The University of South Africa invites suitably qualified service providers to participate in a Public Tender Process to provide the University with the Implementation of Infrastructure as a Service

Tender Specification Document

Tender Ref. No:	PT2020/15	Date of Issue:	August 2020

Contents

1. OVERVIEW

The University of South Africa, through its Open and Distance eLearning (ODeL) philosophy, is committed to providing access to its distance learners wherever they live or work. One of the strategies for meeting this goal is a stable, well supported network and data center environment that allows for delivery of services to both staff and students on all Unisa Campuses and at all regional offices. Unisa services over 350 000 students nationally and internationally, through online services and the regional infrastructure that is made up of 39 campuses and regional offices.

The purpose of this tender is to appoint a strategic partner that will provide a fully managed network and data center infrastructure. This will ensure that Unisa can accommodate the current and anticipated future business requirements as Unisa embarks on its digital transformation journey towards becoming a fully ODeL university. For purposes of this document, the fully managed infrastructure is split into two sections:

Section A:

- Network Infrastructure

Section B:

- Data Center Infrastructure

A. Network Infrastructure

The current network environment enables communication, research and learning services. The current architecture was designed based on best practices, i.e. to enable resiliency, redundancy, interoperability, and scalability. The deployment caters for many technologies which include, routing and switching, wireless networking, Data Centre, Voice over IP, Identity Services (Network Access Control) and Local Area Networking as part of ensuring the continuous operations of the Unisa Cisco network environment.

B. Data Center Infrastructure

The data center infrastructure is a combined set of hardware, software and facilities, to support the delivery of IT services. These servers hosted on-premises and cloud serves as an enabler of technology.

The components that make up the network and data center infrastructure have either reached their end-of-life or support.

2. PROPRIETARY AND CONFIDENTIAL INFORMATION

All material submitted in response to this tender shall become the property of Unisa. Any confidential information provided by a service provider in response to this Tender will be held in confidence and will only be used for the evaluation of this tender.

3. DEALING WITH THE UNIVERSITY OF SOUTH AFRICA

Service providers must not contact any member of Unisa with respect to queries they may have with this tender. The service provider shall not disclose any such information or specification, whether explicit or implied, to any third party without the written consent from Unisa.

Due to Covid-19 site visits to our data centres will not be allowed, all information pertaining to the data centre is provided. Bidders have an opportunity to request any additional information that will be required to prepare proposals

There will be no information session held, all questions must be submitted to tenders@unisa.ac.za by the **18 August 2020** and answers will be published on the tender website by **21 August 2020**.

4. TENDER SUBMISSION AND CLOSING DATE

The original and a soft copy of the tender must be submitted into the official tender box in a sealed envelope located in the Kgorong Building, Security Entrance, Preller

Street, Muckleneuk Campus, Muckleneuk Ridge, Pretoria. Please quote the tender reference number **PT2020/15** on the sealed envelope.

Closing date: 10 September 2020 @ 12:00

Tenders submitted late will not be accepted or considered.
Points will be awarded for Broad-Based Black Economic Empowerment.
The decision of the Unisa Management Committee on awarding a tender is final.

Unisa reserves the right to appoint, contract with and monitor the performance of any service provider it deems will offer the best service in line with its requirements, although it may not necessarily be the lowest Tenderer. Unisa also reserves the right, in its sole discretion, to re-advertise, not to retender or not to award the tender.

The tender awarded will be conditional and subject to successful negotiations and signing of a written contract, failing which Unisa reserves the right to withdraw the tender and to award the tender to another Tenderer without repeating the process.

5. Prequalification criteria

Tenderer must subcontract **minimum of 30%** of the value and scope of the contract to at least 51% of the designated groups as defined by the B-BBEE codes of good practice in order to advance the designated groups. Unisa will use other means of validation to confirm the B-BBEE status. The sub-contracted tenderer should not be the subsidiary company of the tenderer. Tenderer that fail to meet this criterion will be disqualified. Unisa will provide the tenderer with the list of ESD entities for training and development and skills transfer. Tenderer must provide a B-BBEE certificate of sub-contracted Tenderer and shareholder certificates.

