Onderwijsgroep Landstede



Bijlage B

Programma van Eisen

Netwerk- en Securityinfrastructuur

Aanbestedende dienst	:	Alle deelnemende stichtingen binnen Onderwijsgroep Landstede
Datum	:	26-11-2026
Versie	:	1.0
Referentie	:	TN625968

In deze bijlage benoemt Onderwijsgroep Landstede de eisen die verbonden zijn aan de gevraagde leverancier. Indien de inschrijver een offerte indient gaat hij akkoord met deze eisen.

In dit Programma van Eisen wordt met de onderstaande terminologie het volgende bedoeld:

- **'Opdrachtnemer'** verwijst naar de te contracteren partner voor Netwerk- en Securityinfrastructuur die verantwoordelijk is voor de uitvoering van de in dit document beschreven dienstverlening. Waar in dit document wordt gesproken over 'Opdrachtnemer', wordt daarmee de beoogde partner voor Netwerk- en Securityinfrastructuur bedoeld.
- **'Opdrachtgever'** verwijst naar Onderwijsgroep Landstede of personeelsleden die onderdeel uitmaken van Onderwijsgroep Landstede.

1. Algemene eisen

Nummer	Eis
1.	Opdrachtnemer dient bedrijfsprocessen, gerelateerd aan de ICT-omgeving van Opdrachtgever in te richten in overeenstemming met de richtlijnen van informatiebeveiliging ISO27001.
2.	Opdrachtnemer levert zelf of in samenwerking met vendor het hele gamma aan producten en diensten van meerdere fabrikanten ten behoeve van de inschrijving.
3.	Opdrachtnemer adviseert Opdrachtgever bij de selectie van actieve netwerkcomponenten en accessoires.
4.	Het beheerteam beschikt over ten minste één vendor-neutrale certificering op het gebied van netwerkbeheer of informatiebeveiliging (bijvoorbeeld CWNA, ITIL of ISO 27001-auditor).
5.	Het beheerteam van de Opdrachtnemer beschikt over geldige productcertificeringen van de fabrikant(en) van de in de inschrijving aangeboden netwerkproducten (access-points, switches en firewalls). Per product wordt minimaal één teamlid met een geldige certificering van de fabrikant aangewezen, of een gelijkwaardige certificering van een andere fabrikant die op de functionele eisen van het product aansluit. De Opdrachtnemer levert een overzicht van de certificeringen per product, inclusief naam van de certificering, certificeringsnummer en geldigheidsdatum. Gelijkwaardigheid wordt beoordeeld aan de hand van de certificeringseisen en het leerdoel van de certificering.
6.	Opdrachtnemer stelt een vast team van specialisten samen voor Opdrachtgever die gezamenlijk de gehele aangeboden infrastructuur beheren. Dit team is volledig op de hoogte van de infrastructuur inclusief LAN/ WAN, NAC, Firewaling en alle andere geleverde componenten. Tijdens onderhoud en storingen werken zijn nauw samen met elkaar, en beschikken over alle documentatie.
7.	Alle documentatie en CMDB is door Opdrachtnemer te raadplegen. De CMDB is compleet en bevat alle gegevens van de apparatuur inclusief alle configuratie instellingen.
8.	De CMDB is door Opdrachtgever via een API koppeling te raadplegen om de gegevens in de lokale CMDB over te nemen.
9.	De minimale lifecycle van een actief netwerkcomponent is 36 maanden. De Opdrachtnemer stelt ten minste 1x per jaar een roadmap op met verwachte lifecycles van alle geleverde apparatuur. Componenten die het einde van hun lifecycle hebben bereikt, worden vervangen door een vergelijkbaar, actueel model.
10.	Opdrachtnemer garandeert dat de onderdelen van geleverde actieve netwerkcomponenten tot zeven (7) jaar na levering leverbaar zijn of worden vervangen door een vergelijkbaar, actueel alternatief.
11.	Opdrachtnemer heeft een proactieve informatieplicht. Zij informeert de Opdrachtgever uiterlijk zes maanden vóór end-of-sale welke netwerkcomponenten deze status zullen bereiken en dient gelijktijdig een voorstel in voor een gelijkwaardig vervangend alternatief.

