Programma van Eisen

PvE nr.	Eis
	Informatieveiligheid
E001	Onderliggende ICT-componenten, zoals hardware, software enz., waarop de ICT-prestatie is gebouwd en draait dienen altijd door de oorspronkelijke opdrachtnemer/fabrikant van de betreffende hardware/software/framework/ etc. ondersteund te zijn zodanig dat te allen tijde support is gewaarborgd.
E002	Voor het uitvoeren van de ICT-prestatie wordt gebruik gemaakt van systemen die zijn gehardened volgens CIS Benchmarks of soortgelijke richtlijnen. Dit wil zeggen dat overbodige functies, software van het besturingssysteem, technische poorten, etc. zijn uitgezet of van het systeem zijn verwijderd.
E003	De ICT-prestatie wordt minimaal maandelijks gescand op kwetsbaarheden. De resultaten van deze kwetsbaarheidsscans worden gerapporteerd aan de opdrachtgever. Vastgestelde kwetsbaarheden worden geclassificeerd conform de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) (https://vulnerabilities.ncsc.nl/ncsc-score.html) en, waar van toepassing, volgens de CVSS-classificatie (https://nvd.nist.gov/vuln-metrics/cvss). Er is sprake van een spoedpatch indien de kans op misbruik en de verwachte schade beide hoog zijn. In dat geval geldt het volgende: de patch dient uiterlijk binnen 24 uur na de melding geïnstalleerd te zijn. Kwetsbaarheden met een classificatie ‘High’ of ‘Critical’ worden binnen 48 uur na vaststelling gemitigeerd, of – indien een structurele oplossing afhankelijk is van een door de leverancier of fabrikant beschikbaar te stellen beveiligingsupdate – binnen 48 uur na het beschikbaar komen van deze update verholpen. Indien het binnen deze termijnen niet mogelijk is een kwetsbaarheid te mitigeren of structureel op te lossen, treft de leverancier passende tijdelijke mitigerende maatregelen. Deze maatregelen, inclusief een risicoafweging en een herstelplanning, worden vastgelegd en afgestemd met de opdrachtgever. Reguliere updates: Minder kritische beveiligingsupdates worden meegenomen in de eerstvolgende reguliere onderhoudscyclus (release window)
E004	De beveiliging van de ICT-prestatie wordt minimaal jaarlijks getest middels een pentest uitgevoerd door een onafhankelijke binnen de sector erkende partij in opdracht van opdrachtnemer. De resultaten van de pentest en de opvolging daarvan worden volledig kosteloos gerapporteerd aan de gemeente Amersfoort. De opvolging van bevindingen die noodzakelijk zijn, volgt binnen een afgesproken termijn door de opdrachtnemer. De scope van de pentest wordt altijd in afstemming met de opdrachtgever bepaald. De pentest wordt uitgevoerd volgens de richtlijnen van bijv. de Open Source Security Testing Methodology Manual (OSSTMM), de NIST Special Publication 800-115, OWASP testing Guide of soortgelijke.

E005	Na gunning van de opdracht en vóór ingebruikname van de dienstverlening laat de inschrijver een penetratietest (pentest) uitvoeren door een onafhankelijke (op geen enkele wijze gelieerd aan de inschrijver), binnen de sector erkende partij met aantoonbare ervaring met o.a. managed HCI-omgevingen, storage en backup. Het onderzoeksobject van de pentest omvat de door de inschrijver geleverde en beheerde onderdelen van de ICT-prestatie. De planning/ scope van de pentest wordt altijd in afstemming met de opdrachtgever bepaald. Alle kosten voor de pentest, rapportage, her-tests en het doorvoeren van maatregelen zijn inbegrepen in de inschrijving. Bevindingen met een classificatie Critical en High dienen vóór ingebruikname van de ICT-prestatie te zijn opgelost en gevalideerd middels een her-test. Bevindingen met een classificatie Medium dienen vóór ingebruikname te zijn opgelost, of te zijn voorzien van een door de inschrijver opgesteld en door de gemeente Amersfoort goedgekeurd plan van aanpak. De resultaten van de pentest en de opvolging daarvan worden volledig kosteloos gerapporteerd aan de gemeente Amersfoort.
