



higher education
& training

Department:
Higher Education and Training
REPUBLIC OF SOUTH AFRICA



westcol
Western College for Technical, Vocational Education and Training

WESTERN TVET COLLEGE

Herein referred to as (WESTCOL)

REQUEST POTENTIAL BIDDERS FOR PROPOSALS (RFP) FOR

**PROVISION OF ICT PROFESSIONAL SERVICES FOR NETWORK INFRASTRUCTURE,
CYBERSECURITY, SYSTEM SUPPORT AND PATCH MANAGEMENT FOR THIRTY-SIX (36)
MONTHS.**

Tender No: PU8010/038

Prospective Suppliers who are interested in participating in the aforementioned tender are invited to submit a proposal in full compliance to the requirement of this tender document. Completed documents with all attachments must be signed and submitted on the **PURCO SA Website**.

Proposals in response to **PU8010/038 PROVISION OF ICT PROFESSIONAL SERVICES FOR NETWORK INFRASTRUCTURE, CYBERSECURITY, SYSTEM SUPPORT AND PATCH MANAGEMENT FOR THIRTY-SIX (36) MONTHS.**

TENDER DOCUMENTS:

The closing time and date for receipt for online tender **PU8010/038** is at 11h00 AM on **Monday, 12 October 2026**.

Tender number	PU8010/038
Date issued	11 September 2026
Tender closing date	12 October 2026 11h00 am Tender Submission will be Electronic on www.purcosa.co.za Supplier Hub- Online Tender Submission Guide
Non-compulsory Information Session	21 September 2026 11h00 am An online non-compulsory briefing session will be facilitated via MS Teams

Company name	
Address	
Contact person	Mr/Mrs/Ms/Dr/Prof.
Contact numbers	(w) (cell)
Email address	

Page: 1

1.1.1 PRE-QUALIFICATION/MANDATORY INFORMATION REQUIREMENT

The Pre-qualification/Mandatory Information Requirement phase validates the tenderers' compliance with the legal requirements to conduct business in SA, as well as to specific industry requirements for the supply of services where applicable.

Please see table below for the list of mandatory requirements and tick yes if documentation is submitted and no if not submitted.

Description	Requirement	YES	NO
RFP Document	Each page of the RFP document to be initialled by a delegated representative	Yes	No
Completed Technical specifications and pricing	Attach fully signed technical specifications and pricing (Don't change the pricing schedule and specification)	Yes	No
Proof of Bank Account	Signed or electronically stamped letter from bank (not be older than 6 months)	Yes	No
Company registration documents	Submit copy of company registration documents	Yes	No
Tax Compliance Certificate	Copy of valid SARS Tax compliance status (must be valid on the tender closing date)	Yes	No
B-BBEE Certification	A valid B-BBEE certificate from a SANAS accredited agency/Affidavit	Yes	No
Board resolution	Submit a copy of signed board resolution. Unless if you are sole proprietor	Yes	No
ID documents	Certified copy(s) of Identity Document(s) (ID) for directors/shareholders (not be older than 6 months)	Yes	No
Declaration of Interest	Please sign point 9 of this tender document	Yes	No
Bank Rating Letter	Letter of Good Standing from the bank (Bank Rating Letter) (not be older than 6 months)	Yes	No
Registration National Treasury (CSD)	Provide a copy of the full report of registration on National Treasury Central Supplier Database.	Yes	No
Accreditations (Relevant Bodies)	Submit a relevant copy of Accreditation certificate, e.g. State Information Technology Agency (SITA)	Yes	No
COIDA	Submit valid letter of good standing from the department of labour	Yes	No
SBD Forms	Copy of completed and signed SBD 1, SBD 4, SBD 5, SBD 6.1	Yes	No

NB: No points will be allocated to this phase; however, tenders that do not meet the pre-qualification requirements may not advance to the next phase of the evaluation process.

The below mentioned criteria regarding Functionality is required for responsiveness and therefore eligibility for the next stage of evaluation. This is done to determine the ability of each tenderer to successfully execute the contract according to specifications. Failure to score minimum of 70 out 100 points will lead to non-compliance and non-responsiveness.

