Bijlage 1: Programma van eisen

Door voor deze aanbesteding een inschrijving in te dienen, verklaart inschrijver zich onvoorwaardelijk en volledig akkoord met onderstaande eisen. Eventuele voortvloeiende kosten uit onderstaande eisen dient u te verwerken in de opslagmarges op het prijzenblad. Onderstaande eisen kunnen dus niet leiden tot extra kosten, tenzij in de eis expliciet aangegeven.

Algemene eisen	
Eis	**Omschrijving**
1.	<u>Dienstverlening en kwaliteit</u> Opdrachtnemer is in staat en bereid, al dan niet door een beroep te doen op onderaannemers, om de gevraagde dienstverlening ten behoeve van alle locaties van opdrachtgever, conform de in de aanbestedingsstukken gestelde eisen te verzorgen. Opdrachtnemer dient de dienstverlening dusdanig uit te voeren dat er in geen van de gevallen sprake kan zijn van verstoring van het onderwijsproces, tenzij dit uitdrukkelijk is overeengekomen met opdrachtgever. Opdrachtnemer garandeert dat de door opdrachtnemer te leveren apparatuur en dienstverlening gedurende de looptijd van de overeenkomst van onveranderde goede kwaliteit is en blijft en dat de apparatuur en dienstverlening in alle opzichten voldoet aan de gebruikelijke eisen van de wet- en regelgeving, Arbo, deugdelijkheid, doelmatigheid, taakgeschiktheid, afwerking, normen, specificaties, overheidsvoorschriften en milieubepalingen.
2.	<u>Onboarding</u> Opdrachtnemer is verantwoordelijk voor en neemt een actieve rol in het begeleiden van de organisatie bij de onboarding van de aangeboden diensten, met als doel de deadline, zoals beschreven in het tijdpad, te behalen.
3.	<u>Aanspreekpunt</u> Opdrachtnemer fungeert als Single Point of Contact (SPOC) voor alle gerelateerde vragen en problemen in relatie tot de onderdelen in deze aanbesteding. Opdrachtnemer is als intermediair verantwoordelijke voor afstemming met externe leveranciers. Opdrachtnemer fungeert als primair aanspreekpunt voor interne ICT- en stafmedewerkers (zoals de administratie, ICT-medewerker, etc.) voor ondersteuning en advies met betrekking tot incidenten, changes en service requests. De vaste contactpersoon (en diens vervanger) moeten, tijdens kantooruren, rechtstreeks te bereiken zijn door opdrachtnemer. Opdrachtnemer verstrekt de contactgegevens aan opdrachtnemer bij aanvang van de werkzaamheden. De contactpersoon/SPOC betreft geen servicedesk. Deze eis is ook van toepassing op eventuele onderaannemers.
4.	<u>Nederlandse taal</u> Alle medewerkers van opdrachtnemer en diens onderaannemers die in contact (kunnen) komen met medewerkers van opdrachtgever dienen een goede kennis te hebben van de Nederlandse taal en zich goed verstaanbaar te kunnen maken maar met name duidelijk en verstaanbaar te kunnen uitdrukken. Alle communicatie verloopt en documentatie is beschikbaar in de Nederlandse taal.
5.	<u>Huisregels en legitimeren</u> Medewerkers van, dan wel namens, opdrachtnemer die werkzaamheden verrichten op één van de locaties van opdrachtgever dienen zich te allen tijde te houden aan de geldende huisregels en instructies op te volgen van aanwezig personeel. Medewerkers die werkzaamheden op locatie uitvoeren dienen zich op verzoek van opdrachtgever te kunnen legitimeren.
6.	<u>Wet bescherming persoonsgegevens</u> Opdrachtnemer handelt conform de Algemene Verordening Gegevensbescherming (AVG). Alle gegevens door opdrachtgever aan opdrachtnemer ter beschikking gesteld of door de onder de Overeenkomst verrichte werkzaamheden aan opdrachtnemer bekend geworden zullen, anders dan op een door de wet toegelaten wijze, niet aan derden worden verstrekt. Opdrachtgever zal alle door opdrachtnemer verstrekte persoonsgebonden informatie vertrouwelijk behandelen.

