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 B "Netwerk". Inschrijver verklaart onvoorwaardelijk akkoord te gaan met de gestelde eisen door het uitbrengen van een inschrijving op Perceel B. 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) Scope van de opdracht	
A1	Opdrachtnemer is verantwoordelijk voor het leveren van professionele netwerkbeheerdiensten ter ondersteuning van de totale ICT dienstverlening van opdrachtgever. Opdrachtnemer is verantwoordelijk voor het beheer, onderhoud, de beveiliging en de continuïteit van de volledige netwerkinfrastructuur, inclusief zowel de fysieke als de logische componenten. Het doel van dit perceel is het waarborgen van een veilige, betrouwbare, toekomstbestendige en goed gedocumenteerde netwerkomgeving.
A2	De verantwoordelijkheid voor een correcte werking van de netwerkdienst ligt gedurende de volledige contractperiode volledig bij opdrachtnemer.
A3	Indien een hardwarecomponent defect raakt zonder toedoen van opdrachtgever, draagt de opdrachtnemer zorg voor afhandeling van garantie en herstel via de fabrikant. **De verplichting ten aanzien van garantieafhandeling geldt ook voor hardware die niet door opdrachtnemer is geleverd, voor zover deze hardware onderdeel uitmaakt van de in beheer genomen omgeving.** De kosten voor vervanging buiten fabrieksgarantie of bij defect door toedoen van de opdrachtgever zijn voor rekening van de opdrachtgever.

A4	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.
A5	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.
A6	Opdrachtgever heeft de behoefte om het netwerk in beheer te laten nemen vanaf de aanvang van de opdracht. Waar mogelijk optimaliseert opdrachtnemer de bestaande netwerkomgeving ten aanzien van centralisatie en standaardisatie.Het doel hiervan is het borgen van de continuïteit van de dienstverlening, met één verantwoordelijke partij voor het beheer van het gehele netwerk, ook wanneer recente netwerkapparatuur aanwezig is die nog niet vervangen hoeft te worden. Opdrachtnemer neemt hierbij bestaande netwerkcomponenten (zoals access points, switches of gateways/firewalls) in beheer op tenminste best effort-basis en bij voorkeur op basis van de overeengekomen SLA, mits opdrachtgever aan de onderstaande voorwaarden voldoet: • De apparatuur is eigendom van opdrachtgever, of het bestuur is aantoonbaar bevoegd deze door een andere partij in beheer te laten nemen; • De apparatuur maakt deel uit van een productlijn die centraal beheer en monitoring ondersteunt. • De apparatuur is en wordt nog ondersteund door de fabrikant (lifecycle support, inclusief beveiligings- en firmware-updates) gedurende de beheer-periode; • De apparatuur beschikt (i.v.t.) over een geldige beheer- of Cloudlicentie, óf een dergelijke licentie kan nog worden aangeschaft. De opdrachtnemer beoordeelt tijdens de inventarisatiefase of deze voorwaarden zijn vervuld. Mocht dit niet het geval zijn, wordt in overleg afgestemd over een passende oplossing. Opdrachtnemer is hierbij niet verantwoordelijk voor prestatiebeperkingen of storingen die direct voortkomen uit de beperkingen van de bestaande apparatuur, tenzij hierover andere afspraken zijn gemaakt.

A7	Op termijn beoogt opdrachtgever de bestaande netwerkapparatuur en inrichting te vervangen, ten behoeve van standaardisatie en vernieuwing. Opdrachtgever neemt de eventuele vervanging van apparatuur af bij opdrachtnemer tegen de door opdrachtnemer geoffreerde tarieven in de Inschrijving. Hierbij geldt een 'inkoopprijs plus model', waarbij opdrachtnemer gerechtigd is het overeengekomen opslagpercentage te verrekenen bovenop de inkoopprijs van de apparatuur. Het opslagpercentage zoals geoffreerd door opdrachtnemer mag enkel worden gewijzigd met de geldende indexatieregeling, zoals gesteld in de overeenkomst. Opdrachtnemer dient te allen tijde de geldende inkoopprijzen transparant en inzichtelijk te maken voor opdrachtgever, **bijvoorbeeld door het overleggen van inkoopfacturen.** Opdrachtgever is gerechtigd de apparatuur niet bij opdrachtnemer af te nemen, indien de inkoopprijzen niet transparant en inzichtelijk overlegd kunnen worden.
A8	Indien en voor zover de dienstverlening binnen Perceel B na gunning kwalificeert als het verwerken van persoonsgegevens in de zin van de AVG, treden opdrachtgever en opdrachtnemer in overleg over de vaststelling van een verwerkersovereenkomst. Inschrijver verklaart zich er bij voorbaat mee akkoord dat, indien opdrachtgever dit noodzakelijk acht, een verwerkersovereenkomst wordt gesloten op basis van de door opdrachtgever bij de aanbestedingsdocumenten gevoegde concept-verwerkersovereenkomst, waarbij de aard en omvang van de daarin beschreven verwerking worden beperkt tot netwerkbeheer, netwerkbeveiliging, monitoring en logging.

B) Uitvoeringseisen implementatie	
B1	De implementatie van de gestandaardiseerde, centrale netwerkdienst is bij zeer sterke wens uiterlijk 1 januari 2027 gereed. Opdrachtgever gaat er hierbij vanuit dat de migratie uiterlijk vanaf 1 augustus 2026 kan starten. De implementatie zoals bedoeld in deze eis omvat minimaal de in beheer name van de huidige netwerkomgeving, en de start van de beheerwerkzaamheden.
B2	Opdrachtnemer stelt één projectleider 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. Als zodanig is hij/zij eindverantwoordelijk voor het tijdig en adequaat uitvoeren van alle werkzaamheden die door de Opdrachtnemer worden uitgevoerd. De projectleider dient ten minste de volgende werkzaamheden uit te voeren. A) Het in overleg met opdrachtgever opstellen van het definitieve implementatieplan (het concept implementatieplan dient als onderdeel van de inschrijving geleverd te worden); 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.