These criteria shall only determine whether a tender will further be evaluated and will not influence the points scored on Price. If any criterion is rated zero (0) points, the tenderer will be rejected, even if the required 70 out of 100 points are achieved.

For purposes of comparison and in order to ensure meaningful evaluation, bidders are requested to furnish detailed information in substantiation of compliance to functionality.

FUNCTIONALITY CRITERIA		POINTS ALLOCATED
Experience Proven track record with contactable reference letters for similar projects completed within five (5) years in the successful provision of ICT Professional Services for Network & Security Support mentioned in the scope of work. The reference letters must be on legitimate letterhead and clearly indicate the type of service provided, contract duration, contract value, and the relevant contact person's name, surname, position, and contact number(s). Reference letters that are not signed and dated will not be acceptable. 5 - Appointment and reference letters for similar project 4 - Appointment and reference letters for similar project 3 - Appointment and reference letters for similar project	= 30 Points = 20 Points = 10 Points	30
Project Team and key account manager Project team comprising skilled officials to successfully complete the project. Service providers must attach certified copies of three years qualifications and CV of the technicians. 4 or more qualified Technicians = 30 points 3 - qualified Technicians = 20 points 2 - qualified Technicians = 10 points 1 - project manager qualification= 5 points	= 20 Points = 15 Points = 10 Points = 05 Points	20
Regulatory: POPIA Certified		

The bidder is required to provide POPIA compliance as a demonstration that it has the capacity and capability to handle Westcol TVET College's critical data securely and comply with the confidentiality, integrity, and availability (CIA triad). Please provide a valid certificate of POPIA Certificate. Bidder submitted a certificate confirming POPIA certification Bidder did not submit a certificate confirming	= 05 Points = 00 Points	05
Security – Information Security Management System The bidder is required to provide ISO/IEC 27001 as a demonstration that it has the capacity and capability to handle Westcol TVET College's critical data securely and comply with the confidentiality, integrity, and availability (CIA triad). Please provide a valid certificate of ISO/IEC 27001. Bidder submitted a certificate confirming ISO 27001 certification Bidder did not submit a certificate confirming	= 05 Points = 00 Points	05
Project Approach and Methodology The bidder must submit a detailed implementation methodology demonstrating how the services outlined in the Scope of Work will be delivered, including network management, cybersecurity remediation, patch management, reporting, and skills transfer. The methodology must include a project implementation plan and timelines. Comprehensive methodology covering all aspects of the scope with implementation plan and timelines Methodology covers most aspects with limited implementation details Poor or generic methodology	= 20 Points = 10 Points = 05 Points	20
Relevant Certifications and Vendor Partnerships The bidder must submit proof of vendor accreditations relevant to networking and cybersecurity. More or relevant company accreditations 2 relevant accreditations 1 relevant accreditation	= 20 Points = 15 Points = 10 Points	20
Total Points		100

1. Purpose

The purpose of this Terms of Reference is to appoint a service provider capable of delivering comprehensive ICT infrastructure support and security services to ensure the availability, integrity, confidentiality, and resilience of the College's ICT environment.

The bidder will be responsible for:

- Strengthening and optimising the College's network infrastructure.
- Upgrading the server and data centre infrastructure for six (6) college sites.
- Addressing vulnerabilities identified through Internal and External Audit reports.
- Implementing industry best-practice cybersecurity controls.
- Establishing secure backup and disaster recovery solutions.
- Enhancing ICT governance and operational resilience.
- Developing and implementing an enterprise Patch Management Framework.
- Providing proactive systems support and preventative maintenance.
- Improving ICT monitoring and reporting capabilities.
- Transferring technical knowledge and skills to the College ICT staff.

2. Background

Western TVET College has upgraded its network infrastructure across all college six (6) sites to improve the connectivity and digital service delivery. Although the infrastructure has recently been upgraded, the College currently has insufficient internal ICT resources with the specialised expertise required to maintain, secure, monitor, and optimise the environment. Recent Internal Audit and External Audit reports have further identified significant ICT risks and vulnerabilities, including, inadequate cybersecurity controls, patch management weaknesses, backup and disaster recovery deficiencies, server infrastructure risks, network security vulnerabilities, access management weaknesses, ICT governance deficiencies and incomplete documentation and operational procedures

The College currently operates ICT environment comprising of:

- On Premises Active Directory Domain Services
- Microsoft 365
- Firewall infrastructure
- Managed switches and routers
- Wireless network infrastructure
- Business-critical systems hosted on both cloud and on-premises platforms

3. Scope of Work

The successful bidder shall provide professional services in the following areas:

3.1 Network Infrastructure Management

- Conduct a comprehensive assessment of the existing network infrastructure.
- Review network topology and architecture.
- Assess network capacity and utilisation.
- Review network redundancy and resilience.