	Tussen opdrachtgever en opdrachtnemer wordt een verwerkersovereenkomst gesloten. Hiervoor wordt de meest recente versie van de modelovereenkomst (huidige is 4.0) van het privacy convenant gebruikt. www.privacyconvenant.nl
7.	Toegang tot locaties opdrachtnemer Toegang tot locaties van opdrachtnemer kan opdrachtnemer alleen verkrijgen in overleg met opdrachtnemer en bij (ontvangst)begeleiding van een interne medewerker van opdrachtnemer. Opdrachtnemer dient gewenste aanwezigheid op een locatie van opdrachtnemer vooraf aan te kondigen bij een medewerker van afdeling ICT.
8.	Personeel De medewerkers van opdrachtnemer en door opdrachtnemer ingehuurde derden, houden zich op de terreinen van opdrachtgever aan de instructies en veiligheidsvoorschriften. Alle medewerkers die werkzaamheden op locatie van opdrachtgever uitvoeren dienen in het bezit te zijn van een Verklaring Omtrent Gedrag (VOG) en dienen zich te kunnen identificeren. De VOG dient op eerste verzoek overlegd te kunnen worden. Deze VOG mag niet ouder zijn dan drie maanden gerekend vanaf het moment van tewerkstelling.
9.	Servicepunt Opdrachtnemer beschikt over een servicepunt, waar door de ICT-medewerkers van opdrachtgever inlichtingen kunnen worden verkregen, waar vragen gesteld kunnen worden, waar storingen aangemeld kunnen worden en waar klachten ingediend kunnen worden. Dit servicepunt dient op werkdagen tijdens kantooruren (08:00 tot 17:00 uur), telefonisch en per e-mail, bereikbaar te zijn. Tevens beschikt opdrachtnemer over een online portal, waar opdrachtgever storingen/problemen kan melden. Vragen worden binnen twee werkdagen inhoudelijk beantwoord. Op klachten wordt binnen twee werkdagen inhoudelijk gereageerd inclusief een oplostermijn.
10.	Proactief informeren en adviseren Opdrachtnemer dient opdrachtgever gedurende de volledige looptijd van de overeenkomst te informeren over ontwikkelingen met betrekking tot de door opdrachtnemer aangeboden dienstverlening Netwerkbeheer. Opdrachtnemer is een partner die gevoel heeft met de activiteiten van opdrachtgever en levert daar een proactieve, onderscheidende en positieve bijdrage aan.
11.	Managementrapportage Opdrachtnemer levert eens per kwartaal zonder meerkosten managementinformatie digitaal aan en dient tenminste de volgende informatie te bevatten: • aantal incidenten en wijzigingen per kwartaal; • aantal afgehandelde incidenten en wijzigingen per kwartaal; • aantal afgesloten calls binnen/buiten de gestelde hersteltijd; • aantal openstaande calls; • beschikbaarheid van de infrastructuur in de afgelopen periode; • afwijkingen van het overeengekomen serviceniveau, van welke aard dan ook; • lopende en komende ontwikkelingen (trends, belangrijke vervangingen, groot onderhoud, e.d.).
12.	Informatieveiligheid Opdrachtnemer voldoet aan de standaard normenkaders zoals ISO 27001. Deze moeten ten grondslag liggen aan: • aantoonbaar informatiebeveiligingsbeleid • aantoonbare procedures op het gebied van informatiebeveiliging • aantoonbaar werken conform bovenstaande Daarnaast voldoet opdrachtnemer op het gebied van personeel aan aantoonbaar geschoold personeel op het gebied van informatieveiligheid en geheimhoudingsverklaring personeel. Op verzoek moet opdrachtnemer opdrachtgever in staat stellen te controleren of bovenstaande wordt nageleefd.