B3	Waar de migratie impact heeft op de beheerders van VOOR dient hiervoor afdoende communicatie en training ingericht en gegeven te worden. Dit betreft een gedeelde verantwoordelijkheid met opdrachtgever.

C) Functionele en technische eisen	
C1	Opdrachtnemer implementeert maatregelen om continuïteit te waarborgen, zoals redundantie, failovermechanismen en automatische monitoring. De tools die hiervoor gebruikt worden zijn overdraagbaar.
C2	Alle onderdelen van de dienst (inclusief het ingestelde zendvermogen van de access points, ook i.c.m. eventueel gebruik van externe antennes) voldoen steeds ten tijde van aanbieden c.q. ingebruikname en gedurende de volledige looptijd van de overeenkomst aan de geldende wet- en regelgeving in Nederland. Indien tijdens de looptijd gewijzigde wet- en regelgeving aanpassingen noodzakelijk maakt, zal opdrachtnemer deze tijdig en zonder meerkosten doorvoeren, voor zover dit binnen de invloedssfeer van opdrachtnemer ligt.
C3	Opdrachtnemer voorziet in een stabiele, veilige en beheersbare netwerkvoorziening conform de beschreven SOLL architectuur, die de komende jaren voldoet aan de behoeften van opdrachtgever, en de geldende Voortgezet onderwijs-context. Het netwerk functioneert stabiel en veilig . Opdrachtnemer is verantwoordelijk voor inventarisatie, optimalisatie, centralisatie, levering, beheerbaarheid en correcte werking van de infrastructuur. Technische keuzes worden afgestemd op doelmatig gebruik en beheer.
C4	Opdrachtnemer is verantwoordelijk voor een volledige inventarisatie van de bestaande situatie bij aanvang van de dienstverlening. De inventarisatie heeft als doel: - inzicht te verschaffen in de huidige infrastructuur en voorzieningen; - benodigde capaciteit, prestaties en randvoorwaarden te bepalen; - mogelijke knelpunten, afhankelijkheden en randvoorwaarden in kaart te brengen; - de continuïteit en correcte werking van bestaande diensten en apparatuur te waarborgen binnen de nieuwe omgeving. De wijze waarop de inventarisatie wordt uitgevoerd, wordt door opdrachtnemer bepaald en afgestemd met de opdrachtgever. Opdrachtnemer legt de resultaten vast en stemt deze af met de opdrachtgever voordat implementaties plaatvinden.

C5	Opdrachtnemer zet uitsluitend apparatuur in die op het moment van aanbieding en levering door de fabrikant actief wordt ondersteund en waarvoor geen einddatum van ondersteuning of vergelijkbare einddatum is aangekondigd. Dit uitgangspunt geldt voor alle apparatuur, inclusief de later geleverde apparatuur bij de vervanging van netwerkapparatuur. Opdrachtnemer garandeert dat de ingezette apparatuur gedurende ten minste vijf (5) jaar na ingebruikname door de fabrikant wordt ondersteund. Het streven is dat apparatuur langer meegaat dan deze initiële looptijd en bij voorkeur gedurende de volledige looptijd van de overeenkomst inzetbaar blijft. Opdrachtnemer spant zich in om dit op een veilige en beheerste wijze mogelijk te maken, voor zover binnen zijn invloedsfeer. Indien tijdens de optionele verlengingsperiodes blijkt dat ondersteuning of veilig beheer conform het Programma van Eisen niet langer mogelijk is, treedt opdrachtnemer zo spoedig mogelijk in overleg met de opdrachtgever. Samen wordt gezocht naar een passende oplossing om de continuïteit en kwaliteit van de dienstverlening te waarborgen.
C6	Opdrachtnemer draagt te alle tijden verantwoordelijkheid voor de beschikbaarheid van benodigde licenties, updates en upgrades gedurende tenminste de initiële looptijd van de dienstverlening op de locaties en, tenzij opdrachtnemer expliciet aantoont dat zij dit niet kan door externe factoren, ook gedurende de eventuele verlengingsperiodes.
C7	Opdrachtnemer dient, indien door opdrachtgever toestemming is gegeven, oude apparatuur standaard te demonteren en indien gewenst ook standaard af te voeren en te recyclen of te voorzien van een tweede leven. Opdrachtnemer dient verpakkingsmateriaal te scheiden in een milieustraat.
C8	Bij implementatie en ingebruikname van de dienst draagt de opdrachtnemer er zorg voor dat alle bestaande diensten en verbonden apparatuur die deel uitmaken van de huidige situatie volledig en correct functioneren binnen de nieuwe omgeving, voor zover dit binnen zijn directe invloedsfeer ligt. Voor instellingen of functionaliteiten die buiten zijn directe beheer of bevoegdheid vallen, zet opdrachtnemer zich aantoonbaar actief in om, in samenwerking met de betrokken belanghebbenden, de noodzakelijke acties tijdig te faciliteren of te ondersteunen. Het (her)configureren of instellen van clientapparatuur (zoals laptops, tablets, pc's, printers en overige eindgebruikersapparatuur) valt nadrukkelijk buiten de scope van de dienstverlening. Opdrachtgever is verantwoordelijk voor het in contact brengen van opdrachtnemer met deze belanghebbenden. Indien samenwerking met externe belanghebbenden stagneert, rust de primaire verantwoordelijkheid op opdrachtgever, tenzij tussen opdrachtgever en opdrachtnemer expliciet is vastgelegd dat de regierol bij opdrachtnemer ligt. Opdrachtnemer blijft echter verplicht zich aantoonbaar in te zetten om tot een werkbare samenwerking met de betreffende belanghebbenden te komen.

