Bijlage 5 - Programma van Eisen

Netwerk & beheer met kenmerk TN550801

Versie:	1.0 1.1 (aangepast n.a.v. NvI ronde 1) 1.2 (aangepast n.a.v. NvI ronde 2)
Perceel:	Basis
TLP:	**GREEN:** openbaar inzichtelijk, maar alleen te gebruiken binnen het kader van deelname aan de aanbesteding.

1 Eisen – Algemeen

1.1 Algemeen

SIVON wenst namens haar leden Netwerk & beheer uit te vragen. Onder Netwerk & beheer vallen 3 hoofdcomponenten: WLAN/LAN/Gateway of Firewall. Binnen deze dienst ligt de verantwoordelijkheid voor een correcte werking van de dienst gedurende de volledige contractperiode volledig bij de opdrachtnemer.

1.2 Algemeen - defectafhandeling

Indien een hardwarecomponent defect raakt zonder toedoen van afnemer, draagt de opdrachtnemer zorg voor afhandeling van garantie en herstel via de fabrikant. De kosten voor vervanging buiten fabrieksgarantie of bij defect door toedoen van de afnemer zijn voor rekening van de afnemer.

1.3 Algemeen – landelijke dekking

De opdrachtnemer dient de dienstverlening landelijk te kunnen aanbieden. Dit houdt in dat de opdrachtnemer de gevraagde Netwerk & beheer-diensten kan implementeren bij schoollocaties in alle regio's van Nederland, ongeacht provincie of gemeentelijke indeling.

1.4 Algemeen – dataopslag

De opdrachtnemer beschikt over formele en aantoonbare procedures voor dataopslag, archivering en bewaartermijnen in overeenstemming met wet- en regelgeving.

1.5 Algemeen – beveiliging en monitoring

De opdrachtnemer voert periodiek (jaarlijks) penetratietests en beveiligingstesten uit op de componenten van de dienst. De opdrachtnemer richt voor alle relevante componenten binnen haar dienstverlening passende logging- en monitoringsmaatregelen in. Deze maatregelen detecteren ongebruikelijke activiteiten, prestatieproblemen en beveiligingsrelevante gebeurtenissen binnen de Netwerk & beheer-dienst. De opdrachtnemer bewaakt deze signalen binnen het afgesproken supportvenster en volgt dit op. ~~Tevens zijn logging- en monitoringsmaatregelen ingericht ter detectie van ongebruikelijke activiteiten met rapportage van opvolging.~~

1.6 Algemeen – Normenkader IBP-FO

De opdrachtnemer toont aan dat de dienstverlening aansluit op het Normenkader Informatiebeveiliging PO/VO (IBP-FO) die relevant zijn voor Netwerk & beheer op tenminste volwassenheidsniveau 3. Ingeval het volwassenheidsniveau lager is dan 3 toont de opdrachtnemer aan hoe hij zich ontwikkelt naar het minimale volwassenheidsniveau 3.

De opdrachtnemer levert op verzoek van opdrachtgever een onderbouwing waaruit blijkt op welke wijze de aangeboden dienstverlening bijdraagt aan de invulling van de beheersmaatregelen uit het Normenkader. De opdrachtnemer stelt hierbij relevante documentatie, verklaringen of mappings beschikbaar.

Opdrachtgever behoudt zich het recht voor om de naleving van het Normenkader te toetsen, waarbij de opdrachtnemer volledige en tijdige medewerking verleent.

1.7 Algemeen – maatschappelijk verantwoord en duurzaam ondernemen

De opdrachtnemer heeft een inspanningsplicht op het gebied van maatschappelijk verantwoord en duurzaam ondernemen. Inschrijvingen (zowel in de aanbesteding als in minicompetities) waarin dit wordt benadrukt, kunnen hoger worden beoordeeld. Gedurende het contract geldt in elk geval:

- Circulariteit: De opdrachtnemer vergroot de circulariteit van apparatuur, waarbij de R-ladder als richtlijn kan dienen. Een hogere R-score leidt tot een hogere waardering.
- Levensduur: De opdrachtnemer draagt bij aan het verlengen van de levensduur van componenten (langer dan de initiële looptijd van vijf jaar), door advies en mogelijk implementatie van maatregelen. Dit kan ook door overleg met vendoren en het combineren van langere levensduur met licentiemodellen.
- Energieverbruik: De opdrachtnemer zet zich in voor vermindering van energieverbruik, onder andere door bewuste ontwerpkeuzes.

Daarnaast kan aandacht worden besteed aan thema’s zoals ketenverantwoordelijkheid (goede arbeidsvoorwaarden, ook bij productie), diversiteit en inclusie, social return en toegankelijkheid van portalen (bijv. voor doven en slechthorenden). Ook deelname van studenten en mensen met afstand tot de arbeidsmarkt kan hier deel van uitmaken.

Op verzoek rapporteert de opdrachtnemer aan opdrachtgever over de effecten van de genomen duurzaamheidsmaatregelen gedurende de raamovereenkomst en nadere overeenkomsten.

1.8 Algemeen – partnerschap en samenwerking

De opdrachtnemer draagt actief bij aan een goed partnerschap met opdrachtgever. Hieronder kan bijvoorbeeld worden verstaan:

- Proactieve communicatie en transparantie over o.a. ontwikkelingen, risico’s en kansen, marktontwikkelingen, etc.;
- Samenwerking en afstemming middels tactische en operationele overleggen om de dienstverlening blijvend te onderhouden en ontwikkelen;
- Marketinguitingen- en activiteiten waarin opdrachtgever en opdrachtnemer samen optrekken;
- Flexibiliteit en betrouwbaarheid: meebewegen bij veranderende behoeften van scholen of van opdrachtgever, maar ook voorspelbare dienstverlening.

2 Eisen – Functioneel en technisch - Standaard

De dienst voorziet in een stabiele, veilige en beheersbare netwerkvoorziening die de komende jaren voldoet aan de behoeften van het primair onderwijs. De opdrachtnemer is verantwoordelijk voor inventarisatie, ontwerp, levering, beheerbaarheid en correcte werking van de infrastructuur. Technische keuzes worden afgestemd op doelmatig gebruik en beheer. Alle onderstaande paragrafen hebben betrekking op het functioneel en technische standaardaanbod van de Netwerk & beheer dienstverlening. Het standaardaanbod geldt altijd als minimale basis.

2.1 Algemene randvoorwaarden – verantwoordelijkheid en inventarisatie

De opdrachtnemer is verantwoordelijk voor een volledige inventarisatie van de bestaande situatie bij aanvang van de dienstverlening. Deze inventarisatie vormt de basis voor een correcte aansluiting, configuratie en werking van de gehele Netwerk & Beheer-dienst (WLAN, LAN en gateway/firewall). De inventarisatie heeft als doel:

- inzicht te verschaffen in de huidige infrastructuur en voorzieningen;
- benodigde capaciteit, prestaties en randvoorwaarden te bepalen;
- mogelijke knelpunten, afhankelijkheden en randvoorwaarden in kaart te brengen;
- de continuïteit en correcte werking van bestaande diensten en apparatuur te waarborgen binnen de nieuwe omgeving.