E006	Identiteitenbeheer van gebruikers wordt enkel bijgehouden bij de opdrachtgever. Authenticatie van gebruikers van de opdrachtgever verloopt via de Active Directory van opdrachtgever. Na authenticatie via de Active Directory, hebben de gebruikers (beheerders van de opdrachtgever) toegang tot alle onderdelen van de ICT-prestatie, uiteraard voor zover ze daartoe zijn geautoriseerd.
E007	Authenticatie tot de ICT-prestatie vindt altijd plaats middels gebruikersnaam, wachtwoord en een veilige tweede factor (MFA).
E008	De ICT-prestatie voorziet in de mogelijkheid om autorisaties te baseren op Role Based Access Control (RBAC) en/of Attribute Based Access Control (ABAC) of soortgelijke.
E009	De ICT-prestatie zet Transport Layer Security (TLS versie 1.2 of hoger) Protocol in voor het beveiligen van verbindingen en de ICT-prestatie werkt voor data transport conform de meest actuele beveiligingsrichtlijnen van de NCSC.
E010	De ICT-Prestatie dient alle opgeslagen gegevens te beschermen door middel van versleuteling conform de marktstandaarden zoals opgenomen bij het Forum Standaardisatie. De technische implementatielaag en versleutelingstechniek moet aantoonbaar voldoen aan deze standaarden en waarborgt dat bij onbevoegde toegang of een datalek uitsluitend versleutelde, nietszeggende en onleesbare data kan worden verkregen.
E011	De ICT-prestatie hanteert een actuele en gedocumenteerde back-up-, restore- en disaster-recoveryprocedure, de inschrijver test deze jaarlijks (en na relevante infrastructuurwijziging) en levert de volledige testresultaten inclusief opvolging kosteloos binnen 10 werkdagen na afronding van de test aan de opdrachtgever.
E012	De bij de ICT-prestatie behorende backup-oplossing (on-premise en M365) wordt ingericht volgens de richtlijnen uit de meest recente versie van het document "Backup strategie" en "Handreiking-Backup-en-recovery-gemeente" van de VNG inclusief de 3-2-1 backup regel.
E013	Binnen de organisatie van opdrachtnemer is een securitymanager aanwezig die verantwoordelijk is voor het informatiebeveiligingsbeleid van de opdrachtnemer en die contactpersoon is voor de (C)ISO van de opdrachtgever.
E014	De ICT-prestatie is in staat aan te sluiten volgens markt standaarden op diensten van derden zoals bijvoorbeeld SOC/SIEM diensten.
E015	Bij calamiteiten levert de inschrijver extra benodigde inzet, indien het contract hierin niet direct voorziet, (evt. op basis van nacalculatie, in overleg met opdrachtgever).
E016	Indien de inschrijver tijdelijk niet aan informatieveiligheids-eisen dreigt te voldoen, dan dient de inschrijver dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem. Deze afwijking moet tijdig worden gemeld bij opdrachtgever, aangeleverd met een plan om aan de informatieveiligheids-eisen te voldoen met daarin de impact, doorlooptijd en risico's zijn opgenomen.
E017	Producten waar data opgeslagen is en die vervangen worden blijven eigendom van opdrachtgever.

E018	Zero Trust-principes dienen toegepast te worden conform de meest recente richtlijnen van de Informatiebeveiligingsdienst (IBD) en/of Nationaal Cyber Security Centrum (NCSC).
E019	De opdrachtnemer zorgt ervoor dat de ICT-prestatie zodanig is ingericht dat: de Recovery Time Objective (RTO) bij een calamiteit maximaal 4 uur bedraagt; de Recovery Point Objective (RPO) maximaal 1 uur bedraagt. Deze waarden gelden als minimale eisen en dienen aantoonbaar te worden geborgd in de oplossing.
