Bijlage E: Programma van eisen ICT-beheer

1	Algemene eisen
1.1	Opdrachtnemer draagt zorg voor één centraal contactpersoon voor Opdrachtgever, alsmede een vaste back-up bij afwezigheid.
1.2	Indien medewerkers van de Opdrachtnemer werkzaamheden uitvoeren op locaties van de Stichting waarbij zij in contact komen met kinderen, dienen zij in het bezit te zijn van een geldige Verklaring Omtrent Gedrag (VOG). De VOG mag niet ouder zijn dan zes (6) maanden en dient te zijn afgegeven op basis van screeningsprofiel 84 (Belast zijn met de zorg voor minderjarigen) en/of 86 (Kinderopvang), of de daarvoor in de plaats komende profielen. De Opdrachtnemer overlegt de VOG van de betrokken medewerker(s) op eerste verzoek van de Opdrachtgever, uiterlijk vóór aanvang van werkzaamheden op locatie. De kosten voor het verkrijgen van de VOG zijn voor rekening van de Opdrachtnemer. Daarnaast dient de Opdrachtnemer een doorlopend screeningsproces te hanteren, waarmee wordt gewaarborgd dat alle medewerkers blijvend voldoen aan de integriteits- en veiligheidseisen van de Opdrachtgever. Indien een medewerker niet (meer) over een geldige verklaring beschikt, wordt deze de toegang tot de locaties van de Opdrachtgever ontzegd.
1.3	Opdrachtnemer zal, op zowel gevraagd als ongevraagd verzoek, advies verstrekken met betrekking tot alle aspecten binnen de scope. Dit met als doel de Opdrachtgever inzicht te verschaffen in innovaties en mogelijke verbeteringen, waardoor de gestelde doelstellingen op een efficiënte wijze kunnen worden behaald.
1.4	De gegevens in zowel de huidige als de gewenste omgeving blijven eigendom van de Opdrachtgever. De toegepaste instellingen dienen transparant te zijn en eenvoudig overdraagbaar naar een andere beheerder.
1.5	Opdrachtnemer voorziet in een gebruikersinterface die in het Nederlands is.
1.6	Gedurende het gehele eerste jaar van deze Overeenkomst zullen géén prijswijzigingen worden doorgevoerd. Na het eerste jaar van de overeenkomst kan er per 1 mei 2027 een prijswijziging worden doorgevoerd voor dat komende jaar. Een prijswijziging zal nimmer met terugwerkende kracht gebeuren.
1.7	Prijswijzigingen dienen uiterlijk twee maanden voor het verstrijken van het kalenderjaar te worden aangedragen door Opdrachtnemer ter acceptatie op basis van maximaal het CBS-prijsindexcijfer CAO lonen per uur inclusief bijzondere beloningen, categorie zakelijke dienstverlening, waarbij het prijsniveau staat voor 2024 en gelijk is aan 100. Opdrachtnemer stelt de prijswijziging vast op basis van het prijsindexcijfer en meldt dit schriftelijk bij Opdrachtgever.
1.8	Aanbestedende Dienst werkt met een Inrichtingsmodel van de ICT-beheerorganisatie (hierna te noemen blauwdruk). Opdrachtnemer zorgt ervoor dat de blauwdruk up-to-date is. Opdrachtnemer zorgt ervoor dat deze in nader te bepalen frequentie wordt gestuurd naar Aanbestedende Dienst in laatste versie. Deze laatste versie moet indien gewenst per direct beschikbaar zijn in de meest actuele versie.
1.9	In de DAP en SLA worden afspraken vastgelegd over de wijze waarop de blauwdruk wordt gevolgd en geborgd in de dagelijkse uitvoering van het ICT-beheer en de samenwerking.

2	Infrastructuur/netwerk
2.1	Opdrachtnemer is belast met de volledige uitvoering en verantwoordelijkheid van het ICT-beheer, waarbij alle activiteiten die onder systeembeheer en configuratiebeheer vallen, inbegrepen zijn.