De wijze waarop de inventarisatie wordt uitgevoerd, wordt door de opdrachtnemer bepaald en afgestemd met de afnemer. De opdrachtnemer legt de resultaten vast en stemt deze af met de afnemer voordat implementatie en migratie plaatsvinden.

2.2 Algemene randvoorwaarden – naleving wet- en regelgeving

Alle onderdelen van de dienst (inclusief het ingestelde zendvermogen van de access points (ook i.c.m. eventueel gebruik van externe antennes) voldoet steeds ten tijde van aanbieden c.q. ingebruikname en gedurende de volledige looptijd van de overeenkomsten aan de geldende wet- en regelgeving in Nederland. Indien tijdens de looptijd gewijzigde wet- en regelgeving aanpassingen noodzakelijk maakt, zal de leverancier deze tijdig en zonder meerkosten doorvoeren, voor zover dit binnen de invloedssfeer van de leverancier ligt.

2.3 Algemene randvoorwaarden – apparaat ondersteuning en levensduur

Opdrachtnemer zet uitsluitend apparatuur in die op het moment van aanbieding en levering door de fabrikant actief wordt ondersteund en waarvoor geen einddatum van ondersteuning of vergelijkbare einddatum is aangekondigd. Dit uitgangspunt geldt voor alle apparatuur onder de Nadere overeenkomst, inclusief later geleverde apparatuur bij gefaseerde of langdurige implementaties.

De opdrachtnemer garandeert dat de ingezette apparatuur gedurende ten minste vijf (5) jaar na ingebruikname door de fabrikant wordt ondersteund. Het streven is dat apparatuur langer meegaat dan deze initiële looptijd en bij voorkeur gedurende de volledige looptijd van de Nadere overeenkomst (maximaal acht (8) jaar) inzetbaar blijft. De opdrachtnemer spant zich in om dit op een veilige en beheerste wijze mogelijk te maken, voor zover binnen zijn invloedsfeer.

Indien tijdens de optionele verlengingsperiode (tussen vijf (5) en acht (8) jaar na ingebruikname) blijkt dat ondersteuning of veilig beheer conform het Programma van Eisen niet langer mogelijk is, treedt de opdrachtnemer zo spoedig mogelijk in overleg met de opdrachtgever. Samen wordt gezocht naar een passende oplossing om de continuïteit en kwaliteit van de dienstverlening te waarborgen.

~~De opdrachtnemer zet uitsluitend apparatuur in die door de fabrikant wordt ondersteund voor ten minste de initiële looptijd van de nadere overeenkomst (5 jaar). De opdrachtnemer staat er daarnaast voor in dat de apparatuur gedurende de volledige looptijd van de nadere overeenkomst (max. 8 jaar) door hemzelf beheerd, ondersteund en onderhouden kan worden. Indien de fabrikant de ondersteuning beëindigt binnen deze periode, draagt de opdrachtnemer zorg voor gelijkwaardige ondersteuning, bijvoorbeeld door inzet van eigen beheer, patches of vervangende functionaliteit. Indien dat aantoonbaar niet meer mogelijk is, zal de opdrachtnemer ten minste op best effort basis ondersteuning kunnen blijven leveren, zonder additionele kosten voor afnemer.~~

2.4 Algemene randvoorwaarden – licenties, updates en upgrades

De opdrachtnemer draagt te alle tijden verantwoordelijkheid voor de beschikbaarheid van benodigde licenties, updates en upgrades gedurende tenminste de initiële looptijd van de dienstverlening op de locaties en, tenzij opdrachtnemer expliciet aantoont dat zij dit niet kan door externe factoren, ook gedurende de eventuele verlengingsperiode.

2.5 Algemene randvoorwaarden – demontage en recycling

De opdrachtnemer dient, indien door afnemer toestemming is gegeven, oude apparatuur standaard te demonteren en indien gewenst ook standaard af te voeren en te recyclen of te voorzien van een tweede leven. De opdrachtnemer dient verpakkingsmateriaal te scheiden in een milieustraat.

2.6 Algemene randvoorwaarden – migratie en samenwerking met derden

Bij ingebruikname van de dienst draagt de opdrachtnemer er zorg voor dat alle bestaande diensten en verbonden apparatuur die deel uitmaken van de huidige situatie volledig en correct functioneren binnen de nieuwe omgeving, voor zover dit binnen zijn directe invloedsfeer ligt. Voor instellingen of functionaliteiten die buiten zijn directe beheer of bevoegdheid vallen, zet de opdrachtnemer zich aantoonbaar actief in om, in samenwerking met de betrokken stakeholders, de noodzakelijke acties tijdig te faciliteren of te ondersteunen. Het (her)configureren of instellen van clientapparatuur (zoals laptops, tablets, pc's, printers en overige eindgebruikersapparatuur) valt nadrukkelijk buiten de scope van de dienstverlening.

Afnemer is verantwoordelijk voor het in contact brengen van de opdrachtnemer met deze stakeholders. Indien samenwerking met externe stakeholders stagneert, rust de primaire verantwoordelijkheid op afnemer, tenzij tussen afnemer en de opdrachtnemer expliciet is vastgelegd dat de regierol bij de opdrachtnemer ligt. De opdrachtnemer blijft echter verplicht zich aantoonbaar in te zetten om tot een werkbare samenwerking met de betreffende stakeholders te komen.

2.7 Algemene randvoorwaarden – netwerksegregatie en toegangscontrole

Het netwerk biedt gescheiden toegang per gebruikersgroep (zoals leerlingen, personeel, gasten, gebouwsystemen, derden die gebruik maken van het pand, zoals een buitenschoolse opvang of kinderdagverblijf) om veilig en beheersbaar gebruik mogelijk te maken.

Het beheer van deze segregatie moet overzichtelijk en centraal mogelijk zijn. De benodigde netwerksegregatie (zoals VLAN's) en toegangscontrole wordt zodanig ingericht dat deze aansluit op het beleid en de gebruikssituatie van de school. Tussen de VLAN's worden standaard toegangsbeperkingen toegepast, zodat verkeer alleen mogelijk is indien expliciet toegestaan.

2.8 Algemene randvoorwaarden – cloudcomponenten en beheerplatforms

Indien gebruik wordt gemaakt van cloudgebaseerde componenten of beheerplatforms binnen de netwerkoplossing geldt het volgende:

- Verwerking via de cloud mag uitsluitend betrekking hebben op verkeer naar en van het internet (internet-bound). Intern netwerkverkeer (lokaal LAN/WLAN) wordt lokaal afgehandeld, tenzij anders overeengekomen.
- Verwerking en opslag van gegevens vindt uitsluitend plaats binnen Europa.
- Tunnels tussen netwerk en cloudcomponenten zijn end-to-end sterk versleuteld.
- Toegang tot beheerportals vindt uitsluitend plaats via tweefactorauthenticatie (2FA). Het platform biedt logging van beheerdersacties en wijzigingen, met exportmogelijkheden voor audits.
- De opdrachtnemer waarborgt de beschikbaarheid van de dienst, inclusief maatregelen bij verstoring of uitval van de verbinding met de cloud.
- Indien filtering of DNS-diensten via de cloud verlopen, dient bij uitval van de tunnel een automatische fallback plaats te vinden naar een lokale oplossing. Indien dat niet mogelijk is, wordt het verkeer standaard geblokkeerd totdat de verbinding is hersteld.

