Dit Programma van Eisen is een bijlage bij de Offerteaanvraag "ICT Migratie, Dienstverlening en Netwerk" en beschrijft de eisen met betrekking tot de gevraagde dienstverlening. De eisen zoals gesteld op dit tabblad gelden expliciet voor Perceel A "ICT-migratie -en dienstverlening". Inschrijver verklaart onvoorwaardelijk akkoord te gaan met de gestelde eisen door het uitbrengen van een inschrijving op Perceel A. Indien inschrijver vragen en/of opmerkingen heeft bij de beschreven eisen, dient hij deze in de ingerichte vragenrondes (Nota van Inlichtingen) te stellen. VOOR verzoekt u bij de gestelde vraag de naam van het tabblad, inclusief het eisnummer te vermelden van de eis(en) waar uw vraag betrekking op heeft, zodat de vraag concreet en gericht beantwoord kan worden.

Bij iedere eis op dit tabblad wordt bij elke eis impliciet verwezen naar 'Bijlage 2 - Functionele-Technische IST-SOLL V1.0'. Deze bijlage biedt achtergrond in de vorm van de situatie zoals die nu is bij Stichting VOOR (IST) en de doelsituatie zoals die er na de migratie door opdrachtnemer uit moet zien (SOLL). De beschreven SOLL dient door inschrijver als uitgangspunt te worden genomen waar van toepassing bij onderstaande eisen.

A) Uitvoeringseisen support en servicedesk	
A1	Opdrachtnemer is verantwoordelijk voor het technisch fundament van de ICT-omgeving, waaronder minimaal te verstaan de M365 tenant en de IAM-tool en koppelingen.
A2	Opdrachtgever behoudt de regie over de ICT-omgeving. Interne ICT-medewerkers van opdrachtgever voeren functioneel beheer uit op applicaties.
A3	De ICT medewerkers van opdrachtgever vervullen de rol van 1e lijns support op iedere locatie. Opdrachtnemer stelt een directe 2e lijns servicedesk en waar nodig een 3e lijns servicdesk voor ondersteuning bij incidenten beschikbaar.
A4	Opdrachtnemer stelt een passend ticketingsysteem of service management platform beschikbaar om incidenten en verzoeken te registreren, prioriteren, bewaken en rapporteren. Zowel de ICT-medewerkers van opdrachtgever als de werknemers van opdrachtnemer dienen in dit systeem te kunnen werken, waarbij escalaties en incidenten op effectieve, efficiënte en tijdige wijze kunnen worden afgehandeld. Tickets die worden ingeschoten door medewerkers van opdrachtgever worden in eerste instantie te allen tijde door de interne ICT-medewerkers van opdrachtgever opgepakt (1e lijn). Het dient voor alle medewerkers van opdrachtgever mogelijk te zijn meldingen te maken op het systeem of platform van opdrachtnemer.
A5	**Opdrachtnemer stelt op verzoek van opdrachtgever relevante informatie, data en rapportages uit het ticketsysteem beschikbaar.**

A6	Opdrachtnemer neemt tot 10% per jaar van de 1e lijns incidentmeldingen van medewerkers over van opdrachtgever. Dit komt onder andere voor bij onderbezetting van de 1e lijns servicedesk en/of afwezigheid bij opdrachtgever. De kosten hiervoor worden geacht in het maandelijks tarief voor het hanteren van een 2e/3e lijns servicedesk inbegrepen te zijn. Overschrijdingen op voorgenoemde 10% worden per melding/incident (op jaarbasis, achteraf) afgerekend tegen maximaal het daartoe overeengekomen tarief, zoals aangeboden op het Prijzenblad door opdrachtnemer. Na gunning maken opdrachtnemer en opdrachtgever nadere afspraken over de exacte werkwijze van voorgenoemde overname.
A7	Opdrachtnemer stelt een portaal en/of systeem beschikbaar voor ICT-medewerkers van opdrachtgever, waarin zij de voortgang van de dienstverlening kunnen volgen en eventuele FAQ's kunnen raadplegen.
A8	Jaarlijks stemmen opdrachtgever en opdrachtnemer op 1 oktober de relevante afname-aantallen vast waarop de prijs voor het schooljaar wordt gebaseerd. Hierbij wordt uitgegaan van maandelijkse afname en maandelijkse betaling, op basis van de aan het begin van het schooljaar vastgestelde aantal werkplekken/gebruikers/accounts. Indien gedurende het schooljaar een wijziging plaatsvindt in deze aantallen, wordt dit niet doorberekend in de maandelijkse afname. De maandelijkse afname wordt bijgesteld op 1 oktober van het nieuwe schooljaar. De overeengekomen tarieven mogen worden geïndexeerd en gefactureerd conform hetgeen hierover opgenomen in de Overeenkomst. **De jaarlijkse afstemming geldt voor werkplekken en gebruikers; applicaties en VM's worden maandelijks afgestemd.**

