gildeopleidingen

# Beschrijving Beoogde Dienstverlening

## Europese Openbare Aanbesteding

*Network Management Services (SPOC / Regiepartner Netwerkdomein)*

**Opdrachtgever:** Stichting Gilde Opleidingen

**Procedure:** Europese Openbare Procedure volgens Aanbestedingswet 2012

**Kenmerk:** GO-202610-MvdWMH Bijlage A

**Versie:** 1.0

**Datum: 2026-11-17**

**Opgesteld door:** Dienst ICT i.s.m. Marcel Heugen

# Inhoud

1. Opdracht & Partnership ..... 3
1.1 Aanleiding en doelstelling van de aanbesteding ..... 3
1.2 Strategische doelstellingen ..... 3
1.3 De huidige situatie ..... 3
1.4 De Gewenste Situatie ..... 4
1.5 Dienst ICT ..... 5
1.5.1 Organisatie ICT ..... 5
1.5.2 Missie, visie en strategisch kader afdeling ICT ..... 5
1.5.3 Huidige situatie netwerkdomein ..... **Fout! Bladwijzer niet gedefinieerd.**
1.5.4 SIAM/SPOC regiemodel ..... **Fout! Bladwijzer niet gedefinieerd.**
2. Scope van de Dienstverlening ..... 6
2.1 Beheer bestaande LAN, WLAN, Firewall, VPN en NAC ..... 6
2.2 Netwerkmonitoring en netwerksecurity ..... 6
2.3 Lifecycle management, firmware management en configuratiebeheer ..... 6
2.4 Performance, capaciteits- en beschikbaarheidsmanagement ..... 6
2.5 Problem, incident, change en release management ..... 7
2.6 CMDB, documentatie, kennisborging en rapportages ..... 7
2.7 Leveranciersmanagement en contractmanagement ondersteuning ..... 7
3. GEWENST DIENSTVERLENINGSMODEL ..... 8
3.1 Single Point of Contact en Single Point of Responsibility ..... 8
3.2 Rollen en verantwoordelijkheden ..... 8
3.3 Demarcatie tussen opdrachtgever en opdrachtnemer ..... 8
3.4 Escalatiemodel ..... 9
3.5 Governance structuur ..... 9

# 1. OPDRACHT & PARTNERSCHAP

In dit document zal de opdracht en de gewenste situatie nader worden beschreven.

## 1.1 Aanleiding en doelstelling van de aanbesteding

De huidige contracten met betrekking tot het beheer en de regievoering over het netwerkdomein lopen af. Tevens wil Gilde Opleidingen het netwerkbeheer gaan outsourcen.

Stichting Gilde Opleidingen (hierna: **"Gilde Opleidingen"** of **"Opdrachtgever"**) is voornemens een overeenkomst te sluiten met één (1) opdrachtnemer voor de dienstverlening rondom **Network Management Services**, waarbij de opdrachtnemer optreedt als **Single Point of Contact (SPOC)** en **Regiepartner** voor het volledige netwerkdomein.

De Opdrachtnemer is een professionele merk onafhankelijke welke de complete netwerkinfrastructuur van Stichting Gilde Opleidingen (een Nederlandse MBO onderwijsstichting) zal gaan beheren en onderhouden. Ook dienen alle benodigde documenten en tekeningen door de leverancier up to date gehouden te worden. Gilde Opleidingen moet wel altijd permanent toegang tot deze gegevens hebben.

Opdrachtgever zoekt nadrukkelijk geen leverancier voor de levering van hardware of licenties. De focus van deze aanbesteding ligt op het contracteren van een partner die de operationele verantwoordelijkheid (Single Point of Responsibility) draagt voor de beschikbaarheid, security, performance en lifecycle van de bestaande multi-vendor netwerkinfrastructuur.