12.	Opdrachtnemer garandeert dat onderdelen tot vijf (5) jaar naar end-of-sale datum als part, of spare part leverbaar blijven tegen de geldende garanties of kortingspercentages. Onderdelen die het einde van hun lifecycle hebben bereikt, worden vervangen door een vergelijkbaar, actueel model.
13.	Alle door de Opdrachtnemer uitgebrachte offertes zijn gebaseerd op fabrieksnieuwe actieve netwerkcomponenten.
14.	Opdrachtnemer hanteert een maximale levertijd van 20 werkdagen voor nieuwe netwerkcomponenten. Indien er sprake is van een uitgestelde levering meldt Opdrachtnemer dit uiterlijk 2 werkdagen na besteldatum.
15.	Opdrachtnemer handelt proactief en is innovatief. Hieronder wordt in ieder geval maar niet uitputtend verstaan: • Opdrachtnemer denkt proactief mee door Opdrachtgever o.a. tijdig op de hoogte te stellen van end-of-sales, nieuwe ontwikkelingen, software upgrades, 'known bugs', alternatieve mogelijkheden, etc.; • Deel te nemen aan beta programma's, directe kennisuitwisseling met fabrikanten die componenten leveren, samen ontwikkelen van innovatieve onderdelen binnen de netwerk infrastructuur van Opdrachtgever etc.
16.	Opdrachtnemer dient innovaties, software-upgrades, firmware-updates, configuratiewijzigingen en nieuwe functionaliteiten zodanig te introduceren dat de stabiliteit, prestaties, beschikbaarheid en beveiliging van de netwerk- en securityinfrastructuur niet negatief worden beïnvloed.
17.	Opdrachtnemer dient gedurende de looptijd van de overeenkomst een representatieve Proof of Concept (PoC)- en testomgeving beschikbaar te stellen die qua architectuur, configuratie en functionaliteit aansluit. De omgeving dient minimaal te bestaan uit distributie-switches, access-switches, draadloze access-points en bijbehorende management- en securitycomponenten.
18.	Opdrachtnemer garandeert dat, indien gewenst door Opdrachtgever, apparatuur kosteloos ter beschikking wordt gesteld voor een Proof of Concept van een aangeboden omgeving die functioneel en technisch representatief is voor de dagelijkse praktijk. PoC gebeurt op basis van een van tevoren overeengekomen testplan.
19.	Eventuele projectkosten kunnen op basis van voorcalculatie overeengekomen worden die bij het slagen van de PoC en geaccepteerd door Opdrachtgever doorbelast mogen worden.
20.	Opdrachtgever bepaalt de eisen met betrekking tot configuratie, denk daarbij aan: IP-plan, VLAN-segmentering, securityinstellingen.
	Configuratie en acceptatie
21.	Opdrachtnemer gaat voor levering van de apparatuur akkoord met een configuratietest (Proof of concept).
22.	Opdrachtnemer adviseert Opdrachtgever bij de selectie van actieve netwerkcomponenten en accessoires.
23.	De juridische verplichting tot betaling van de geleverde dienst ontstaat na succesvolle voltooiing van de configuratietest van de apparatuur.
	Garantie
24.	Opdrachtnemer garandeert dat de door haar te leveren apparatuur geschikt is voor gebruik in educatieve omgeving.
25.	Opdrachtnemer garandeert dat de apparatuur ook bij piekbelasting de geëiste eigenschappen bevat.