Service en Beheer-eisen	
Eis	**Omschrijving**
13.	De beschikbaarheid is minimaal 99,5% per maand binnen de invloedssfeer van opdrachtnemer gedurende het service window van 24*7.
14.	Opdrachtnemer voert zelfstandig monitoring, analyse en opvolging uit van security incidenten gedurende 24*7 waarbij er een centraal meldpunt is bij opdrachtgever.
15.	De helpdesk van de opdrachtnemer, die zowel telefonisch als per e-mail bereikbaar is, hanteert een duidelijke werkwijze om prioriteiten toe te kennen aan meldingen, zoals incidenten of storingen, die betrekking hebben op gebreken in de functionaliteit van de te leveren Dienst.
16.	De wijze van het in stand houden van de geleverde functionaliteit met preventief, correctief en adaptief onderhoud.
17.	In het beheerplan staan duidelijk de maatregelen beschreven die bijdragen aan beschikbaarheid, integriteit en vertrouwelijkheid van de beheerde systemen.
18.	Opdrachtgever heeft een omgeving te continueren die in hoge mate beschikbaar moet zijn, en voldoet aan de hedendaagse eisen van de beschikbaarheid, integriteit en vertrouwelijkheid.
19.	Opdrachtgever wil nadrukkelijk de technische verantwoordelijkheid bij opdrachtnemer beleggen. Als partner met expertise verwacht opdrachtgever dat deze hier op een (kosten)efficiënte wijze invulling aan kan geven. Daarnaast verwacht opdrachtgever proactief beheer en dus een grote mate van ontzorging.
20.	Opdrachtnemer doet aan continuïteitsplanning en is bewust van risico's en de maatschappelijke trend om bewust en actief met potentiële dreigingen om te gaan.
21.	Opdrachtnemer heeft de volgende processen ingericht: incident, change en problem management.
22.	Opdrachtnemer is in staat om per maand één beheerdag (voor werkzaamheden die buiten de scope van het afgesloten service contract vallen) en bij problemen (van verstoring tot calamiteit die buiten de scope van het afgesloten service contract vallen) expertise te bieden op locatie.

Samenwerkingseisen	
Eis	**Omschrijving**
23.	Opdrachtnemer formuleert werk- en procesafspraken. Opdrachtnemer geeft een beschrijving van de: • standaard service requests die opdrachtnemer onderkent i.c.m. de normtijden die opdrachtnemer hanteert voor de afhandeling ervan; • de werkwijze en ondersteuning die opdrachtnemer biedt in de rol van Single Point of Contact (SPOC); • verschillende overlegstructuren die u voorstelt, bijvoorbeeld onderverdeeld naar operationeel, tactisch en strategisch i.c.m. frequentie van overleg en de aanwezige rollen; • wijze waarop de geleverde service geëvalueerd wordt door u en een beschrijving van de gebruikte metrieken; • omstandigheden en door wie de serviceniveaus gewijzigd kunnen worden; • escalatiepaden zowel vanuit het startpunt van opdrachtnemer als van opdrachtgever. De procedure voorziet in paden waarbij alleen inschrijver en opdrachtgever betrokken zijn en ook in paden waarbij een derde, onafhankelijke partij ingeschakeld kan worden.
24.	Opdrachtnemer heeft focus op klanten, en heeft een aantoonbare brede visie op ontwikkelingen en de rol van opdrachtnemer hierin. Opdrachtnemer investeert in (technische) ontwikkelingen en heeft innovatie ook in haar missie opgenomen. Opdrachtgever eist een houding van haar leveranciers waarbij het oplossen van een issue voorop staat en op dat moment niet belemmerd wordt door in beton gegoten processen. Hierbij is risicobeheersing van belang. Opdrachtnemer moet bereid zijn in deze samenwerking te investeren.
25.	Als een service niet wordt verleend of een servicelevel niet wordt behaald zal minimaal binnen een twee weken een root-cause analyse gedaan worden en een verbeterplan worden gepresenteerd waaruit blijkt dat de service voor komende periode verbeterd zal worden.
26.	Het onderhoudswindow voor gepland onderhoud valt binnen 22:00 uur en 06:00 uur en is beperkt tot één vaste dag en tijd per maand gedurende een relatief korte periode. Afwijkingen zijn mogelijk in overleg met opdrachtgever.