B) Uitvoeringseisen Single Point of Contactrol (regierol)	
B1	De ICT dienstverlener fungeert als Single Point of Contact (SPOC) voor dagelijkse ondersteuning en technische wijzigingen. Hieronder valt het coördineren van werkzaamheden en het verzorgen van afstemming met derde partijen binnen de ICT-keten, zoals de internetprovider en de leverancier van de printoplossing, alsook de netwerkbeheerder van Perceel B. Bij wijzigingen met bijkomende kosten, organisatie impact of benodigde interne communicatie levert de SPOC de benodigde informatie (impact, risico's, kosten) voor het maken van een beslissing. VOOR behoudt hierbij zelf de regie over besluitvorming, prioritering en communicatie richting de organisatie. De voorlopig gegunde inschrijver levert na voorlopige gunning een Dossier Afspraken en Procedures (DAP) aan, waarin exacte rollen en verantwoordelijkheden worden overeengekomen. Deze wordt in samenspraak met VOOR vastgesteld en definitief gemaakt. Het DAP mag niet afwijken van de bepalingen zoals beschreven in dit programma van eisen en de overige aanbestedingsdocumentatie. Opdrachtnemer is gedurende de looptijd van de Overeenkomst verantwoordelijk voor het beheer van het DAP. Eventuele wijzigingen worden door Opdrachtnemer doorgevoerd. **Indien het (definitieve) DAP niet tijdig wordt of kan worden afgerond, waarbij afhankelijkheden bestaan van VOOR, opdrachtnemer en derden, kunnen hierover afwijkende afspraken worden gemaakt in de overeenkomst.**

B2	Opdrachtnemer is verantwoordelijk voor het afhandelen van alle incidenten die verband houden met de ICT-omgeving van opdrachtgever, inclusief de eventuele benodigde aansturing van derden, en het uitvoeren van probleem management, zodat opdrachtgever zo min mogelijk hinder ondervindt van herhalende incidenten. Opdrachtnemer treedt na gunning in overleg met de opdrachtnemer op Perceel B, indien van toepassing, om concrete afspraken te maken over de praktische uitwerking van de SPOC-relatie.
B3	Opdrachtnemer verkrijgt toegang tot systemen en data van opdrachtgever voor zover strikt noodzakelijk voor de uitvoering van de SPOC-dienstverlening.
B4	Opdrachtnemer levert ondersteuning op afstand voor incidentoplossing. Indien noodzakelijk, levert opdrachtnemer on-site ondersteuning. Opdrachtnemer bepaalt in deze de noodzaak.
B5	De minimale beschikbaarheid van de SPOC-dienst (telefonisch en online, **zoals gemeten ten aanzien van de bereikbaarheid en beschikbaarheid van de SPOC-dienst binnen de overeengekomen servicetijden**) en van de onderliggende ICT-diensten van opdrachtnemer is 99,5% op maandbasis, gemeten tijdens overeengekomen servicetijden, exclusief vooraf aangekondigd en met opdrachtgever afgestemd gepland onderhoud.