The scope of subcontracting must cover the following areas:

- Solution design,
- Solution acquisition,
- Solution implementation and

- Solution maintenance and support

6. MANDATORY REQUIREMENTS

Mandatory requirements will include the following and must be labelled and submitted in the following order. **Failure to comply and submit any one of the documents will disqualify the submission:**

Annexure A1: Completed and signed Supplier List Application Form (F25) including the PSP form and bank account details from the bank. (www.unisa.ac.za/tenders)

Annexure A2: Resolution to sign on behalf of the tendering unit (www.unisa.ac.za/tenders)

Annexure A3: Current and valid original SARS Clearance Certificate

Annexure A4: Copy of company registration documents indicating list of shareholders / members from CIPC. Copies of share certificates must be included (excluding close corporations)

Annexure A5: Pricing template. (The pricing template must be completed)

Annexure A6: Reference Template

Minimum of **three** recent (not older than 3 years) contactable references from customers to which the tenderer has provided or is providing goods/services that are substantially **similar (size, nature & quantity)** to the goods/service required. If current references are provided these must be in place for a minimum of 3 years. Annexure A6 must be completed.

Annexure A7: Financial Statements

a. One set (2 years comparative figures) of the most recent audited Annual Financial Statements together with a signed Independent Auditor's Report or a signed letter from the Accounting Officer for Close Corporations must be submitted unless the reporting entity is exempted in terms of the new South African Companies Act from obtaining an Independent Auditor's Report. The exempted entity must then submit a signed Independent Reviewer's report or signed compilation

engagement (ISRS 4410) report from any recognised accounting professional body. The annual financial statement submitted must be within six months of the financial year-end to qualify for evaluation.

A complete set of Annual Financial Statements including the following:

- Independent Auditor's Report (Letter from an External Accountant/Accounting Officer for Close Corporations)
- Statement of Comprehensive Income (Income Statement)
- Statement of Financial Position (Balance Sheet)
- Statement of Cashflows
- Statement of Changes in Equity
- Notes to the Financial Statements

No summarized Financial Statements or Extracts of financial statements will be accepted.

b. Where the financial statements of the holding company are submitted, a signed letter be included from the holding company, on their letterhead signed by the CEO/CFO, that they would be liable if the subsidiary defaulted. This must be attached to the financials being submitted. Failure to submit such signed letter will disqualify the tender submission.

c. The financial statements should be submitted as a separate bound document.

Annexure A8: Unisa General Terms and Conditions of the tender (www.unisa.ac.za/tenders)

Annexure A9: IaaS Specification and Response Template

Annexure A10: SLA Response Template

Annexure A11: Letter of authority from the OEM; OEM local presence and/or footprint, local capability to support the proposed solution, empowerment of local companies.

Annexure A14: Bidders must provide a complete IaaS solution (inclusive of Section A – Network Infrastructure and B – data centre) partial solution will not be accepted.

Annexure A15: Sub-contracting Template

7. OTHER REQUIREMENTS

Supplier documents and information

Annexure B1: A valid B-BBEE certificate or proof of exemption from an accredited SANAS / IRBA verification agency / auditor. An affidavit certifying their total annual income and level of black ownership will be sufficient for EMEs and QSEs. Failure to submit the above will result in a zero score for B-BBEE.

Note: All documents submitted in support of this tender must be the documents of the tendering unit and may not pertain to different companies or units within a group. As an example, a tenderer cannot submit its own B-BBEE certificate, but the SARS certificate of its holding company.

8. PRICING

The tenderer must state whether the price quoted is fixed for the duration of the agreement or whether the price is subject to escalation. In the absence of an indication in this regard the price will be considered as fixed for the full period of the agreement.

- All pricing must be quoted in South African Rand (ZAR) including VAT.
- The pricing **must remain valid for 90 days** from the closing date of the tender.
- Pricing / costing template **must be completed** (Annexure A5)
- Any pricing not included in the pricing template will not be considered.

Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his tender, and any variance will render the contract null and void.