26.	Opdrachtnemer neemt geleverde apparatuur zonder extra kosten voor Opdrachtgever retour, indien bij ingebruikname door Opdrachtgever blijkt dat er sprake is van 'Dead on arrival' (hierna te noemen 'DOA') van de apparatuur. In dat geval levert Opdrachtnemer binnen 24 uur nieuwe apparatuur.
27.	De garantie welke door de fabrikant wordt afgegeven op geleverde apparatuur geeft Opdrachtnemer onverminderd door aan Opdrachtgever.
28.	Opdrachtnemer is bereid en in staat on-site garantie op actieve componenten te garanderen gedurende de contractperiode.
29.	Opdrachtnemer is bereid en in staat storingen binnen de termijn van de gekozen onderhoudsvorm na de storingsmelding op locatie te verhelpen gedurende contractperiode.
30.	Opdrachtnemer is bereid en in staat een deugdelijke storingsadministratie bij te houden en Opdrachtgever, door middel van rapportages, inzicht te geven in deze administratie.
31.	De on-site garantie is all-in, gedurende de garantietermijn kunnen geen kosten in rekening worden gebracht voor: • Voorrijden; • Arbeidsloon; • Vervanging van onderdelen; • Gebruiksmaterialen; • Administratiekosten of dergelijke.
32.	Indien bij het uitvoeren van de on-site garantie onderdelen worden vervangen, worden deze vervangen door nieuwe onderdelen of onderdelen die minimaal gelijkwaardig zijn qua kwaliteit en resterende levensduur.
33.	Opdrachtnemer biedt trainingen voor studenten op het gebied van firewall, routing, switching en infrastructuur.
34.	Opdrachtnemer organiseert minimaal 2 keer per jaar een innovatieve sessie voor de IT-medewerkers van Opdrachtgever. In deze sessies worden nieuwe innovatieve functies, mogelijkheden en oplossingen getoond en besproken.

2. Eisen aan de dienstverlening

Nummer	Eis
35.	Opdrachtnemer beschikt over een Nederlandssprekende helpdesk/servicedesk welke 24 uur per dag telefonisch bereikbaar is.
36.	Opdrachtnemer beschikt over een internetportaal voor het aanmelden en beheren van storingen. Opdrachtgever heeft kosteloos toegang tot het portaal en kan via het portaal en telefonisch storingen aanmelden en volgen.
37.	Het internetportaal met de meldingen (cases en changes) is via een API-koppeling beschikbaar.
38.	Een aangemelde storing dient tijdens reguliere werkdagen binnen twee (2) uur middels een e-mail door Opdrachtnemer te worden bevestigd met opgave van het call-nummer. Afgaande op de afgenomen service zal Opdrachtnemer gehouden worden aan de oplostijden.
39.	Opdrachtgever ontvangt een notificatie per mail, als er activiteiten op het internetportaal plaatsvinden.
40.	Opdrachtnemer biedt de mogelijkheid om notificaties per webhook aan Opdrachtgever aan te bieden.