C) Rapportage

C1	Opdrachtnemer rapporteert maandelijks aan opdrachtgever met betrekking tot: *Security-status (Defender scores), licentieverbruik en SLA-prestaties; *"First Time Fix Rate". Dit percentage geeft aan welk deel van de incidenten bij het eerste contact (servicedesk) definitief is opgelost; *Beschikbaarheid en continuïteit: Overzicht gerealiseerde beschikbaarheid per dienst/component, Vergelijking met afgesproken SLA-normen, Geconstateerde overschrijdingen en oorzaken, Impact op de bedrijfsvoering van opdrachtgever, Herstelmaatregelen en preventieve acties; *Incidentmanagement: Aantal incidenten per categorie en prioriteit, Doorlooptijden (respons- en oplostijden) t.o.v. SLA, Top 10 terugkerende incidenten, Incidenten met hoge impact (P1/P2), inclusief root cause (RCA), Structurele verbetermaatregelen; *Servicerequests: Aantal afgehandelde servicerequests, Gemiddelde en maximale doorlooptijd, Trends in type aanvragen, Eventuele knelpunten in processen of capaciteit. *Wijzigingen en releases (Change & Release Management): Uitgevoerde wijzigingen en releases, Type wijzigingen (standaard, normaal, spoed), Succesgraad (met/zonder verstoring), Geplande wijzigingen komende periode, Afwijkingen van change-procedures; *Capaciteit en performance: Gebruik en trends van relevante ICT-middelen (bijv. storage, netwerk, licenties), Performance-indicatoren van kritische systemen, Verwachte capaciteitsknelpunten, Advies m.b.t. schaalvergroting of optimalisatie; *Security & compliance: Beveiligingsincidenten en meldingen, Patch- en updategraad, Status kwetsbaarheden (bijv. bekende CVE's), AVG-gerelateerde signalen of datalekken, Compliance met relevante normen en afspraken; *Verbeteringen en roadmap: Lopende verbeteracties en status, Lessons learned uit incidenten en changes, Voorstellen voor proces- of dienstverbetering, Relevante ontwikkelingen voor EA ICT-dienstverlening, Aandachtspunten en risico's komende maand; *Managementsamenvatting: Samenvatting van belangrijkste bevindingen, Belangrijkste risico's en aandachtspunten, Conclusies en aanbevelingen, Beslis- of actiepunten voor opdrachtgever. Voorgenoemde geldt als uitgangspunt voor de uitvoering van de dienstverlening. Gedurende de looptijd van de overeenkomst treden opdrachtnemer en opdrachtgever in overleg om te toetsen of de maandelijkse rapportagefrequentie passend is gebleken. Indien een lagere frequentie door opdrachtgever is gewenst, kan de rapportagefrequentie worden gewijzigd.
C2	Opdrachtnemer rapporteert ieder kwartaal aan opdrachtgever met betrekking tot de dienstverlening. **De frequentie en exacte inhoud van deze rapportage wordt na gunning tussen opdrachtgever en opdrachtnemer afgestemd.** ~~*De beschikbaarheid van werkplekken en MS365 vanuit eindgebruikersperspectief:~~ ~~*Kwartaalcijfers over de meest voorkomende typen vragen en incidenten (top 5). Deze rapportage bevat tegens een proactief verbeteradvies om het aantal herhaalvragen te reduceren.~~

C3	Opdrachtnemer rapporteert jaarlijks an opdrachtgever met betrekking tot: *Een overzicht van de actieve ten opzichte van de toegewezen licenties (M365), inclusief een proactief advies over het saneren van ongebruikte licenties (bijv. accounts die >30 dagen niet zijn ingelogd).
C4	Aanvullend levert opdrachtnemer periodiek een rapportage aan de Functionaris Gegevensbescherming (FG) van Opdrachtgever over **bijvoorbeeld** de status van MFA-adoptie, externe deellinks (OneDrive/SharePoint) en eventuele geblokkeerde 'risky sign-ins'. De frequentie **en exacte inhoud** van deze rapportage wordt na gunning tussen opdrachtgever en opdrachtnemer afgestemd.

D) Uitvoeringseisen beheer, onderhoud en support	
Configureren en beheren van werkplekken	
D1	Opdrachtnemer configureert en beheert de benodigde (virtuele) server- en servicecomponenten ten behoeve van de nieuwe ICT omgeving. De omgeving voldoet aan eisen voor beschikbaarheid, performance, schaalbaarheid en beveiliging.
D2	Opdrachtnemer richt de nieuwe werkplekomgeving in volgens de SOLL-beschrijving (Bijlage 2). De werkplekken functioneren stabiel, veilig en conform de geldende standaarden binnen het onderwijs.
D3	Alle mobiele apparaten van de opdrachtgever (inclusief laptops, tablets) dienen via MDM beheerd en beveiligd te worden.
D4	Gevoelige gegevens op devices moeten versleuteld zijn. Dit betekent bijvoorbeeld het inschakelen vanuit het MDM van BitLocker op Windows.
D5	Elk apparaat moet voorzien zijn van actuele anti-malware software. Het normenkader stelt dat bescherming tegen virussen en malware up-to-date gehouden moet worden op mobiele devices. Opdrachtnemer draagt zorg voor deze inrichting.
D6	Via MDM moeten beveiligingsinstellingen centraal worden afgedwongen. Denk aan het verplicht stellen van een apparaatwachtwoord/PIN, automatische vergrendeling na inactiviteit, en het blokkeren van niet-goedgekeurde apps. Dergelijke “standaardconfiguratie” voor devices (baseline) wordt centraal beheerd en gemonitord.
D7	Bij verlies of diefstal van een device moet het MDM de mogelijkheid bieden om op afstand het apparaat te vergrendelen of te wissen (remote wipe) om misbruik van data te voorkomen.