9. PAYMENT TERMS

The payment terms of the University are 30 days after receipt of goods and services and upon receipt of the required documentation. **No upfront payments will be considered.**

10. SUB-CONTRACTING

Sub-contracting will be allowed for this tender.

11. JOINT ARRANGEMENTS

No Joint Ventures will be accepted for this tender.

12. Pre-qualification

Only tenderers that meet all the mandatory requirements including the financial evaluation will proceed to stage 1 of the adjudication.

Stage 1 – Technical Evaluation (Functional and non-functional)

Tenderer response in Annexure A9: IaaS Response Template and Annexure A10: SLA Response Template supporting the assertion that the proposed solution meets the requirements as specified in Annexure A9: IaaS Response Template and Annexure A10: SLA Response Template.

The following scoring criteria will be used to evaluate each response:

Criteria	**Score**
None of the 4 criteria are met	1
1 to 3 criteria met	2
All 4 criteria met	3
All 4 plus One or more additional criteria met	4

Tenderers must meet a minimum of 90% in the technical evaluation in order to proceed to stage 2 of the evaluation.

Stage 2: Pricing and BBBEE

DESCRIPTION	POINTS
1. **Price** $Ps = 75\left(1 - \frac{Pt - P\min}{P\min}\right)$ Where: Ps = Points scored for price of tender under consideration Pt = Rand value of tender under consideration Pmin = Rand value of lowest acceptable tender	75
B-BBEE LEVEL	25

13. TENDER SPECIFICATION

The tender specification section for this document will be broken down into two sections, i.e. **Section A** – Network Infrastructure and **Section B** – Data Centre Infrastructure. Bidders are encouraged to propose a single IaaS solution for both sections to ensure seamless interoperability and ease of solution management.

Section A: Network Infrastructure

Service Layer	Data Center & Core Layer	Access Layer	Wireless	Management & Monitoring
Service Description	Enterprise Data Center & Core, Design Requirements Build & Implementation Managed Service	Local Area Network & Wide Area Network Network Access Control Design Requirements Build & Implementation Managed Service	Enterprise Wireless Design Requirements Build & Implementation Managed Service	Solution Management and Monitoring 24x7x365 Support Services

12.1 Network Infrastructure

This section entails requirements for a fully managed software defined network infrastructure platform that will form the complete network environment required to support ODeL within Unisa. The fully managed software defined network infrastructure will have the following components:

- Solution acquisition
- Solution design
- Solution implementation (including migration)
- Solution monitoring and management

12.1.1 Network datacenter and core – High Level As-Is

In preparation for digital transformation and for Unisa to be able to fully embrace ODeL the new ICT network infrastructure must be agile, flexible, resilient and scalable to meet ODeL requirements the next 5+ years.

The ICT Datacentre and core network infrastructure must be SDN-ready and offer a fully programmable and automated solution across all campuses and sites.

The proposed network must be managed as a software defined resource, with the ability to define an application's infrastructure requirements once off, and then choose where the application runs, i.e. on premises or in the cloud.

This consistency and automation translate into applications that are easier to scale, reduced deployment times and can seamlessly run anywhere with equal confidence with regards to security, performance, quality of service, and availability. To achieve this, the data centre network infrastructure must have the ability to centrally configure and manage physical and virtual network devices such as routers, switches and gateways in the data centre.

The proposed solution design and implementation must follow the Leaf-and-Spine design which will provide the ability to divide the network into various zones sharing a

common control plane. A high-level conceptual design can be seen in Figure 1, Leaf and Spine design.