E020	De geleverde ICT-prestatie moet effectief zijn beveiligd tegen Distributed Denial of Service (DDoS) aanvallen op alle relevante lagen (o.a. opslag-, netwerk-, transport- en applicatielaag), in lijn met de relevante publicaties van het NCSC, zoals de factsheet 'Continuïteit van online diensten' en de factsheet 'Technische maatregelen voor de continuïteit van online diensten'
E021	De ICT-Prestatie voert logging uit, in lijn met de meest recente "Handreiking Logging" van de Informatiebeveiligingsdienst VNG. Hierbij moeten activiteiten van gebruikers en beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen worden gemonitord en vastgelegd in audit-logbestanden, met inachtneming van relevante wetgeving, BIO, waarbij geldt: a. Dat deze audit-logbestanden minimaal zes maanden worden bewaard. b. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden. c. Van audit-logbestanden rapportages worden gemaakt die periodiek, zoals afgesproken met opdrachtgever te worden gedeeld en beoordeeld. d. Handelingen van gebruikers moeten te allen tijde te herleiden zijn naar een natuurlijk persoon. e. Handelingen van systemen moeten te allen tijde te herleiden zijn naar een systeem. De volgende gebeurtenissen worden in ieder geval opgenomen in de logs: f. Gebruik van technische beheerfuncties, zoals een backup maken. g. Gebruik van functionele beheerfuncties, zoals het wijzigen van instellingen, updates van de applicaties. h. Handelingen van autorisatiebeheer, zoals het aanmaken van een gebruiker, wachtwoord reset. i. Inlogpogingen zowel succesvol als onsuccesvol worden vastgelegd. j. Handelingen van gebruikers, het uitvoeren van acties zoals het raadplegen van bestanden/informatie, uitvoeren van overige acties die binnen de applicatie kunnen worden uitgevoerd (bewerken, verwijderen, kopiëren etc) k. Foutmeldingen van applicaties. l. logbestanden mogen niet gewijzigd worden. Een logregel bevat minimaal: - de gebeurtenis. - de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon. - het gebruikte apparaat, - het resultaat van de handeling. - een datum en tijdstip van de gebeurtenis.
E022	Op verzoek van de opdrachtgever, bijv. n.a.v. een beveiligingsincident, dienen relevante logs en auditgegevens aan de opdrachtgever kosteloos aangeleverd te worden via een algemeen gehanteerd formaat.
E023	Gedurende de overeenkomst tussen opdrachtgever en opdrachtnemer kunnen informatiebeveiligingsincidenten optreden. Indien deze leiden of hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen worden deze zo snel mogelijk, maar in ieder geval binnen 4 uur na bekendwording gemeld bij opdrachtgever.
E024	Opdrachtnemer neemt bij succesvolle of vermoedelijke pogingen tot ongeautoriseerde toegang tot de ICT-prestatie alle noodzakelijke maatregelen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De succesvolle ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen tijdig en uiterlijk binnen 24 uur aan de opdrachtgever worden gerapporteerd.
Architectuur	

E025	Opdrachtnemer levert een onpremise storage en compute oplossing (S&C-infra) met een capaciteit voor 350 Virtuele Machines een minimale capaciteit van 8TB geheugen (exclusief SQL en Oracle cluster) en logische storage opslag van minimaal 100TB, waarbij de storage omgeving een piekbelasting aan moet kunnen van minimaal 130.000 Read IOPS of 85.000 mixed IOPS en de latency van de omgeving niet hoger mag zijn dan 5ms round trip.
E026	Opdrachtnemer levert een van backupvoorziening voor de onpremise omgeving met een minimale capaciteit van 523TB.
E027	Opdrachtnemer levert een backupvoorziening voor de M365 omgeving. Het aantal gebruikers is 2200.
E028	Wanneer meerdere klanten van opdrachtnemer dezelfde infrastructuur, database of applicatiecode delen, zijn er maatregelen getroffen om ervoor te zorgen dat de gegevens en configuraties van opdrachtgever geïsoleerd en beschermd blijven. Dit omvat onder andere waarborgen voor multi-tenancy en segmentatie. Opdrachtnemer dient dit aan te tonen.
E029	Bij een ontwerp volgt opdrachtnemer de landelijke en de gemeentelijke architectuurprincipes (NORA / Gemma)
E030	De bij de ICT-prestatie behorende on-premise omgeving moet Active-Active op datacenterniveau functioneren. Bij uitval van één datacenter moet 100% van capaciteit beschikbaar blijven.