D8	Indien mogelijk mogen geen gevoelige bedrijfsgegevens permanent op devices worden opgeslagen (“zero footprint”). Het normenkader adviseert om te voorkomen dat er onderwijsdata op devices thuis of elders blijft staan. Opdrachtnemer spant zich maximaal in dit advies op te volgen bij het inrichten van de ICT-omgeving.
D9	Er wordt verschillende gebruikersgroepen (b.v. leerlingen, medewerkers) onderscheiden, waarvoor beleid wordt opgesteld waarbij per groep wordt ingesteld of het installeren van applicaties is beperkt tot vertrouwde, door de school goedgekeurde apps.
D10	Licenties die benodigd zijn voor de uitvoering van de dienstverlening worden geacht door opdrachtnemer te worden geleverd. Deze licenties dienen te allen tijde schaalbaar te worden geleverd. Uitzonderingen hierop zijn beschreven in de Aanbestedingsdocumenten, waaronder de Microsoft-licenties en overige licenties die met onderwijskorting kan worden afgenomen door opdrachtgever.
D11	Opdrachtnemer moet Windows-devices kunnen configureren en beheren vanuit MS InTune om te zorgen voor optimale functionaliteit en beveiliging, met specifieke aandacht voor de behoeften van het voortgezet onderwijs, waaronder het installeren en configureren van besturingssystemen, het periodiek toepassen van beveiligingspatches en updates, het implementeren van beveiligingsmaatregelen en de naleving van schoolbeleid en regelgeving. Zie Bijlage 2 voor welke functionele eisen en randvoorwaarden hierbij gesteld worden.
D12	Opdrachtnemer moet nieuwe devices kunnen integreren in de MS InTune-omgeving, met aandacht voor beveiliging en gebruiksvriendelijkheid in een onderwijssetting, waaronder het koppelen van devices met bestaande MDM-systemen en het configureren van devices volgens schoolvereisten.
D13	Opdrachtnemer moet uitgebreide ondersteuning kunnen bieden voor MS365 applicaties en educatieve software binnen het voortgezet onderwijs, waaronder het bieden van technische ondersteuning, probleemoplossing en assistentie bij installatie en configuratie. Zie Bijlage 2 voor een actuele lijst van applicaties die beschikbaar gesteld moeten worden in de nieuwe omgeving.
D14	Tijdens de Centrale Examens en de week daaraan voorafgaand geldt een 'Change Freeze'. Er worden geen wijzigingen in de configuratie doorgevoerd, tenzij dit noodzakelijk is voor de directe continuïteit of veiligheid, en na expliciete goedkeuring van de examencommissie/ICT-manager van het bestuur.
D15	Opdrachtnemer is verantwoordelijk voor het leveren van proactief technisch beheer van de betrokken ICT-infrastructuur.
Toegangsbeheer	
D16	Opdrachtnemer is verantwoordelijk voor IAM. Alle (beheer)toegang tot systemen dient te verlopen via de IAM-dienst van opdrachtnemer, ter waarborging van toegang. Opdrachtnemer conformeert zich hierbij aan de functionele eisen en randvoorwaarden zoals gesteld in Bijlage 2.