C9	Het netwerk biedt gescheiden toegang per gebruikersgroep (zoals leerlingen, personeel, gasten, gebouwsystemen, derden die gebruik maken van het pand, zoals een buitenschoolse opvang of kinderdagverblijf) om veilig en beheersbaar gebruik mogelijk te maken. Het beheer van deze segregatie moet overzichtelijk en centraal mogelijk zijn. De benodigde netwerksegregatie (zoals VLAN's) en toegangscontrole wordt zodanig ingericht dat deze aansluit op het beleid en de gebruikssituatie van de schoollocatie. Tussen de VLAN's worden standaard toegangsbeperkingen toegepast, zodat verkeer alleen mogelijk is indien expliciet toegestaan.
C10	Indien gebruik wordt gemaakt van cloudgebaseerde componenten of beheerplatforms binnen de netwerkoplossing geldt het volgende: - Verwerking via de cloud mag uitsluitend betrekking hebben op verkeer naar en van het internet (internet-bound). Intern netwerkverkeer (lokaal LAN/WLAN) wordt lokaal afgehandeld, tenzij anders overeengekomen. - Verwerking en opslag van gegevens vindt uitsluitend plaats binnen de EER. **Deze eis is van toepassing is op alle gegevens die direct of indirect persoonsgegevens kunnen bevatten, waaronder logging van netwerkverkeer, gebruikersauthenticatie en beheerdata die gebruikersinformatie bevat, in lijn met de AVG. Configuratiebackups, telemetrie en supportdata die aantoonbaar geen persoonsgegevens bevatten vallen niet onder de EER-vereiste.** - Tunnels tussen netwerk en cloudcomponenten zijn end-to-end sterk versleuteld. - Toegang tot beheerportals vindt uitsluitend via tweefactorauthenticatie (2FA). Het platform biedt logging van beheerdersacties en wijzigingen, met exportmogelijkheden voor audits. - Opdrachtnemer waarborgt de beschikbaarheid van de dienst, inclusief maatregelen bij verstoring of uitval van de verbinding met de cloud. - Indien filtering of DNS-diensten via de cloud verlopen, dient bij uitval van de tunnel een automatische fallback plaats te vinden naar een lokale oplossing. Indien dat niet mogelijk is, wordt het verkeer standaard geblokkeerd totdat de verbinding is hersteld. **De in deze eis opgenomen vereisten zijn uitsluitend van toepassing indien de inschrijver gebruikmaakt van cloudgebaseerde componenten of beheerplatforms binnen de aangeboden netwerkoplossing. Indien geen cloudcomponenten worden ingezet, zijn deze specifieke eisen niet van toepassing.**

C11	Indien in de dienstverlening AI-technologie wordt toegepast (bijv. voor netwerkbeheer, incidentdetectie of capaciteitsanalyse), borgt opdrachtnemer dat deze technologie op een aantoonbaar veilige, betrouwbare en controleerbare wijze wordt ingezet. - Voor AI-functionaliteit die door opdrachtnemer zelf wordt ontwikkeld en/of beheerd, richt opdrachtnemer een passend proces in voor periodieke beoordeling van nauwkeurigheid, prestaties en relevante risico's (zoals foutgevoeligheid of ongewenste bias) en voor het vooraf valideren van significante wijzigingen. - Voor AI-functionaliteit die wordt geleverd door een derde partij(vendor) zet opdrachtnemer zich aantoonbaar in om (binnen haar invloedsfeer) gebruik te maken van beschikbare documentatie, testrapporten en controles van deze derde partij en waar nodig aanvullende maatregelen te treffen, zodat de inzet van deze AI-functionaliteit zoveel mogelijk voldoet aan de genoemde uitgangspunten. - Op verzoek verstrekt opdrachtnemer aan opdrachtgever een toelichting op de gebruikte AI-functionaliteit, voor welk doeleinde deze wordt ingezet en welke bekende beperkingen of risico's daarbij gelden.
C12	Opdrachtnemer gebruikt waar mogelijk bestaande bekabeling bij het doorvoeren van vervanging en/of optimalisaties. Indien nieuwe bekabeling vereist is (bijv. voor switches of access points), wordt deze aangelegd conform benodigde en toekomstig verwachtte prestatie-eisen.
C13	Het draadloze netwerk moet geschikt zijn voor moderne, interactieve en media intensieve onderwijstoepassingen. Hierbij moeten applicaties zoals streaming video (1080p), videobellen en online educatieve platforms zonder merkbare vertraging, buffering of wegvallende verbindingen functioneren. In de door opdrachtnemer in te richten netwerkomgeving wordt rekening gehouden met roaming, automatische load balancing, interferentie en netwerkbelasting.