E031	Opdrachtnemer levert overzicht van gebruikte technieken en architectuur van de ICT-prestatie en onderliggende systemen. Waar van toepassing zijn - het actuele gegevensmodel, - de onderlinge samenhang en - afhankelijkheden van de IT-functionaliteiten beschreven. De opdrachtnemer stelt deze informatie initieel en op verzoek tijdens de looptijd van de overeenkomst aan de ICT-prestatie beschikbaar
E032	Waar van toepassing is een juist, actueel en volledig overzicht van de aanwezige systemen, hard- en software in hun onderlinge samenhang beschikbaar.
E033	Opdrachtnemer voert werkings- en functionele testen uit en begeleidt tijdens acceptatietesten.
E034	Handleidingen, documentatie en spraaktaal is tijdens de implementatie fase en operationele fase in de Nederlandse taal.
E035	Opdrachtnemer ontwikkelt en onderhoudt actuele en sluitende documentatie van de technische inrichting en operationele processen en procedures zodat werkzaamheden controleerbaar en overdraagbaar zijn. Deze is periodiek opvraagbaar door opdrachtgever en wordt binnen maximaal 5 werkdagen door Opdrachtnemer verstrekt aan opdrachtgever.
E036	Authenticatie wordt ondersteund met een van beide protocollen OpenID en SAML. De volgende scenario's kunnen daarvoor worden ingezet met als voorkeur scenario 3, dan 2 en als het echt niet anders kan dan 1. 1. Gebruikersaccount wordt vertaald naar een user in de applicatie Rollen worden in de applicatie toegekend en geautoriseerd Bij NIET BESTAANDE user wordt er een creatie proces geleverd en gestart. 2. Gebruikersaccount wordt vertaald naar een user in de applicatie Rollen worden obv claims gemapt op de rollen die binnen de applicatie worden gebruikt. 3. Gebruikersaccount wordt o.b.v. usertoken gebruikt in de toepassing Rollen worden o.b.v. claims gemapt op de rollen die binnen de applicatie worden gebruikt
E037	Gebruikersaccounts die aangemaakt worden binnen de ICT-prestatie voldoen aan de BIO 2.0 richtlijnen en hebben een wachtwoord lengte van van minimale 14 karakters.
E038	De ICT-prestatie kent een lifecycle management conform de meest stabiele laatste versie.
E039	ICT-prestatie dient device onafhankelijk gebruikt te kunnen worden en kent geen hardware afhankelijkheden (dongles,etc).
E040	De ICT-prestatie sluit aan op de bestaande infrastructuur van opdrachtgever wat betreft netwerk, systemen, devices, generieke kantoorautomatisering etc... Zie bijlage I Architectuur overzicht voor de technische beschrijving.

E041	Opdrachtnemer brengt de opdrachtgever proactief (bijv. via een roadmap) op de hoogte van aankomende aanpassingen die betrekking hebben op de ICT-prestatie en afhankelijkheden (bijv. uitfaseren ondersteuning van afhankelijke software- of hardware componenten)
E042	Het gebruik en inregelen van licenties is eenvoudig en geheel softwarematig en maakt geen gebruik van hardware-devices.
E043	De servers voor het Oracle cluster dienen te voldoen aan de volgende eisen: - 2 fysieke servers - maximaal 8 cores per server - Minimaal 512Gb geheugen Dit ivm de beperkingen vanuit de Oracle licentie.
E044	De servers voor SQL cluster dienen te voldoen aan de volgende eisen: - 2 fysieke servers - maximaal 8 cores per server - Minimaal 768Gb geheugen Dit ivm de beperkingen vanuit de SQL licentie.
E045	Het aantal servers dat de virtualisatie ondersteunt bestaat uit minimaal 4 en maximaal 8 servers (exclusief SQL en Oracle cluster)
E046	De bij de ICT-prestatie behorende on-premise storage moet volledig gebaseerd zijn op SSD (geen HDD tiering).
E047	De ICT-prestatie ondersteund granulair herstel zijn op item-, account- en siteniveau.
E048	Standaarden conform https://www.forumstandaardisatie.nl/ worden toegepast voor interoperabiliteit, koppelingen, berichtenverkeer e.d.