2.9 Algemene randvoorwaarden – AI-modellen

Indien in de dienstverlening AI-technologie wordt toegepast (bijv. voor netwerkbeheer, incidentdetectie of capaciteitsanalyse), borgt opdrachtnemer dat deze technologie op een ~~aantoonbaar~~ veilige, betrouwbare en controleerbare ~~functioneert~~ wijze wordt ingezet.

- Voor AI-functionaliteit die door opdrachtnemer zelf wordt ontwikkeld en/of beheerd, richt opdrachtnemer een passend proces in voor periodieke beoordeling van nauwkeurigheid, prestaties en relevante risico's (zoals foutgevoeligheid of ongewenste bias) en voor het vooraf valideren van significante wijzigingen.
- Voor AI-functionaliteit die wordt geleverd door een derde partij(vendor) zet opdrachtnemer zich aantoonbaar in om (binnen haar invloedsfeer) gebruik te maken van beschikbare documentatie, testrapporten en controles van deze derde partij en waar nodig aanvullende maatregelen te treffen, zodat de inzet van deze AI-functionaliteit zoveel mogelijk voldoet aan de genoemde uitgangspunten.
- Op verzoek verstrekt opdrachtnemer aan opdrachtgever een toelichting op de gebruikte AI-functionaliteit, voor welk doeleinde deze wordt ingezet en welke bekende beperkingen of risico's daarbij gelden.

~~De opdrachtnemer:~~

- ~~Test periodiek (minimaal jaarlijks) de gebruikte AI-modellen op bias, nauwkeurigheid en prestatie, en legt de resultaten vast in een toetsingsrapport.~~
- ~~Documenteert de toegepaste testmethodiek en eventuele verbetermaatregelen, en stelt deze op verzoek beschikbaar aan opdrachtgever.~~
- ~~Test en valideert elke wijziging of update van AI-modellen voorafgaand aan ingebruikname.~~
- ~~Levert bewijs van naleving op verzoek van opdrachtgever of SIVON.~~

2.10 Algemene randvoorwaarden – gebruik van bestaande bekabeling

De opdrachtnemer gebruikt waar mogelijk bestaande bekabeling.

2.11 WLAN – profielen en prestaties

Het draadloze netwerk moet geschikt zijn voor moderne, interactieve en media-intensieve onderwijstoepassingen. Op basis van een door de afnemer aangeleverde plattegrond met profielen en aantallen gebruikers, ontwerpt de opdrachtnemer een oplossing die per profiel voldoende dekking en capaciteit biedt. Hierbij moeten applicaties zoals streaming video (1080p), videobellen en online educatieve platforms zonder merkbare vertraging, buffering of wegvallende verbindingen functioneren. Het ontwerp houdt rekening met roaming, automatische load balancing, interferentie en netwerkbelasting.

De volgende profielen worden als standaard genomen, maar hier kan van afgeweken worden.

Profiel	**Gebruik**
Klaslokaal	Gelijktijdig streamen van video, videobellen, cloudopslag en interactieve educatieve platforms door alle gebruikers in de ruimte.

Leerplein/aula	Grote verzamelruimte waar meerdere groepen gebruikers gelijktijdig actief zijn met streaming en educatieve platforms.
Verkeersruimte/gang	Continue in- en uitroamen van apparaten.
Speellokaal	Gebruik van lichte educatieve apps en streaming. Beperkte, maar stabiele capaciteit vereist.
Kantoor	Continue en gelijktijdig gebruik door gebruikers in de ruimte van administratieve systemen, streaming, cloudopslag, kantoortoepassingen en videobellen.
Derden	Ruimte voor bijvoorbeeld Buitenschoolse opvang (BSO) of kinderopvang (KDV). Gebruik van lichte apps en mogelijk streaming op een beperkt aantal apparaten. Belasting is gemiddeld. Stabiele verbinding nodig.

Dekking in toiletten, trappenhuizen, magazijnen/bergingen en outdoor wordt standaard niet geleverd, tenzij dit expliciet wordt gevraagd in de nadere offerteaanvraag.

2.12 WLAN – standaard

Het WLAN voldoet minimaal aan de Wi-Fi 6 (802.11ax)-standaard.

- zendt gelijktijdig uit op de 2,4 GHz- en 5 GHz-band;
- De ondersteuning van oudere clientprotocollen moet uitgeschakeld kunnen worden;
- De access points zijn backwards compatible met oudere Wi-Fi-standaarden.

Access points die op een hoogte tot en met 3 meter worden geïnstalleerd, vallen onder de standaard dienstverlening.

2.13 WLAN - schaalbaarheid

De wifi is schaalbaar en geschikt voor een inzet van ten minste 30 access points binnen één locatie, zonder functionele of prestatiebeperkingen.

2.14 WLAN - gastennetwerk

De wifi biedt de mogelijkheid om een gastnetwerk op te zetten waarbij gebruikers akkoord dienen te gaan met de voorwaarden die de school hieraan stelt. Daarnaast ondersteunt het gastnetwerk de mogelijkheid tot client isolation, zodat gebruikers op het gastennetwerk geen toegang hebben tot andere apparaten op hetzelfde netwerk.

2.15 LAN – capaciteit, prestaties ~~en PoE-voorziening~~

Het LAN-netwerk moet voldoende capaciteit en snelheid ~~en PoE-vermogen~~ bieden voor stabiel gebruik van de dienst op alle werkplekken, access points en andere aangesloten apparatuur. De opdrachtnemer borgt dat de interne netwerkstructuur geen knelpunten vormt bij gelijktijdig gebruik van de infrastructuur.

2.16 LAN - PoE

De switches ~~ondersteunen~~ dienen te alle tijden voldoende ~~de~~ stroomvoorziening te leveren om de volledige functionaliteit van de aangesloten apparatuur zoals access points, VoIP-telefoons en andere PoE-apparaten, ~~indien van toepassing.~~ te ondersteunen, zonder dat deze in een beperkte of low-power modus hoeven te functioneren

2.17 LAN - Verdeling

Access points worden waar mogelijk verdeeld over meerdere switches.