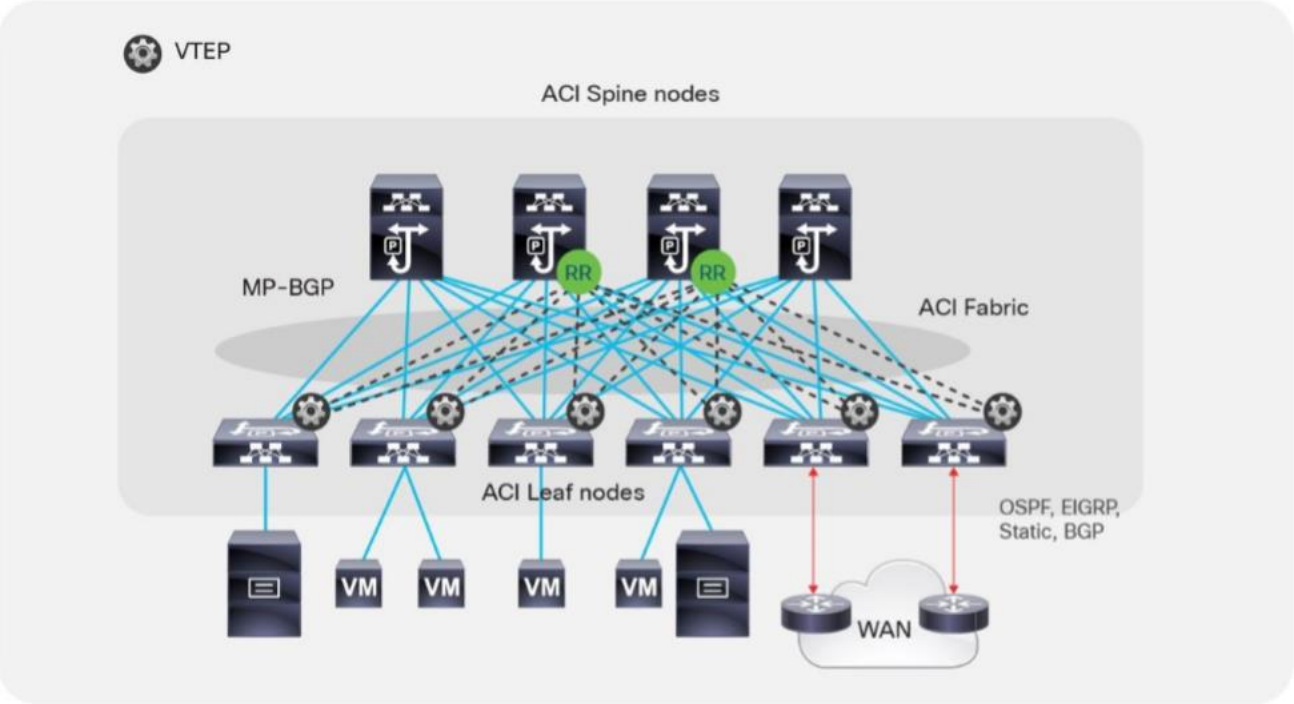

Figure 1 Leaf-and-Spine design

The spine nodes will be deployed in the Muckleneuk and Florida data centres and should the need arise, they can be extended to other offices depending on latency. During implementation and migration of services from the current environment existing networks must remain operational whilst the appliance refresh/upgrade is conducted on the spine nodes.

The spine node must provide a switching capacity of 40Tbps or greater.

The spine node must be modular with support of at least 4-line cards.

The spine node must cater for 100GE support and the support of VXLAN.

The spine node must cater for 100GE support and the support of VXLAN.

The spine node must have separate management, switching forwarding, data plane service interface cards and control plane service cards.

The spine node must cater for modular cooling fans in a 1+1 redundancy configuration.

The leaf node must support capacity of 2Tbps of larger

The leaf node uplinks must support capacity of 6 X 40GE or 6 X 100GE and downlinks should cater for 48 X 10GE.

The leaf node must support modularity with a redundant configuration of 1+1 and cooling fans need to support a 3+1 redundant modular configuration

The Software Defined Network (SDN) must provide the following functionality:

- Dynamically create, secure, and connect the Unisa network to meet the evolving needs of all applications.
- Speed up the deployment of workloads in a non-disruptive manner.
- Contain security vulnerabilities (or malicious content) from spreading across the network.
- Define and control policies that govern both physical and virtual networks.
- Implement network policies consistently at scale.
- Provide an element of quality assurance in a consistent manner for each deployment of devices and applications.
- Must support the stretching of VLAN across WAN. Note: Current latency equals to 5ms

12.1.2 Network data center and core – Design Requirements

The service provider will be responsible for the High-Level Design (HLD) of the proposed Network Data Center based on the specifications outlined below and the current architecture.