Duurzaamheid	
E049	Wanneer kartonnen dozen worden gebruikt voor secundaire en/of tertiaire verpakkingen, dienen deze voor minstens 80% uit post-consumer gerecycled karton te bestaan. Wanneer niet-biobased kunststof folie of -vellen worden gebruikt voor secundaire en/of tertiaire verpakkingen, dienen deze voor minstens 75% uit gerecycled materiaal te bestaan.
E050	Klikverbindingen of aansluitingen van door opdrachtnemer geleverde hardware zijn, om goede demontage en recycling te vereenvoudigen, eenvoudig te vinden, te openen zonder gereedschap of met gangbaar gereedschap en voor zover mogelijk genormaliseerd.
E051	De opdrachtnemer dient, bij defect en vervanging, zoveel mogelijk gebruik te maken, in overleg, van hergebruikte, refurbished, remanufactured of soortgelijke producten
E052	Voertuigen voor vervoer goederen en dienstverleners voldoen ten minste aan emissieklasse 6
E053	Opdrachtnemer stelt hardware (waar mogelijk) standaard zo energie zuinig mogelijk in alvorens een product wordt uitgeleverd. Bij plaatsing wordt samen met de leveranciers van beide Datacenters ervoor gezorgd dat de totale inrichting zo efficient mogelijk wordt gerealiseerd
E054	De opdrachtnemer mag alleen producten leveren van fabrikanten die zich committeren aan het bijhouden van een herkomstlijst waarin, voor op zijn minst de geleverde productgroep, transparant wordt vastgelegd in welke productie- en assemblagefabrieken de onderdelen worden geproduceerd/geassembleerd.
Beheer	
E055	Opdrachtnemer beheert de bij de ICT-prestatie behorende hardware en virtualisatielaag. De opdrachtgever beheert de virtuele machine, het OS en de applicaties.
E056	Opdrachtnemer moet garanderen dat de ICT-prestatie een minimale beschikbaarheid van 99,9% heeft gemeten over de afgelopen 3 maanden.
E057	Opdrachtnemer stelt herstelprocedures beschikbaar voor het geval van storingen, zodat de continuïteit van de dienstverlening gewaarborgd blijft. Deze procedures moeten inzichtelijk en direct uitvoerbaar zijn om de impact van storingen tot een minimum te beperken.
E058	De ICT-prestatie kan nieuw uitgebrachte functionaliteiten toepassen. Toepassing van wordt afgestemd met de opdrachtgever

E059	Een nieuwe component dient over minimaal dezelfde functionaliteit te beschikken als het component die erdoor vervangen wordt.
E060	Monitoring van de ICT-prestatie dient op een veilige, eenvoudige en overzichtelijke manier vanuit één centrale plek gedaan kunnen worden.
E061	De ICT-prestatie is in staat om statusinformatie aan te leveren t.b.v. de monitoringsoftware van opdrachtgever (Paessler PRTG) door gebruik te maken van SNMP.
E062	De ICT-prestatie is in staat om te schrijven naar een SYSLOG-server.
E063	Binnen de IT-afdeling van opdrachtgever is uitgebreide kennis aanwezig op het gebied van onze huidige ICT-prestatie. Wanneer er nieuwe componenten worden geintroduceerd in de nieuwe ICT-prestatie geleverd door opdrachtnemer dan voorziet deze in een passende training aan de it-specialisten (5) en architecten (1) van opdrachtgever. Alle noodzakelijke kosten hiervoor dienen te zijn opgenomen in de aanbieding.
E064	De ICT-prestatie moet schaalbaar zijn, zodat bijvoorbeeld uitbreiding van opslagcapaciteit mogelijk is zonder onderbreking van de dienstverlening
E065	De ICT-prestatie moet redundantie en hoge beschikbaarheid garanderen, bijvoorbeeld via RAID, replicatie of synchrone opslag over meerdere locaties
E066	Beheer en monitoring van de ICT-prestatie moet centraal en real-time mogelijk zijn, inclusief automatische waarschuwingen bij storingen of capaciteitsproblemen
E067	De ICT-prestatie moet ondersteuning bieden voor deduplicatie, compressie en automatische tiering voor efficiënt gebruik van opslagruimte
E068	De ICT-prestatie moet eenvoudig te integreren zijn met de cloud- en hybride omgevingen van opdrachtgever voor flexibiliteit en schaalbaarheid.