C14	Het WLAN voldoet, na vervanging door opdrachtnemer, minimaal aan de Wi-Fi 7-standaard: * De access points moeten gelijktijdig kunnen uitzenden op 2,4 GHz, 5 GHz en de 6 GHz-band. Access points die twee van deze drie banden gelijktijdig kunnen uitzenden zijn toegestaan, mits de leverancier motiveert dat deze configuratie voldoet aan de prestatie- en dekkingsbehoeften van opdrachtgever en geen afbreuk doet aan de continuïteit en veiligheid van het netwerk. **Een Wi-Fi 7-oplossing zonder gelijktijdige inzet van 6 GHz is acceptabel wanneer uit ontwerp, survey en clientanalyse blijkt dat dit beter aansluit op de onderwijsbehoefte en bestaande clientpopulatie.** * De ondersteuning van oudere clientprotocollen moet uitgeschakeld kunnen worden; * De access points zijn backwards compatible met oudere Wi-Fi-standaarden. Indien opdrachtgever vraagt om access points met geïntegreerde ondersteuning voor Bluetooth (bij voorkeur BLE) en/of Zigbee, geldt: * De Bluetooth- en Zigbee-radio's zijn geïntegreerd in het access point. Er zijn geen aparte gateways en/of extra bekabeling benodigd. * Verkeer van Bluetooth- en Zigbee-apparatuur kan worden ondergebracht in passende, logisch gescheiden netwerksegmenten (bijvoorbeeld een IoT/gebouwbeheernetwerk).
C15	De wifi is schaalbaar en geschikt voor een inzet van ten minste 50 access points binnen één locatie, zonder functionele of prestatiebeperkingen.
C16	De wifi biedt de mogelijkheid om een gastnetwerk op te zetten waarbij gebruikers akkoord dienen te gaan met de voorwaarden die de school hieraan stelt. Daarnaast ondersteunt het gastnetwerk de mogelijkheid tot client isolation, zodat gebruikers op het gastennetwerk geen toegang hebben tot andere apparaten op hetzelfde netwerk.
C17	Het LAN-netwerk moet voldoende capaciteit en snelheid bieden voor stabiel gebruik van de dienst op alle werkplekken, access points en andere aangesloten apparatuur. De opdrachtnemer borgt dat de interne netwerkstructuur geen knelpunten vormt bij gelijktijdig gebruik van de infrastructuur.
C18	De switches ondersteunen te alle tijden voldoende stroomvoorziening (PoE) om de volledige functionaliteit van de aangesloten apparatuur zoals access points, VoIP-telefoons en andere PoE-apparaten, te ondersteunen, zonder dat deze in beperkte of low-power modus hoeven te functioneren.
C19	Access points worden waar mogelijk verdeeld over meerdere switches.

C20	Eén van de andere diensten waar opdrachtgever van gebruik maakt is de dienst Veilig Internet. De dienst Veilig Internet kan op verschillende manieren worden aangesloten, bijvoorbeeld op een schoollocatie of via een datacenter. De dienst Veilig Internet wordt op de locatie gedemarqueerd met een Customer Premises Equipment (CPE). Middels deze CPE wordt er een verbinding opgezet naar het Nationaal diensten Centrum (NDC) waar de beveiliging wordt verzorgd en vervolgens het internet op wordt gegaan. Scholen die gebruik willen maken van Veilig Internet hebben zelf een routerend device (laag 3) nodig die aangesloten wordt op de CPE. We noemen dit een gateway. Opdrachtnemer dient een gateway te kunnen leveren die minimaal voldoet aan de volgende eisen: • IP-routing op IPv4 en IPv6; • Nat-translatie; • VLAN segmentatie en aggregatie; • Instellen van statische routes; • Minimaal 2x 1Gbit UTP poort; • Voldoende verwerkingscapaciteit die past bij de internetverbinding en het aantal actieve devices in het netwerk; • Throughput van 1 Gbps. • VPN-tunnel opzetten
C21	Opdrachtnemer inventariseert indien van toepassing bestaande firewallregels en eventuele VPN-tunnels en draagt zorg voor het correct overzetten hiervan naar de nieuwe situatie, voor zover dit binnen zijn directe invloedsfeer ligt. Opdrachtgever zorgt ervoor dat opdrachtnemer ten behoeve van deze inventarisatie ten minste over alleen-lezen toegang tot de bestaande configuratie kan beschikken (bijvoorbeeld via een read-only account of een configuratie-export).
C23	Indien opdrachtgever BYOD toepast, dient het geleverde netwerk veilig gebruik van persoonlijke apparaten (zoals laptops, tablets en smartphones) te ondersteunen. Scholen die beperkt of geen BYOD gebruiken, kunnen volstaan met het gastennetwerk.

C24	De netwerkoplossing ondersteunt standaard toewijzing van toegangsrechten op basis van centraal beheerde gebruikersrollen uit een directory (bijv. Microsoft 365, of vergelijkbaar). De oplossing zorgt ervoor dat: • identificatie, authenticatie en autorisatie van gebruikers altijd worden afgedwongen; • alle gebruikersactiviteiten traceerbaar zijn tot unieke gebruikers; • functiescheiding en autorisatiematrix van opdrachtgever technisch kunnen worden afgedwongen; • rapportages/exports beschikbaar zijn waarmee de feitelijke toegangsrechten (IST) periodiek door opdrachtgever vergeleken kunnen worden met de vastgestelde SOLL-matrix die opdrachtgever in haar eigen autorisatiebeleid heeft opgenomen. • toekenning, wijziging en intrekking van netwerktoegang verlopen via de centrale identity-provider van opdrachtgever (bijv. Microsoft Entra ID,of vergelijkbaar), waarbij intrekking van rechten automatisch plaatsvindt op basis van wijzigingen in de directoryrollen. Opdrachtnemer draagt er zorg voor dat ook apparaten zonder standaardondersteuning voor gebruikersauthenticatie op passende wijze veilig en traceerbaar toegang krijgen.

