

Programma van Eisen

Openbare Europese aanbesteding integrale ICT-dienstverlening

Projectnummer: VLC/2603396

TenderNed-kenmerk: TN614679

Datum: 16-10-2026

Bijlage 3

Stichting TWijs Europese aanbesteding integrale ICT-dienstverlening

Opdrachtgever: Stichting TWijs, Haarlem

In samenwerking met VLC Inkoop & Advies en Beks advies

Inhoudsopgave

HOOFDSTUK 1 Algemeen en juridisch.....	3
HOOFDSTUK 2 Organisatie, rollen en contractmanagement.....	3
HOOFDSTUK 3 Servicedesk en ondersteuning.....	3
HOOFDSTUK 4 Incidentbeheer en servicelevels	4
HOOFDSTUK 5 Wijzigingsbeheer	5
HOOFDSTUK 6 Werkplek- en devicebeheer.....	5
HOOFDSTUK 7 Firewall, switches en netwerkbeveiliging.....	6
HOOFDSTUK 8 Wifi	9
HOOFDSTUK 9 Microsoft 365	10
HOOFDSTUK 10 DLWO en applicatieontsluiting	10
HOOFDSTUK 11 Identity en Access Management en koppelingen	11
HOOFDSTUK 12 Informatiebeveiliging en privacy	12
HOOFDSTUK 13 Asset- en configuratieregistratie	12
HOOFDSTUK 14 Rapportage en overleg.....	13
HOOFDSTUK 15 Training en adoptie	13
HOOFDSTUK 16 Implementatie en migratie	13
HOOFDSTUK 17 Exit en overdracht	14
HOOFDSTUK 18 Duurzaamheid en MVO.....	14
HOOFDSTUK 19 Prijzen, facturatie en indexering	14
Bijlage 1 Prioritering en servicelevels.....	15

HOOFDSTUK 1 Algemeen en juridisch

- 1.1 Werkzaamheden door opdrachtnemer voldoen te allen tijde aan alle relevante wet- en regelgeving en aan alle geldende wettelijke normen.
- 1.2 Communicatie tijdens de contractduur geschiedt in de Nederlandse taal.
- 1.3 Werkzaamheden in ruimtes van de opdrachtgever worden uitgevoerd door herkenbaar geklede medewerkers die zich vooraf melden bij de contactpersoon van de betreffende locatie en zich na voltooiing weer afmelden.
- 1.4 Medewerkers van opdrachtnemer die werkzaamheden verrichten op schoollocaties beschikken over een geldige Verklaring Omtrent het Gedrag (VOG).
- 1.5 De Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten (ARBIT-2022) zijn van toepassing, tenzij daarvan in de overeenkomst uitdrukkelijk wordt afgeweken.
- 1.6 De leverings-, betalings- en/of algemene voorwaarden van opdrachtnemer worden uitdrukkelijk verworpen.
- 1.7 Inzet van onderaannemers vindt uitsluitend plaats na voorafgaande schriftelijke instemming van de opdrachtgever. Opdrachtnemer blijft integraal verantwoordelijk voor de dienstverlening.
- 1.8 Alle data, configuraties en documentatie die in het kader van deze opdracht ontstaan, zijn en blijven eigendom van de opdrachtgever.

HOOFDSTUK 2 Organisatie, rollen en contractmanagement

- 2.1 Opdrachtnemer stelt een operationeel, een tactisch en een strategisch aanspreekpunt beschikbaar, met een schriftelijk vastgelegde escalatieladder.
- 2.2 Wisseling van sleutelfunctionarissen wordt vooraf gemeld en vindt uitsluitend plaats met aantoonbaar gelijkwaardig gekwalificeerde vervanging.
- 2.3 Opdrachtnemer levert bij aanvang een overzicht van rollen, verantwoordelijkheden en bevoegdheden, dat bij wijziging wordt geactualiseerd.

HOOFDSTUK 3 Servicedesk en ondersteuning

- 3.1 Opdrachtnemer beschikt over een Nederlandstalige servicedesk, bereikbaar op werkdagen van 07:30 tot 17:30 uur.
- 3.2 Opdrachtnemer fungeert als Single Point of Contact voor alle ICT-vragen van medewerkers en scholen. Na gunning deelt de opdrachtgever een lijst van leveranciers waarvoor opdrachtnemer deze rol vervult, waaronder de leverancier van de internetverbindingen, de licentieleverancier, de hardware leverancier, de printerleverancier, de telefonieleverancier, de beheerder van de wifi-omgeving en leveranciers van onderwijsapplicaties. De lijst wordt gedurende de looptijd in overleg geactualiseerd.
- 3.3 Bij een melding die feitelijk een van deze leveranciers betreft, coördineert opdrachtnemer de opvolging en houdt de school op de hoogte. Opdrachtnemer is verantwoordelijk voor de communicatie in de SPOC-rol, niet voor het nakomen van afspraken door die derden.
- 3.4 Het is voor de opdrachtgever mogelijk om incidenten aan te melden per e-mail, telefoon en via een portaal. Er geldt geen restrictie voor het soort aanmelders.
- 3.5 Ten minste 80% van de telefonische meldingen wordt binnen twee minuten door een medewerker van de servicedesk aangenomen, gemeten per kwartaal over alle oproepen binnen de servicetijden. Het aandeel niet-aangenomen oproepen bedraagt maximaal 10% per kwartaal.

- 3.6 Ten minste 70% van de gemelde incidenten wordt tijdens het eerste contact met de servicedesk afgehandeld, zonder overdracht naar een tweede lijn en zonder vervolcontact, gemeten per kwartaal. Wijzigingsverzoeken volgens hoofdstuk 5 blijven hierbij buiten beschouwing. Het aandeel meldingen dat binnen vijf werkdagen na afhandeling wordt heropend of opnieuw wordt gemeld, bedraagt ten hoogste 5% per kwartaal.
- 3.7 De normen uit de eisen 3.5 en 3.6 worden opgenomen in de kwartaalrapportage volgens hoofdstuk 14.
- 3.8 Opdrachtgever heeft via een portaal inzicht in de voortgang van incidenten, zowel op school- als op bovenschools niveau.
- 3.9 Remote ondersteuning en meekijken op een werkplek vinden uitsluitend plaats met expliciete toestemming van de gebruiker en worden vastgelegd.
- 3.10 On-site ondersteuning is beschikbaar wanneer remote afhandeling niet mogelijk is.
- 3.11 Technische handelingen op locatie voert opdrachtnemer zelf uit; op de schoollocaties is geen technische expertise aanwezig.