E069	De ICT-prestatie moet schaalbaar zijn, zodat eenvoudig extra capaciteit (CPU, geheugen) kan worden toegevoegd, zowel fysiek als virtueel
E070	De ICT-prestatie moet minimaal dezelfde prestaties leveren als onze huidige ICT-prestatie. Zie hiervoor bijlage I, Architectuur overzicht'
E071	De ICT-prestatie moet redundantie en hoge beschikbaarheid bieden, inclusief failover-mogelijkheden en ondersteuning voor onderhoud zonder downtime via software-defined infrastructuur, zodat resources dynamisch kunnen worden toegewezen op basis van de actuele vraag
E072	De ICT-prestatie ondersteunt segmentatie, beveiligde toegang en integratie met bestaande securitymaatregelen
E073	De ICT-prestatie moet 24/7 automatische, geplande back-ups ondersteunen, met de mogelijkheid tot handmatige back-ups.
E074	Er moet centrale monitoring zijn van de back-upstatus, inclusief automatische waarschuwingen bij fouten of mislukte back-ups. Rapportages moeten eenvoudig te genereren zijn.
E075	Back-ups moeten geïsoleerd zijn van de productieomgeving (immutable storage of air gap) om besmetting door ransomware te voorkomen. Opdrachtnemer moet dit periodiek aantonen middels security-tests
E076	De ICT-prestatie ondersteunt directe herstelmogelijkheden via point-in-time snapshots. Deze kunnen door opdrachtgever zelfstandig worden uitgevoerd.
E077	De backup-oplossing biedt de mogelijkheid om meerdere versies van bestanden te bewaren en te herstellen. Ook wel restore points genoemd.
E078	Opdrachtnemer mag geen data, back-ups of archieven van de opdrachtgever verwijderen, vernietigen of ontoegankelijk maken zonder voorafgaande schriftelijke toestemming van de opdrachtgever.
E079	De ICT-oplossing dient de industriestandaarden voor Oracle, Linux, Windows en Windows server te ondersteunen voor operating systems die in support zijn bij de betreffende fabrikant.
E080	Opdrachtgever kan zelfstandig Virtuele Machines aanmaken, verwijderen of aanpassen, waarbij de configuratie in vCPU, vNIC, RAM en vDISK door opdrachtgever aangepast moet kunnen worden.
E081	De bestaande NetApp-omgeving blijft in gebruik en technisch beheer wordt overgenomen door opdrachtnemer.

E082	De opdrachtnemer dient bij het aanbieden van de M365 backup oplossing rekening te houden met de opgebouwde retentie data in de huidige Barracuda M365 backup oplossing.
E083	De bij de ICT-prestatetie behorende M365 backup oplossing moet minimaal de volgende onderdelen kunnen backuppen en restoren: - Exchange online - Teams - One-drive for Business - Sharepoint online - Microsoft 365 groups - OneNote - Planner - Entra ID (minimaal Directory objects, Users, Groups, Enterprise application, app-registrations, audit logs, Authentication Method Policies, Authentication Strength Policies, BitLocker Keys, Conditional Access Policies, Device Management (Intune Policies), Enterprise Applications, Named Locations)
Regie	
E084	Werkzaamheden aan de ICT-prestatie in de vorm van patches, updates en upgrades die van invloed zijn op de dienstverlening van opdrachtgever worden tijdig afgestemd. Voor deze werkzaamheden wordt onderscheid gemaakt tussen Kritisch en Regulier. Kritische werkzaamheden worden op basis van ad hoc overleg ingepland; Reguliere werkzaamheden via een changekalender of in overleg minimaal 2 weken van tevoren
E085	Opdrachtgever is en blijft eigenaar van de in de ICT-prestatie opgenomen informatieobjecten en alle daarop uitgevoerde bewerkingen en aanvullingen (zoals metadata, indexen, zoekingangen, managementinformatie, geaggregeerde informatie).
E086	Opdrachtnemer levert Support en Maintenance op de afgesproken ICT-prestatie afgestemd op en conform de overeengekomen service- en kwaliteitsniveaus.