2.2	Opdrachtnemer draagt de verantwoordelijkheid voor het beheren van de volledige huidige en toekomstige installed base van Opdrachtgever, zoals beschreven in eis 3.1 tot 3.9. Hieronder vallen onder andere, maar niet beperkt tot: multifunctionals (inclusief onderhoud van adresboeken), devices, switches, touchscreens, routers, software (besturingssystemen, kantoor- en onderwijsapplicaties) en beveiligingssoftware
2.3	Opdrachtnemer neemt het beheer van alle bestaande systemen over.
2.4	Opdrachtnemer installeert geen servers (data- print of mailservers) op de locaties van Opdrachtgever.
2.5	Opdrachtnemer garandeert dat de aangeboden oplossing kan samenwerken met de huidige en toekomstige software.
2.6	Detectie van alle apparaten op het netwerk (bekend én onbekend).
2.7	Toegangscontrole op basis van apparaattype, gebruiker, locatie, enz.
2.8	Automatische response op verdacht gedrag, zoals isoleren van geïnfecteerde hosts.
2.9	De mogelijkheid om bepaalde hosts te blokkeren of hun verkeer te beperken.
3	**Beheer & Monitoring**
3.1	Asset management: Opdrachtnemer is verantwoordelijk voor het complete proces van aanschaf tot afschrijving van IT-middelen van Opdrachtgever. Opdrachtnemer voert activiteiten uit die leiden tot een adequaat administratief beheersproces van ICT-middelen. Opdrachtnemer registreert alle aanwezige devices (inclusief kenmerken) van de Opdrachtgever en maakt dit inzichtelijk voor Opdrachtgever. Opdrachtgever kan te allen tijde periodiek (nader af te stemmen) een rapportage opvragen zonder bijkomende kosten.
3.2	Configuratie management: Het beheren van programmastuursystemen (software) en apparatuur door middel van een speciaal informatiesysteem als gereedschap (tool) om wijzigingen (change) te controleren en beheersen en de integriteit van het systeem te waarborgen.
3.3	Change management: Opdrachtnemer maakt gebruik van gestandaardiseerde methoden en procedures om wijzigingen (changes) te kunnen afhandelen, waarbij het onderwijsproces zo min mogelijk wordt onderbroken.
3.4	Incident management: Opdrachtnemer hanteert incident management als proces, waarbij het doel is om een incident terug te brengen naar het normale en overeengekomen kwaliteitsniveau.
3.5	Problem management: Opdrachtnemer is verantwoordelijk voor het volledige proces van het afhandelen van problemen, met als doel storingen en incidenten proactief te verminderen. Hierbij neemt Opdrachtnemer ook de verantwoordelijkheid voor het proactief monitoren van de gehele ICT-omgeving.
3.6	Release management: Opdrachtnemer is verantwoordelijk voor het plannen en toezicht houden op de uitrol van nieuwe releases voor hard- en software. De planning wordt te allen tijde voorgelegd aan de opdrachtgever.
3.7	Capaciteit management: Opdrachtnemer is verantwoordelijk voor het waarborgen van de juiste capaciteit voor alle IT-middelen om te kunnen voldoen aan de huidige en toekomstige behoeften van opdrachtgever.
3.8	WAAS (Wifi as a service), omvat inrichting / beheer en onderhoud / monitoring / security / apparatuur en vervangingscyclus.

3.9	Opdrachtnemer is verantwoordelijk voor het technisch beheer en onderhoud van de Microsoft 365 Tenant van Aanbestedende Dienst. Dit omvat minimaal: • Gebruikers-, groeps- en licentiebeheer; • SharePoint-, OneDrive- en Teams-beheer; • Beheer van beveiligings- en compliance-instellingen (waaronder Conditional Access en MFA); • Rapportage over gebruik, capaciteit en incidenten; • Afstemming met het ICT-team over wijzigingen in beleid en inrichting. De Tenant blijft eigendom van Aanbestedende Dienst; configuraties en instellingen zijn volledig inzichtelijk en overdraagbaar.
4	**Toegang en beveiliging**
4.1	Opdrachtnemer beheert alle accounts zoals bijvoorbeeld die van groepen, medewerkers en kinderen.
4.2	Opdrachtgever maakt gebruik van EduConnector of een vervangende connector binnen de stichting. Opdrachtnemer beheert en faciliteert dit. Dit omvat toegangsbeheer, autorisatiebeheer, monitoring en logging en zorg voor updates en configuratiebeheer.
4.3	De Opdrachtnemer draagt bij dat de Opdrachtgever uiterlijk 1 januari 2027 voldoet aan het Normenkader (IBP) voor informatiebeveiliging en privacy, of op het moment dat dit wettelijk verplicht wordt. Opdrachtnemer zal, gevraagd en ongevraagd, adviseren op alle onderdelen binnen het Normenkader (IBP).
4.4	Opdrachtnemer is verantwoordelijk voor het leveren, installeren, configureren, beheren en up-to-date houden van beveiligingssoftware. Het doel van de Aanbestedende Dienst is ervoor te zorgen dat zij beschikt over een veilige IT-omgeving. Opdrachtnemer biedt hier een passende oplossing voor, conform de meest recente standaarden.