HOOFDSTUK 4 Incidentbeheer en servicelevels

- 4.1 Prioritering van incidenten en de opvolging daarvan vinden plaats volgens de matrix omschreven in Bijlage 1 van dit document. Prioritering is gebaseerd op de impact op het onderwijs en de bedrijfsvoering.
- 4.2 De ICT-voorzieningen welke in direct beheer van de opdrachtnemer zijn, zijn ten minste 99% beschikbaar gedurende de servicetijden, gemeten per locatie.
- 4.3 Servicetijden zijn maandag tot en met vrijdag van 07:30 tot 17:30 uur, met uitzondering van algemeen erkende feestdagen.
- 4.4 Van elk incident met prioriteit 1 wordt een herstelrapportage opgesteld met oorzaak, herstelmaatregel en preventieve maatregel.
- 4.5 Bij herhaald optreden van vergelijkbare incidenten voert opdrachtnemer op eigen initiatief een oorzaakanalyse uit en doet voorstellen tot structurele oplossing.
- 4.6 De gerealiseerde servicelevels worden per kwartaal gerapporteerd volgens hoofdstuk 14.

Creditering bij het niet halen van de servicelevels

- 4.7 De prestaties worden per kwartaal getoetst aan drie normen: de oplostijden per prioriteit volgens eis 4.1, de beschikbaarheid volgens eis 4.2 en de servicedesknormen volgens de eisen 3.5 en 3.6. Andere onderdelen van de dienstverlening vallen buiten deze regeling.
- 4.8 Wordt een norm in een kwartaal niet gehaald, dan meldt opdrachtnemer dit in de kwartaalrapportage en levert binnen twintig werkdagen een verbeterplan met concrete maatregelen en een termijn. Aan het eerste kwartaal waarin een norm niet wordt gehaald, is geen creditering verbonden.
- 4.9 Wordt dezelfde norm in het daaropvolgende kwartaal opnieuw niet gehaald, dan crediteert opdrachtnemer 2% van de over dat kwartaal gefactureerde beheervergoeding per niet gehaalde norm, tot een maximum van 6% per kwartaal.
- 4.10 Wordt dezelfde norm in een derde opeenvolgend kwartaal niet gehaald, dan bedraagt de creditering 4% per niet gehaalde norm, tot een maximum van 12% per kwartaal. Partijen stellen in dat geval gezamenlijk een verbetertraject vast met een vaste einddatum.
- 4.11 Wordt dezelfde norm in vier opeenvolgende kwartalen niet gehaald, dan heeft de opdrachtgever het recht de overeenkomst tussentijds te beëindigen zonder tot enige vergoeding gehouden te zijn.
- 4.12 De totale creditering over een contractjaar bedraagt ten hoogste 15% van de over dat jaar gefactureerde beheervergoeding.

- 4.13 Geen creditering is verschuldigd voor zover het niet halen van een norm aantoonbaar voortkomt uit omstandigheden buiten de invloedssfeer van opdrachtnemer, waaronder een storing in de internetverbinding, uitval van elektriciteit, of een storing in apparatuur of diensten die buiten de scope van deze opdracht vallen. Opdrachtnemer onderbouwt een beroep hierop in de kwartaalrapportage.
- 4.14 Creditering vindt plaats door middel van een creditnota op de eerstvolgende kwartaalfactuur. De regeling laat het recht van de opdrachtgever op nakoming, ontbinding en schadevergoeding onverlet.

HOOFDSTUK 5 Wijzigingsbeheer

- 5.1 Wijzigingen worden getest, gedocumenteerd en vooraf met de opdrachtgever afgestemd.
- 5.2 Standaardwijzigingen worden zonder afzonderlijke offerte uitgevoerd binnen de volgende doorlooptijden, gerekend vanaf een volledige aanvraag:
- aanmaken, wijzigen of blokkeren van een account: één werkdag;
 - activeren van een bestaande netwerkpoort of toekennen van een bestaand VLAN: drie werkdagen;
 - aanvraag voor een uitzondering op de internetfiltering: volgens eis 7.12.
- 5.3 Opdrachtnemer onderhoudt een wijzigingskalender die inzichtelijk is voor de opdrachtgever.
- 5.4 Het onderhoudsvenster loopt van 21:00 uur 's avonds tot 07:00 uur 's ochtends. Onderhoudswerkzaamheden worden minimaal vijf werkdagen van tevoren per e-mail aangekondigd.
- 5.5 Wijzigingen met impact op de beschikbaarheid worden uitsluitend binnen het onderhoudsvenster uitgevoerd.
- 5.6 Voor elke impactvolle wijziging is vooraf een rollback-scenario beschreven.

