WESTERN TVET COLLEGE

Herein referred to as (WESTCOL)

REQUEST POTENTIAL BIDDERS FOR PROPOSALS (RFP) FOR

SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, MIGRATION FROM EXISTING SERVER TO NEW SERVER INFRASTRUCTURE, BACKUP AND CLOUD-BASED DISASTER RECOVERY SOLUTION, MICROSOFT 365, MAINTENANCE AND SUPPORT FOR THIRTY-SIX (36) MONTHS.

Tender No: PU8111/081

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 **PU8111/081** **SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION, IMPLEMENTATION, MIGRATION FROM EXISTING SERVER TO NEW SERVER INFRASTRUCTURE, BACKUP AND CLOUD-BASED DISASTER RECOVERY SOLUTION, MICROSOFT 365, MAINTENANCE AND SUPPORT FOR THIRTY-SIX (36) MONTHS.**

TENDER DOCUMENTS:

The closing time and date for receipt for online tender **PU8111/081** is at 11h00 AM on **Monday, 12 October 2026.**

Tender number	**PU8111/081**
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** **13h00 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		

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
Original Equipment Manufacturer (**OEM**)	Submit valid copy of certificate/letter/Agreement from OEM	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.

1.1.2 STAGE 1: EVALUATION OF FUNCTIONALITY

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 criteria mentioned and shall only determine whether a tender will further be evaluated.

FUNCTIONALITY CRITERIA		**POINTS ALLOCATED**
A detailed Technical Approach, Design, and Methodology The bidder must demonstrate a thorough understanding of the objectives and deliverables of this request by providing a detailed implementation plan with the following: • Implementation guideline • Work Breakdown Structure/ Milestone and related duration • Backup Services in relation to: 1. Data Backup: Frequency (e.g., daily, real-time), retention periods, and types of data (e.g., databases, virtual machines, file systems). 2. Backup Methods: Full, incremental, differential, or synthetic backups. 3. Storage: On-premises, cloud-based, or hybrid storage solutions. 4. Encryption: Ensure data is encrypted both in transit and at rest. 5. Backup Verification: Regular testing and validation of backup integrity.	= 10 Points	**10**
Disaster Recovery Services • Recovery Time Objective (RTO): Maximum acceptable downtime. • Recovery Point Objective (RPO): Maximum acceptable data loss. • Failover and Failback: Automated or manual processes for switching to disaster recovery systems and returning to normal operations. • Disaster Recovery Testing: Regular testing of Disaster Recovery plans to ensure effectiveness.	= 10 Points	**10**

• Monitoring and Management in relation to: 1. 24/7 monitoring of backup and Disaster Recovery systems. 2. Proactive alerts and incident management. 3. Regular reporting on backup success rates, storage usage, and Disaster Recovery readiness		
Backup Appliance: Bidder must provide solution architecture focusing on Tiered storage capacity, throughput, redundancy, retention tier, scale-out architecture, and archiving. • 100 Terabytes of Storage Onsite for production • Out of the box immutability • Raid self-healing • Ransomware proof • Application Programming Interface integration capability and security (Creating S3 keys and S3 buckets) • Disaster Recovery site must have immutability in place Provide backup appliance Hardware Failure to provide Server and Storage Hardware	= 20 Points = 00 Point	**20**
Reference letters from clients to whom they have successfully provided the backup and disaster Recovery projects within the last five years. 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. • 8 reference letters • 6 reference letters • 4 reference letters • 2 reference letters • Non-submission will lead to zero scoring. **Reference checks will be conducted as part of the confirmation process. This includes physical visits to the institutions/organisation's listed in the reference letters submitted.** A maximum of **05 points** subject to an evaluation form conducted on two references will be allocated.	= 20 Points = 15 Point = 10 Points =05 Points	**20**
Regulatory: POPIA Certified		**05**