The successful service provider will need to analyse the current Unisa CISCO network data centre environment which must be migrated to the proposed environment. The service provider must indicate whether elements of the current environment can be repurposed into the proposed solution. These would include elements such as the current 10Gb Cisco Small Form-Factor Pluggable (SFP) modules.

The proposed design must allow for dual 40Gb interfaces between the proposed 2 spine nodes and 5 leaf nodes for Muckleneuk Campus, and for Florida Science campus the proposed design caters for 2 Spine nodes and 2 Leaf nodes with dual 40GB interfaces. The solution proposed must allow for 100Gb ready and service

providers must ensure that all proposals support the 100Gb design depending on the analysis and price points of the solution.

The proposed Network Data Centre solution should cater for a minimum of 60 * 40GB modules, 270 * 10GB Modules for both Muckleneuk and Florida datacentres. Service providers will be required to plan the migration of the current Data Center environment and / or the implementation of the Cloud Computing solution as outlined in this specification document. The HLD design of the current environment is outlined in Annexure B1 and is based on the Cisco Nexus 7000 and 5000 devices.

Based on the HLD, service providers will be required to provide a Low-Level Design (LLD) of the entire Network Data Centre which will provide for all the network, network security, wired and wireless components as outlined in this specification document. The LLD will provide the basis for the build component of the proposed solution.
The proposed solution must provide automation of repetitive tasks, reducing configuration errors with a centralized real-time health monitoring of physical and virtual networks. This must be done through visibility into application performance combined with intelligent placement decisions to enable faster troubleshooting.

The solution must enable connectivity for physical and virtual workloads with complete visibility on virtual machine traffic and provide compatibility and integration with Hypervisors without the need to add software to the hypervisor. The proposed solution must allow Unisa to insert and automate firewall, load balancers and other L4-7 services through application programmable interfaces (APIs) as outlined in sections 12.5 and 12.6

The solution must allow for the capture of all configuration changes required for audit and compliance tracking solutions. Detailed role-based access control (RBAC) granular fabric segmentation is required. Hardware-based security and the ability to eliminate of flooding from the fabric is essential.

The proposed solution must also allow for the ease of mapping application architectures into the networking configuration. Application agility must be part of the

proposal by providing management of application lifecycle from development, to deployment, to decommissioning in the shortest possible time.

Service providers must ensure that automatic application deployment and faster provisioning based on predefined profiles is part of the proposed solution that will allow continuous and rapid delivery of virtualized and distributed applications.

The proposed Data Center fabric must enable Unisa to move traffic from physical and virtualized servers, bring it in the best possible way to its destination and while doing so apply required services such as:

- Traffic optimization that improves application performance.
- Telemetry and analysis services that go beyond classic port counters.
- Overall health monitoring for what constitutes an application.
- Applying security rules embedded with forwarding.

The proposed LLD for the Data Centre environment must support the current deployment of threat management solution (DarkTrace) appliances with the ability to monitor and mirror multiple (5+) concurrent sessions per device. DarkTrace's Autonomous Response Technology called Antigena uses artificial intelligence and self-learning to determine the best possible action to take in the shortest time to effectively respond to cyber-attacks within the Data Centre. The proposed Data Centre design must ensure that the platforms are able to mirror all traffic to ensure effective visibility of the entire network within the current DarkTrace deployment. These devices are currently deployed in the Muckleneuk Data Center and provide visibility of the Data Centre and perimeter traffic.

The proposed design must cater for the current deployment of the perimeter security environment which is based on Checkpoint firewalls that are deployed in a three 3 clusters across the two main campuses, 2 clusters of 2 at the Muckleneuk and 1 cluster of 2 at the Florida Data Centers with dual 40Gb interfaces. The proposed solution must cater for the deployment of firewall cluster setup. Service providers must ensure total

integration with the CheckPoint environment without the need for 3rd party tools or application.