HOOFDSTUK 6 Werkplek en devicebeheer

- 6.1 Opdrachtnemer verzorgt de volledige configuratie en het beheer van de werkplekken.
- 6.2 Op alle beheerde devices is endpointbescherming actief met ten minste bescherming tegen virussen en malware en gedragsgebaseerde detectie van verdacht gedrag, passend bij het betreffende besturingssysteem. Opdrachtnemer beheert deze bescherming centraal vanuit de beheeromgeving volgens eis 6.9, houdt configuratie en detectiedefinities actueel en zorgt dat de bescherming niet door de gebruiker kan worden uitgeschakeld. Voor devices waarvoor een afzonderlijke virusscanner niet gangbaar of niet mogelijk is, waaronder Chromebooks en iPads, dwingt opdrachtnemer in plaats daarvan de beveiligingsinstellingen van het platform centraal af.
- 6.3 Meldingen uit de endpointbescherming komen centraal samen en worden door opdrachtnemer beoordeeld. Alertering vindt 24 uur per dag plaats richting opdrachtnemer; opvolging geschiedt binnen de servicetijden, met uitzondering van meldingen die wijzen op een actief beveiligingsincident: die worden direct opgepakt en gemeld volgens eis 12.3. Bij een bevestigde besmetting neemt opdrachtnemer onverwijld maatregelen om verspreiding te voorkomen, waaronder het ontnemen van netwerktoegang aan het betreffende device volgens eis 7.19.
- 6.4 Remote beheer is de standaardwerkwijze.
- 6.5 Lokale beheerrechten op Windows-devices zijn uitsluitend toegekend aan een daartoe aangewezen gebruikersgroep. Overige gebruikers, waaronder medewerkers en leerlingen, beschikken niet over lokale beheerrechten. De samenstelling van deze groep wordt in overleg met de opdrachtgever vastgelegd en ten minste jaarlijks getoetst volgens eis 11.10.
- 6.6 Opdrachtnemer ondersteunt de respectievelijke hardwareleverancier in het opnemen van devices (Windows, Chromebooks, iPads) in de omgeving, met de juiste beheertoegang.

- 6.7 Opdrachtnemer verzorgt het provisioning- en beheerproces voor alle in gebruik zijnde devicetypen. Het overzicht van devicetypen en aantallen per locatie is opgenomen in Bijlage 7 Overzicht scholen en hardware met de beschrijving van de huidige situatie.
- 6.8 Opdrachtnemer beheert en onderhoudt de werkplekken van medewerkers en leerlingen volgens de overeengekomen specificaties per gebruikersgroep.
- 6.9 Het werkplekbeheer wordt georganiseerd binnen gangbare standaardapplicaties: Microsoft Intune voor Windows devices en Google Admin voor Chromebooks. iPads worden beheerd binnen een aparte JAMF omgeving welke buiten scope van de opdracht valt.
- 6.10 Opdrachtnemer beschrijft en hanteert een werkwijze voor opname van nieuwe devices in de betreffende beheeromgeving.
- 6.11 Uitgifte, inname en vervanging van devices worden verwerkt in de registratie volgens hoofdstuk 13.
- 6.12 Op de schoollocaties wordt nu Uniflow gebruikt als printoplossing, deze omgeving wordt opnieuw aanbesteed. Opdrachtnemer verzorgt de uitrol en het beheer van de clientcomponenten op de werkplekken, waaronder installatie via de beheeromgeving en de koppeling met gebruikersaccounts, en fungeert als meldpunt richting de nog te bepalen printleverancier. Het beheer van de printer-serveromgeving en van de multifunctionals valt buiten deze opdracht.

HOOFDSTUK 7 Firewall, switches en netwerkbeveiliging

Capaciteit en levering

- 7.1 De aangeboden firewalls hebben een threat protection throughput van minimaal **1 Gbps** per locatie, gemeten met IPS, application control en webfiltering gelijktijdig actief en zonder SSL-inspectie. Inschrijver vermeldt de opgave van de fabrikant en het meetprofiel waarop deze is gebaseerd. De internetaansluitingen van de opdrachtgever hebben een capaciteit van 1 Gbps; de firewall mag geen beperkende factor vormen.
- 7.2 De aangeboden firewalls hebben minimaal vier 1Gbps ethernetpoorten en ondersteunen een tweede WAN-aansluiting voor redundantie of load balancing. De WAN-poort kan de volledige capaciteit van de aangesloten internetverbinding benutten.
- 7.3 De te leveren apparatuur is nieuw en wordt betrokken via een door de fabrikant erkend distributiekanaal. Bij oplevering draait op elke component een firmwareversie die door de fabrikant wordt ondersteund. Alle voor gebruik en beheer benodigde licenties en gebruiksrechten zijn in de aanbieding begrepen en gelden voor ten minste vijf jaar na oplevering.

Functionaliteit van de firewall

- 7.4 De aangeboden firewalls bieden de volgende functionaliteiten:
 - IP-routing op IPv4 en IPv6;
 - VLAN-segmentatie en aggregatie voor ten minste 15 VLANs;
 - VPN-ondersteuning, zowel SSL-VPN als IPsec-VPN;
 - statische routes (IPv4 en IPv6).
- 7.5 De firewall beschikt over een Intrusion Prevention System dat in preventiemodus wordt ingericht, met automatisch bijgewerkte signatures.
- 7.6 De firewall inspecteert verkeer op malware op gatewayniveau, aanvullend op de bescherming op de endpoints.

- 7.7 De firewall ondersteunt SSL-inspectie. De opdrachtgever schrijft de inzet hiervan niet voor: de contentfiltering volgens de eisen 7.8 tot en met 7.11 functioneert zonder decryptie van verkeer, op basis van SNI en DNS. Inschrijver geeft in het inschrijfbiljet informatief op welke doorvoersnelheid het aangeboden model haalt met SSL-inspectie actief. Besluit de opdrachtgever gedurende de looptijd alsnog tot inzet, dan gebeurt dat na een gezamenlijke afweging waarin ten minste de gevolgen voor privacy, beheerlast en doorvoersnelheid zijn beschreven.

Filtering van internetverkeer

- 7.8 De firewall filtert internetverkeer op basis van categorieën, waarbij afwijkend beleid kan worden ingesteld per gebruikersgroep: leerlingen, medewerkers en gasten.
- 7.9 SafeSearch en een beperkte modus voor videoplatforms kunnen centraal worden afgedwongen.
- 7.10 De oplossing maakt gebruik van een beveiligde DNS-resolver die bekende kwaadaardige domeinen blokkeert.
- 7.11 Verkeer naar externe DNS-over-HTTPS- en DNS-over-TLS-resolvers en naar bekende VPN- en proxydiensten wordt geblokkeerd, zodat de filtering niet vanaf het device kan worden omzeild.
- 7.12 Een school kan via een vastgelegd proces een uitzondering op de filtering aanvragen. De doorlooptijd bedraagt maximaal twee werkdagen. Voor een aanvraag die een op dat moment lopende les blokkeert, geldt een spoedprocedure met een doorlooptijd van maximaal vier uur binnen de servicetijden.
- 7.13 Opdrachtnemer rapporteert per school over geblokkeerd verkeer als onderdeel van de kwartaalrapportage volgens hoofdstuk 14.