D17	Opdrachtnemer richt een volledig functionerend IAM-landschap in, inclusief identity lifecycle management, autorisatiebeheer en integratie met bronsystemen. Rollen, rechten en toegang worden ingericht volgens het leastprivilegeprincipe. Het proces voor toevoegen, muteren en verwijderen van gebruikers is volledig geautomatiseerd.
D18	Iedere gebruiker (leerling of medewerker) moet een eigen account hebben, zodat acties altijd tot een individu te herleiden zijn. Er worden geen generieke accounts gedeeld. Alle gebruikersactiviteiten moeten gelogd en traceerbaar zijn tot een unieke gebruikersnaam binnen M365 en zijn uitgerust met MFA.
D19	Opdrachtnemer stelt in samenspraak met opdrachtgever voorafgaand aan de migratie een autorisatiematrix voor M365 op waarin toegangsrechten per rol/groep zijn vastgelegd op basis van de functies binnen de organisatie van opdrachtgever. Hiervoor dient een RBAC inrichting gebruikt te worden.
D20	Voor alle accounts worden sterke auhenticatiemiddelen toegepast, zeker voor gevoelige systemen. Opdrachtnemer past hierbij minimaal MFA toe.
D21	Opdrachtnemer en opdrachtgever treden na gunning in overleg om procedures in te richten om accounts en rechten tijdig aan te maken, te wijzigen en in te trekken. Nieuwe gebruikers krijgen via een formeel proces de juiste rechten toegewezen en accounts van oud-leerlingen of -medewerkers worden direct gedeactiveerd/verwijderd zodra ze de school verlaten.
D22	Opdrachtnemer beperkt het aantal accounts met beheerdersrechten en monitort het gebruik ervan. Superuser- of beheerdersaccounts dienen apart beheerd te worden (met aparte accounts voor beheer) en voorzien van extra bescherming (zoals MFA). Opdrachtnemer dient alle handelingen die met hoge rechten worden uitgevoerd te loggen. Superuser-toegang wordt alleen toegestaan na goedkeuring door het management van opdrachtgever.
Encryptie	
D23	Opdrachtnemer garandeert dat wanneer encryptie wordt toegepast, hij zorgdraagt voor goed beheer van de cryptografische sleutels. Encryptiesleutels worden veilig opgeslagen (bij voorkeur in een gecertificeerde key-vault of een MDM-beheerde oplossing) en toegang ertoe wordt beperkt.
Monitoring en logging	
D24	Opdrachtnemer monitort real-time op afwijkend inloggedrag (bijv. 'impossible travel', brute force pogingen of inlogpogingen vanuit verdachte geografische locaties) en handelt hierop proactief volgens een opgesteld incident response plan.
D25	Alle logs van acties uitgevoerd door accounts met verhoogde rechten (Global Admins, Privileged Accounts) dienen onwijzigbaar te worden vastgelegd. Deze logs moeten gedurende minimaal 12 maanden beschikbaar blijven voor audit-doeleinden door opdrachtgever.
Gegevens	

D26	Opdrachtnemer hanteert transparante richtlijnen voor opslag en transport van (vertrouwelijke) gegevens. Tijdens de uitvoering van werkzaamheden voor opdrachtgever maakt opdrachtnemer gebruik van versleutelde verbindingen (TLS/SSL, VPN waar nodig).
Actualiteit	
D27	Opdrachtnemer waarborgt de actualiteit van de ICT-dienst als volgt: * Software wordt voortdurend geüpdatet. Het uitgangspunt hierbij is het gebruik van de voorlaatste (N-1) stabiele versie. **Updates (tenzij geinitieed door beveiligingskwesties) worden aangevraag via functioneel beheer van opdrachtgever.** * Vernieuwingen worden actief voorgesteld aan opdrachtgever en na instemming van opdrachtgever doorgevoerd.
Changes	
D28	Op alle niet standaard changes wordt een risicoanalyse uitgevoerd. Hierbij worden zowel het implementatieplan voor de change als de change zelf belicht en wordt de risicodrager bepaald. Voor risico's die de risicobereidheid overstijgen dienen compenserende maatregelen getroffen te worden. Opdrachtnemer kan als bewijs hiervoor reeds gemaakte analyses aanvoeren; alle risicoanalyses worden gedocumenteerd en zijn inzichtelijk voor opdrachtgever.