2.18 Gateway

Eén van de andere diensten van opdrachtgever is de dienst Veilig Internet. De dienst Veilig Internet kan op verschillende manieren worden aangesloten, bijvoorbeeld op een schoollocatie of via een datacenter. De dienst Veilig Internet wordt op de locatie gedemarqueerd met een Customer Premises Equipment (CPE). Middels deze CPE wordt er een verbinding opgezet naar het Nationaal diensten Centrum (NDC) waar de beveiliging wordt verzorgd en vervolgens het internet op wordt gegaan. Scholen die gebruik willen maken van Veilig Internet hebben zelf een routerend device (laag 3) nodig die aangesloten wordt op de CPE. We noemen dit een gateway. Opdrachtnemer dient een gateway te kunnen leveren die minimaal voldoet aan de volgende eisen:

- IP-routing op IPv4 en IPv6;
- Nat-translatie;
- VLAN segmentatie en aggregatie;
- Instellen van statische routes;
- Minimaal 2x 1Gbit UTP poort;
- Voldoende verwerkingscapaciteit die past bij de internetverbinding en het aantal actieve devices in het netwerk;
- Throughput van 1 Gbps.

2.19 Gateway/Firewall - inventarisatie

Opdrachtnemer inventariseert indien van toepassing bestaande firewallregels en eventuele VPN-tunnels en draagt zorg voor het correct overzetten hiervan naar de nieuwe situatie, voor zover dit binnen zijn directe invloedsfeer ligt. Afnemer zorgt ervoor dat opdrachtnemer ten behoeve van deze inventarisatie ten minste over alleen-lezen toegang tot de bestaande configuratie kan beschikken (bijvoorbeeld via een read-only account of een configuratie-export).

2.20 DNS

Standaard dient opdrachtnemer Domain Name System (DNS) af te handelen middels de geleverde gateway/firewall. Er kan hiervan worden afgeweken als afnemer een separate DNS-oplossing heeft draaien.

2.21 DHCP

De opdrachtnemer handelt Dynamic Host Configuration Protocol (DHCP) af via de geleverde gateway of firewall. Deze moet DHCP-services kunnen leveren aan netwerkclients, waaronder het toewijzen van IP-adressen, subnetmaskers, standaardgateways en DNS-serveradressen. Afwijkingen hiervan zijn mogelijk indien afnemer een eigen DHCP-oplossing gebruikt.

3 Eisen – Functioneel en technisch - Aanvullend

De aangeboden dienstverlening en productlijn van opdrachtnemer dienen geschikt te zijn om onderstaande aanvullende eisen te kunnen aanbieden indien hierom wordt gevraagd in een nadere offerteaanvraag. Onderstaande opsomming is indicatief en sluit andere toekomstige aanvullende eisen niet uit.

Niet alle componenten die in dit hoofdstuk worden genoemd, staan opgenomen in het Prijzenblad (Bijlage 8).

- Componenten die niet in het Prijzenblad zijn opgenomen: Deze kunnen later worden uitgevraagd in een nadere offerteaanvraag. Voor deze componenten gelden geen maximale tarieven.
- Componenten die wél in het Prijzenblad zijn opgenomen: Voor deze componenten geldt dat de opgegeven tarieven tijdens de looptijd van de overeenkomst als maximale tarieven moeten worden gehanteerd.

3.1 ~~Nieuwe~~ WLAN ~~standaarden~~

3.1.1 WLAN-standaarden

Naast de basisstandaard kan afnemer in een nadere offerteaanvraag vragen om:

- Wi-Fi 6E (802.11ax met 6 GHz-band);
- Wi-Fi 7 (802.11be);

Voor deze nieuwere standaarden gelden dezelfde kwaliteitseisen als voor Wi-Fi 6 en aanvullend geldt:

- De access points moeten gelijktijdig kunnen uitzenden op 2,4 GHz, 5 GHz en (voor Wi-Fi 6E/7) de 6 GHz-band.
    - access points die twee van deze drie banden gelijktijdig kunnen uitzenden zijn toegestaan, mits de leverancier motiveert dat deze configuratie voldoet aan de prestatie- en dekkingsbehoeften van afnemer en geen afbreuk doet aan de continuïteit en veiligheid van het netwerk.

3.1.2 Bluetooth/Zigbee

Naast de WLAN-standaarden kan afnemer in een nadere offerteaanvraag vragen om access points met geïntegreerde ondersteuning voor Bluetooth (bij voorkeur BLE) en/of Zigbee. Hiervoor geldt:

- De Bluetooth- en Zigbee-radio's zijn geïntegreerd in het access point. Er zijn geen aparte gateways en/of extra bekabeling benodigd.
- Verkeer van Bluetooth- en Zigbee-apparatuur kan worden ondergebracht in passende, logisch gescheiden netwerksegmenten (bijvoorbeeld een IoT-/gebouwbeheernetwerk).

3.1.3 Plaatsing access points op hoogte

Access points die op een hoogte van meer dan 3 meter moeten worden geïnstalleerd. De extra kosten en benodigde voorbereiding worden voor deze installatie apart geoffreerd in de nadere offerteaanvraag of in de offerte naar aanleiding van de inventarisatie.

3.2 Bekabeling

Indien nieuwe bekabeling vereist is (bijv. voor switches of access points), wordt deze aangelegd conform benodigde en toekomstig verwachtte prestatie-eisen.

3.3 LAN

Als aanvullende dienst kan afnemer één of meerdere van onderstaande eisen in de nadere offerteaanvraag opnemen:

- Opschonen en labelen van patchkasten.
- Inventariseren en documenteren van actieve poorten, patchkabels en verbindingen.

3.4 BYOD

Indien afnemer BYOD toepast, dient het geleverde netwerk veilig gebruik van persoonlijke apparaten (zoals laptops, tablets en smartphones) te ondersteunen. Scholen die beperkt of geen BYOD gebruiken, kunnen volstaan met het gastennetwerk zoals beschreven in het standaardaanbod.

3.5 Toegangsbeheer en traceerbaarheid

De netwerkoplossing ondersteunt standaard toewijzing van toegangsrechten op basis van centraal beheerde gebruikersrollen uit een directory (bijv. Microsoft 365, Google Workspace of vergelijkbaar). De oplossing zorgt ervoor dat:

- identificatie, authenticatie en autorisatie van gebruikers altijd worden afgedwongen;
- alle gebruikersactiviteiten traceerbaar zijn tot unieke gebruikers;
- functiescheiding en autorisatiematrix van afnemer technisch kunnen worden afgedwongen;
- rapportages/exports beschikbaar zijn waarmee de feitelijke toegangsrechten (IST) periodiek door afnemer vergeleken kunnen worden met de vastgestelde SOLL-matrix die afnemer in haar eigen autorisatiebeleid heeft opgenomen.
- toekenning, wijziging en intrekking van netwerktoegang verlopen via de centrale identity-provider van afnemer (bijv. Microsoft Entra ID, Google Workspace of vergelijkbaar), waarbij intrekking van rechten automatisch plaatsvindt op basis van wijzigingen in de directoryrollen.

De leverancier draagt er zorg voor dat ook apparaten zonder standaardondersteuning voor gebruikersauthenticatie op passende wijze veilig en traceerbaar toegang krijgen.