Implementatie eisen	
Eis	**Omschrijving**
27.	Opdrachtnemer dient vanaf medio juni 2025 te beginnen met de voorbereidingen voor de implementatie. Gedurende de zomervakantie van 2025 (van 16 juli t/m 26 augustus) is de school gesloten. De daadwerkelijke implementatie moet eind juni 2025 in overleg met de opdrachtgever worden besproken en vastgesteld met de contactpersoon van de opdrachtgever, rekening houdend met de zomervakantie. Opdrachtnemer committeert zich aan een volledige in beheer name per 27 augustus 2025.
28.	Opdrachtnemer werkt op basis van het antwoord op open vraag 1 (implementatie en onboarding) een concreet implementatieplan uit. De eerste versie hiervan, die besproken wordt met opdrachtgever, is uiterlijk eind juni 2025 gereed. De definitieve versie van het implementatieplan is uiterlijk begin juli 2025 gereed en goedgekeurd door opdrachtgever.
29.	In dezelfde periode als het implementatieplan wordt ook de definitieve SLA vastgesteld. In de definitieve SLA wordt de beantwoording van de open vragen verwerkt.
30.	Opdrachtgever en opdrachtnemer vormen een projectgroep die gezamenlijk de implementatieperiode zal doorlopen. Opdrachtnemer is voorzitter van deze projectgroep. Binnen de beantwoording van de open vragen dient inschrijver aan te geven welke resources er worden verwacht vanuit opdrachtgever.
31.	Beveiligings- en Continuïteitsplan (waarin een risicoanalyse en passende technische en organisatorisch maatregelen worden genomen om beveiligings- en continuïteitsrisico's te mitigeren) opgesteld. Deze plannen worden jaarlijks bijgewerkt.
32.	De randvoorwaarden die vooraf aan opdrachtgever en huidige leverancier worden gesteld zijn hierin expliciet opgenomen en volledig.
33.	De zwaarte van deze randvoorwaarden dient zo beperkt mogelijk te zijn voor opdrachtgever en huidige leverancier.
34.	Een goed doordachte transitie en onboarding (te beoordelen bij plan van aanpak) is een belangrijk onderdeel van de uiteindelijke aanbieding. Opdrachtnemer is in de lead om invulling te geven aan dit plan.
35.	Opdrachtgever verwacht minimaal een evenwichtige verdeling in verantwoordelijkheden tussen opdrachtnemer en opdrachtgever en waardeert een grote verantwoordelijkheid bij opdrachtnemer positief.

Service Level Agreement (SLA) eisen	
Eis	**Omschrijving**
36.	Opdrachtgever wenst een helpdesk, die gedurende werkdagen van 08.00 – 17.00 uur bereikbaar is en waarvan de medewerkers goed en begrijpelijk Nederlands spreken. Incidenten moeten worden geregistreerd en gecommuniceerd naar de ICT-contactpersoon van opdrachtgever. Incidenten worden gestructureerd afgehandeld, met een helder escalatieproces voor kritieke storingen.
37.	Opdrachtnemer garandeert dat opdrachtgever zonder tussenkomst van opdrachtnemer aan medewerkers autorisaties kan toekennen, waarbij autorisaties worden onderscheiden naar mutatierechten (te onderscheiden in wijzigen en verwijderen/toevoegen) en leesrechten.
38.	Opdrachtnemer garandeert een (pro)actieve samenwerking met derden die betrokken zijn bij het netwerk dan wel het systeem, bijvoorbeeld maar niet uitsluitend WLAN-leveranciers, systeembeheerders, leveranciers van software zoals Magister en NIVO. Opdrachtnemer garandeert de vervulling van de rol van Single Point of Contact (SPOC).
39.	Kritieke storingen, die grote impact hebben op het onderwijsproces, worden binnen 1 uur na melding opgepakt . De service window hiervoor beperkt zich niet tot de eerdergenoemde kantoortijden (08:00 tot 17:00). Bij kritieke storingen die niet remote opgelost kunnen worden, moet een technicus binnen anderhalf uur op locatie kunnen zijn om de problemen op te lossen. Overige incidenten en storingen met gemiddelde of beperkte impact en serviceverzoeken worden binnen 8 uur opgepakt.
40.	Opdrachtnemer handelt (pro)actief bij (security) incidenten/calamiteiten en hierbij het volgende te hanteren: • Responsetijd: binnen vier uur op werkdagen vanaf melding incident door opdrachtgever. • Time to fix: binnen één werkdag vanaf melding incident door opdrachtgever.
41.	Opdrachtnemer handelt proactief en preventief naar aanleiding van monitoringssignalen.
42.	Opdrachtnemer lost uit incidenten voortvloeiende gebreken op en handelt deze af.