E087	Controle op de door opdrachtnemer vastgelegde CI's behorende bij de ICT-prestatie in de CMDB van opdrachtnemer vindt minimaal 1 keer per jaar plaats door de vastgelegde gegevens te vergelijken met de werkelijk geïnstalleerde configuratie items.
E088	Standaardwijzigingen worden in de DAP vastgelegd. Nieuwe changes die als standaard kunnen worden beschouwd worden toegevoegd aan de lijst in de DAP. Een standaard change voldoet aan: - Uitvoeringsduur < 2 uur; - Laag risico; - Geen service impact; - Remote uitvoerbaar; - Geen afhankelijkheid van 3e partijen voor uitvoering.
E089	Bij storingen dienen de volgende responstijden te worden aangehouden: - P1 verstoring: max 15 min responstijd en max 4 uur oplostijd. - P2 verstoring: max 30 min responstijd en max 8 uur oplostijd - P3 verstoring: max 1 uur responstijd en max 2 werkdagen oplostijd - P4 verstoring: max 24 uur responstijd en max 2 a 3 werkdagen oplostijd.
E090	Voor de ICT-prestatie wordt 24x7 support worden geleverd. De Servicedesk van opdrachtnemer is buiten kantoortijden bereikbaar voor P1 en P2 incidenten
E091	Na elke P1 verstoring van de ICT-prestatie wordt binnen 5 werkdagen een document opgeleverd in de vorm van een Root Cause Analysis (RCA) of Major Indicent Report (MIR)
E092	Prioriteit van een incident wordt daar waar nodig door een contactpersoon van opdrachtgever vastgesteld.
E093	Facturering wordt als volgt opgeleverd: Aparte factuur voor elk onderdeel, Compute, Storage, Backup on Prem en Backup M365;

E094	De Servicedesk van opdrachtnemer maakt gebruik van ITSM-tooling waar opdrachtgever gebruik van kan maken ten behoeve van het volgen van tickets en het communiceren hierover waar geen kosten aan verbonden zijn. Opdrachtnemer legt een koppeling tussen de ICT-prestatie en de ITSM tooling van de Gemeente om (near-real-time track and trace) informatie uit te wisselen over changes en incidenten.
E095	De Servicedesk van opdrachtnemer beschikt over incident-, problem- en change- management processen (IPC-processen) die zijn vastgelegd en beschikbaar worden gesteld aan opdrachtgever.
E096	De Servicedesk van opdrachtnemer beschikt over release- en patch management en onderhoudsprocessen die zijn vastgelegd en beschikbaar worden gesteld aan opdrachtgever.
E097	Opdrachtnemer onderneemt activiteiten ten aanzien van gebruikerstevredenheid en opvolging hiervan en stelt deze processen beschikbaar (XLA).
E098	Opdrachtnemer houdt minimaal 1 keer per jaar een klanttevredenheidsonderzoek en stelt de resultaten hiervan beschikbaar.
E099	Opdrachtnemer houdt minimaal 1 keer per jaar een klantenpanel of klantendag, waarbij de klantbevindingen van de dienstverlening centraal staan.
E100	Opdrachtnemer voert minimaal 1 keer per jaar een overleg met de klant over reflectie op en toegevoegde waarde van de samenwerking.
E101	Opdrachtnemer beschikt over (online) SLA rapportages en stelt deze beschikbaar. Rapportage data moet ook los beschikbaar gesteld worden om op te nemen in datawarehouse voor verwerking in bron overstijgende rapportages.
E102	Opdrachtnemer stelt gedetailleerde documenten beschikbaar ten behoeve van disaster recovery en business continuity plannen.
E103	Opdrachtnemer levert, presenteert en bespreekt regulier maar minimaal jaarlijks een vernieuwingsplan om haar producten en diensten te verbeteren die concrete waarde toevoegen aan de opdrachtgever in termen van kosten, kwaliteit, samenwerking, duurzaamheid, veiligheid, schaalbaarheid, snelheid en continuïteit.
E104	Opdrachtnemer sluit aan bij de markt standaarden op diensten van derden zoals bijvoorbeeld monitoring, rapportage en data diensten diensten.
E105	Opdrachtnemer verzorgt, zowel gevraagd als ongevraagd strategisch advies tijdens periodiek in te plannen overleg. Met strategisch advies wordt bedoeld advies op het vlak van zowel innovatie als kwaliteitsverbetering.