3.6 Basisfirewall

U dient een basisfirewall te kunnen leveren met de volgende functionaliteiten:

- De firewall moet ~~in staat zijn om~~ de minimaal de huidige verwachte maximale bandbreedte van de internetaansluiting van de locatie op volle capaciteit ~~te~~ kunnen verwerken inclusief NAT en VPN en daarnaast ten minste 30% extra verwerkingscapaciteit bieden voor toekomstige groei in bandbreedte en gebruik.
- De firewall moet voldoende sessiecapaciteit leveren voor het volledige aantal gebruikers, inclusief gelijktijdig gebruik van video, streaming en cloudapplicaties.
- De firewall moet ~~in staat zijn~~ specifieke websites of domeinen ~~te~~ blokkeren of toe ~~te~~ staan op basis van beheerde lijsten (URL-filtering).
- Pakketfiltering: de firewall moet ~~in staat zijn om~~ netwerkverkeer kunnen ~~te~~ inspecteren op basis van IP-adressen, poorten, protocollen en mogelijk andere criteria. Het moet regels kunnen toepassen om te bepalen of pakketten al dan niet worden doorgelaten.
- Stateful inspection: de firewall moet de staat van verbindingen kunnen bijhouden en alleen inkomend verkeer toestaan dat betrekking heeft op geautoriseerde uitgaande verbindingen.
- Network Address Translation (NAT): De firewall dient IP-adressen en poortnummers van pakketten te kunnen wijzigen wanneer deze tussen het interne en externe netwerk worden doorgegeven. Dit kan helpen bij het verbergen van interne IP-adressen en het beheren van de toegang tot interne bronnen vanaf externe netwerken.
- Toegangscontrolelijsten (ACL’s): de firewall moet ~~in staat zijn~~ ACL’s ~~te~~ kunnen beheren van het inkomende en uitgaande verkeer op basis van bron- en bestemmingsadressen, poorten en protocollen.
- VPN-ondersteuning: De firewall moet Virtual Private Network (VPN) tunnels kunnen opzetten en beheren voor beveiligde externe toegang tot het netwerk.
- Beheer en configuratie: De firewall moet een intuïtieve gebruikersinterface en centraal beheerplatform hebben voor eenvoudige configuratie, monitoring en onderhoud van de firewall en het netwerk. afnemer dient leesrechten te krijgen voor de firewall indien gewenst.
- De firewall wordt inclusief rackmount geleverd.

3.7 Firewall

U dient een geavanceerde firewall te kunnen leveren met de basisfunctionaliteiten zoals hierboven geschreven en met één of meerdere onderstaande functionaliteiten, zoals in nadere offerteaanvraag zal worden gespecificeerd:

- Applicatie-laag filtering: De firewall moet op applicatieniveau kunnen inspecteren, waardoor het mogelijk is om specifiek verkeer te blokkeren op basis van applicatieprotocollen (bijv. HTTP, FTP, SMTP).
- Content filtering: De firewall moet ~~in staat zijn om~~ webinhoud kunnen ~~te~~ filteren en blokkeren op basis van vooraf gedefinieerde categorieën en beleidsregels.
- Web filtering: De firewall moet de toegang tot websites kunnen beheren op basis van URL-categorieën, content en reputatie.
- Intrusion Prevention System (IPS): De firewall moet ~~in staat zijn om~~ verdacht verkeer kunnen ~~te~~ detecteren en ~~te~~ blokkeren dat mogelijk wijst op een aanval, zoals poging tot inbraak, malware of andere kwaadaardige activiteiten.
- Usertracking, Logging en rapportage: De firewall dient uitgebreide logging en rapportagemogelijkheden te hebben om netwerkactiviteit te volgen, beveiligingsgebeurtenissen te analyseren en nalevingsvereisten te ondersteunen. In sommige gevallen kan dit op gebruikersniveau worden uitgevraagd (usertracking). Daarbij kan gewenst zijn wie welk internet adres wanneer heeft bezocht en vanaf welk device.
- Netwerksegmentatie en VLAN's: De firewall dient ~~de mogelijkheid te hebben om~~ het netwerk op te kunnen delen in logische segmenten met behulp van VLAN's en andere segmentatietechnieken om de beveiliging te verbeteren en het verkeer te isoleren.
- Beheer en configuratie: De firewall moet optioneel kunnen beschikken over een aparte appliance (speciaal (virtueel of fysiek) systeem) voor log- en beveiligingsinformatieanalyse. Daarnaast dient het een centraal beheerplatform te hebben, waarin gecentraliseerd de configuratie, monitoring, rapportage en beleidsbeheer wordt afgevangen.

3.8 Regierol

In de Nadere offerteaanvraag of na gunning (meerwerk) kan afnemer de opdrachtnemer vragen een regierol op zich te nemen gedurende de implementatie. Dit houdt in dat hij regie over externe partijen op zich neemt en uitgebreide ondersteuning biedt buiten zijn directe invloedsfeer.

3.9 Tijdelijk in beheer nemen

Sommige scholen hebben de behoefte om (een deel van) hun netwerk tijdelijk in beheer te laten nemen. Het doel hiervan is het borgen van de continuïteit van de dienstverlening, met één verantwoordelijke partij voor het beheer van het gehele netwerk, ook wanneer op sommige locaties nog recente netwerkapparatuur aanwezig is die nog niet vervangen hoeft te worden.

Indien afnemer hiervoor kiest, kan de opdrachtnemer bestaande netwerkcomponenten (zoals access points, switches of gateways/firewalls) tijdelijk beheren op tenminste best effort-basis en bij voorkeur op basis van de SLA, mits afnemer aan de onderstaande voorwaarden voldoet:

- De apparatuur is eigendom van afnemer, of het bestuur is aantoonbaar bevoegd deze door een andere partij in beheer te laten nemen;
- De apparatuur maakt deel uit van een productlijn die centraal beheer en monitoring ondersteunt.
- De apparatuur is en wordt nog ondersteund door de fabrikant (lifecycle support, inclusief beveiligings- en firmware-updates) gedurende de tijdelijke beheer-periode;
- De apparatuur beschikt (i.v.t.) over een geldige beheer- of Cloudlicentie, óf een dergelijke licentie kan nog worden aangeschaft;

De opdrachtnemer beoordeelt tijdens de inventarisatiefase of deze voorwaarden zijn vervuld. Mocht dit niet het geval zijn, wordt in overleg afgestemd over een passende oplossing.

De opdrachtnemer is hierbij niet verantwoordelijk voor prestatiebeperkingen of storingen die direct voortkomen uit de beperkingen van de bestaande apparatuur, tenzij hierover andere afspraken zijn gemaakt in de nadere offerteaanvraag.

3.10 Aanvullende SLA-eisen

De in hoofdstuk 5 beschreven SLA geldt als minimumniveau. Afnemer kan per Nadere Offerteaanvraag aanvullingen of aanscherpingen uitvragen. Onderstaande is illustratief en niet limitatief:

- Uitbreiding in supportvenster en bereikbaarheid;
- Verscherpte respons- en oplostijden;
- Hogere beschikbaarheidseisen (bijv. in combinatie met redundantie);
- Meer of frequentere rapportages en/of evaluaties.