4.5	Opdrachtnemer is verantwoordelijk voor het correct en consequent naleven van de Algemene Verordening Gegevensbescherming (AVG) en eventuele toekomstige opvolgende wet- en regelgeving. Daarbij moet worden voldaan aan alle geldende wettelijke verplichtingen op het gebied van ICT-beveiliging en gegevensbescherming.
4.6	Opdrachtnemer beschikt over minimaal een ISO 27001 informatiebeveiligingscertificering.
4.7	Opdrachtnemer is verantwoordelijk voor het firewall beheer inclusief hardware
4.8	Opdrachtnemer mag bemiddelen in de levering van licenties (hardware en software). In dat geval draagt opdrachtnemer zorg voor een correcte tenaamstelling van de software, waarbij de software altijd te naam wordt gesteld op naam van Opdrachtgever.
4.9	Opdrachtnemer realiseert en beheert een storingsvrije toegang naar alle software gedurende de openingstijden van Opdrachtgever.
4.10	Opdrachtnemer is verantwoordelijk voor het installeren, configureren, beheren en up-to-date houden van alle software en besturingssoftware.
4.11	De Opdrachtnemer dient expertise te hebben op het gebied van beveiliging en security van ICT-systemen.
4.12	De aangeboden ICT-omgeving dient maximale bescherming te bieden tegen bekende en opkomende bedreigingen, zoals malware, ransomware, phishing en DDoS-aanvallen. Hierbij is het essentieel dat de Opdrachtnemer expertise kan aantonen in het implementeren van effectieve beveiligingsmaatregelen.
4.13	Er dient een geïntegreerd authenticatie- en autorisatiesysteem te zijn om de toegang tot systemen en gegevens te beheren. Dit systeem moet sterke

	wachtwoordbeleidsregels omvatten en de mogelijkheid bieden voor MFS (Multi Factor Authenticatie).
4.14	De Opdrachtnemer monitort 24/7 de beschikbaarheid, prestaties en beveiliging van: • Servers en onderliggende infrastructuur; • Modem, switch, firewall en router; • Microsoft 365 Tenant. Afwijkingen worden proactief gesignaleerd en opgevolgd volgens de overeengekomen prioriteiten en responstijden binnen de SLA. De monitoring omvat logging, trendanalyse en rapportage.
5	**Servicedesk beschikbaarheid en bereikbaarheid**
5.1	De Opdrachtnemer vervult de SPOC-rol en moet snel, efficiënt en proactief reageren op alle vragen, incidenten en verzoeken van Opdrachtgever met betrekking tot de ICT middels een dedicated Servicedeskteam. Indien nodig wordt er met derden geschakeld. De Opdrachtnemer fungeert als probleemhouder en neemt verantwoordelijkheid voor het oplossen van de gemelde problemen, waarbij heldere communicatie en een minimale impact op het onderwijsproces centraal staan.
5.2	Opdrachtnemer voorziet in een webbased platform dat aansluit op het ticketsysteem (PowerApp) van Opdrachtgever. Incidenten, problemen en wijzigingen worden via dit ticketsysteem gemeld. Op elk moment heeft Opdrachtgever zicht op de status, doorlooptijd en genomen acties met betrekking tot het oplossen van gemelde incidenten, problemen of wijzigingen. Afmelding van deze gemelde zaken gebeurt te allen tijde door de Opdrachtgever.
5.3	Opdrachtnemer stelt een vast Servicedeskteam beschikbaar voor Aanbestedende Dienst, bestaande uit: • Eén vast aanspreekpunt (Single Point of Contact); • Eén vaste back-up, die volledig op de hoogte is van de omgeving van Aanbestedende Dienst; • Medewerkers met aantoonbare ervaring binnen onderwijsinstellingen en Microsoft-omgevingen. Het team is verantwoordelijk voor continuïteit, kennisborging en korte communicatielijnen met de ICT-afdeling.
5.4	Opdrachtnemer hanteert gestandaardiseerde procedures, zoals ASL en ITIL, voor de afhandeling van incidenten, problemen en wijzigingen.
5.5	De Servicedesk ondersteuning is beschikbaar in de Nederlandse taal.
5.6	De Servicedesk van de Opdrachtnemer is in ieder geval beschikbaar voor Opdrachtgever op werkdagen (maandag t/m vrijdag) van 07:30 uur tot 17:00 uur.