Segmentatie

- 7.14 Het netwerk kent gescheiden segmenten voor ten minste: leerlingen, medewerkers, gasten, beheer, en gebouwgebonden apparatuur en overige IoT zoals intercom, alarm- en brandmeldinstallaties, zonwering en gebouwbeheersystemen.
- 7.15 Verkeer tussen de segmenten wordt gefilterd op de laag 3-switch door middel van access control lists, volgens het principe van default deny: alleen expliciet toegestaan verkeer tussen segmenten wordt doorgelaten. Het segment voor gebouwgebonden apparatuur en IoT heeft geen toegang tot systemen of data van leerlingen en medewerkers.
- 7.16 Opdrachtnemer herijkt in samenspraak met de opdrachtgever het VLAN-plan en de bijbehorende ACL-set, documenteert deze, houdt beide gedurende de looptijd actueel en toetst ze ten minste jaarlijks op nog bestaande noodzaak. Van het VLAN-plan en de ACL-set wordt een back-up bijgehouden, evenals van de configuraties van de firewalls en switches; jaarlijks wordt hiervan een hersteltest uitgevoerd.

Switches

- 7.17 Alle toegepaste switches zijn volledig managed en bieden:
- VLAN-ondersteuning voor het scheiden van de segmenten uit eis 7.14;
 - laag 3-routing tussen VLANs;
 - access control lists die hardwarematig worden verwerkt, zodat filtering tussen segmenten geen invloed heeft op de doorvoersnelheid;
 - logging van geweigerd verkeer naar de centrale logvoorziening volgens eis 7.26;
 - 802.1X port authentication;
 - SNMP en logging naar een centrale server;
 - veilig beheer: geen onbeveiligde HTTP-interfaces, beheer via HTTPS of SSH;
 - Optioneel PoE+ (802.3at);

- uplinkmogelijkheid 2× 10Gbit (SFP+);
 - cloud-based of gecentraliseerd management.
- 7.18 Apparatuur die 802.1X niet ondersteunt, zoals digiborden, printers, camera's en intercoms, wordt aangesloten via MAC Authentication Bypass. Deze uitzonderingen worden vastgelegd in de asset- en configuratieregistratie volgens hoofdstuk 13, met vermelding van het apparaat, de locatie, de poort en het toegekende VLAN, en worden ten minste jaarlijks getoetst op nog bestaande noodzaak.
- 7.19 Een poort waarop de authenticatie mislukt wordt niet opengesteld, maar geplaatst in een quarantaine-VLAN zonder toegang tot interne systemen en data. Mislukte authenticatiepogingen worden gelogd volgens eis 7.26.
- 7.20 Niet-beheerde devices, waaronder privételefoons van medewerkers, krijgen geen toegang tot het medewerkers- of leerlingennetwerk. Zij maken gebruik van het gastnetwerk volgens eis 7.14.
- 7.21 Iedere switch kan afzonderlijk worden geüpdatet of geüpgraded zonder de functionaliteit van het netwerk te beïnvloeden.

Beheerplatform en toegang

- 7.22 De firewalls en switches worden beheerd via één centraal, beveiligd beheerplatform met tweefactorauthenticatie of single sign-on, logging van beheeracties en rollenbeheer waarin onderscheid wordt gemaakt tussen bovenschools en schoolniveau.
- 7.23 Beheerinterfaces zijn niet vanaf internet benaderbaar. Beheer op afstand vindt uitsluitend plaats via een beveiligde verbinding met tweefactorauthenticatie.
- 7.24 De opdrachtgever beschikt gedurende de gehele looptijd over ten minste leesrechten op het beheerplatform en op de configuratie.
- 7.25 Toegang op afstand tot het netwerk van de opdrachtgever, voor zover die wordt ingericht, vindt uitsluitend plaats via een versleutelde verbinding met multifactorauthenticatie, is beperkt tot daartoe aangewezen beheerde devices en tot de daarvoor noodzakelijke segmenten, en wordt gelogd volgens eis 7.26. De toegekende rechten worden vastgelegd en ten minste jaarlijks getoetst volgens eis 11.10.

Logging en monitoring

- 7.26 De firewall kan logs in realtime exporteren naar een externe, beveiligde locatie zoals een syslogserver of SIEM-oplossing. Logs van firewall en switches komen op één centrale plek samen.
- 7.27 Netwerkverkeer wordt geautomatiseerd en doorlopend gemonitord op verdachte patronen. Alertering vindt 24 uur per dag plaats richting opdrachtnemer. Opvolging geschiedt binnen de servicetijden, met uitzondering van bevindingen die wijzen op een actief beveiligingsincident: die worden direct opgepakt en gemeld volgens de procedure in eis 12.3.

Patchbeheer

- 7.28 Opdrachtnemer houdt de firmware en software van de geleverde componenten actueel en installeert securitypatches binnen de door de fabrikant geadviseerde termijn. Patches voor kwetsbaarheden met een hoge of kritieke classificatie worden uiterlijk binnen één week na beschikbaarstelling doorgevoerd. Installatie vindt plaats binnen het onderhoudsvenster volgens eis 5.4 en wordt opgenomen in de wijzigingskalender volgens eis 5.3.

Support, eigendom en documentatie

- 7.29 De aangeboden componenten staan gedurende ten minste vijf jaar na oplevering onder actieve fabrikantssupport met beveiligingsupdates.