4 Eisen aan de organisatie en het beheer van de dienst

4.1 Projectorganisatie en communicatie tijdens implementatie

De opdrachtnemer dient per gegunde offerteaanvraag een vaste projectorganisatie te formeren voor de inrichting van de dienst met de volgende eisen:

- Een vast aanspreekpunt per schoolbestuur (en schoollocatie) die verantwoordelijk is voor de voortgang, afstemming en terugkoppeling tenminste gedurende de voorbereiding en implementatie (tot overgang naar beheer);
- Tenminste een tweewekelijkse voortgangsoverleg met afnemer inclusief voortgangsrapportage;
- Gebruik van een gedeelde online omgeving waarin de actuele status en planning inzichtelijk zijn evenals de offertes voor de locaties worden gedeeld en opgeslagen.

4.2 Test- en acceptatieprocedure

Voorafgaand aan iedere oplevering voert de opdrachtnemer, in afstemming met afnemer, een test- en acceptatieprocedure uit om aan te tonen dat de functionaliteit, prestaties en kwaliteit van de dienstverlening voldoen aan de overeengekomen eisen. Het test- en acceptatieprocedure omvat minimaal:

- Het opstellen en ter akkoord voorleggen van een testplan waarin wordt beschreven: de testrondes, testgevallen, beoogde resultaten, gebruikte testmethodiek, rollen/ verantwoordelijkheden en planning;
- Het uitvoeren van de overeengekomen testen door de opdrachtnemer (en waar van toepassing afnemer) met gebruik van representatieve data en omstandigheden;
- Het vastleggen van testresultaten in een testrapport, inclusief geconstateerde afwijkingen, analyse en herstelacties;
- In geval van gebreken worden deze binnen redelijk termijn worden verholpen en opnieuw getest;
- Een (her)testslaag na uitvoering herstelacties;
- Formele acceptatie door afnemer.

4.3 Aanvullende bepalingen test- en acceptatieprocedure

- Wordt de dienstverlening bij de tweede acceptatie opnieuw afgekeurd, dan kan opdrachtgever de nadere overeenkomst geheel of gedeeltelijk ontbinden, herstel verlangen of voorwaardelijk accepteren met herstelverplichting.
- Gebreken die het productief gebruik niet verhinderen, zijn geen grond voor weigering van acceptatie, maar moeten door opdrachtnemer worden hersteld. Voor structurele of kritieke gebreken kan in overleg een tijdelijke oplossing worden toegepast.
- Bij deelleveringen vindt acceptatie per deel én een integrale eindacceptatie plaats.

4.4 Opleverrapport

Nadat de test- en acceptatieprocedure is uitgevoerd kan over worden gegaan op oplevering. Bij oplevering wordt per locatie een opleverrapport verstrekt met daarin tenminste:

- Geleverde hardware (aantallen, types, specificaties);

- Aftersurvey met dekking/capaciteitseisen op 2.4/5 Ghz (en optioneel 6 GHz), inclusief bandbreedtemeting;
- Eventuele restpunten, gebreken en adviezen;
    - In geval van restpunten of gebreken binnen de eigen invloedsfeer en dienst van de opdrachtnemer zal een redelijk termijn worden afgestemd waarin de opdrachtnemer deze gebreken verhelpt. Er zal, indien van toepassing, een nieuwe aftersurvey en/of testverslag kosteloos worden opgesteld om aan te tonen dat de betreffende restpunten of gebreken zijn verholpen.
- Ingangsdatum van dienstverlening en facturatie;
- Acceptatie van afnemer.
- Oplevering inclusief akkoord aanleveren per mail aan opdrachtgever.

Opdrachtnemer levert binnen één maand na uitvoering van de acceptatieprocedure per locatie het opleverrapport. Het rapport wordt digitaal beschikbaar gesteld aan afnemer en opdrachtgever in de samenwerkingsomgeving en beide partijen worden hiervan op de hoogte gebracht. Na aanlevering van het opleverrapport beoordeelt afnemer deze binnen twee weken (uitgezonderd schoolvakanties) en maakt bekend of het rapport wordt geaccepteerd. Bij uitblijven van een reactie van afnemer geldt het rapport als geaccepteerd.

4.5 Nazorg en overdracht

Na oplevering van de dienst (per locatie) voorziet de opdrachtnemer in een nazorgperiode van ten minste twee weken. In deze periode:

- Worden eventuele restpunten kosteloos verholpen (tenzij restpunten buiten scope zijn, bijv. bekabelingswerkzaamheden die bij de gemeente of andere bekabelaar zijn belegd);
- Is de opdrachtnemer beschikbaar voor ondersteuning bij eventuele gebruiksvragen van het schoolteam;
- Wordt indien nodig finetuning verricht aan de instellingen van het netwerk, zoals bijstellen van zendvermogen, VLAN-configuratie of toegang tot applicaties;
- Worden afnemer en/of de ICT-beheerder indien overeengekomen in de Nadere offerteaanvraag kort ingewerkt in het beheerportaal (op leesrechten).

De opdrachtnemer zorgt voor een soepele overgang naar de structurele beheerfase, zodat de dienstverlening vanaf de ingangsdatum zonder verstoringen kan doorlopen.

4.6 Monitoring en beheer

De opdrachtnemer levert op verzoek van afnemer documentatie aan over de dienst. Dit is tenminste:

- Een grafisch overzicht van de componenten/voorziening;

- De uiteindelijke locatie van de geïnstalleerde componenten;
- Merk, type en MAC-adressen en naam van geïnstalleerde componenten*;

** De opdrachtnemer levert deze informatie in een digitaal gangbaar leesbaar formaat, zoals CSV of Excel. De opdrachtnemer zorgt dat de dienst indien nodig wordt aangepast als de situatie op een locatie is veranderd, bijvoorbeeld na een interne verbouwing.*

4.7 Beheer

De opdrachtnemer hanteert een formeel vastgelegd beleid en procedure voor het beheer van super-userrechten/ beheeraccounts op netwerkcomponenten en beheerplatformen:

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

~~4.8 Overleg en evaluatie tijdens beheer~~

~~De afspraken over periodieke overleggen en evaluaties tijdens de beheerfase zijn vastgelegd in de raamovereenkomst.~~

5 Eisen aan Service Level Afspraken (SLA)

De SLA schetst de minimale eisen voor ondersteuning, continuïteit en probleemoplossing. De opdrachtnemer voldoet minimaal aan onderstaande afspraken.

Supportstructuur

5.1 Eerstelijnssupport

Als standaard levert afnemer eerstelijnssupport, waarbij wordt uitgegaan dat afnemer de basisprobleemoplossing kan oppakken waarvoor geen diepgaande technische kennis is vereist. De verwachtte doelgroep zal doorgaans de eerstelijnssupport beperkt ingeregeld hebben en worden verzorgd door een (per locatie aangewezen) ICT-coördinator met mogelijk beperkte inhoudelijke technische kennis. Opdrachtnemer ondersteunt afnemer hierin en kan eerstelijnssupport remote leveren per telefoon, chat en/of ticketsysteem aan afnemer.