## 1.2 Strategische doelstellingen

De strategische doelstellingen van deze aanbesteding zijn:

1. Maximale beschikbaarheid en continuïteit: Garanderen van een stabiele, veilige en hoogpresterende netwerkinfrastructuur ter ondersteuning van het primaire onderwijsproces en onderzoek (24/7 beschikbaarheid).
2. Operationele ontzorging: Minimaliseren van de operationele beheerlast voor de interne IT-organisatie van Opdrachtgever, zodat zij zich kan focussen op strategische IT-projecten en onderwijsinnovatie.
3. Merkonafhankelijkheid en multi-vendor ondersteuning: Effectief beheer van een heterogene infrastructuur zonder vendor lock-in of merkvoorkeur.
4. Informatiebeveiliging en compliance: Waarborgen van een hoogwaardig securityniveau conform ISO 27001 en de AVG, passend binnen de context van een onderwijsinstelling.
5. Voorspelbaarheid en transparantie: Duidelijke kostenstructuren (FinOps), heldere rapportages en sturing op basis van Service Level Agreements (SLA's) en Experience Level Agreements (XLA's).

## 1.3 De huidige situatie

De huidige netwerkinfrastructuur van Opdrachtgever ondersteunt circa 9.500 studenten en c.a. 900 medewerkers, verspreid over 14 geografische locaties (campussen en onderwijslocaties). Ook zijn er verschillende kleine locaties waar Gilde gebruik van maak, hier is geen netwerk van Gilde in de locatie aanwezig. De infrastructuur is organisch gegroeid en bestaat uit een multi-vendor omgeving met componenten van diverse fabrikanten (waaronder Cisco, Fortinet).

De omgeving omvat:

- LAN: Circa 170 switches (core enaccess).
- WLAN: Circa 550 Wireless Access Points, aangestuurd via zowel on-premise als cloud-gebaseerde controllers.
- Firewall & VPN: Redundante Next-Generation Firewalls op de centrale datacentrum locaties ( 2 keer ) en lokale firewalls per vestiging van Gilde Opleidingen ( 14 keer ) . VPN-koppelingen voor thuiswerkers en externe partners
- Network Access Control (NAC): Een centrale NAC-oplossing voor de authenticatie en autorisatie van gebruikers en apparaten ( b.v. eduroam).
- Beheer: Het operationele beheer wordt momenteel deels intern en deels door verschillende externe partijen ad-hoc uitgevoerd. Dit leidt tot versnippering, onduidelijke demarcatielijnen en een hoge coördinatielast voor de interne IT-afdeling.

## 1.4 De Gewenste Situatie

Opdrachtgever streeft naar een strategisch partnerschap gebaseerd op transparantie, pro activiteit en continue verbetering. Opdrachtnemer treedt op als regiepartner binnen een Service Integration and Management (SIAM) model. Dit betekent dat Opdrachtnemer niet alleen de eigen diensten beheert, maar ook de coördinatie en operationele aansturing verzorgt van externe ketenpartners (zoals hardware fabrikanten, telecomleveranciers en internet serviceproviders). Opdrachtgever wordt hierdoor volledig ontzorgd op operationeel niveau, terwijl zij zelf de regie behoudt op het gebied van Enterprise architectuur, beleid, prioriteitstelling en investeringsbeslissingen.

| | | |
|---|---|---|
| **OPDRACHTGEVER — Beleid, Enterprise Architectuur, Budgetten, Investeringen** | | |
| **OPDRACHTNEMER (Managed Service Provider / SPOC) — Single Point of Responsibility, Operationele Regie & SIAM, 24/7 Monitoring & Security Operations** | | |
| **LAN/WLAN/FW Fabrikanten** | **Telecom & ISP Leveranciers** | **Cloud & SaaS Partners** |

De gewenste eindsituatie kenmerkt zich door:

- Eén loket (SPOC): Alle incidenten, wijzigingen en vragen met betrekking tot het netwerkdomein verlopen via de servicedesk van Opdrachtnemer.
- End-to-end verantwoordelijkheid: Opdrachtnemer is operationeel verantwoordelijk voor de gehele keten, inclusief de aansturing van derden.
- Proactief beheer: Problemen worden geïdentificeerd en opgelost voordat ze impact hebben op het onderwijsproces.
- Up-to-date documentatie: Een continu actuele CMDB en netwerkdocumentatie die direct toegankelijk is voor Opdrachtgever.
- Continuïteit: Een soepel transitietraject waarbij de dienstverlening zonder onderbreking wordt overgedragen van de huidige situatie naar de nieuwe Managed Service.