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		
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 Point	**05**
Governance and Business Continuity Management Compliance To prove experience and understanding of the scope, size, and scale of this project for Disaster Recovery and Business Continuity Management. Please provide a valid certificate of **ISO 22301.** Bidder submitted a certificate confirming **ISO 22301** certification Bidder did not submit a certificate confirming	= 05 Points = 00 Point	**05**
Personal Identifiable Information (PII) in Public Cloud Computing. To prove experience and understanding of Personally Identifiable Information (PII) and the Protection of Personal Information Act. Please provide a valid certificate of **ISO 27018:2019.** Bidder submitted a certificate confirming **ISO 27018:2019** certification Bidder did not submit a certificate confirming	= 05 Points = 00 Point	**05**

Engineers' experiences and Project Manager **Bidders must provide 3 x CVs of bidder-employed engineers with technical skills and 1 CV of a project manager in ICT, certification, and experience in backup and recovery solutions and project management.** CVs with 8 years or more CVs with 6 to 7 years CVs with 4 to 5 years CVs with 3 to 4 years CVs with 2 to 3 years CVs with less than 2 years =	 = 10 Points = 08 Points = 06 Points = 04 Points = 02 Points = 00 Point	**10**
Engineer technical qualifications of proposed solution. **Bidders must provide technical qualifications of engineers employed by a bidder for a proposed solution by OEM, and certificates to be provided.** 3 x Engineers OEM qualified = 7 2 x Engineers OEM qualified = 5 1 x Engineers OEM qualified = 3 0 x Engineers OEM qualified = 0 AND 1 x Project Management qualified (PMBOK or PRINCE2) = **3** 0 x Project management qualified = **0**	 = 07 Points = 05 Points = 03 Points = 00 Point = 03 Points = 00 Point	**10**
Total Points		**100**

1. PURPOSE

Western TVET College intends to implement a Disaster Recovery (DR), Backup, and Business Continuity (BC) solution that protects the College's critical ICT infrastructure for both on-premises and cloud environments. The project also includes the upgrade of the College's existing server infrastructure and the provision of support and maintenance services for a period of three (3) years.

2. BACKGROUND AND CURRENT INFRASTRUCTURE

Western TVET College currently operates an on-premises ICT infrastructure that supports the delivery of academic, administrative, and business services across the institution. The College has an existing backup solution in place to ensure the protection and recovery of institutional data. However, the current infrastructure has reached the end of its operational life and no longer meets the College's requirements.

The existing server environment consists of three (3) physical servers that host twelve (12) virtual servers. These virtual servers support the College's critical business applications and services, including file and print services, Active Directory, databases, and other critical systems required for the day-to-day operations of the College. The three physical servers have reached their end-of-life (EOL)

The College also has a single enterprise storage system connected to the three physical servers through a Fibre Channel.

3. SCOPE OF SERVICES REQUIRED: (BACKUP AND CLOUD-BASED DISASTER RECOVERY)

The College seeks to appoint a qualified service providers to install and configure the following:

- The Backup and Recovery solution should be an Enterprise edition adapted for data center environments.
- The solution provided should support both on-premises and cloud platforms.
- The solution application or virtual appliance should be installed on an OS compatible with any of the following virtualization technologies: Backup and Replication Licenses Required.
- The solution must be able to perform online block-level de-duplication of data across backup and archive without requiring proprietary disk appliances or additional licenses.
- Datacenter Cloud must be based within the borders of South Africa
- The software must provide Client-side de-duplication.
- Hosting datacenter must have ISO 27001, SOC 2, PCI-DSS, or other relevant standards