5.2 Tweede- en derdelijns support

Opdrachtnemer levert een tweede- en derdelijns support. De opdrachtnemer beschikt over diepgaande kennis om tot de juiste probleemoplossing te komen. Daarbij geldt dat de opdrachtnemer zich proactief inzet bij problemen om de oorzaak en de oplossing zo snel als mogelijk en adequaat te bewerkstelligen, ook als op voorhand onduidelijk is in welk domein een probleem zich bevindt. Als supportkanaal wordt tenminste telefonische bereikbaarheid vereist. Daarnaast tenminste één schriftelijke vorm van support, bijvoorbeeld chat, mail of portal.

5.3 Supportvenster

De opdrachtnemer biedt een supportvenster aan van maandag tot en met vrijdag tussen 08.00-17.00 uur, met uitzondering van officiële feestdagen. Dit komt neer op maximaal 2340 uur supportvenster per jaar. Binnen dit supportvenster levert zij haar diensten en voldoet zij aan de hieronder gestelde reactie- en oplostijden.

Classificatie, responstijden en beschikbaarheid

5.4 Prioriteiten, urgentie en impactniveaus

Incidenten worden geclassificeerd naar urgentie en impact (locatie, groep of individu). De opdrachtnemer hanteert de volgende minimale reactietijden, oplostijden en KPI's.

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

Prioriteit	Urgentie		
Impact	*(Volledig) onmogelijk om te werken. Directe verstoring van het onderwijs of veiligheid.*	*Mogelijk om te werken, maar met verminderde functionaliteit.*	*Mogelijk om te werken met meeste functionaliteit.*
Eén of meerdere locaties	Prio 1	Prio 2	Prio 3
Een of meerdere groepen	Prio 2	Prio 3	Prio 4
Individu	Prio 3	Prio 4	Prio 4

5.5 Beschikbaarheid van de dienst

De beschikbaarheid van de WLAN, LAN en Gateway/firewall bedraagt minimaal 99% per locatie per jaar, exclusief vooraf aangekondigd onderhoud. Deze beschikbaarheid is gebaseerd op enkelvoudige uitvoering (van chassis). Er is sprake van beschikbaarheid van de dienst, als:

WLAN:

- 95% van de gebruikers in één ruimte binnen 30 seconden kunnen verbinden met het wifinetwerk;
- De beschreven prestatie-eisen door het aantal gebruikers in de benoemde ruimtes wordt behaald;
- De packetloss minder is dan 2% over een periode van 5 minuten en de reactietijden lager liggen dan 75ms tussen het access point en een vast meetpunt in het vaste netwerk, op basis van metingen vanuit de wifi-infrastructuur. ~~de gebruiker en een willekeurig netwerkapparaat in het vaste netwerk.~~

LAN (uitgangspunt: maximale belasting van 80% van de netto beschikbare bandbreedte):

- De verbindingen behalen tenminste een netto doorvoersnelheid van 90% van de linksnelheid;
- Packetloss van minder dan 0,5% over een periode van 5 minuten en reactietijden dienen lager te zijn dan 15ms tussen client en een willekeurig netwerkapparaat in het vaste netwerk.

Onderhoud en wijzigingsbeheer

5.6 Configuratiebeheer

De opdrachtnemer hanteert een geformaliseerd configuratiebeheer waarin alle configuratie-items, hun relaties en wijzigingen gedurende de levenscyclus centraal worden vastgelegd en bewaakt in een CMDB, ondersteund door een configuratiemanagementtool met monitoring en automatisering. Minimaal wordt geborgd dat:

- middelen (hardware, software, licenties) en wijzigingen automatisch worden geregistreerd;
- configuratie-baselines worden vastgelegd na wijzigingen;
- relaties tussen CI's worden onderhouden;
- procedures zijn gedocumenteerd, gestandaardiseerd en afgestemd met change/incident/problemmanagement;
- bedrijfsmiddelen worden gelabeld en bij inkoop geregistreerd;
- licenties levenscyclus breed worden beheerd volgens beleid.

5.7 Onderhoud en geplande uitval

De opdrachtnemer voert updates, upgrades, patches en ander preventief onderhoud uitsluitend uit binnen een vooraf met afnemer overeengekomen onderhoudsvenster (ma–vr 20:00–07:00 uur en in het weekend).

Gepland ~~Het~~ onderhoud wordt minimaal 10 werkdagen vooraf aangekondigd en afgestemd met afnemer, waarbij rekening wordt gehouden met onderwijsspecifieke activiteiten (zoals ouderavonden). Voor onderhoud dat zeer beperkte impact heeft (geen merkbare verstoring, prestatievermindering, netwerkonderbreking of herstart van apparatuur) kan een verkorte aankondigingstermijn van minimaal 5 werkdagen worden gehanteerd, mits deze vooraf is afgestemd met én expliciet is goedgekeurd door de afnemer. Onderhoud dat mogelijk enige impact, uitval of prestatievermindering kan veroorzaken valt altijd onder de standaardtermijn van minimaal 10 werkdagen.

Uitval als gevolg van gepland onderhoud telt niet mee voor de beschikbaarheid, tenzij de oorzaak ligt bij tekortkomingen van de opdrachtnemer. Voor kritieke security-updates mag van de voorafgaande aankondiging worden afgeweken.

5.8 Wijzigingsbeheerproces

De opdrachtnemer beschikt over een formeel wijzigingsbeheerproces voor alle netwerkcomponenten. Binnen dit proces geldt:

- Classificatie: alle wijzigingen worden vooraf geclassificeerd op impact en risico.
- Kleine of standaardwijzigingen: wijzigingen met beperkte impact (bijvoorbeeld een SSID toevoegen of VLAN aanpassen) worden na eenvoudige toetsing uitgevoerd.
- Wijzigingen met hoge impact: wijzigingen met aanzienlijke gevolgen voor continuïteit, prestaties of beveiliging worden vooraf getoetst, getest en goedgekeurd voordat deze in productie worden doorgevoerd.
- Testomgeving: voor wijzigingen met hoge, kritieke impact* vindt validatie plaats in een gescheiden, beveiligde testomgeving of een gelijkwaardig alternatief (bijv. leverancierslab of virtuele testopstelling), met een testplan, vastgelegde acceptatiecriteria, terugvalplan en formele overdracht naar productie. **met wijzigingen met hoge of kritieke impact worden alle*

wijzigingen bedoeld die een significant risico vormen voor de continuïteit, prestaties of beveiliging van het netwerk, waaronder wijzigingen die kunnen leiden tot uitval van één of meerdere locaties of die betrekking hebben op centrale of routerende componenten.