C25	U dient een firewall te kunnen leveren met de volgende functionaliteiten: • De firewall moet in staat zijn om de minimaal de huidige verwachte maximale bandbreedte van de internetaansluiting van de locatie op volle capaciteit te kunnen verwerken inclusief NAT en VPN en daarnaast ten minste 30% extra verwerkingscapaciteit bieden voor toekomstige groei in bandbreedte en gebruik. De firewall moet voldoende sessiecapaciteit leveren voor het volledige aantal gebruikers, inclusief gelijktijdig gebruik van video, streaming en cloudapplicaties. • De firewall moet in staat zijn specifieke websites of domeinen te blokkeren of toe te staan op basis van beheerde lijsten (URL-filtering). • Pakketfiltering: de firewall moet in staat zijn om netwerkverkeer kunnen te inspecteren op basis van IP-adressen, poorten, protocollen en mogelijk andere criteria. Het moet regels kunnen toepassen om te bepalen of pakketten al dan niet worden doorgelaten. • Stateful inspection: de firewall moet de staat van verbindingen kunnen bijhouden en alleen inkomend verkeer toestaan dat betrekking heeft op geautoriseerde uitgaande verbindingen. • Network Address Translation (NAT): De firewall dient IP-adressen en poortnummers van pakketten te kunnen wijzigen wanneer deze tussen het interne en externe netwerk worden doorgegeven. Dit kan helpen bij het verbergen van interne IP-adressen en het beheren van de toegang tot interne bronnen vanaf externe netwerken. • Toegangscontrolelijsten (ACL's): de firewall moet in staat zijn ACL's te kunnen beheren van het inkomende en uitgaande verkeer op basis van bron- en bestemmingsadressen, poorten en protocollen. • VPN-ondersteuning: De firewall moet Virtual Private Network (VPN) tunnels kunnen opzetten en beheren voor beveiligde externe toegang tot het netwerk. • Beheer en configuratie: De firewall moet een intuïtieve gebruikersinterface en centraal beheerplatform hebben voor eenvoudige configuratie, monitoring en onderhoud van de firewall en het netwerk. opdrachtgever dient leesrechten te krijgen voor de firewall indien gewenst. • Usertracking, Logging en rapportage: De firewall dient uitgebreide logging en rapportagemogelijkheden te hebben om netwerkactiviteit te volgen, beveiligingsgebeurtenissen te analyseren en nalevingsvereisten te ondersteunen. In sommige gevallen kan dit op gebruikersniveau worden uitgevraagd (usertracking). Daarbij kan gewenst zijn wie welk internet adres wanneer heeft bezocht en vanaf welk device. • Applicatie-laag filtering: De firewall moet op applicatieniveau kunnen inspecteren, waardoor het mogelijk is om specifiek verkeer te blokkeren op basis van applicatieprotocollen (bijv. HTTP, FTP, SMTP). • Netwerksegmentatie en VLAN's: De firewall dient het netwerk op te kunnen delen in logische segmenten met behulp van VLAN's en andere segmentatietechnieken om de beveiliging te verbeteren en het verkeer te isoleren. • De firewall wordt inclusief rackmount geleverd. In het Prijzenblad dient Inschrijver een prijs te offreren voor de optionele firewall. De aangeboden firewall dient minimaal te voldoen aan bovenstaande eisen. Gedurende de looptijd van de overeenkomst treden opdrachtnemer en opdrachtgever in overleg of de firewall afgenomen wordt.
C26	Opdrachtnemer neemt een regierol op gedurende vervanging- en optimalisatieprojecten. Dit houdt in dat hij regie over externe partijen op zich neemt en uitgebreide ondersteuning biedt buiten zijn directe invloedsfeer.

D) Uitvoeringseisen

D1	Opdrachtnemer dient een vaste projectorganisatie te formeren voor de opdracht met de volgende eisen: • Een vast aanspreekpunt die verantwoordelijk is voor de voortgang, afstemming en terugkoppeling tenminste gedurende de voorbereiding en implementatie (tot overgang naar beheer); • Tenminste een tweewekelijkse voortgangsoverleg met opdrachtgever inclusief voortgangsrapportage; • Gebruik van een gedeelde online omgeving waarin de actuele status en planning inzichtelijk zijn.
D2	Voorafgaand aan iedere oplevering (zowel gedurende de implementatie als latere vervangingstrajecten) voert opdrachtnemer, in afstemming met opdrachtgever, een test- en acceptatieprocedure uit om aan te tonen dat de functionaliteit, prestaties en kwaliteit van de dienstverlening voldoen aan de overeengekomen eisen. Het test- en acceptatieprocedure omvat minimaal: • Het opstellen en ter akkoord voorleggen van een testplan waarin wordt beschreven: de testrondes, testgevallen, beoogde resultaten, gebruikte testmethodiek, rollen/ verantwoordelijkheden en planning; • Het uitvoeren van de overeengekomen testen door de opdrachtnemer (en waar van toepassing opdrachtgever) met gebruik van representatieve data en omstandigheden; • Het vastleggen van testresultaten in een testrapport, inclusief geconstateerde afwijkingen, analyse en herstelacties; • In geval van gebreken worden deze binnen redelijk termijn verholpen en opnieuw getest; • Formele acceptatie door opdrachtgever.
D3	Wordt de dienstverlening bij de tweede acceptatie opnieuw afgekeurd, dan kan opdrachtgever de nadere overeenkomst geheel of gedeeltelijk ontbinden, herstel verlangen of voorwaardelijk accepteren met herstelverplichting. • Gebreken die het productief gebruik niet verhinderen, zijn geen grond voor weigering van acceptatie, maar moeten door opdrachtnemer worden hersteld. Voor structurele of kritieke gebreken kan in overleg een tijdelijke oplossing worden toegepast. • Bij deelleveringen vindt acceptatie per deel én een integrale eindacceptatie plaats.