5.7	Opdrachtnemer dient voorafgaand aan elk kalenderjaar een planning van preventieve onderhoudswerkzaamheden te overleggen en te leveren aan Opdrachtgever.
5.8	Opdrachtnemer plant in overleg met Opdrachtgever correctieve onderhoudswerkzaamheden zo spoedig mogelijk in.
5.9	Indien een storing/melding niet onder de verantwoording valt van Opdrachtnemer dan dient dit vooraf gecommuniceerd te worden met Opdrachtgever.
5.10	Opdrachtnemer overlegt een volledige SLA en DAP nadat de voorlopige gunning is ontvangen. In de SLA worden verschillende onderwerpen beschreven, waaronder maar niet beperkt tot: responstijden, escalatieafhandeling, overlegstructuur, beveiligingsbeheer, callintake, changemanagement, configuratiemanagement, releasemanagement, capaciteits- en performancemanagement. Deze SLA en DAP maken integraal deel uit van de Overeenkomst en bevatten de minimale eisen zoals vermeld in de conceptovereenkomst en de nader te bepalen KPI's (Key Performance Indicators).

5.11	Opdrachtnemer biedt, indien de storing niet op afstand (remote) opgelost kan worden, on site support aan.
6	**Certificering en deskundigheid**
6.1	De medewerkers van de Opdrachtnemer die werkzaamheden verrichten binnen het beheer van de Microsoft-omgeving beschikken aantoonbaar over actuele Microsoft-certificeringen passend bij hun functie, waaronder (of gelijkwaardig aan): • MD-102 (Modern Desktop Administrator), • AZ-104 (Azure Administrator), • MS-100 of MS-101 (Microsoft 365 Identity & Services). De Opdrachtnemer toont dit aan middels certificeringsbewijzen of een personeelsmatrix.
7	**Migratie**
7.1	Opdrachtnemer is verantwoordelijk voor de gehele migratiefase inclusief een voorbereidende training voor bovenschoolse ICT-medewerkers waarbij ze leren hoe de omgeving werkt.
7.2	Opdrachtnemer stelt altijd in overleg met Opdrachtgever een migratie/overgangsdatum vast. Opdrachtgever geeft hier een schriftelijk akkoord voor.
7.3	De migratie vindt bij voorkeur in de schoolvakantie plaats, waarbij Opdrachtgever faciliteert dat de Opvang (geopend tijdens de schoolvakanties) tijdens de migratiefase kan blijven werken.
7.4	Bij iedere (deel) migratie geeft opdrachtgever een Go/No Go. In het geval van een No Go beslissing worden de extra kosten niet vergoed door Opdrachtgever. Indien een no go beslissing door een derde partij wordt veroorzaakt is Opdrachtnemer niet verantwoordelijk.
7.5	Nazorg is onderdeel van de migratie en wordt niet apart doorbelast aan Opdrachtgever. In de nazorg fase wordt er ook een evaluatiegesprek met Opdrachtgever gehouden. Een basis training is onderdeel van de nazorg fase en dient binnen de migratiekosten zijn inbegrepen.
8	**Rapportage en communicatie**
8.1	Opdrachtnemer en Opdrachtgever evalueren half jaarlijks de IT-dienstverlening. Opdrachtnemer is verantwoordelijk voor het organiseren van dit half jaarlijkse overleg. Na gunning wordt een standaard agenda door Opdrachtnemer gedeeld met Opdrachtgever en onderling afgestemd.
8.2	Opdrachtnemer rapporteert periodiek (minimaal 1 keer per kwartaal) over de resultaten van de Servicedesk, conform de SLA. Op verzoek van Opdrachtgever overlegt Opdrachtnemer deze te allen tijde.
8.3	De Opdrachtnemer levert maandelijks een Service Level Rapportage (SLR) aan met ten minste de volgende onderdelen: • Beschikbaarheid en responstijden per SLA-categorie; • Overzicht van incidenten, trends en herhaalde meldingen; • Beveiligingsmeldingen en compliance-alerts; • Verbeteracties en aanbevelingen voor optimalisatie. Het rapportageformat wordt in overleg vastgesteld bij aanvang van de overeenkomst.