43.	Tekortkomingen en risico's dienen tijdig gesignaleerd te worden, voorzien van advies voor oplossing of beperking van het risico.

Netwerkbeheer	
Eis	**Omschrijving**
44.	Opdrachtnemer adviseert opdrachtgever (pro)actief over de inrichting van het netwerk, netwerkcomponenten en de security.
45.	Opdrachtnemer beveiligt het netwerk adequaat, en voorziet in voldoende veiligheidsmaatregelen voor de netwerkomgeving en geeft ook na gunning schriftelijk bij Opdrachtgever aan hoe de beveiliging is opgebouwd en gewaarborgd.
46.	Opdrachtnemer zorgt voor adequate beveiliging van de accounts die zij nodig heeft voor het beheer en onderhoud (tenminste 2FA).
47.	Opdrachtnemer gebruikt geen algemene accounts voor het netwerkbeheer. In alle gevallen is te achterhalen wie welke wijziging heeft gemaakt in de omgeving (traceerbaarheid).
48.	Opdrachtnemer is verantwoordelijk voor het correct functioneren van de lokale netwerken en de aansluiting op de WAN-verbindingen.
49.	Opdrachtgever verwacht een proactieve houding van opdrachtnemer t.a.v. het bijhouden van ontwikkelingen. Alle locaties van opdrachtgever hebben identieke systemen. Opdrachtgever verwacht derhalve van opdrachtnemer dat als deze een ontwikkeling voorstelt en na akkoord van Opdrachtgever doorvoert op één van de locaties van opdrachtgever, die ook doorvoert voor de overige locaties zonder dat daarvoor een opdracht van opdrachtgever nodig is.
50.	Opdrachtnemer adviseert opdrachtgever actief over de aanschaf van nieuwe netwerkcomponenten.
51.	Opdrachtnemer garandeert indien nodig de installatie en vervanging van nieuwe netwerkcomponenten.
52.	Opdrachtnemer houdt digitaal een overzicht bij welke netwerkapparatuur van opdrachtgever onder zijn beheer valt, welk overzicht op verzoek van opdrachtgever door opdrachtnemer aan opdrachtgever wordt aangeleverd.
53.	Opdrachtnemer installeert periodiek updates van netwerkcomponenten.
54.	Opdrachtnemer neemt alle bestaande Extreme Networks accesspoints en switches van opdrachtgever in beheer.
55.	Opdrachtnemer monitort alle accesspoints en switches en neemt proactieve maatregelen om mogelijke problemen op te lossen voordat deze de werking van het netwerk beïnvloeden. Opdrachtgever krijgt read-only toegang tot de monitoring.
56.	Toegang tot netwerkcomponenten is strikt beveiligd en toegang wordt nauwkeurig gelogd. Opdrachtnemer moet in staat zijn om het netwerk veilig op afstand te kunnen beheren.
57.	Voor monitoring en remote toegang wordt het 'cloud-only' principe gehanteerd. Opdrachtgever streeft naar het gebruik van bestaande functionaliteiten op de aanwezige netwerkcomponenten of maakt gebruik van SaaS-oplossingen. Het gebruik van lokale appliances of clients heeft niet de voorkeur.
58.	De switches en accesspoints moeten stabiel en veilig functioneren, met minimaal 99,5% uptime tijdens kantoortijden. Het beheer omvat periodieke back-ups van alle configuraties en instellingen, waarbij de back-upprocedures regelmatig getest worden.
59.	Opdrachtnemer is verantwoordelijk voor tijdige updates van firmware en beveiligingspatches voor alle switches en accesspoints, waarbij het updaten het onderwijsproces niet verstoort en buiten de kantoortijden wordt uitgevoerd.
60.	Het opstellen van testprocedures inclusief acceptatiecriteria's, die worden toegepast bij o.a. het updaten van netwerkcomponenten, is een verantwoordelijkheid van opdrachtnemer. De testprocedure houdt rekening met de volledige werking van het netwerk, inclusief de goede werking van de third-party oplossing Wiflex en de internetverbinding van SIVON/Kennisnet.
61.	Opdrachtnemer streeft naar een betrouwbaar en stabiel draadloos netwerk en zal proactief aanbevelingen doen en verbeteringen doorvoeren om de prestaties van het draadloze netwerk te waarborgen.
62.	Opdrachtnemer inventariseert en maakt documentatie van de al aanwezige switches en accesspoints en houdt deze documentatie gedurende de looptijd van het contract up-to-date, inclusief de gebruikte configuraties.