- 7.30 Wordt de overeenkomst verlengd tot voorbij vijf jaar na oplevering, dan biedt opdrachtnemer tijdig een ten minste gelijkwaardige firewall aan. Prijsstelling volgens eis 19.7.
- 7.31 Het eigendom van de geleverde firewalls en switches gaat bij oplevering per locatie over op de opdrachtgever.
- 7.32 De configuratie en de netwerktekeningen worden gedocumenteerd en bij elke wijziging geactualiseerd.

HOOFDSTUK 8 Wifi

Raakvlak met een extern beheerde wifi-omgeving

- 8.1 Opdrachtnemer levert en beheert de switchpoorten, de PoE-voeding en de VLAN-configuratie die de wifi-omgeving nodig heeft, en stemt wijzigingen daarin vooraf af met de beheerder van de wifi-omgeving.
- 8.2 Opdrachtnemer levert en beheert de authenticatievoorziening voor 802.1X en is daarmee verantwoordelijk voor zowel de bekabelde poorten als de aansluiting van de draadloze omgeving. De opdrachtgever werkt volledig in de cloud en beschikt niet over een on-premises Active Directory; authenticatie met gebruikersnaam en wachtwoord op basis van PEAP-MSCHAPv2 is daarmee uitgesloten. Authenticatie vindt plaats op basis van certificaten die via de beheeromgeving worden uitgegeven en ingetrokken, gekoppeld aan Entra ID als identity provider. Inschrijver beschrijft in zijn aanbieding hoe hij deze voorziening inricht. Opdrachtnemer bewaakt de geldigheidsduur van de gebruikte certificaten en vernieuwt deze tijdig; het verlopen van een servercertificaat wordt aangemerkt als incident met prioriteit 1.
- 8.3 Bij een storing waarbij niet direct duidelijk is of de oorzaak in de bekabelde of de draadloze omgeving ligt, neemt opdrachtnemer de melding aan, voert de analyse aan zijn zijde uit en lost de melding in samenspraak met de beheerder van de wifi-omgeving op. Opdrachtnemer blijft aanspreekpunt voor de school tot de melding is afgehandeld.

Uitbreiding en vervanging van accesspoints

- 8.4 Accesspoints die opdrachtnemer levert, ter vervanging of uitbreiding, zijn geschikt voor plaatsing binnen in schoolgebouwen en voor de gebruiksdichtheid in het primair onderwijs: per accesspoint ten minste 40 gelijktijdig actieve apparaten, zoals een volledige groep met Chromebooks of iPads tijdens een digitale toets, met een doorvoersnelheid van ten minste 10 Mbit/s per apparaat. Opdrachtnemer onderbouwt de dekking en het aantal accesspoints per locatie met een site survey of een voorspellende dekkingsmeting.
- 8.5 De nieuw te leveren accesspoints ondersteunen ten minste Wi-Fi 6E (IEEE 802.11ax) met gelijktijdige werking in de 2,4 GHz-, 5 GHz- en 6 GHz-band en zijn gecertificeerd door de Wi-Fi Alliance. Accesspoints ondersteunen snelle roaming (IEEE 802.11k, 802.11r en 802.11v), band steering en automatisch kanaal- en zendvermogenbeheer.
- 8.6 De nieuw te leveren accesspoints worden gevoed via Power over Ethernet en werken met volledige functionaliteit op IEEE 802.3at (PoE+), zonder uitschakeling van radio's of poorten. Vereist een aangeboden accesspoint IEEE 802.3bt voor volledige functionaliteit, dan vermeldt inschrijver dit in zijn aanbieding en is het PoE-budget van de switches daarop afgestemd. De uplink ondersteunt ten minste 1 Gbit/s.

- 8.7 De nieuw te leveren accesspoints ondersteunen WPA3-Enterprise met 802.1X-authenticatie op basis van certificaten (EAP-TLS) via de authenticatievoorziening van opdrachtnemer, met dynamische VLAN- en roltoewijzing op basis van RADIUS-attributen. Ten minste afzonderlijke netwerken voor medewerkers, leerlingen, gasten en apparaten zijn mogelijk, elk gescheiden in een eigen VLAN. Apparaten die geen 802.1X ondersteunen worden aangesloten met een unieke sleutel per apparaat of apparaatgroep. Het gastnetwerk kent isolatie tussen apparaten onderling. Protected Management Frames (IEEE 802.11w) zijn ingeschakeld; WPA2 wordt uitsluitend als overgangsmodus ingezet voor apparaten die WPA3 niet ondersteunen.
- 8.8 De nieuw te leveren accesspoints worden centraal beheerd vanuit een beheeromgeving waarvan de gegevens binnen de Europese Unie worden opgeslagen, en zijn geïntegreerd met de firewall en de switches. Daartoe ondersteunen zij ten minste VLAN-tagging (IEEE 802.1Q), LLDP, RADIUS-accounting en Change of Authorization, doorgifte van logging via syslog aan de centrale logvoorziening en monitoring via SNMPv3 of een API. Gebruikers- en apparaatidentiteit wordt aan de firewall beschikbaar gesteld, zodat filtering en beleid per doelgroep ook voor draadloos verkeer werken. Accesspoints detecteren en melden onbekende accesspoints en draadloze aanvallen.
- 8.9 Accesspoints zijn op het moment van levering niet aangekondigd als end-of-sale. De fabrikant levert firmware- en beveiligingsupdates gedurende ten minste vijf jaar na levering. Accesspoints zijn geschikt voor plafond- of wandmontage en zijn beveiligd tegen diefstal en eenvoudige manipulatie.
- 8.10 Bij vervanging of uitbreiding van accesspoints gedurende de looptijd doet opdrachtnemer een aanbod tegen de dan geldende netto inkoopprijs vermeerderd met een in het prijzenblad op te geven opslagpercentage. Dit percentage staat gedurende de gehele looptijd vast. Zie ook 19.7.