- Hosting datacenter must be minimum Tier III or Higher.
- On-site backup storage should have 1 X 500 Terabytes storage scalable, Built-in immutability, Raid self-healing, Ransomware proof and Application Programming Interface integration capability and security (Creating S3 keys and S3 buckets)
- Connectivity SP should provide a suitable network connection between the Westcol datacenter and the cloud datacenter.
- The software must be able to compress and Encrypt data at the client's side. These should be available even when utilizing de-duplication.
- The solution must support measuring, analyzing, and organizing storage utilization based on systems and applications priorities.
- The software should provide dashboards, including granular dashboard management, such as Viewing, Modifying, and Creating Custom Dashboards.
- The software must be able to limit the amount of network bandwidth assigned for each scheduled backup job.
- The software must be SAN-ready. It should be able to support Unix/Windows/Linux in the same FC loop and allow sharing of storage resources like tape drive, disk drive, optical, etc., in a SAN environment across backup.
- The proposed software architecture must be scalable to allow spanning across the data center, including the Disaster Recovery site.
- The software must maintain indexes of all the data objects backed up from the source server to provide quick access for browser/restore operations.
- The contracted Service Provider will be expected to assign dedicated resources to install and configure the proposed Backup and Restore solution in the Westcol TVET College Office, Randfontein, Westrand, Gauteng.
- The solution should be robust with appropriate mechanisms to protect data against corruption.
- The software must support auto-failover and load-balancing of scheduled backup jobs.
- The software architecture should allow the addition of new storage infrastructure without disrupting ongoing operations.
- The software should be optimized to provide for advanced protection of virtual environments like: - Auto-discovery of new VMs – Auto inclusion of VMs into a Backup policy-based affinity rule – Tracking of VMs through the infrastructure.
- The solution should inherently be able to support a disk-to-disk-to-tape approach and provide the option to de-duplicate the data.
- The software should include a feature for copying backup sets to other backup media upon every successful backup session as required.
- The solution should be capable of using other storage as a disk target such as a disk

target such as DAS/NAS or built server storage capacity.

- The software must have the ability to perform a bare-metal restore of a client or server in the backup environment.
- The software must be able to support NDMP-based backup.
- The software should provide reporting capabilities with the following features but not limited to: - Job Summary – Job Schedule – Resource Utilization – License Utilization – Offline Reports – Hypervisor infra (Microsoft Hyper-V, VMware vSphere) reports.
- Monitoring – Performance charts of Hypervisors and VMs, Virtual infrastructure monitoring.
- The software should come with a scheduler to automate tasks such as backup, reporting, etc.
- The software should allow the administrator to define customized calendar slots for scheduling backup jobs.
- The administrative console should be password-protected to prevent unauthorized access to the system.
- The software must maintain an audit trail to track users' operations and changes.

4. BACKUP AND CLOUD-BASED DISASTER RECOVERY:

A comprehensive and versatile backup and restore solution is needed for on-premises, cloud (including Microsoft 365 services) and endpoint devices. This solution should cater to both on-premises and cloud backup requirements while ensuring the backup of servers (virtual and physical), and various databases and applications, including SQL, Exchange, and Directory.

- To ensure compatibility across different environments, the solution should seamlessly support various operating system versions, such as Windows Server 2022, Linux, Unix, Windows 10, and Windows 11. It should also have the capability to back up different types of databases across Windows, Linux, and Unix operating systems.
- To cater to different backup needs, the solution should offer a range of backup options, including full, incremental, differential, and transactional backups.
- Moreover, it should empower users with both full system restores and granular restores for maximum flexibility in data recovery.
- A vital aspect of the solution is generating comprehensive and easily readable reports/logs.
- These logs should provide detailed insights into successful backups, failed backups, and exceptions, ensuring transparency and facilitating easy monitoring.
- To efficiently manage backups, the solution should offer a dedicated platform with robust features for monitoring, scheduling, and verifying backups.
- This centralized management system will simplify backup administration.

- As the organization's needs evolve, scalability is crucial.
- The solution should be flexible enough to accommodate future growth and additional backup requirements without complications.
- Ensuring data security is of utmost importance, and the solution must incorporate strong measures to protect data during the backup and restore processes.
- Additionally, for Microsoft 365 data, the solution should offer a seamless option to back up the data to the on-premises data center, providing an extra layer of protection.
- Furthermore, there should be an alternative to back up the Microsoft 365 data directly to the cloud, offering data residency options that comply with regulatory requirements, including the ability to store data within the borders of the Republic of South Africa.