63.	Opdrachtnemer zal aanbevelingen doen voor de inrichting van een veilig en gebruiksvriendelijk gastennetwerk.

Beheer – Microsoft 365 en Microsoft Azure (incl. Microsoft Entra)	
Eis	**Omschrijving**
64.	Opdrachtnemer voert periodiek beheer en onderhoud uit om de omgeving veilig, up-to-date en overzichtelijk te houden. Dit omvat o.a. het opruimen van inactieve gebruikers en groepen, het doorvoeren van noodzakelijke updates en changes volgens de best-practice van Microsoft.
65.	Opdrachtnemer implementeert en beheert een cloud-gebaseerde third-party back-up oplossing voor data binnen Microsoft 365, waaronder Exchange, Teams, OneDrive en SharePoint, om gegevensverlies te voorkomen en herstel bij calamiteiten mogelijk te maken.
66.	Opdrachtnemer voert periodieke controles uit op de back-up omgeving om de integriteit en beschikbaarheid van back-ups te waarborgen en rapporteert eventuele problemen of afwijkingen direct aan opdrachtgever.
67.	Opdrachtnemer ontwikkelt en implementeert samen met opdrachtgever een gedegen plan voor het gebruik en het beveiligen van de omgeving.
68.	Opdrachtnemer neemt het volledige beheer van Exchange Online over, inclusief het aanmaken en beheren van (gedeelde) mailboxen, het configureren van mailflows en het waarborgen van een optimale mailfunctionaliteit binnen de organisatie.
69.	Opdrachtnemer voert periodieke beveiligingscontroles uit om betrouwbaarheid en veiligheid van mailverkeer te kunnen waarborgen, zodat deze voldoet aan de nieuwste beveiligingsstandaarden en best-practices, inclusief correcte configuratie van DNS-records en andere relevante instellingen.
70.	Opdrachtnemer beheert de gebruikers en groepen binnen Entra ID en ondersteunt het proces waarbij gebruikers en groepen automatisch worden provisioned door de IAM oplossing NIVO. Opdrachtnemer zorgt voor een effectieve inrichting van Conditional Access (CA) en Role-Based Access Control (RBAC) om toegangsrechten nauwkeurig te beheren en de toegang tot informatiesystemen veilig en gebruiksvriendelijk te houden. *Toelichting: Het streven is om zoveel mogelijk groepen en gebruikers provisioned te hebben vanuit NIVO (Idfocus). Opdrachtnemer is SPOC voor de organisatie en kan direct schakelen met Idfocus wanneer het gaat om de onderdelen waar NIVO & Azure elkaar raken (Gebruikers, Groepen en Teams).*
71.	Opdrachtnemer beheert alle typen groepen binnen Microsoft 365 (dynamisch, statisch, security, etc.), inclusief het aanmaken, wijzigen en verwijderen, om een gestructureerde en veilige toegangscontrole te garanderen.
72.	Opdrachtnemer implementeert en beheert een Conditional Access en Multi-Factor Authentication (MFA)-beleid om ongeautoriseerde toegang te voorkomen. Dit omvat het instellen en beheren van beleidsregels op basis van gebruikerslocaties, apparaten, en gebruikersrollen om alleen veilige toegang te verlenen.
73.	Opdrachtnemer implementeert en beheert Enterprise Applications en ondersteunt bij de configuratie van Single Sign-On (SSO) met het Microsoft-platform. De leverancier zorgt ervoor dat de applicaties voldoen aan de beveiligingsrichtlijnen zoals Conditional Access en Multi-Factor Authentication (MFA). Het beheer omvat de configuratie, monitoring, en ondersteuning van de bedrijfsapplicaties.
74.	Opdrachtnemer ontwikkelt en implementeert een applicatiebeleid voor Microsoft 365-applicaties, waarbij wordt bepaald welke applicaties binnen Microsoft 365 beschikbaar zijn voor de verschillende gebruikersgroepen (docenten, leerlingen, etc.), om beveiliging en efficiëntie te bevorderen.
75.	Opdrachtnemer voert periodiek beveiligingscontrole en optimalisaties uit, inclusief het opvolgen van aanbevelingen uit de Microsoft Secure Score of gelijksoortige alternatieve scoringtools, om de algehele beveiligingsstatus continu te verbeteren.
76.	Opdrachtnemer monitort de volledige Microsoft omgeving om proactief potentiële issues te identificeren en snelle incidentrespons en -resolutie te garanderen bij verstoringen of beveiligingsincidenten.
77.	Opdrachtnemer zorgt voor gedetailleerde en up-to-date documentatie van de inrichting van de door Opdrachtnemer beheerde onderdelen, bijvoorbeeld in de vorm van een technisch ontwerp. De documentatie bevat de volgende elementen: a. Technische inrichting van de Microsoft 365 tenant;