HOOFDSTUK 9 Microsoft 365

- 9.1 Opdrachtnemer beheert de Microsoft 365-omgeving en zorgt voor de provisioning van Entra ID. De firma PlexSys is verantwoordelijk voor Exchange Online, Teams, SharePoint, OneDrive en de inrichting hiervan binnen de tenant.
- 9.2 De opdrachtgever is en blijft eigenaar van de tenant. Ten minste één global administrator-account berust bij de opdrachtgever.
- 9.3 Opdrachtnemer hanteert een security baseline met ten minste conditional access, multifactorauthenticatie en beperking van legacy-authenticatie.
- 9.4 Licenties worden afgenomen via APS IT-diensten. Opdrachtnemer signaleert benodigde licentiemutaties, verwerkt deze in de tenant en fungeert als meldpunt richting APS.
- 9.5 Wijzigingen in de tenantconfiguratie worden gedocumenteerd en zijn herleidbaar naar persoon en moment.
- 9.6 Opslag en verwerking van gegevens vinden plaats binnen de Europese Unie.
- 9.7 Opdrachtnemer adviseert proactief over nieuwe functionaliteit binnen Microsoft 365 die relevant is voor het onderwijsproces.
- 9.8 Licentiebeheer, waaronder toewijzing bij in- en uitstroom en kostenoptimalisatie, is onderdeel van de dienstverlening.

HOOFDSTUK 10 DLWO en applicatieontsluiting

- 10.1 De leer- en werkomgeving is geschikt voor alle in gebruik zijnde devicetypen en ontsluit alle software: educatieve software, kantoorautomatisering en bestuursapplicaties.
- 10.2 De omgeving beschikt over een koppeling met Basispoort.
- 10.3 Applicaties en hyperlinks kunnen worden toegekend per leerling, per groep en per leerjaar, en zijn door een leerkracht of een (bovenschoolse) ICT-coördinator zelf in te stellen zonder tussenkomst van opdrachtnemer.

- 10.4 Leerlingen die nog niet kunnen lezen kunnen zelfstandig inloggen door middel van een grafische of op QR gebaseerde inlogmethode.
- 10.5 Toegang tot applicaties verloopt via single sign-on op basis van de identity provider van de opdrachtgever.
- 10.6 De omgeving is buiten geplande onderhoudsmomenten beschikbaar volgens de norm in eis 4.2.
- 10.7 Het portaal is beschikbaar op alle binnen TWiJS gangbare devices: Chromebooks, Windows-devices, digiborden en iPads.
- 10.8 Opdrachtnemer is als netwerkleverancier gekoppeld met Basispoort, of maakt binnen het aanbod gebruik van een met Basispoort gekoppeld platform.
- 10.9 De opdrachtgever kan het toevoegen en verwijderen van in het portaal ontsloten applicaties en hyperlinks en het toekennen van rechten daarop zelfstandig uitvoeren, zonder tussenkomst van opdrachtnemer. Opdrachtnemer draagt zorg voor de onderliggende koppelingen en ondersteunt bij het inrichten van een koppeling die niet zelfstandig tot stand te brengen is.
- 10.10 De leerkracht kan de schermen van de devices waarop zijn leerlingen werken bekijken, overnemen en blokkeren.
- 10.11 Opdrachtnemer biedt inzicht via een dashboard of rapportage in het gebruik van het portaal en de gekoppelde applicaties.
- 10.12 De omgeving is toegankelijk en bruikbaar voor leerlingen met een ondersteuningsbehoefte.

HOOFDSTUK 11 Identity en Access Management en koppelingen

- 11.1 Opdrachtnemer realiseert en onderhoudt de koppelingen met AFAS als personeelsadministratiesysteem en ParnasSys als leerlingadministratiesysteem.
- 11.2 Accounts voor medewerkers en leerlingen worden automatisch aangemaakt, gewijzigd en gedeactiveerd op basis van deze koppelingen. Groepsindelingen en klassenoverzichten volgen eveneens automatisch uit het leerlingadministratiesysteem en vergen geen handmatige verwerking door opdrachtnemer of school.
- 11.3 De accountlifecycle omvat instroom, doorstroom en uitstroom. Accounts van medewerkers worden geblokkeerd op de laatste dag van het dienstverband en verwijderd na zes maanden. Accounts van leerlingen worden geblokkeerd bij uitschrijving en verwijderd aan het einde van het daaropvolgende schooljaar. Postvak- en bestandsgegevens blijven gedurende de blokkeringsperiode beschikbaar voor de opdrachtgever.
- 11.4 Het onderhoud van alle koppelingen valt binnen de opdracht, ook wanneer wijzigingen aan de zijde van een derde partij aanpassingen vergen.
- 11.5 Waar beschikbaar worden open en in het onderwijs gangbare koppelvlakken en standaarden toegepast, waaronder ECK iD en Basispoort.
- 11.6 Opdrachtnemer richt een IAM-oplossing in die accounts, autorisaties en groepslidmaatschappen geautomatiseerd afleidt uit de bronadministraties.
- 11.7 Mutaties in de bronsystemen — in-, door- en uitstroom van leerlingen en medewerkers — worden binnen 24 uur verwerkt in alle gekoppelde systemen, waaronder Microsoft 365 en de DLWO.
- 11.8 Medewerkers die uit dienst zijn gemeld, worden automatisch geblokkeerd in alle gekoppelde systemen.
- 11.9 Opdrachtnemer levert een beheerdersrol waarmee een ICT-coördinator op schoolniveau een beperkte set beheertaken zelf kan uitvoeren, zoals het resetten van wachtwoorden, met heldere afspraken over de rolverdeling.
- 11.10 Toegang tot systemen en data is geregeld volgens het principe van least privilege en wordt ten minste jaarlijks gecontroleerd.
- 11.11 Mutaties in accounts werken door in de printoplossing, zodat medewerkers en leerlingen die in- of uitstromen daar niet handmatig hoeven te worden aangemaakt of verwijderd.

- 11.12 Opdrachtnemer ondersteunt een eventuele migratie van het personeels- of leerlingadministratiesysteem gedurende de looptijd, zonder dat daarvoor een nieuwe opdracht nodig is.