## 1.5 Dienst ICT

### 1.5.1 Organisatie ICT

Binnen Gilde Opleidingen is de afdeling ICT verantwoordelijk voor het functioneren van de ICT-dienstverlening. De afdeling is ingericht volgens een **regieorganisatie**, waarbij demand-management, functioneel beheer en informatiemanagement in eigen huis worden uitgevoerd, en technisch beheer grotendeels wordt belegd bij externe partners.

### 1.5.2 Missie, visie en strategisch kader afdeling ICT

De ICT-strategie van Gilde Opleidingen is gebaseerd op vier pijlers:
1. **Onderwijs eerst** – ICT ondersteunt het onderwijsproces en de studentbeleving.
2. **Regie in eigen huis** – Gilde Opleidingen voert regie, marktpartijen leveren uitvoering.
3. **Cloud, tenzij** – een cloud-first benadering met behoud van soevereiniteit over data.
4. **Standaardisatie en professionalisering** – werken volgens erkende frameworks (ITIL
4, SIAM, NORA/ROSA, ISO 27001).

## 1.6 Huidige Situatie Netwerkdomein

Het netwerkdomein van Gilde Opleidingen omvat onder meer:

- Een **WAN-infrastructuur** (geleverd door externe partijen) die alle locaties verbindt met het datacenter en met cloudomgevingen (middels lokale of centrale internet);
- Een **LAN-infrastructuur** per locatie, waaronder bekabelde en draadloze netwerken (Wi-Fi);
- Een **Centrale Firewall omgeving en security-appliances** (perimeter en interne segmentatie);
- Een **Lokale FIrewall omgeving** (perimeter en interne segmentatie);
- Een **Netwerkmonitoring, logging en observability**;
- Een **Identity- en Access-services** gekoppeld aan het netwerk  NAC).

De huidige technologie-stack is een **multi-vendor omgeving** met componenten van onder meer:

- **Cisco** (routing/switching, ISE);
- **Fortinet** (SD-WAN, firewalls);

Het beheer is momenteel belegd bij meerdere leveranciers en interne teams, wat leidt tot fragmentatie in verantwoordelijkheden, escalatiepaden en performancesturing. Met deze aanbesteding beoogt Gilde Opleidingen deze fragmentatie op te heffen door introductie van een **SPOC-regiemodel**. Zie verder hoofdstuk 3

# 2. Scope van de Dienstverlening

De scope van de dienstverlening omvat het volledige operationele beheer en de regie over het netwerkdomein van Opdrachtgever. De diensten worden geleverd conform ITIL4-best practices en SIAM-principes .hoofdstuk wordt de te volgen aanbestedingsprocedure beschreven.

## 2.1 Beheer bestaande LAN, WLAN, Firewall, VPN en NAC

- LAN-beheer: Operationeel beheer van alle core- en access-switches. Dit omvat poortconfiguraties, VLAN-beheer, Spanning Tree optimalisatie, en het oplossen van fysieke en logische storingen.
- LAN-Beheer: De fysieke koppelingen op switches naar lokale device wordt door de afdeling Front Office van Stichting Gilde Opleidingen uitgevoerd.
- WLAN-beheer: Beheer van de draadloze netwerkinfrastructuur, inclusief controllers gesitueerd per locatie in de firewalls, access points, RF-optimalisatie, gastennetwerken en eduroam- en IoTroam-integratie.
- Firewall-beheer: Onderhoud en configuratie van Next-Generation Firewalls (NGFW). Dit omvat het beheer van firewall-rulesets, NAT-tabelbeheer, intrusion prevention (IPS) profielen en web- en app-filtering.
- VPN-beheer: Beheer van site-to-site VPN-tunnels met externe partners en client-to-site VPN-toegang voor medewerkers. Tevens bestaan er per locaties VPN tunnels met het Productie data centrum en Uitwijk locatie. Deze tunnels zijn voor uitwijk mogelijkheid wanneer de lokale internet koppeling niet werkt.
- NAC-beheer: Beheer van de Network Access Control-omgeving voor veilige netwerktoegang op basis van certificaten, Active Directory-koppelingen.