D4	Nadat de test- en acceptatieprocedure is uitgevoerd kan over worden gegaan op oplevering. Bij oplevering wordt per locatie een opleverrapport verstrekt met daarin tenminste: • Geleverde hardware (aantallen, types, specificaties); • Aftersurvey met dekking/capaciteitseisen, inclusief bandbreedtemeting; • Eventuele restpunten, gebreken en adviezen; - In geval van restpunten of gebreken binnen de eigen invloedsfeer en dienst van de opdrachtnemer zal een redelijk termijn worden afgestemd waarin de opdrachtnemer deze gebreken verhelpt. Er zal, indien van toepassing, een nieuwe aftersurvey en/of testverslag kosteloos worden opgesteld om aan te tonen dat de betreffende restpunten of gebreken zijn verholpen. • Ingangsdatum van dienstverlening en facturatie; • Acceptatie van opdrachtgever. • Oplevering inclusief akkoord aanleveren per mail aan opdrachtgever. Opdrachtnemer levert binnen één maand na uitvoering van de acceptatieprocedure per locatie het opleverrapport. Het rapport wordt digitaal beschikbaar gesteld aan opdrachtgever en opdrachtgever in de samenwerkingsomgeving en beide partijen worden hiervan op de hoogte gebracht. Na aanlevering van het opleverrapport beoordeelt opdrachtgever deze binnen twee weken (uitgezonderd schoolvakanties) en maakt bekend of het rapport wordt geaccepteerd. Bij uitblijven van een reactie van opdrachtgever geldt het rapport als geaccepteerd.
D5	Opdrachtnemer levert op verzoek van opdrachtgever documentatie aan over de geleverde dienst. Dit is tenminste: • Een grafisch overzicht van de componenten/voorziening; • De uiteindelijke locatie van de geïnstalleerde componenten; • Merk, type en MAC-adressen en naam van geïnstalleerde componenten*; ** Opdrachtnemer levert deze informatie in een digitaal gangbaar leesbaar formaat, zoals CSV of Excel. Opdrachtnemer zorgt dat de dienst indien nodig wordt aangepast als de situatie op een locatie is veranderd, bijvoorbeeld na een interne verbouwing.*

D6	Opdrachtnemer hanteert een formeel vastgelegd beleid en procedure voor het beheer van super-userrechten/ beheeraccounts op netwerkcomponenten en beheerplatformen: • Toekenning van dergelijke rechten is uitsluitend toegestaan aan vooraf aangewezen personen, op basis van aantoonbare autorisatie door het verantwoordelijke management van opdrachtnemer en opdrachtgever. • Gebruik van super-userrechten wordt volledig gelogd en periodiek geëvalueerd (minimaal halfjaarlijks). • Voor situaties waarin noodtoegang noodzakelijk is (noodprocedure), beschikt opdrachtnemer over een gescheiden, formeel vastgelegde noodprocedure waarbij het gebruik van noodrechten en/of noodwachtwoorden wordt geregistreerd, achteraf geëvalueerd en bijstelling van rechten plaatsvindt indien noodzakelijk. • opdrachtgever behoudt het recht inzage te krijgen in de logging en evaluaties van het gebruik van super-user- en noodrechten.

E) Uitvoeringseisen beheer en support	
E1	Het netwerk dient een minimale beschikbaarheid te hebben van 99,8%, exclusief gepland onderhoud. **De beschikbaarheidseisen zijn exclusief verstoringen zijn die aantoonbaar voortkomen uit beperkingen van bestaande, nog niet vervangen apparatuur of door opdrachtgever/derden beheerde afhankelijkheden.**
E2	Opdrachtgever levert zelf eerstelijnssupport, waarbij wordt uitgegaan dat opdrachtgever de basisprobleemoplossing kan oppakken waarvoor geen diepgaande technische kennis is vereist. Opdrachtnemer levert een tweede- en derdelijns support. De opdrachtnemer beschikt over diepgaande kennis om tot de juiste probleemoplossing te komen. Daarbij geldt dat de opdrachtnemer zich proactief inzet bij problemen om de oorzaak en de oplossing zo snel als mogelijk en adequaat te bewerkstelligen, ook als op voorhand onduidelijk is in welk domein een probleem zich bevindt. Als supportkanaal wordt tenminste telefonische bereikbaarheid vereist. Daarnaast tenminste één schriftelijke vorm van support, bijvoorbeeld chat, mail of portal.

E3	De beschikbaarheid van de WLAN, LAN en Gateway/firewall bedraagt minimaal 99% per locatie per jaar, exclusief vooraf aangekondigd onderhoud **en verstoringen zijn die aantoonbaar voortkomen uit beperkingen van bestaande, nog niet vervangen apparatuur of door opdrachtgever/derden beheerde afhankelijkheden.** Deze beschikbaarheid is gebaseerd op enkelvoudige uitvoering (van chassis). Er is sprake van beschikbaarheid van de dienst, als: WLAN: • 95% van de gebruikers in één ruimte binnen 30 seconden kunnen verbinden met het wifinetwerk; • De beschreven prestatie-eisen door het aantal gebruikers in de benoemde ruimtes wordt behaald; • De packetloss minder is dan 2% over een periode van 5 minuten en de reactietijden lager liggen dan 75ms tussen het access point en een vast meetpunt in het vaste netwerk, op basis van metingen vanuit de wifiinfrastructuur. LAN (uitgangspunt: maximale belasting van 80% van de netto beschikbare bandbreedte): • De verbindingen behalen tenminste een netto doorvoersnelheid van 90% van de linksnelheid; • Packetloss van minder dan 0,5% over een periode van 5 minuten en reactietijden dienen lager te zijn dan 15ms tussen client en een willekeurig netwerkapparaat in het vaste netwerk.
E4	Opdrachtnemer hanteert een geformaliseerd configuratiebeheer waarin alle configuratie-items, hun relaties en wijzigingen gedurende de levenscyclus centraal worden vastgelegd en bewaakt in een CMDB, ondersteund door een configuratiemanagementtool met monitoring en automatisering. Minimaal wordt geborgd dat: • middelen (hardware, software, licenties) en wijzigingen automatisch worden geregistreerd; • configuratie-baselines worden vastgelegd na wijzigingen; • relaties tussen CI's worden onderhouden; • procedures zijn gedocumenteerd, gestandaardiseerd en afgestemd met change/incident/problemmanagement; • bedrijfsmiddelen worden gelabeld en bij inkoop geregistreerd; • licenties levenscyclus breed worden beheerd volgens beleid.