E) Uitvoeringseisen advisering	
E1	Opdrachtnemer adviseert opdrachtgever op eerste verzoek met betrekking tot ICT-vraagstukken. Dit kunnen bijvoorbeeld vragen zijn over gewenste functionaliteit en/of aanpassingen (changes), het beschikbaar maken van nieuwe applicaties, of input leveren met betrekking tot projecten met een ICT-component.
E2	Opdrachtnemer treedt op als sparringspartner voor de doorontwikkeling van de ICT-omgeving, bijvoorbeeld ten aanzien van de inzet van AI-tools.
E3	Opdrachtnemer heeft hiertoe consultants ter beschikking met aantoonbare kennis en ervaring op minimaal de volgende domeinen: applicatie-integratie, werkplekbeheer, MS365 en informatiebeveiliging.
E4	De gevraagde adviesdiensten/consultants zijn voor opdrachtgever uiterlijk één maand na de ingangsdatum van de overeenkomst beschikbaar.

F) Uitvoeringseisen migratie	
F1	De door opdrachtnemer in te richten ICT-omgeving wordt door opdrachtnemer gebaseerd op de SOLL-architectuur zoals beschreven in Bijlage 2 en de Offerteaanvraag.

F2	Opdrachtnemer is, tenzij uitdrukkelijk anders overeengekomen, verantwoordelijk voor het ontwerp, de levering, installatie, configuratie, migratie en het technisch beheer van alle benodigde technische infrastructuur. Inclusief de coördinatie van de accountaanpassingen in de samenhangende systemen. **Hiermee doelt opdrachtgever op het aanleveren van de relevante informatie en het coördineren van de aanpassingen. Bijvoorbeeld het aanleveren van lijsten waarmee in de samenhangende systemen de nieuwe account prefix kan worden gelijk getrokken door een import, zoals naar de AFAS applicatie.** Tevens is opdrachtnemer verantwoordelijk voor de migratie en conversie van alle relevante data, het projectmanagement tijdens de migratie en de communicatie naar relevante belanghebbenden.
F3	De migratie naar de nieuwe ICT-omgeving dient bij zeer sterke voorkeur 1 januari 2027 gereed te zijn, met uitloop naar 1 februari 2027. Opdrachtgever gaat er hierbij vanuit dat de migratie uiterlijk op 1 augustus 2026 kan starten.
F4	Opdrachtnemer stelt één projectmanager aan die gedurende de gehele migratie als aanspreekpunt fungeert voor opdrachtgever. Deze projectmanager coördineert alle uit te voeren werkzaamheden ten aanzien van dit project. Daarmee is de projectmanager verantwoordelijk voor het tijdig en adequaat uitvoeren van alle werkzaamheden die door opdrachtnemer worden uitgevoerd. De projectleider dient ten minste de volgende werkzaamheden uit te voeren. **A) Het in overleg met opdrachtgever opstellen van het definitieve migratieplan (het concept migratieplan dient als onderdeel van de inschrijving geleverd te worden, als beantwoording op gunningscriterium 1). Het definitieve migratieplan dient uiterlijk vóór het verstrijken van de bezwaartermijn aangeleverd te worden door opdrachtnemer, indien anders overeengekomen. Onder het definitieve migratieplan wordt verstaan een uitgewerkt plan waarin minimaal de fasering, afhankelijkheden, globale planning, verantwoordelijkheden en acceptatiecriteria zijn vastgelegd, op basis van de beschikbare informatie ten tijde van voorlopige gunning. Nadere technische detaillering volgt na intake en validatie van de IST-situatie, in afstemming met Opdrachtgever.** B) Bijwonen en voorbereiden van de werk- en voortgangsbesprekingen. C) Opstellen en bewaken van de tijdsplanning. D) Tijdig vooraf melden van meer- en minderwerk en toestemming vragen voor de uitvoering. E) Tijdig signaleren van knelpunten. **Opdrachtgever begrijpt dat bij A) kosten gemaakt worden door de voorlopig gegunde inschrijver. Mocht in verband met onvoorziene omstandigheden geen overeenkomst worden getekend tussen VOOR en de voorlopig gegunde inschrijver, vergoedt VOOR de eventueel gemaakte aantoonbare kosten ten aanzien van het definief stellen van het migratieplan.** **Indien VOOR aantoonbaar verzaakt in haar taken en verantwoordelijkheden gedurende de periode bij A), worden afwijkende afspraken gemaakt met opdrachtnemer ten aanzien van het definitieve migratieplan. Indien het definitieve migratieplan nog niet is opgesteld ten tijde van contractondertekening, zullen hierover nadere afspraken gemaakt worden in de te ondertekenen overeenkomst.**