	b. Genomen besluiten en de onderbouwing achter deze beslissingen; c. Mogelijke risico's en aandachtspunten, inclusief voorgestelde beheersmaatregelen.

Beheer – Microsoft Intune	
Eis	**Omschrijving**
78.	Opdrachtnemer is verantwoordelijk voor het softwarematig configureren, beheren en onderhouden van alle werkplekken van opdrachtgever die worden beheerd via Microsoft Intune. Dit omvat (maar is niet beperkt tot): • Het implementeren en beheren van beleidsregels (compliance, beveiliging, apparaatbeheer); • Het uitrollen van software-updates, inclusief beveiligingspatches en nieuwe functionaliteiten; • Proactieve monitoring van de Intune-omgeving om de veiligheid en prestaties van de werkplekken te waarborgen.
79.	Het beheren van de hardware van de werkplekken is de eigen verantwoordelijkheid van opdrachtgever. Opdrachtnemer mag worden geraadpleegd voor advies bij aanschaf van nieuwe hardware of wanneer er hardwarematig problemen zijn met de werkplekken die mogelijk softwarematig (drivers, firmware, etc.) kunnen worden verholpen.
80.	Opdrachtnemer beheert de uitrol en het onderhoud van alle benodigde softwaretoepassingen op de werkplekken via Microsoft Intune. Dit omvat zowel verplichte applicaties (push) als optionele softwarepakketten voor specifieke gebruikersgroepen (bedrijfsportal).
81.	Opdrachtnemer implementeert en beheert BitLocker-apparaatcodering en andere preventieve maatregelen via Intune om ervoor te zorgen dat gevoelige gegevens beschermd zijn tegen ongeautoriseerde toegang of verlies bij diefstal of verlies van het apparaat.
82.	Opdrachtnemer is verantwoordelijk voor het implementeren van beveiligingsconfiguraties en beleid binnen Intune om de werkplekken te beschermen tegen beveiligingsincidenten, zoals malware-infecties, ongeautoriseerde toegang en gegevensverlies.
83.	Opdrachtnemer zet Windows Autopilot in om nieuwe apparaten automatisch in te stellen en te configureren via Intune, zodat nieuwe werkplekken direct kunnen worden ingezet volgens het vooraf gedefinieerde beleid van de school.
84.	Opdrachtnemer zorgt voor gedetailleerde en up-to-date documentatie van de inrichting van de Microsoft Intune-omgeving, bijvoorbeeld in de vorm van een technisch en/of functioneel ontwerp. De documentatie bevat minimaal de volgende elementen: a. Technische en/of functionele inrichting van de Intune-omgeving; b. Genomen besluiten en de onderbouwing achter deze beslissingen; c. Mogelijke risico's en aandachtspunten, inclusief voorgestelde beheersmaatregelen.
85.	De documentatie wordt op een begrijpelijke manier geschreven, zodat ook niet-technische stakeholders deze kunnen begrijpen. De documentatie dient minimaal eenmaal per halfjaar te worden herzien. Indien er wijzigingen zijn, moet deze worden bijgewerkt, of na significante wijzigingen in de Intune-omgeving.
86.	Opdrachtnemer is verantwoordelijk voor het proactief documenteren en delen van de genomen beveiligingsmaatregelen binnen Microsoft Intune. Deze documentatie dient invulling te geven aan het Normenkader IBP en bruikbaar te zijn voor de organisatie als bewijslast. *Toelichting: De organisatie moet binnen het domein 'Securitymanagement' (Domein 11) kunnen aantonen welke securitymaatregelen binnen Microsoft Intune zijn genomen, zoals MDM (SM.03), Patchmanagement (SM.06) en malwarebeheersing (SM.12). Door het gebrek aan expertise in de organisatie, wordt van de leverancier verwacht dat zij op structurele basis (bijv. eens in het half jaar) technische documentatie aanleveren en updaten, zoals een technisch ontwerp of een gedetailleerd beveiligingsrapport, om aan deze normenkaderverplichtingen te voldoen.*
87.	Opdrachtnemer levert periodiek rapportages over de compliance van alle werkplekken en mobiele apparaten die via Intune worden beheerd, inclusief een overzicht van mogelijke niet-conforme apparaten en actieplannen om deze in overeenstemming te brengen met het beleid.