HOOFDSTUK 12 Informatiebeveiliging en privacy

- 12.1 Opdrachtnemer beschermt de omgeving tegen onbevoegde toegang, bescherming van de devices is geregeld in 6.2.
- 12.2 Twefactorauthenticatie is verplicht voor alle beheeraccounts en voor accounts van medewerkers.
- 12.3 Opdrachtnemer monitort proactief op privacy-incidenten en datalekken en meldt deze onverwijld, doch uiterlijk binnen 24 uur na constatering, aan de opdrachtgever.
- 12.4 Opdrachtnemer verleent volledige medewerking aan externe securitytests, waaronder penetratietesten in opdracht van de opdrachtgever.
- 12.5 Opdrachtnemer geeft inzicht in de naleving van het Normenkader IBP funderend onderwijs voor de onderdelen die binnen deze opdracht vallen, door ten minste jaarlijks een overzicht te leveren waarin per relevante maatregel is aangegeven hoe daaraan invulling wordt gegeven, welke afwijkingen bestaan en welke maatregelen worden voorgesteld. Dit overzicht wordt besproken in het kwartaalgesprek volgens eis 14.2.
- 12.6 Opdrachtnemer sluit een verwerkersovereenkomst met de opdrachtgever volgens het privacyconvenant onderwijs, model verwerkersovereenkomst 4.0.
- 12.7 Alle data blijft eigendom van de opdrachtgever. Opslag en verwerking vinden plaats binnen de Europese Unie.
- 12.8 Toegang van beheerders tot systemen en data is geregistreerd, herleidbaar en beperkt tot wat noodzakelijk is voor de uitvoering van de opdracht.

HOOFDSTUK 13 Asset- en configuratieregistratie

- 13.1 Opdrachtnemer stelt een CMDB-omgeving beschikbaar. Deze CMDB ondersteunt ten minste de velden soort, merk, model of type, serienummer, locatie, aanschafdatum, aanschafwaarde, garantietype en garantieduur, supporttermijn en afschrijvingstermijn. Opdrachtnemer beschrijft en hanteert een werkwijze voor opname van nieuwe devices in de respectievelijke beheeromgevingen, zoals Intune en Google Admin, en voor registratie van devices in de CMDB. Bij herinstallatie van een device worden de aanwezige CMDB-gegevens van dat device niet overschreven maar hergebruikt.
- 13.2 Opdrachtnemer neemt de netwerkcomponenten die onder deze opdracht worden beheerd op in de CMDB en houdt deze registratie actueel. Het betreft ten minste switches en firewalls, en accesspoints voor zover deze binnen het contract worden geleverd.
- 13.3 Softwaretitels die op devices worden geïnstalleerd of als dienst worden afgenomen, worden in de CMDB geregistreerd met ten minste de naam, de leverancier, de licentievorm, het aantal licenties, de ingangs- en einddatum en de locaties of gebruikersgroepen waarvoor deze gelden. Applicaties die uitsluitend als hyperlink via de leer- en werkomgeving worden ontsloten, vallen hierbuiten.
- 13.4 De opdrachtgever heeft doorlopend inzage in de registratie en kan deze op elk moment exporteren in een open, machineleesbaar formaat.
- 13.5 Bij beëindiging van de overeenkomst worden de gegevens uit de registratie overgedragen in een open, machineleesbaar formaat volgens hoofdstuk 17. De opdrachtgever is daarbij niet gebonden aan voortzetting van het door opdrachtnemer gebruikte systeem.

HOOFDSTUK 14 Rapportage en overleg

- 14.1 Een concept-DAP en een concept-SLA worden meegeleverd met de inschrijving. De opdrachtgever schrijft de minimale servicelevels voor in het PvE. De inschrijver werkt deze zelf uit in een concept-SLA en levert die bij zijn inschrijving aan.
- 14.2 De DAP legt de overlegcyclus vast en bevat ten minste een operationeel overleg per maand, een kwartaalgesprek waarin opdrachtnemer met de opdrachtgever de SLA-rapportage bespreekt en van daaruit advies uitbrengt over eventueel te nemen maatregelen, en een jaarlijks leveranciersevaluatiegesprek.
- 14.3 De kwartaalrapportage bevat ten minste: gerealiseerde servicelevels, de normen uit de eisen 3.5 en 3.6, incidentoverzicht en trends, doorgevoerde wijzigingen, beveiligingsbevindingen en openstaande risico's.
- 14.4 Technische documentatie wordt continu actueel gehouden door opdrachtnemer en de laatste versie wordt actief gedeeld met de opdrachtgever.
- 14.5 De opdrachtgever heeft toegang tot dashboards en logboeken van de omgeving.

HOOFDSTUK 15 Training en adoptie

- 15.1 Opdrachtnemer verzorgt een verdiepingstraining voor de ICT-medewerkers van de opdrachtgever.
- 15.2 Per school wordt een instructie van maximaal drie uur verzorgd.
- 15.3 Halfjaarlijks wordt een training aangeboden voor nieuwe medewerkers.
- 15.4 Nederlandstalige handleidingen en instructievideo's zijn beschikbaar en worden actueel gehouden.

HOOFDSTUK 16 Implementatie en migratie

- 16.1 Het migratieplan wordt gezamenlijk met de opdrachtgever opgesteld. Opdrachtnemer start met de werkzaamheden na goedkeuring van de planning door de opdrachtgever.
- 16.2 Het onderwijs ondervindt zo min mogelijk hinder van de werkzaamheden. Werkzaamheden met impact op de beschikbaarheid worden vooraf met de betreffende school afgestemd.
- 16.3 De uitrol over de schoollocaties vindt plaats vanaf de voorjaarsvakantie. Oplevering vindt plaats uiterlijk op 28 mei 2027.
- 16.4 Met oplevering wordt bedoeld dat de nieuwe omgeving actief is, de oude omgeving buiten gebruik is gesteld en de omgeving door opdrachtnemer in beheer is genomen.
- 16.5 Voorafgaand aan de brede uitrol wordt een proof of concept uitgevoerd op één school, met een evaluatiemoment waarna de opdrachtgever besluit over voortzetting.
- 16.6 Per locatie vindt een acceptatietest plaats op basis van vooraf vastgestelde acceptatiecriteria. Oplevering van een locatie geldt pas na schriftelijke acceptatie door de opdrachtgever.
- 16.7 Opdrachtnemer voert een inventarisatie uit van de bestaande omgeving en neemt de documentatie over van de huidige beheerder. De opdrachtgever draagt zorg voor de contractuele medewerking van de huidige leverancier.
- 16.8 Tijdens de werkzaamheden worden de patchkasten opgeschoond en worden niet meer in gebruik zijnde verbindingen en apparatuur geïdentificeerd en gerapporteerd.
- 16.9 Opdrachtnemer draagt zorg voor projectmanagement waarin ten minste periodiek projectinhoudelijk voortgangsoverleg en begeleiding plaatsvindt.