3.1.1. Network Management

Maintain and monitor:

- Core switches
- Distribution switches
- Access switches
- Routers
- Firewalls
- Wireless controllers
- Wireless access points
- Network authentication services

3.1.2. Network Optimisation

- Configure VLANs.
- Implement network segmentation.
- Configure Access Control Lists (ACLs).
- Optimise Quality of Service (QoS).
- Monitor bandwidth utilisation.
- Secure remote access services.
- Perform firmware upgrades.
- Monitor network availability 24/7.
- Produce monthly network health reports.
- Recommend infrastructure improvements.

4. Cybersecurity Services

- Review Internal Audit findings.
- Review External Audit findings.
- Develop remediation plans.
- Implement corrective actions.

4.1. Vulnerability Management

- Vulnerability assessments and remediation
- Penetration testing
- Security risk assessments
- Security hardening
- Configuration reviews

4.1.2. Security Controls

Maintain and monitor:

- Firewall policies
- Endpoint protection
- Intrusion Detection Systems (IDS)

- Intrusion Prevention Systems (IPS)
- Multi-Factor Authentication (MFA)
- Microsoft 365 security
- User account administration
- Active Directory security
- Privileged Access Management
- Password policies

5. Systems Support

Provide preventative, corrective, and proactive support for:

- Windows Servers
- Active Directory
- Microsoft 365
- DNS
- DHCP
- Group Policy
- File Services
- Print Services
- Application Servers
- Storage Infrastructure
- Virtual Infrastructure

6. Patch Management

- Patch Management Policy
- Patch testing procedures
- Patch approval workflow
- Emergency patch process
- Rollback procedures
- Maintenance schedules

6.1.1. Patch deployment shall cover:

- Windows Servers
- Domain Controllers
- Virtual Servers
- Microsoft 365
- Active Directory
- Routers
- Switches
- Firewalls
- Wireless Controllers
- End-user computers
- Network appliances

6.1.2. The service provider shall:

- Test patches before deployment.
- Deploy monthly security updates.
- Deploy critical patches within agreed SLA timelines.
- Maintain a patch inventory register.
- Produce monthly compliance reports.

7. Reporting & Documentation

- Network availability
- Network performance
- Server performance
- Backup status
- Disaster Recovery readiness
- Patch compliance
- Security incidents
- Vulnerability status
- Risks and mitigation plans
- Recommendations

7.1.1. Documentation shall include:

- Network diagrams
- Server architecture diagrams
- IP Address Register
- Configuration documentation
- Standard Operating Procedures (SOPs)
- Technical manuals
- Asset configuration records

8. Skills Transfer

- Technical workshops
- Hands-on training
- On-site mentoring
- System administration training
- Cybersecurity awareness sessions
- Standard Operating Procedures
- Administration manuals
- User guides

9. Service level agreement (SLA)

The SLA shall include the following:

- Scope of Services
- Service Availability
- Response and Resolution Times
- Preventative Maintenance Schedule
- Key Performance Indicators (KPIs)
- Escalation Procedures
- Reporting Requirements
- Change Management
- Security Incident Response

- Confidentiality and Data Protection
- Performance Monitoring
- Penalties for non-performance
- Exit Management

No work shall commence until a formal Service Level Agreement has been signed by the successful bidder and Western TVET College.

11. Conditions

A briefing session will be held to address any clarification questions.

12. Pricing schedule

No.	Description	Total (INCL. VAT)
1.	Provision of ICT professional services for network infrastructure, server upgrading, cybersecurity, system support, and patch management for a period of 36 months	R
TOTAL BID PRICE (VAT INCLUSIVE) FOR THIRTY-SIX (36) MONTHS		R

Signature of person authorized to sign the tender

Date