5. SERVER INFRASTRUCTURE

Production Compute (Server and storage) Requirements

The production compute platform must provide sufficient capacity for current workloads, high availability during host failure (Redundancy, Failover), and growth headroom for future academic, administrative, identity, security, and backup management services. The recommended design is a two- to three-node virtualization cluster sized for N+1 resilience.

Requirement Area	Minimum Production Requirement	Recommended Target	Design Notes
Cluster Size	2 physical hosts	3 physical hosts	Three hosts provide improved maintenance flexibility, failover capacity, and workload distribution.
Server Platform	Enterprise 2U dual-socket rack server	Server	Suitable for virtualization, enterprise workloads, distributed storage, and general compute use cases.
CPU	Dual processors per host, minimum 24 cores per processor	Dual Intel Xeon Scalable processors, 48 physical cores or higher per host	Size CPU allocation to allow for host failure while maintaining critical workloads.
Memory	256 GB RAM per host	512 GB RAM per host, expandable	Memory must accommodate production VMs, HA failover, hypervisor overhead, and growth.
Boot Device	Redundant SSD or mirrored boot media 512 Disk x2 RAID 1	Mirrored M.2/SSD boot set	Used for hypervisor installation only; production VM data must reside on shared storage.

Network Interfaces	Minimum dual 10GbE per host	Four 10GbE ports or dual 25GbE per host	Separate or logically segment management, VM, storage, vMotion/live migration, and backup traffic.
Management	Out-of-band server management	HDM with centralised UniSystem visibility	Required for firmware, hardware health, remote access, alerting, and operational support.
Power	Dual redundant power supplies	Dual hot-swappable PSUs connected to separate UPS-backed feeds	Power design must align with UPS runtime and generator availability.
Availability	Host clustering and shared storage access	N+1 compute capacity with live migration enabled	Cluster must sustain failure or maintenance of one host without service interruption to critical workloads.

Production Storage Requirements

The production storage platform must provide shared datastore capacity for the virtualization cluster, predictable performance for business workloads, and resilience against disk or controller failure. The design must separate production workload storage from backup repository storage to reduce operational and ransomware recovery risk.

Requirement Area	Minimum Production Requirement	Recommended Target	Design Notes
Usable Capacity	50 TB usable	100 TB usable scalable design	Final capacity must be confirmed after VM inventory, file data, database growth, and retention validation.
Storage Type	Hybrid SAN/NAS types of storages with SSD cache	Hybrid or all-flash shared storage with SSD performance tier	SSD cache improves latency for active workloads while HDD capacity supports cost-effective scale.

RAID Protection	RAID-6 or RAID-10	RAID-10 for performance-sensitive workloads; RAID-6 for capacity-focused tiers	RAID selection must balance write performance, rebuild time, usable capacity, and resilience.
Connectivity	10GbE iSCSI/NFS/SMB connectivity	Redundant 10GbE or 25GbE storage fabric	Storage paths must be redundant with multipathing enabled where supported.

Controller Design	Redundant controllers or equivalent HA architecture	Dual-controller storage array with non-disruptive failover	Required to avoid a single point of failure in the shared datastore layer.
Snapshots	Storage snapshots supported	Snapshot capability for short-term operational recovery	Snapshots are not a replacement for backup and must not reside as the only recovery copy.
Data Services	Thin provisioning and monitoring	Thin provisioning, compression, alerting, and capacity reporting	Deduplication and compression may be used where workload and vendor support allow.
Security	Role-based management access	RBAC, audit logging, secure management, and restricted administrative access	Storage management must be protected by general user and workstation access.