	SLA (Service Level Agreement)
41.	De aard en het niveau van de dienstverlening t.a.v. support wordt tussen Opdrachtnemer en Opdrachtgever vastgelegd in een SLA.
42.	Opdrachtnemer heeft een SLA voorstel in zijn offerte meegeleverd.
43.	De SLA kan gedurende de looptijd van het contract aangepast worden op verzoek van één van beide partijen, bij overeenstemming door beide partijen over de aanpassing.
44.	Als standaard levert Opdrachtgever eerste lijnsupport, waarbij wordt uitgegaan dat de Opdrachtgever de basisprobleemoplossing kan oppakken, waarvoor geen diepgaande technische kennis is vereist. Opdrachtgever heeft een volwaardige ICT-afdeling waarbij de wens is om zelf basis changes uit te kunnen voeren. Opdrachtgever is op zoek naar een partner die deze werkwijze ondersteunt.
45.	Opdrachtnemer levert een tweede- en derdelijns support. Opdrachtnemer beschikt over diepgaande kennis om tot de juiste probleemoplossing te komen. Daarbij geldt dat Opdrachtnemer zich proactief inzet bij problemen om de oorzaak en de oplossing zo snel als mogelijk en adequaat te bewerkstelligen, tevens als op voorhand onduidelijk is in welk domein een probleem zich bevindt.
46.	Opdrachtnemer biedt een 24/7-supportvenster aan op Firewall en Core.
47.	Opdrachtnemer biedt op LAN-omgeving en netwerkcomponenten een supportvenster van maandag tot en met vrijdag tussen 07.00-18.00 uur, met uitzondering van officiële feestdagen.
48.	Opdrachtnemer verzorgt monitoring om zorg te kunnen dragen voor een correcte en veilige werking van de dienst. De monitoring van de dienst omvat tenminste: • Alle hoofdcomponenten van het netwerk welke 24/7 worden gemonitord. Dit houdt in dat er 24/7 wordt gemonitord op storingen en/of uitval. In de basis dient Opdrachtnemer te handelen bij een melding tijdens het supportvenster, zoals vermeld onder eis 46 en 47. In aanvulling op deze optie kan Opdrachtgever een storingsdienst uitvragen, waarbij Opdrachtgever de Opdrachtnemer 24/7 kan benaderen (telefonisch, mail of ticketsysteem) voor uitval en/of storingen. • Er worden real-time gegevens verzameld en geanalyseerd en daarmee inzichten geboden in het (gebruik van het) netwerk. • Opdrachtgever krijgt standaard inzage (leesrechten) in het monitoringsportaal.
49.	Opdrachtnemer dient op verzoek van Opdrachtgever inzage te kunnen verlenen in de configuraties voor de dienst, die wordt afgenomen door Opdrachtgever.
50.	Opdrachtnemer levert per kwartaalrapportages van leveringen, reparaties en incidenten van apparatuur die bij Opdrachtgever in onderhoud is gegeven. Verder houdt Opdrachtnemer een CMDB bij van alle in onderhoud gegeven apparatuur.
	Bugfixes
51.	Opdrachtnemer stelt gedurende de looptijd van de overeenkomst bugfixes beschikbaar voor alle netwerkcomponenten en voert deze, na afstemming met de Opdrachtgever, door binnen een overeengekomen onderhoudsvenster.
	Security updates
52.	Opdrachtnemer informeert de Opdrachtgever onverwijld over kwetsbaarheden in de netwerkcomponenten en implementeert security patches binnen een vooraf overeengekomen termijn, afhankelijk van de ernst van de kwetsbaarheid kritiek binnen 1 dag en hoog binnen 4 dagen (volgens CVSS v3.1).

	Functionele updates
53.	Opdrachtnemer biedt functionele updates en nieuwe softwareversies aan, voor zover deze zijn opgenomen in de standaardlicenties, zonder extra kosten voor de Opdrachtgever. Grote releases worden vooraf aangekondigd en getest, en worden pas uitgerold na akkoord van de Opdrachtgever.

3. Financiële eisen

Nummer	Eis
54.	De door de Opdrachtnemer opgegeven tarieven zijn maximumtarieven en marktconform gedurende de looptijd van de Overeenkomst. Opdrachtnemer garandeert dat aangeboden tarieven voor de gehele looptijd van deze aanbieding inclusief optionele verlengingsperiodes van toepassing is. Tarieven gelden voor Apparatuur, Software en Licenties die aangeschaft worden na aanvang contract.
55.	Prijzen kunnen jaarlijks, voor het eerst op 1 mei 2028, worden aangepast conform de CBS Dienstenprijsindex (DPI), 2021=100. Als peilmoment geldt hiervoor de jaarmutatie ten opzichte van het voorgaande jaar. Opdrachtnemer informeert Opdrachtgever uiterlijk twee maanden voorafgaand aan de indexatie. Indexeren is alleen toegestaan na schriftelijke toestemming van Opdrachtgever.
56.	Alle opgegeven bedragen/tarieven/percentages zijn exclusief BTW en inclusief alle bijkomende kosten, zoals (doch niet uitsluitend): • Afleverkosten (levering DDP op door Opdrachtgever aangegeven locatie (Incoterms 2020)); • De ten behoeve van de opdracht gemaakte reis- en verblijfkosten; • De kosten van het vermenigvuldigen van overeenkomsten, bestekken, tekeningen, berekeningen, rapporten e.d. door middel van lichtdrukken, fotokopiëren, plotten, printen of anderszins; • Premies van verzekeringen; • Kosten van consumpties; • Eventuele kosten ter zake van ondersteuning vanuit de eigen organisatie; • (Overige) overheadkosten.
57.	De opgegeven uurtarieven zullen ook worden gehanteerd voor eventuele meer-/ minderwerkzaamheden.
58.	Kortingen dienen te worden verwerkt in de uurlonen, materiaalprijzen en dergelijke, algemene kosten, winst en risico, enzovoort.
59.	Het opnemen van negatieve bedragen of negatieve kortingen en/of negatieve percentages in de Inschrijving is niet toegestaan en leidt tot uitsluiting van deelname aan de aanbesteding.
60.	Voor de opgegeven uurtarieven is een maximale opslag toegestaan van: • 15 % op werkdagen tussen 18.00 – 24.00 uur • 25% op werkdagen tussen 0.00 – 08.00 uur • 50% op zaterdagen, zondagen en feestdagen
61.	Weglatingen, vergissingen en dergelijke in het prijzenformulier zijn voor rekening en risico van Opdrachtnemer.
62.	Opdrachtnemer stuurt facturen in volgens de bepalingen die zijn vastgesteld door Opdrachtgever. Zie hiervoor **Bijlage K.**