8.4	Gebruikstevredenheid: De Opdrachtnemer voert jaarlijks een gebruikerstevredenheidsmeting uit onder de eindgebruikers van de Aanbestedende Dienst over de geleverde ICT-dienstverlening. • De resultaten worden besproken in het periodiek overleg; • Eventuele verbetermaatregelen worden vastgelegd en opgevolgd; De kosten voor deze meting zijn inbegrepen in de dienstverlening
8.5	Overlegfrequenties:

	Opdrachtgever wenst frequent te overleggen op operationeel, tactisch en strategisch niveau. De initiële inrichting is als volgt vastgesteld; - Operationeel: eens per vier weken - Tactisch: twee keer per jaar - Strategisch: eenmaal per jaar Opdrachtgever behoudt zich te allen tijde het recht voor om deze frequenties aan te passen naar eigen inzicht en oordeel, op basis van de voortgang en performance van Opdrachtnemer, alsmede de realisatie van de gestelde doel-en subdoelstellingen.
9	**Exit plan**
9.1	Op verzoek van Opdrachtgever zullen Partijen binnen 3 maanden of, indien dit op kortere termijn is, voor het einde van de Overeenkomst, gezamenlijk een Exit Plan opstellen. Opdrachtnemer zal alle medewerking verlenen die nodig is bij het invullen van dit Exit Plan. Het exit plan is minimaal 1 maand voor de einddatum gereed.
9.2	Het Exit Plan bewerkstelligt de volledige migratie en/of overstap van de Diensten naar een nieuwe door Opdrachtgever gekozen dienstverlener. Alle werkzaamheden in verband met de migratie en/of overstap zullen geschieden tegen de standaardtarieven van Opdrachtnemer. Partijen zullen ieder de eigen kosten dragen voor het opstellen en bijhouden van het Exit Plan.
9.3	Het Exit Plan bevat in elk geval een volledige omschrijving van: (i) de taken die Opdrachtnemer op zich zal nemen in verband met de overdracht van de Diensten en overige informatie; (ii) de samenwerking tussen Opdrachtnemer enerzijds en Opdrachtgever of een door Opdrachtgever aangestelde derde anderzijds; (iii) het elektronische formaat waarin de relevante informatie ter beschikking zal worden gesteld (waaronder configuraties, Documentatie en codes).
9.4	Tot aan de einddatum voor de Diensten, zoals bepaald in de Overeenkomst, door welke vorm van beëindiging dan ook, blijft Opdrachtnemer volledig verantwoordelijk voor een volledige, tijdige en juiste uitvoering van de Diensten.
10	**Consultancy en advies**
10.1	Consultancy-strippenkaart De Opdrachtnemer stelt jaarlijks een consultancy-strippenkaart van 20 uur beschikbaar voor specialistisch advies, optimalisatie of architectuurvraagstukken. • Deze uren zijn op afroep inzetbaar door de ICT-afdeling van Aanbestedende Dienst; • Uren worden niet afzonderlijk verrekend zolang het jaarvolume van 20 uur niet is overschreden; • De inzet wordt per kwartaal gerapporteerd.
11	**Governance ondersteuning**
11.1	De Opdrachtnemer ondersteunt de Aanbestedende Dienst bij het up-to-date houden van het ICT-governanceplan en de vertaling hiervan naar beleid en inrichting van de Microsoft 365 Tenant. • Deze ondersteuning vindt plaats in maximaal drie sessies per jaar van elk acht uur; De activiteit is inbegrepen in de vaste prijsstelling van de opdracht.
12	**Kennisontwikkeling en innovatie**
12.1	• De Opdrachtnemer draagt zorg voor de structurele kennisontwikkeling van de bovenschoolse ICT-medewerkers van de Aanbestedende Dienst met betrekking tot innovaties binnen het Microsoft-platform.

	• Maandelijks wordt een kort digitaal overlegmoment georganiseerd waarin relevante updates, releases en nieuwe functionaliteiten binnen Microsoft 365, Azure, Intune en aanverwante diensten worden toegelicht. • De Opdrachtnemer verstrekt hierbij beknopte releasenotes en toelichtingen op de mogelijke impact op de omgeving van Aanbestedende Dienst • Deze activiteit is onderdeel van de vaste dienstverlening.
13	**Ondersteuning Power Platform**
13.1	De Opdrachtnemer biedt optionele ondersteuning bij het beheer, de beveiliging en doorontwikkeling van de Microsoft Power Platform-omgeving (Power Apps, Power Automate, Power BI). • De ondersteuning richt zich op governance, lifecyclebeheer, integratie met bestaande processen en adoptie; • Opdrachtnemer levert waar nodig technische ondersteuning bij koppelingen en automatisering; • De dienstverlening kan op afroep plaatsvinden via de consultancy-strippenkaart
14	**IAM (optioneel)**
14.1	Beheer van identiteiten en rolgebaseerde toegang op basis van de toekomstige IAM-oplossing van de Aanbestedende Dienst kan optioneel in de offerte worden opgenomen.