HOOFDSTUK 17 Exit en overdracht

- 17.1 Opdrachtgever ontvangt bij een migratie naar een nieuwe leverancier alle noodzakelijke medewerking, waaronder toegang tot de configuraties van de componenten, de eventueel openstaande wijzigingen en de meest recente documentatie.
- 17.2 Kosten die betrekking hebben op de migratie naar een nieuwe leverancier worden vooraf inzichtelijk gemaakt.
- 17.3 Binnen drie maanden na aanvang van de overeenkomst levert opdrachtnemer een exitplan op, dat jaarlijks wordt geactualiseerd.
- 17.4 Alle data en registraties worden bij beëindiging aangeleverd in een open, machineleesbaar formaat.
- 17.5 De medewerking omvat beheertoegang tot alle gebruikte platformen, waaronder de Microsoft 365-omgeving.

HOOFDSTUK 18 Duurzaamheid en MVO

- 18.1 De aangeboden apparatuur is energiezuinig en heeft een aantoonbaar lange levensduur.
- 18.2 Opdrachtnemer neemt vrijkomende apparatuur in en verwerkt deze circulair, zowel bij de initiële vervanging als bij een latere vervangingsronde. Van de verwerking wordt een verklaring verstrekt.
- 18.3 Opdrachtnemer beperkt het aantal transportbewegingen bij levering, onderhoud en inname zoveel mogelijk, onder meer door werkzaamheden per locatie te bundelen.
- 18.4 Opdrachtnemer beschikt over een MVO-beleid en geeft invulling aan sociale duurzaamheid.
- 18.5 Opdrachtnemer conformeert zich aan de milieudoelstellingen van maatschappelijk verantwoord inkopen (MVI) bij de aangeboden oplossing.

HOOFDSTUK 19 Prijzen, facturatie en indexering

- 19.1 Alle gegeven en genoemde prijzen zijn exclusief btw.
- 19.2 De prijsstelling bestaat uit een eenmalige aanschaf van de netwerkcomponenten, eenmalige implementatiekosten en een beheer- en onderhoudsbedrag per school, dat per kwartaal vooraf wordt gefactureerd. De kosten voor de migratie van het bestuurskantoor (TWijs Services, 46 werkplekken) worden volledig verdisconteerd in de eenmalige migratie- en implementatiekosten van de 34 schoollocaties en mogen niet afzonderlijk worden gefactureerd. Uitsluitend de levering van de firewall en eventueel benodigde switches voor het bestuurskantoor wordt afzonderlijk gespecificeerd en geprijsd in het prijzenblad. De installatie en configuratie van deze componenten vallen onder de hiervoor bedoelde migratie- en implementatiekosten.
- 19.3 De beheervergoeding voor een school gaat in na schriftelijke acceptatie van die school volgens eis 16.6.
- 19.4 De opdrachtnemer heeft het recht de tarieven naar boven of beneden aan te passen tot een maximum volgens de CBS-index dienstenprijzen (DPI), jaarlijks op 1 januari met ingang van 2028. De basis hiervoor vormt de daling of stijging van het DPI-indexcijfer over twaalf maanden voorafgaand aan de maand oktober van het afgelopen jaar. De indexering valt onder de categorie Dienstenprijzen; commerciële dienstverlening en transport.
- 19.5 Aanpassingen van de prijzen worden met voldoende onderbouwing schriftelijk twee maanden voor ingang van de indexering kenbaar gemaakt aan de opdrachtgever.
- 19.6 Opdrachtgever heeft binnen het contract de mogelijkheid om per jaar het aantal locaties met maximaal twee aan te passen. De beheerkosten worden dienovereenkomstig bijgesteld.

- 19.7 Vervanging of levering van netwerkcomponenten gedurende de looptijd, voortvloeiend uit de eisen 7.30 of 8.10, vindt plaats tegen de dan geldende en te verifiëren netto inkoopprijs vermeerderd met het in het prijzenblad opgegeven opslagpercentage. Dit percentage staat gedurende de gehele looptijd vast en wordt in het prijzenblad op één plaats opgegeven.
- 19.8 Aanvullende dienstverlening buiten de overeengekomen scope wordt afgerekend tegen de in het prijzenblad opgegeven uurtarieven per rol.

Bijlage 1 Prioritering en servicelevels

Prioriteitsbepaling op basis van impact en urgentie:

Impact ↓ / Urgentie →	Volledig onmogelijk om te werken; directe verstoring van onderwijs of veiligheid	Mogelijk om te werken, met verminderde functionaliteit	Mogelijk om te werken, met de meeste functionaliteit
Eén of meerdere locaties	Prio 1	Prio 2	Prio 3
Eén of meerdere groepen	Prio 2	Prio 3	Prio 4
Individu	Prio 3	Prio 4	Prio 4

Reactie- en oplostijden:

Classificatie	Reactietijd	Oplostijd remote	Oplostijd on-site	KPI oplostijd
Prio 1	30 minuten	6 uur	8 uur	> 98%
Prio 2	1 uur	9 uur	11 uur	> 95%
Prio 3	4 uur	24 uur	32 uur	> 90%
Prio 4	9 uur	32 uur	40 uur	> 90%