4. Communicatie en rapportages

Nummer	Eis
63.	Partijen wijzen een vaste en een vervangend contactpersoon binnen de organisatie aan die operationeel verantwoordelijk is en gedurende de uitvoering van de Opdracht het vaste aanspreekpunt is voor Opdrachtgever en Opdrachtnemer.
64.	Partijen wijzen een vaste en vervangende contactpersoon binnen de organisatie aan die op tactisch/ strategisch niveau verantwoordelijk en beslissingsbevoegd is.
65.	Communicatie tussen de contactpersonen als bedoeld in eis 63 zal op continue basis plaatsvinden teneinde de correcte uitvoering van de Overeenkomst te bewaken.
66.	Tenminste eenmaal (1x) per kwartaal vindt overleg plaats tussen de tactisch/strategisch verantwoordelijken bedoeld in eis 64 van Opdrachtgever en Opdrachtnemer.
67.	Tenminste eenmaal (1x) per kwartaal vindt strategisch overleg plaats tussen de contactpersonen als bedoeld in eis 64 over onder meer, doch niet uitsluitend, de uitvoering van de Opdracht ten opzichte van de afgesproken Servicelevels en bijbehorende KPI's.
68.	Uiterlijk drie (3) maanden voor het verstrijken van de dan geldende contractperiode of zoveel vaker als door Opdrachtgever noodzakelijk wordt geacht, vindt op initiatief van Opdrachtgever een evaluatiebespreking plaats tussen de contactpersonen zoals bedoeld in eis 65. Onderwerp van deze bespreking zijn in ieder geval de rapportages, procedures, organisatorische kwesties, projecten en relevante nieuwe ontwikkelingen.
69.	De verslaglegging van de overleggen zoals bedoeld in eis 66 en 67 dient binnen vijf (5) werkdagen door Opdrachtnemer digitaal te worden aangeleverd aan de tactisch/strategisch verantwoordelijken van Opdrachtgever.

5. Retransitie

Nummer	Eis
70.	De retransitie is de overdracht van de Dienstverlening (d.w.z. de implementatie en migratie) door Opdrachtnemer aan Opdrachtgever of een opvolgend Opdrachtnemer na beëindiging van de Overeenkomst om welke reden dan ook. Opdrachtnemer dient proactief mee te werken aan het opstellen van het retransitieplan (exitplan). Tijdens de retransitie dient Opdrachtnemer alle benodigde informatie over te dragen.
71.	Opdrachtnemer verleent op eerste verzoek van Opdrachtgever zijn medewerking aan de retransitie.