## 2.2 Netwerkmonitoring en netwerksecurity

- 24/7 Monitoring: Continue monitoring van de beschikbaarheid, performance en capaciteit van alle netwerkcomponenten met behulp van geavanceerde monitoringtooling.
- Security Monitoring: Detectie van afwijkend netwerkverkeer, potentiële inbreuken en kwetsbaarheden. Directe opvolging van security-alerts en nauwe samenwerking met de CISO van Opdrachtgever.
- Vulnerability Management: Periodiek scannen van netwerkcomponenten op bekende kwetsbaarheden en het proactief adviseren over en uitvoeren van mitigerende maatregelen.

## 2.3 Lifecycle management, firmware management en configuratiebeheer

- Lifecycle Management: Monitoren van de End-of-Life (EoL) en End-of-Support (EoS) status van hardware en software. Opstellen van een jaarlijks lifecycle-advies ten behoeve van het investeringsplan van Opdrachtgever.
- Firmware Management: Planmatig en risicogebaseerd testen en installeren van firmware-updates, patches en hotfixes om stabiliteit en security te garanderen.
- Configuratiebeheer: Automatische back-up van alle apparaatconfiguraties (minimaal dagelijks bij wijzigingen) en het bewaken van configuratie-compliance (golden templates).

## 2.4 Performance, capaciteits- en beschikbaarheidsmanagement

- Performance Management: Continue analyse van netwerklatency, packet loss en jitter om een optimale gebruikerservaring (XLA) te garanderen.
- Capaciteitsmanagement: Monitoren van bandbreedteverbruik, CPU/geheugenbelasting van netwerkapparatuur en poortbezetting. Proactieve signalering wanneer drempelwaarden worden overschreden.
- Beschikbaarheidsmanagement: Analyseren van de redundantie van kritieke netwerkpaden en het minimaliseren van Single Points of Failure (SPOF).

## 2.5 Problem, incident, change en release management

- Incident Management: Registratie, prioritering, diagnose en herstel van netwerkstoringen conform de overeengekomen SLA-hersteltijden.
- Problem Management: Trendanalyse op incidenten om structurele fouten te identificeren. Uitvoeren van Root Cause Analyses (RCA) en het implementeren van definitieve oplossingen (workarounds of structural changes).
- Change Management: Gestructureerde afhandeling van wijzigingen (Standard, Normal en Emergency Changes) via een gezamenlijk Change Advisory Board (CAB).
- Release Management: Coördinatie en gecontroleerde uitrol van grootschalige software- of configuratiereleases binnen de netwerkomgeving.

## 2.6 CMDB, documentatie, kennisborging en rapportages

- CMDB-beheer: Up-to-date houden van de Configuration Management Database (CMDB) met alle Configuration Items (CI's), inclusief relaties, locaties, serienummers en firmwareversies.
  De hardware CMDB wordt door Gilde Opleidingen zelf in eigen beheer gedaan, daar Gilde ook zelf de hardware aanschaft.
- Documentatie: Onderhouden van actuele netwerktekeningen (L1/L2/L3 diagrammen), high-level en low-level designs (HLD/LLD) en beheerhandleidingen.
- Kennisborging: Vastleggen van klantspecifieke procedures en oplossingsrichtingen in een centrale kennisbank (Knowledge Base).
- Rapportages: Periodieke oplevering van operationele, tactische en strategische rapportages (zie Hoofdstuk 7).

## 2.7 Leveranciersmanagement en contractmanagement ondersteuning

- Leveranciersmanagement: Operationele aansturing van externe leveranciers (bijv. internet service providers, glasvezelleveranciers en hardware-onderhoudspartijen) bij incidenten en wijzigingen.
- Contractmanagement Ondersteuning: Ondersteunen van de contractmanager van Opdrachtgever door het leveren van input over de prestaties van onderliggende leveranciers en het signaleren van contractuele risico's of optimalisatiekansen.

## 2.8 Buiten Scoop

**Uitdrukkelijk buiten scope** vallen:

- **Levering van hardware** (routers, switches, access points, firewalls, appliances);
- **Levering van software-/vendor-licenties** (deze worden separaat door Opdrachtgever ingekocht);
- **Levering van internet connectiviteit / WAN-transport** (separaat gecontracteerd);
- **Werkplekbeheer en applicatiebeheer** (belegd bij andere domein-leveranciers);
- **Fysieke bekabelingsinfrastructuur** (onderdeel van gebouwbeheer).

