Optioneel: 1^{ste} lijns Gebruikersondersteuning (vervanging Servicedesk ICT)		
F01	Optioneel kan de 1^{ste} lijns gebruikersondersteuning van de medewerkers en de rol van SPoC voor gebruikers worden overgedragen aan Opdrachtnemer, Uitgangspunten daarbij zijn: - Invulling van de taken zoals beschreven in bijlage 10: "Taken servicedesk"; - Ondersteuning tijdens kantoortijden (zie Eis A12), waarvan drie (3) dagdelen per week op locatie Gemeentehuis Meerssen.	
F02	Als Opdrachtnemer voor het registreren van meldingen gebruik wil maken van een eigen ticketsysteem, dan moeten de lopende en reeds afgesloten meldingen uit NeoForce (ticketsysteem van Opdrachtgever) worden geïmporteerd naar dit ticketsysteem.	
F03	De aan te leveren service rapportages wordt uitgebreid met: - Aantal 1^{ste} lijns incidenten, problemen (vragen, storingsmeldingen, klachten) per kalendermaand;	