6. Technische eisen

Nummer	Eis
72.	De oplossing ondersteunt IEEE 802.1X (EAP-TLS en PEAP) voor bedrade en draadloze toegang, met RADIUS-integratie (RFC 2865/5176, incl. CoA).
73.	De oplossing ondersteunt Identity PSK (per gebruiker of apparaat een unieke PSK op dezelfde SSID), inclusief intrekken en vervallen van individuele sleutels zonder impact op andere apparaten.
74.	De internetaansluiting ondersteunt eBGP voor IPv4 en IPv6, inclusief BFD, prefix-filtering, RPKI-validatie en multihoming.
75.	De oplossing integreert met Microsoft Entra ID via SAML 2.0 of OIDC voor beheerders-SSO. Voor gebruikers- en groepsinformatie gebruikt ze SCIM of Microsoft Graph, en voor authenticatie en autorisatie gebruikt ze Entra-attributen of groepslidmaatschap.
76.	De oplossing ondersteunt device profiling en classificatie (bijv. op DHCP-, LLDP- en HTTP-fingerprinting) en gebruikt de compliancestatus van Entra/Intune als input voor toegangsbeleid. Beheerde apparaten (certificaat via Intune) en BYOD krijgen aantoonbaar verschillende toegangsrechten en segmenten.
77.	Alle switchpoorten, inclusief poorten waar access-points op aangesloten zijn, worden beveiligd met poortauthenticatie (802.1X, of MAB als fallback). Voor AP-poorten is dat bijvoorbeeld 802.1X met een AP-certificaat of een equivalente beveiligde methode. Ongeautoriseerde apparaten komen in een quarantaine-VLAN of worden geblokkeerd.
78.	Op distributielagen worden ACL's ondersteund met minimaal 512 regels per ACL, voor IPv4 en IPv6, in hardware (geen CPU-impact), met logging van hits.
79.	De firewall ondersteunt content filtering (URL-categorieën, applicatiecontrole, malwarescan) en TLS-inspectie. De opgegeven doorvoer geldt met content filtering en TLS-inspectie ingeschakeld.
80.	Alle netwerkcomponenten sturen logging via syslog (RFC 5424, bij voorkeur over TLS) naar een door de opdrachtgever aan te wijzen lokale SIEM of syslog-server. Alle logging is volledig, tijd-gesynchroniseerd (NTP) en niet afhankelijk van een cloudomgeving.
81.	De oplossing biedt een lokaal bereikbare API (REST, RESTCONF/NETCONF of gNMI) met volledige lees- en schrijfrechten, OpenAPI-documentatie en token- of certificaatauthenticatie. Beheer via de API werkt ook als de cloudverbinding wegvalt.
82.	Beheer op afstand verloopt uitsluitend via een stepping stone in het netwerk van opdrachtgever (jump host) en met multifactorauthenticatie. Beheerhandelingen worden gelogd en zijn herleidbaar tot een persoon (RBAC, geen gedeelde accounts). Beheer via een Cloud oplossing dient gelimiteerd te kunnen worden tot de publieke IP-Adressen van Onderwijsgroep Landstede.
83.	Logging is nagenoeg realtime beschikbaar: maximaal 5 seconden tussen gebeurtenis en beschikbaarheid in de SIEM. Wijzigingen worden binnen een nader te bepalen tijd uitgerold. De inschrijver beschrijft de gemeten vertraging.
84.	Access-switches leveren PoE (IEEE 802.3at/bt) in voldoende vermogen voor alle aangesloten access-points en andere apparaten, met een 60 W PoE-budget per poort en een volledig vermogensplan per locatie.
85.	Data en logging blijven binnen de EU/EER, en er is geen verplichte afhankelijkheid van een cloudcontroller voor de basisfunctionaliteit.

86.	Poorten ondersteunen multigigabit (2,5/5 Gbps) voor access-points waar Wi-Fi 6E of 7 dat vereist.
87.	De switches ondersteunen DHCP snooping, Dynamic ARP Inspection, IP Source Guard, BPDU guard en storm control.
88.	Distributieswitches ondersteunen layer 3-routering met OSPF en eventueel BGP, voor IPv4 en IPv6 (dual-stack), in hardware.
89.	Distributie switches zijn voorzien van een redundante voeding.
90.	Core switches zijn voorzien van redundante voeding.
91.	Alle aangeboden netwerkcomponenten binnen het LAN- , Wi-Fi- en Firewall domein (campusswitches, access-points, firewalls, NAC en de bijbehorende beheer- en monitoringsoftware) zijn afkomstig van dezelfde fabrikant en worden beheerd vanuit één gezamenlijk beheerplatform, waarmee wired en wireless en security centraal worden geconfigureerd, gemonitord en voorzien van firmware-updates.