E106	Opdrachtnemer stelt binnen 8 weken na de voorlopige gunning een exitplan op waarin ook is opgenomen: - De informatieobjecten en gegevens die wel en niet worden overgedragen, de tijdspanne, de vorm en de rapportage van de overdracht. - De vernietiging van de informatieobjecten en gegevens na de exit uit de oplossing.
E107	Life Cycle Management, zoals End of Life / End of Support, wordt proactief door opdrachtnemer opgepakt.
E108	On Site Support (engineer van opdrachtnemer werkt op locatie opdrachtgever) dient minimaal 2 keer per jaar plaats te vinden .
E109	Standaard changes dienen binnen 2 werkdagen te worden uitgevoerd.
E110	Niet standaard changes worden in overleg met opdrachtgever uitgevoerd.
E111	De Servicedesk van opdrachtnemer is op werkdagen (ma-vrij) telefonisch bereikbaar vanaf 07:00 uur tot 18:00 uur.
E112	De definitieve SLA wordt in afstemming met opdrachtgever uiterlijk 1 september 2026 opgeleverd.
E113	De SLA heeft dezelfde looptijd als de overeenkomst.
E114	Opdrachtnemer initieert jaarlijks een gezamenlijke review van het SLA document.
E115	Wijzigingen in de SLA en DAP vinden enkel doorgang wanneer deze door beide partijen is goedgekeurd.
E116	In het Dossier Afspraken en Procedures (DAP) wordt een verdere uitwerking van de werkafspraken en procedures vastgelegd.
E117	IT Service Management wordt uitgevoerd volgens ITIL 4 best practices

E118	Opdrachtnemer beschikt over een klachtenmanagement procedure, waarbij klachten worden geregistreerd en een verbeterplan uiterlijk binnen 5 dagen wordt opgeleverd .
E119	Apparatuur behorende bij de te leveren ICT-prestatie dient gedurende de gehele looptijd van de SLA te worden ondersteund door de oorspronkelijke fabrikant of opdrachtnemer. Deze ondersteuning omvat in ieder geval: beschikbaarheid en beveiligingsupdate, bugfixes, onderhoud, technische ondersteuning en vervangingsonderdelen. Apparatuur en software mogen gedurende de looptijd niet de end-of-support of end-of-life status bereiken.
E120	Rapportages kunnen door opdrachtgever zonder tussenkomst van opdrachtnemer minimaal in de navolgende bestandsformaten geleverd worden: Excel, Word, PDF, TXT, CSV, en XML. De gegevens zijn in vaste formats te printen.
Transitie	
E121	Transitie van de ICT-prestatie dient uiterlijk 1 september 2026 gerealiseerd te zijn.
E122	Opdrachtnemer is verantwoordelijk voor coordinatie en uitvoering van de transitie.
E123	Opdrachtnemer stelt bij inschrijving een concept transitieplan op. Deze wordt na gunning in overleg met opdrachtgever definitief gemaakt. Opdrachtnemer is verantwoordelijk voor de transitie van de huidige ICT-prestatie naar de nieuwe ICT-prestatie.
E124	De transitie wordt afgesloten met een acceptatietest. Opdrachtgever behoudt zich het recht voor om bij de acceptatietest één of meer (deel)tests door derden te laten uitvoeren. Opdrachtnemer zegt hiervoor reeds nu zijn volledig medewerking toe.
E125	Facturering wordt als volgt opgeleverd: Aparte factuur voor elk onderdeel, Compute, Storage, Backup on Prem en Backup M365;
E126	ict-prestatie dient device onafhankelijk gebruikt te kunnen worden en kent geen hardware afhankelijkheden (dongles,etc).
Levering en Support hardware	
E127	Opdrachtnemer dient alle bij de ICT-prestatie behorende hardware te leveren aan de opdrachtnemer. Alle hardware wordt eigendom van de opdrachtgever.
E128	Alle hardware als onderdeel van de ICT-prestatie moet in een 19" rack passen en heeft een maximale diepte van 120cm.
E129	De leverancier geeft voor alle bij de ICT prestatie behorende hardware een garantie (levenscyclus) af van 7 jaar.