Levering & Beheer Nieuwe Gateway	
Eis	**Omschrijving**
88.	De nieuwe gateway zullen de huidige firewalls vervangen. Opdrachtnemer onderbouwt de keuze van het type gateway. De oplossing sluit aan op de aanwezige Veilig Internet oplossing van SIVON/Kennisnet, zie Bijlage 9.
89.	SIVON/Kennisnet levert met de Veilig Internet oplossing een aantal veiligheidsfunctionaliteiten (Virtuele Firewall (VDOM), anti-DDoS, web- en applicatiefiltering en IDS/IPS). Opdrachtnemer overlegt met SIVON welke benodigde functionaliteiten ontbreken (bv. NAT routing) en draagt zorg voor een gateway die deze benodigde functionaliteiten faciliteert.
90.	De gateway moet voldoende capaciteit bieden om de gehele contractduur te kunnen voorzien in de groei van het aantal gebruikers en de toekomstige beschikbare bandbreedte (internetverbinding).
91.	De voorgestelde gateway moet integreren met de bestaande netwerkinfrastructuur, inclusief de Extreme Networks switches en accesspoints.
92.	Het voorstel moet een volledig overzicht bevatten van alle kosten, waaronder initiële installatie, onderhoud, licenties, en geschatte kosten over de levensduur van de gateway.
93.	Bij oplevering van de nieuwe gateway levert opdrachtnemer een opleveringsrapport waarin staat beschreven wat er is opgeleverd en hoe de gateway is ingericht.
94.	Opdrachtnemer monitort doorlopend de prestaties van de gateway op kernindicatoren zoals snelheid, stabiliteit en betrouwbaarheid. Bij afwijkingen van de normale waarden worden direct meldingen gegenereerd en maatregelen genomen. Opdrachtgever krijgt read-only toegang tot de monitoring.
95.	Opdrachtnemer is verantwoordelijk voor het tijdig doorvoeren van patches op de gateway, met prioriteit voor kritieke beveiligingsupdates. Kritieke patches dienen binnen 24 uur na vrijgave door de fabrikant geïnstalleerd te worden om kwetsbaarheden direct te verhelpen en de beveiliging van het netwerk te waarborgen.
96.	Opdrachtnemer beheert het routeren en doorsturen van verkeer via de gateway, zorgt voor stabiele verbindingen en optimaliseert het netwerkverkeer om overbelasting te voorkomen.
97.	Opdrachtnemer rapporteert periodiek over de prestaties en beveiliging van de gateway. Logboeken van de gateway moeten toegankelijk zijn voor audits en moeten alle belangrijke activiteiten vastleggen, zoals wijzigingen in configuratie, beveiligingsincidenten en updates.

Licentiebeheer eisen	
Eis	**Omschrijving**
98.	Opdrachtgever eist het rechtmatig gebruik van software.
99.	Opdrachtgever eist dat het aantal verschillende standaardprogramma's en/of versies tot een minimum beperkt blijven.
100.	Opdrachtnemer dient een administratie bij te houden van de bij hem in gebruik zijnde programmatuur die te allen tijde beschikbaar kan worden gesteld aan opdrachtgever.