6. MIGRATION SERVICES

6.1. Discovery and Assessment

- Conduct an automated and manual discovery of all in-scope servers, storage, applications, and their interdependencies, using industry-standard discovery tooling.
- Produce an application dependency map identifying communication flows, shared services, and migration groupings (move groups).
- Assess each workload and recommend a migration treatment — e.g. live migration, replication-based migration, backup/restore, rebuild on new OS, physical-to-virtual (P2V) conversion, or retire — with rational per workload.
- Identify workloads running on end-of-life or unsupported operating systems and recommend whether they should be migrated as-is, upgraded during migration, or isolated, with the risks of each option stated.
- Identify licensing implications of the migration, including operating system, hypervisor, database, and application licensing on the new infrastructure.
- Provide a capacity and performance analysis that maps current compute, memory, storage, and IOPS consumption to the new infrastructure, confirming that the target platform is adequately sized with the stated headroom for [three] years' growth.

6.2.New Infrastructure Installation and Commissioning

- Perform rack-and-stack, cabling, and physical installation of the new server and storage infrastructure in accordance with the manufacturer's guidelines and the organisation's

datacenter standards.

- Install, configure, and patch the hypervisor platform, management tooling, and storage arrays to current stable firmware and software versions, following vendor best-practice and hardening guidelines.
- Configure storage layout (pools, LUNs/volumes, datastores, file shares), multipathing, and data protection features (snapshots, replication) per an agreed design.
- Configure the virtual networking layer, including VLANs, uplinks, and any required integration with the organisation's physical network. [State whether physical network switching is in or out of scope.]
- Integrate the new environment with existing supporting services: Active Directory/identity, DNS, NTP, monitoring, antivirus/EDR, and backup.
- Commission the backup solution for the new environment and demonstrate successful backup and restore of a test workload before production migrations begin.
- Conduct burn-in and acceptance testing of the new infrastructure, including redundancy/failover tests (power, storage path, network path, node failure), with documented results, before any production workload is migrated.

6.3. Migration Strategy, Design and Planning

- Produce a migration design describing the method(s) to be used per workload category (e.g. cross-cluster live migration, storage migration, replication, backup/restore, P2V), the tooling required, and the network paths used for data transfer.
- Develop a detailed migration plan covering move groups, sequencing, migration windows, resource requirements, and dependencies on the organisation's staff.
- Develop a detailed cutover runbook for each move group, including step-by-step tasks, owners, timings, validation checkpoints, and explicit rollback procedures.
- Produce a data migration strategy for storage and file data addressing initial bulk copy, incremental synchronization, final cutover synchronizations, and verification of data integrity.
- Where the source and target environments are in different locations, provide bandwidth calculations, estimated transfer durations, and any requirements for temporary links or physical media transport.

6.4.Migration Execution

- Execute server/workload migrations using proven, vendor-supported migration methods and tooling appropriate to the platforms involved, stating in the proposal which tooling will be used and why.
- Execute storage and file data migrations preserving file metadata, permissions (ACLs), timestamps, and directory structures, with a documented reconciliation of source versus target.
- Migrate databases with an agreed method per database (native backup/restore, log shipping,

replication, or storage-level migration), with pre- and post-migration consistency checks.

- Where physical servers are converted to virtual machines (P2V), validate driver, licensing, and application behaviour on the new platform before cutover.
- Perform all migrations with zero data loss; any deviation must be formally risk-accepted by the organisation in writing before cutover.
- Maintain full rollback capability for every workload, the source system must remain intact and restorable until formal acceptance of that workload is issued by the organisation.
- Manage and report on migration progress against the plan at agreed intervals, including a live migration tracker accessible to the organisation.

6.5.Testing, Validation and Acceptance

- Define and execute a test approach per workload, covering functional smoke testing, performance comparison against a pre-migration baseline, integration testing, and user acceptance testing support.
- Validate data integrity for all migrated data using checksums or equivalent verification and provide signed validation reports per move group.
- Formal acceptance criteria for each workload must be agreed before its migration begins; workloads are only deemed migrated once acceptance is signed off by the organisation.

6.6. Cutover, Decommissioning and Exit

- Plan and execute DNS, IP addressing, firewall, and integration endpoint changes required at cutover, coordinated with the organisation's change management process.
- Following an agreed retention period after acceptance, power down and decommission the legacy infrastructure, including removal from monitoring, backup, and licensing inventories.