E5	Opdrachtnemer voert updates, upgrades, patches en ander preventief onderhoud uitsluitend uit binnen een vooraf met opdrachtgever overeengekomen onderhoudsvenster (uitgangspunt ma–vr **19:00**–07:00 uur en in het weekend). Gepland onderhoud wordt minimaal 10 werkdagen vooraf aangekondigd en afgestemd met opdrachtgever, waarbij rekening wordt gehouden met onderwijsspecifieke activiteiten (zoals ouderavonden). Voor onderhoud dat zeer beperkte impact heeft (geen merkbare verstoring, prestatievermindering, netwerkonderbreking of herstart van apparatuur) kan een verkorte aankondigingstermijn van minimaal 5 werkdagen worden gehanteerd, mits deze vooraf is afgestemd met én expliciet is goedgekeurd door de opdrachtgever. Onderhoud dat mogelijk enige impact, uitval of prestatievermindering kan veroorzaken valt altijd onder de standaardtermijn van minimaal 10 werkdagen. Uitval als gevolg van gepland onderhoud telt niet mee voor de beschikbaarheid, tenzij de oorzaak ligt bij tekortkomingen van de opdrachtnemer. Voor kritieke security-updates mag van de voorafgaande aankondiging worden afgeweken.
E6	De opdrachtnemer beschikt over een formeel wijzigingsbeheerproces voor alle netwerkcomponenten. Binnen dit proces geldt: • Classificatie: alle wijzigingen worden vooraf geclassificeerd op impact en risico. • Kleine of standaardwijzigingen: wijzigingen met beperkte impact (bijvoorbeeld een SSID toevoegen of VLAN aanpassen) worden na eenvoudige toetsing uitgevoerd. • Wijzigingen met hoge impact: wijzigingen met aanzienlijke gevolgen voor continuïteit, prestaties of beveiliging worden vooraf getoetst, getest en goedgekeurd voordat deze in productie worden doorgevoerd. • Testomgeving: voor wijzigingen met hoge, kritieke impact vindt validatie plaats in een gescheiden, beveiligde testomgeving of een gelijkwaardig alternatief (bijv. leverancierslab of virtuele testopstelling), met een testplan, vastgelegde acceptatiecriteria, terugvalplan en formele overdracht naar productie.
E7	Opdrachtnemer voert kleine, standaard wijzigingen in de netwerkconfiguratie kosteloos uit, mits deze binnen 30 minuten af te handelen zijn. Onder kleine wijzigingen kan bijvoorbeeld verstaan worden: configuratiewijzigingen zonder impact op het ontwerp, capaciteit of beveiligingsarchitectuur zoals een SSID toevoegen of het toevoegen/verwijderen van een MAC-adres. De responstijd voor standaard wijzigingen wordt overeengekomen in het SLA. Bij een wijzigingsverzoek geeft de opdrachtnemer altijd vooraf een terugkoppeling of het verzoek wordt aangemerkt als een standaard wijziging (kosteloos) of als een niet-standaard wijziging, waarbij een prijsindicatie wordt verstrekt vóór uitvoering. Het is niet toegestaan grotere wijzigingen op te delen in meerdere kleine wijzigingen om deze als standaardwijzigingen aan te merken.

E8	Niet standaard wijzigingen kunnen zeer uiteenlopend zijn. Opdrachtnemer dient tenminste binnen de responstijd zoals overeengekomen in het SLA antwoord te geven op een verzoek voor een niet standaard wijziging. Afhankelijk van de aard wordt tussen opdrachtgever en opdrachtnemer afgestemd wat de uiterste oplostijd is voor deze wijziging. Daarbij geldt dat opdrachtnemer proactief handelt en een redelijk termijn afstemt t.b.v. deze wijziging. Indien van toepassing en afhankelijk van de impact stelt opdrachtnemer een plan van aanpak en offerte op en wordt een test- en acceptatieprocedure opgesteld alvorens een wijziging wordt doorgevoerd.
E9	De opdrachtnemer beschikt over een formeel gedocumenteerde noodwijzigingsprocedure met concrete toegewezen verantwoordelijkheden. Noodwijzigingen worden geautoriseerd, uitgevoerd volgens procedure en achteraf geregistreerd en geëvalueerd.

F) Monitoring en Beveiliging	
F1	Opdrachtnemer voert netwerkbeheer uit conform geldende beveiligingsstandaarden, waaronder ISO 27001 en NEN ISO 27002, of gelijkwaardig. Opdrachtnemer implementeert en onderhoudt een beveiligde segmentatie van het netwerk (VLAN's, microsegmentatie waar relevant). Opdrachtnemer draagt zorg voor logging en centrale opslag van relevante netwerkgebeurtenissen. Opdrachtnemer ondersteunt de opdrachtgever in naleving van de AVG, inclusief logging, toegangsbeheer en dataminimalisatie. Indien gewenst past opdrachtnemer firewall regels en NAC policies toe conform het beleid van de opdrachtgever.
F2	Opdrachtnemer voert periodiek (jaarlijks) penetratietests en beveiligingstesten uit op de componenten van de dienst en richt voor alle relevante componenten binnen haar dienstverlening passende logging- en monitoringsmaatregelen in. Deze maatregelen detecteren ongebruikelijke activiteiten, prestatieproblemen en beveiligingsrelevante gebeurtenissen binnen de dienst. Opdrachtnemer bewaakt deze signalen binnen het afgesproken supportvenster en volgt dit op.