F5	Opdrachtgever dient het definitieve migratieplan goed te keuren alvorens opdrachtnemer start met de uitvoering van de migratie.
F5	Opdrachtnemer vervult gedurende de migratie de rol van projectmanager en SPOC. Hierbij is opdrachtnemer ook verantwoordelijk voor de afstemming met de opdrachtnemer op Perceel B.
F6	Waar de migratie impact heeft op de eindgebruikers dient hiervoor afdoende communicatie en training ingericht en gegeven te worden. Dit betreft een gedeelde verantwoordelijkheid met opdrachtgever. **De verantwoordelijkheid van VOOR binnen de training en communicatie betreft het organiseren van aanwezigheid door medewerkers en het verspreiden van communicatie en informatie, indien gewenst en/of noodzakelijk door opdrachtnemer.**
F7	Na gunning treden de opdrachtnemer en VOOR in overleg over de mogelijkheden om een inrichting te realiseren waarbij de data-opslag op devices wordt geminimaliseerd.
F8	Opdrachtgever gaat er op dit moment vanuit dat alle benodigde storage is ondergebracht in overige overeenkomsten en dat storage geen onderdeel is van de opdracht binnen perceel A. Echter kan het voorkomen dat gedurende de migratie wordt gezien dat één of meerdere storagecomponenten nog niet zijn ondergebracht bij een leverancier, of dat additionele storage benodigd is. Opdrachtgever behoudt zich het recht voor om de benodigde storage af te nemen bij opdrachtnemer tegen een marktconform tarief. Hierover maken opdrachtnemer en opdrachtgever na gunning nadere afspraken.
F9	De opdrachtnemer handelt Dynamic Host Configuration Protocol (DHCP) af. Onder afhandeling wordt minimaal de levering van een oplossing en het uitvoeren van het beheer hierop verstaan. Opdrachtnemer dient hiervoor een invulling aan te bieden. Indien opdrachtnemer hierbij een verantwoordelijkheid identificeert voor de netwerkdienstverlener (Perceel B), dient opdrachtnemer na gunning met de gegunde leverancier op het netwerkbeheer perceel afspraken te maken over de invulling van de DHCP.
F10	Nieuwe werkplekken dienen gedurende het lesjaar efficiënt te worden uitgerold, indien door VOOR gewenst.
F11	Opdrachtnemer is verantwoordelijk voor de inrichting van een adequaat beveiligde ICT-omgeving die aansluit bij het gevoeligheidsniveau van de verwerkte gegevens, in overeenstemming met vigerende wet- en regelgeving en ISO 27001/27002.
F12	Indien door opdrachtgever gewenst levert opdrachtnemer de in de Offerteaanvraag gedefinieerde optionele diensten. Opdrachtgever is gerechtigd deze diensten af te nemen bij opdrachtnemer tegen maximaal de in de inschrijving geoffreerde tarieven. Dit betreft een afnamemogelijkheid en geen afnameverplichting voor opdrachtgever.

G) Exit

G1	Opdrachtnemer maakt gebruik van een IAM-tool waarvan het beheer overdraagbaar is bij een eventuele exit en/of beëindiging.
G2	Alle historische data uit het ticketingsysteem en monitoringtools dienen bij exit te worden opgeleverd in een machine-leesbaar en herbruikbaar formaat (bijv. .JSON of .CSV), inclusief de volledige audit-logs van de contractperiode.
G3	Uiterlijk 3 maanden voor de einddatum van de Overeenkomst levert Opdrachtnemer een geactualiseerd 'As-built' dossier op van de gehele inrichting (M365, IAM-koppelingen, applicatie-instellingen). Bij gebrekkige documentatie wordt de laatste termijnbetaling (maand) opgeschort.
G4	Opdrachtgever behoudt te allen tijde het recht om in geval van calamiteiten (zoals faillissement of grove nalatigheid) directe 'Global Admin' toegang op te eisen tot de eigen tenants en omgevingen, zonder tussenkomst van de servicedesk van Opdrachtnemer.
G5	Opdrachtnemer verplicht zich bij beëindiging van de overeenkomst tot deelname aan een overdrachtsperiode van minimaal 2 maanden, waarin de nieuwe leverancier meeloopt ('shadow run'). De kosten hiervoor dienen in de inschrijfprijs te zijn opgenomen.