Perform certified data sanitization or physical destruction of all storage media in the

- legacy environment in accordance with certificates of sanitization/destruction provided per asset.
- Where applicable, manage trade-in, buy-back, or environmentally compliant disposal of decommissioned hardware in accordance with applicable e-waste regulations, with disposal documentation provided. [State whether disposal is in scope or handled by the organisation.]
- Provide complete as-built documentation of the new environment, including architecture diagrams, configuration baselines, IP and storage layout schedules, credentials handover (via secure mechanism), and operational runbooks.
- Provide knowledge transfer and training sessions to the organisation's IT staff on operating and maintaining the new infrastructure, with a minimum of [x] structured sessions.

6.7. Post-Migration Support (Hypercare)

- Provide a hypercare support period of no less than 30 days following the final cutover, with

defined response and resolution targets for migration-related incidents.

- Conduct a post-migration review within 60 days of completion, covering performance against baseline, capacity utilization, and any outstanding optimization actions.
- Optionally, bidders may propose ongoing support or managed services for the new environment as a separately priced line item; this will not influence the evaluation of the core migration scope.

7. SERVICE LEVEL AGREEMENT (SLA)

The bidder will enter into an SLA that will be used to monitor and manage the service. The acceptance of any proposal shall only be confirmed with the conclusion of a written service level agreement between the College and the successful service provider, in terms of which the rights and duties of the parties are recorded, which agreement shall regulate the relationship between the parties.

Until such time that an appropriate service level agreement has been concluded between the Western TVET College and the successful service provider, no rights shall be conferred, nor shall any legitimate expectations be conferred to the successful Service Provider to carry out the works or services provided for in this call for proposals.

8. WARRANTY AND SUPPORT

- Three (3) years of Support and Maintenance 24x7, 2-hour Response.

The maintenance and support period shall commence upon successful implementation, testing, commissioning, and formal handover of the solution to Western TVET College.

- Assist with software license renewals throughout the contract period.
- Send monthly reports.
- Send monthly logs and errors.
- Provide necessary training/ skills transfer to Westcol TVET College ICT staff about the product.
- Assist with the updating of the Backup and Disaster Recovery plan policy.

9. BACKUP WINDOWS

- Incremental Backup Windows (hours) – normally, 10 Hours is good.
- FULL Backup Windows (hours) – 6 to 48 Hours.

10. RETENTIONS

- Daily Full and incremental – we keep for 4 weeks.

- Weekly Full – we keep for 4 weeks.
- Annual Full – We keep the financial year-end for 3 years.

11. PRODUCTION DATA

- The estimated amount of data currently stored is 80 TB.
- The total required storage capacity is 500 TB over three years.
- Average amount of data that changes each day – Estimated at 2% at most.

12. SKILLS REQUIREMENTS

The following soft skills are essential:

- Communication.
- Report writing.
- Relationship management

13. CONDITIONS

The awarded supplier will be required to demonstrate their Disaster Recovery Site prior to the final appointment.

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

14. PRICING SCHEDULE

Pricing and invoices

- All prices must be inclusive of 15% VAT for all registered VAT vendors.
- Thirty (30) days after receipt of the invoice should be allowed for payments to be made by the Finance Department.

NO.	Description	Once-off Price INCL. VAT
1.	Servers	R
2.	Storage	R
3.	Backup Solution	R
Grand total (INCL. VAT)		R

NO.	Description	Storage Size	Years	Total Annual Price INCL. VAT
1.	**Backup and Restore Solution Description**	**?**	Year 1	**R**
	Backup and Restore Solution Description	?	Year 2	**R**
	Backup and Restore Solution Description	?	Year 3	**R**
Grand total (INCL. VAT)				**R**

SUMMARY PRICING SHEDULE

NO.	Description	Total Price (INCL. VAT)
1	Servers, Storage & Backup Solution	**R**
2	Backup and Restore Solution Description (YR 1,YR 2 & YR 3	**R**
TOTAL BID (INCL. VAT)		**R**

Signature of person authorized to sign a tender: _____Date: _____