# 3. GEWENST DIENSTVERLENINGSMODEL

Het gewenste dienstverleningsmodel is gebaseerd op het principe van volledige operationele ontzorging via een SIAM-raamwerk.

## 3.1 Single Point of Contact en Single Point of Responsibility

- Single Point of Contact (SPOC): Opdrachtnemer levert één centraal aanspreekpunt voor alle operationele netwerkaangelegenheden. Dit geldt voor zowel de interne IT-medewerkers van Opdrachtgever als voor de door Opdrachtgever aangewezen key-users.
- Single Point of Responsibility (SPOR): Opdrachtnemer is end-to-end verantwoordelijk voor het functioneren van de netwerkketen. Indien een storing wordt veroorzaakt door een externe partij (bijv. een haperende internetverbinding van een telecomprovider), blijft Opdrachtnemer verantwoordelijk voor de coördinatie en het herstel van de dienst, zonder dat Opdrachtgever zelf contact hoeft op te nemen met deze derde partij.

## 3.2 Rollen en verantwoordelijkheden

De belangrijkste rollen binnen het dienstverleningsmodel zijn:

- Service Delivery Manager (SDP) (Opdrachtnemer): Verantwoordelijk voor de kwaliteit van de dienstverlening, SLA-compliance, tactische governance en continue verbetering.
- Lead Network Engineer / Architect (Opdrachtnemer): Technische sparringpartner voor de enterprise architect van Opdrachtgever, verantwoordelijk voor de technische vertaling van beleid naar operationele configuraties.
- Incident / Change Manager (Opdrachtnemer): Verantwoordelijk voor de procesmatige afhandeling van incidenten en wijzigingen conform ITIL4.
- Contractmanager (Opdrachtgever): Bewaakt de contractuele afspraken, stuurt de SDM van Opdrachtnemer aan en neemt besluiten over contractuele wijzigingen.
- Enterprise Architect (Opdrachtgever): Bepaalt de technologische roadmap, standaarden en beleidskaders.

## 3.3 Demarcatie tussen opdrachtgever en opdrachtnemer

De grens tussen de verantwoordelijkheden is als volgt gedefinieerd:

| Activiteit | Opdrachtgever | Opdrachtnemer |
|---|---|---|
| **Strategie & Beleid** | Bepalen van IT-strategie, securitybeleid en budgetten. | Adviseren op basis van operationele trends en marktontwikkelingen. |
| **Architectuur** | Vaststellen van netwerkarchitectuur en standaarden. | Vertalen van architectuur naar operationele ontwerpen en configuraties. |
| **Investeringen** | Aanschaf van hardware, licenties en onderhoudscontracten. | Adviseren over benodigde capaciteit en lifecycle-vervangingen. |
| **Operationeel Beheer** | Geen (uitgezonderd lokale 'smart hands' indien overeengekomen). | Volledige uitvoering van dagelijks beheer, monitoring en onderhoud. |
| **Security Incidenten** | Besluitvorming over ingrijpende maatregelen (bijv. isoleren locatie). | Detectie, analyse, isolatie en herstel van netwerkgerelateerde security-incidenten. |

## 3.4 Escalatiemodel

Indien incidenten of problemen niet binnen de reguliere operationele lijnen kunnen worden opgelost, treedt het volgende escalatiemodel in werking:

| Escalatie Nivo | Gilde Opleidingen | Opdrachtnemer |
|---|---|---|
| Nivo 1 Operationeel | Contractverantwoordelijke | Incident Manager |
| Nivo 2 Tactisch | Teamleider ICT | Accountmanager |
| Nivo 3 Strategisch | Directie Bedrijfsvoering | Directielid |

## 3.5 Governance structuur

De governance is ingericht op drie niveaus om een effectieve sturing en continue afstemming te waarborgen:

- Operationeel overleg (Wekelijks): Evaluatie van openstaande incidenten, geplande changes, operationele performance en actuele risico's.
- Tactisch overleg (Maandelijks): Bespreking van de maandrapportage, SLA/XLA-compliance, service credits, voortgang van het verbeterregister en tactische capaciteitsplanning.
- Strategisch overleg (Kwartaal / Halfjaarlijks): Evaluatie van de samenwerking, technologische roadmap, financiële performance (FinOps), marktontwikkelingen en strategische doelstellingen.