5.9 Kleine standaardwijzigingen

Opdrachtnemer voert kleine, standaard wijzigingen in de netwerkconfiguratie kosteloos uit, mits deze binnen 30 minuten af te handelen zijn. Onder kleine wijzigingen kan bijvoorbeeld verstaan worden: configuratiewijzigingen zonder impact op het ontwerp, capaciteit of beveiligingsarchitectuur zoals een SSID toevoegen of het toevoegen/verwijderen van een MAC-adres. De responstijd voor standaard wijzigingen is gelijk aan classificatie prioriteit 4. Bij een wijzigingsverzoek geeft de opdrachtnemer altijd vooraf een terugkoppeling of het verzoek wordt aangemerkt als een standaard wijziging (kosteloos) of als een niet-standaard wijziging, waarbij een prijsindicatie wordt verstrekt vóór uitvoering. Het is niet toegestaan grotere wijzigingen op te delen in meerdere kleine wijzigingen om deze als standaardwijzigingen aan te merken.

5.10 Niet-standaardwijzigingen

Niet standaard wijzigingen kunnen zeer uiteenlopend zijn. Opdrachtnemer dient tenminste binnen de responstijd van prioriteitsklasse 4 antwoord te geven op een verzoek voor een niet standaard wijziging. Afhankelijk van de aard wordt tussen afnemer en opdrachtnemer afgestemd wat de uiterste oplostijd is voor deze wijziging. Daarbij geldt dat opdrachtnemer proactief handelt en een redelijk termijn afstemt t.b.v. deze wijziging. Indien van toepassing en afhankelijk van de impact stelt opdrachtnemer een plan van aanpak en offerte op en wordt een test- en acceptatieprocedure opgesteld alvorens een wijziging wordt doorgevoerd.

5.11 Noodwijzigingsprocedure

De opdrachtnemer beschikt over een formeel gedocumenteerde noodwijzigingsprocedure met concrete toegewezen verantwoordelijkheden. Noodwijzigingen worden geautoriseerd, uitgevoerd volgens procedure en achteraf geregistreerd en geëvalueerd.

Monitoring, beveiliging en preventie

5.12 Monitoring van de dienst

De opdrachtnemer biedt een centrale beheer- en monitoromgeving waarmee alle netwerkcomponenten op afstand kunnen worden beheerd en bewaakt. Afnemer krijgt op verzoek leesrechten op deze omgeving en kan, indien overeengekomen, beperkte wijzigingen uitvoeren (bijv. het toevoegen van een SSID). Dit is optioneel en wordt per schoolbestuur afgestemd.

De opdrachtnemer verzorgt doorlopende monitoring om de beschikbaarheid, prestaties en veiligheid van de dienst te waarborgen. Minimaal wordt geborgd dat:

- Alle hoofdcomponenten van het netwerk tijdens het supportvenster continu worden gemonitord;

- Real-time gegevens over capaciteit, gebruik, storingen en beveiligingsgebeurtenissen worden verzameld en geanalyseerd;
- Afnemer en opdrachtgever via dashboards of rapportages inzicht krijgen in netwerkgebruik en -capaciteit (bijv. per SSID/VLAN, access point of poort);
- Signalen van afwijkingen of dreigingen proactief worden opgevolgd en, indien relevant, gedeeld met afnemer.

5.13 Configuratie- en beveiligingsupdates

De opdrachtnemer voorziet alle apparatuur tijdig van de juiste configuratie en (security) updates volgens de voorschriften van de opdrachtnemer(s) van de apparatuur, software en (cloud)diensten. Hierbij geldt dat de opdrachtnemer security patches binnen 1 maand na het uitkomen ervan door de fabrikant installeert. Deze verplichting heeft betrekking op componenten waarvoor de fabrikant nog updates en patches beschikbaar stelt.

5.14 Beveiligingskwetsbaarheden

Beveiligingskwetsbaarheden worden beoordeeld volgens de CVSS-methode. Kwetsbaarheden met een score van 7–8 worden binnen vijf (5) werkdagen verholpen; bij een score van 9–10 binnen achtenveertig (48) uur. Tot herstel treft Opdrachtnemer alle mogelijke maatregelen om de dienst en gebruikers te beschermen. Indien deze termijnen door externe afhankelijkheden (bijv. fabrikant) niet haalbaar zijn, licht Opdrachtnemer dit op eerste verzoek toe aan opdrachtgever, inclusief genomen acties, afhankelijkheden en verwachte oplostermijn.

5.15 Incidentbeheer en beveiligingsmeldingen

De opdrachtnemer volgt een formeel incidentproces waarbij beveiligingsincidenten op het netwerk worden gedetecteerd, beoordeeld, gemeld en opgevolgd. Incidenten worden geclassificeerd naar ernst, acties worden geregistreerd, geëvalueerd en waar nodig gerapporteerd. Incidenten met mogelijke privacy-impact worden binnen 24 uur gemeld aan (de FG van) afnemer.

5.16 Problem management

Bij terugkerende storingen of prestatieproblemen analyseert de opdrachtnemer de onderliggende oorzaak (root-cause) en treft structurele maatregelen. De opdrachtnemer levert hiervan een problemmanagementrapportage aan opdrachtgever.

Rapportage en evaluatie

5.17 Capaciteit- en performance management

De opdrachtnemer beschikt over een formeel proces en ondersteunende tooling voor capaciteit- en performancemanagement van de dienst. Dit omvat ten minste:

- Het geautomatiseerd verzamelen en vastleggen van performance- en capaciteitsmetingen (bijv. CPU/memory load, bandbreedte, latency, throughput per netwerkcomponent of logical partition);
- Tenminste 1 keer per jaar vindt monitoring plaats en wordt en rapportage van deze metingen aan afnemer voorgelegd. De rapportage bevat een trendanalyse zodat tijdige signalering van capaciteitsknelpunten, degradatie in performance of afwijkingen t.o.v. KPI's mogelijk is;
- Proactieve voorstellen aan afnemer om uitbreiding of bijsturing van de netwerkinfrastructuur tijdig te initiëren indien trends daartoe aanleiding geven.

5.18 Storingsrapportage

In geval van een Prio-1 incident is de opdrachtnemer verplicht om op verzoek van het opdrachtgever een free format storingsrapportage te sturen. In deze rapportage staat ten minste:

- Beschrijving van incident met daarbij de gevolgen voor de gebruikers;
- Startdatum en tijdstip van het incident;
- Einddatum en tijdstip van het incident;
- Een samenvatting van de gevolgde oplosprocedure met de daarbij relevante timestamps;
- De oorzaak van het incident;
- Door de opdrachtnemer genomen maatregelen om herhaling in de toekomst te voorkomen.

5.19 Incidentenrapportage

De opdrachtnemer voorziet opdrachtgever op aanvraag een incidentenrapportage waarin een overzicht wordt verschaft van alle aangemelde incidenten per schoolbestuur. In deze rapportage staat ten minste:

- Type storing (major of minor);
- Beschrijving van de aangemelde storing;
- Beschrijving van de oorzaak en oplossing;
- Start datum en tijdstip van het incident;
- Eerste reactie datum en tijdstip op het incident;
- Eind datum en tijdstip van het incident;
- Percentage behaalde KPI's per type storing (major/minor) conform de SLA.

Samenwerking en escalaties

5.20 Incident-escalatieprocedure

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

5.21 Domein-onduidelijkheid

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