F3	De opdrachtnemer biedt een centrale beheer- en monitoromgeving waarmee alle netwerkcomponenten op afstand kunnen worden beheerd en bewaakt. opdrachtgever krijgt op verzoek leesrechten op deze omgeving en kan, indien overeengekomen, beperkte wijzigingen uitvoeren (bijv. het toevoegen van een SSID). De opdrachtnemer verzorgt doorlopende monitoring om de beschikbaarheid, prestaties en veiligheid van de dienst te waarborgen. Minimaal wordt geborgd dat: • Alle hoofdcomponenten van het netwerk tijdens het supportvenster continu worden gemonitord; • Real-time gegevens over capaciteit, gebruik, storingen en beveiligingsgebeurtenissen worden verzameld en geanalyseerd; • opdrachtgever via dashboards of rapportages inzicht krijgen in netwerkgebruik en -capaciteit (bijv. per SSID/VLAN, access point of poort); • Signalen van afwijkingen of dreigingen proactief worden opgevolgd en, indien relevant, gedeeld met opdrachtgever.
F4	De opdrachtnemer voorziet alle apparatuur tijdig van de juiste configuratie en (security) updates volgens de voorschriften van de opdrachtnemer(s) van de apparatuur, software en (cloud)diensten. Hierbij geldt dat de opdrachtnemer security patches binnen 1 maand na het uitkomen ervan door de fabrikant installeert. Deze verplichting heeft betrekking op componenten waarvoor de fabrikant nog updates en patches beschikbaar stelt.
F5	Beveiligingskwetsbaarheden worden beoordeeld volgens de CVSS-methode. Kwetsbaarheden met een score van 7–8 worden binnen vijf (5) werkdagen verholpen; bij een score van 9–10 binnen achtenveertig (48) uur. Tot herstel treft Opdrachtnemer alle mogelijke maatregelen om de dienst en gebruikers te beschermen. Indien deze termijnen door externe afhankelijkheden (bijv. fabrikant) niet haalbaar zijn, licht Opdrachtnemer dit op eerste verzoek toe aan opdrachtgever, inclusief genomen acties, afhankelijkheden en verwachte oplostermijn. **Wanneer een fabrikant nog geen patch beschikbaar stelt, is een aantoonbare mitigerende maatregel of workaround tijdelijk als passende invulling van deze eis acceptabel.**
F6	De opdrachtnemer volgt een formeel incidentproces waarbij beveiligingsincidenten op het netwerk worden gedetecteerd, beoordeeld, gemeld en opgevolgd. Incidenten worden geclassificeerd naar ernst, acties worden geregistreerd, geëvalueerd en waar nodig gerapporteerd. Incidenten met mogelijke privacy-impact worden binnen 24 uur gemeld aan (de FG van) opdrachtgever.
F7	Bij terugkerende storingen of prestatieproblemen analyseert de opdrachtnemer de onderliggende oorzaak (root-cause) en treft structurele maatregelen. De opdrachtnemer levert hiervan een problemmanagementrapportage aan opdrachtgever.

G) Rapportage	
G1	In geval van een Prio-1 incident, conform de classificering zoals overeengekomen in de SLA, is opdrachtnemer verplicht om op verzoek van het opdrachtgever een storingsrapportage te sturen. In deze rapportage staat ten minste: • Beschrijving van incident met daarbij de gevolgen voor de gebruikers; • Startdatum en tijdstip van het incident; • Einddatum en tijdstip van het incident; • Een samenvatting van de gevolgde oplosprocedure met de daarbij relevante timestamps; • De oorzaak van het incident; • Door de opdrachtnemer genomen maatregelen om herhaling in de toekomst te voorkomen.
G2	De opdrachtnemer voorziet opdrachtgever op aanvraag een incidentenrapportage waarin een overzicht wordt verschaft van alle aangemelde incidenten. In deze rapportage staat ten minste: • Type storing (major of minor); • Beschrijving van de aangemelde storing; • Beschrijving van de oorzaak en oplossing; • Start datum en tijdstip van het incident; • Eerste reactie datum en tijdstip op het incident; • Eind datum en tijdstip van het incident; • Percentage behaalde KPI's per type storing (major/minor) conform de SLA.

H) Samenwerking en escalaties	
H1	De opdrachtnemer hanteert een formeel vastgelegde incident-escalatieprocedure (inclusief escalatiecriteria) die gebaseerd is op serviceniveaus. Categorisering en prioritering van incidenten vindt aantoonbaar plaats op impactanalyse met bijbehorende escalatie naar verantwoordelijken.

H2	In gevallen waarbij na implementatie opdrachtgever problemen blijft ondervinden en het onduidelijk is in welk domein dit probleem zich afspeelt, moet opdrachtnemer proactief tot een oplossing proberen te komen. Indien achteraf blijkt dat de problemen komen vanuit het domein van de opdrachtnemer zal de opdrachtnemer dit ook kosteloos doen. In geval de oorzaak van de problemen buiten het domein van de opdrachtnemer ligt, staat het de opdrachtnemer vrij hier naar alle redelijkheid kosten voor in rekening te brengen op basis van nacalculatie tegen maximaal de vooraf in de aanbesteding vastgelegde uurtarieven.