Unisa has a pair of F5 load balancers with Big bundle licenses that are deployed at the Muckleneuk data centre for hardware load balancing. Service providers must ensure total integration with the F5 environment without the need for 3rd party tools or application. The current deployment is primarily focused on the load balancing of services and workloads in the Data Centre, however service providers must identify how to fully use the various modules included in the licensing within the F5 devices to supplement network security and provide secure services within the Data Centre without duplicating these requirements with new services.

Unisa makes use of VMware and the proposed Data Centre design must support the current deployment of VMware that is deployed in both Muckleneuk and Florida Science Campus. The proposed solution must cater for stretched VLANS to support the VMware environment. The current interconnection between the Muckleneuk and Florida Data Centers is a Layer 2 – 10Gb service with a latency of 5ms. Additional information regarding this environment can be found in section 12.3 Compute / Storage

The proposed solution must provide Unisa with a holistic application-based solution that delivers flexibility and automation to enable Agile IT through the automatic fabric deployment and configuration with single point of management. This must be provided using either GUI or REST API.

The required data center solution must provide the capability to create portable configuration templates. The data center proposal must ensure seamless interoperability and support for the following environments as part of the proposed solution i.e. LAN, WAN, Wireless and Network Security. Service providers must ensure that the proposed solution must be cloud ready, support multi-tenancy, network security compliance, improved network traffic flows and visibility.

All tools and applications that are required for the successful implementation, management and support of the environment must be hosted in the current virtualized environment if appliances are not available.

Service Providers must ensure that the proposed solution must be flexible and scalable to meet requirements over the next 5+ years. Both the Data Center and network infrastructure must be implemented in a scalable, redundant and interoperable manner that takes advantage of open standards through application programmable interfaces (API), that will allow for better service previsioning with minimal development time.

12.1.3 Network Data Centre – Build / Implementation Requirements

The verified, vetted and completed HLD and LLD of the Network Data Center by service providers will allow for the commencement of the build / implementation phase of the project. It will be the service provider's responsibility to ensure that the entire build, testing and commissioning of the proposed Data Center is completed as per the agreed HLD and LLD.
Service providers must ensure that the proposed build / implementation includes elements that will have minimal impact to staff and students through effective change management, service transition and awareness campaigns.

The SDN solution must ensure that users are provisioned the same security access policy regardless of location and automation of network configuration and policies.
The SDM solution must have a capability to capture and provide a view of received signal strength indication (RSSI) for all end node wireless LAN variables for historic purposes.

The SDN solution must proactively identify WLAN issues, provide a suggestion to resolve and AI capabilities that will allow the ability to preempt future issues.

The SDN solution must be able to track each TCP and UDP flow on the Wireless LAN network, providing deep packet inspection and analysis showing delay between each step in any communication stream.

In order to provide a better overall user experience. The SDN solution must have capability to segregate users on the data plane into separate IP flows using hierarchical quality of service and class of service, matching traffic based on user and application profiles.

Authorization must be integrated into the network topology at the access layer edge, resulting in more secure and faster enforcement of security policies.

The solution must have a capability to capture first time authentications and authorizations, this information must be stored in a central repository. This pre-evaluated information will be used to onboard users faster during future authentications.

12.1.4 Network Data Center – Managed Service Requirements

Service providers must ensure that the Network Data Centre is fully managed and supported throughout the entire engagement. Service providers must indicate what platforms, tools and applications are required to fully manage and support the proposed environment. The proposal should allow for a 24/7/365 managed service that will provide Unisa the functionality to:

a. Improve security that will allow consistent implementation of policies across the entire network.
b. Have visibility of all devices that are connected to the network.
c. Perform network wide data collection and analysis.
d. Optimize cloud access to enhance the hybrid cloud environment.
e. Ensure reliable application performance and availability.
f. Provide visibility of customer experiences/trends, allowing for analysis.
g. Implement automated fault identification, fault prediction and analysis.
h. Do Reporting based on detailed management information (automated, scheduled and ad-hoc reporting)

The proposed solution must assist in defining adequate roles and responsibilities to provide a fully managed and supported environment.

The proposed solution must cater for a requirement of an SLA for an on-site mid-level qualified resource that will be responsible to provide support (including troubleshooting) for the Network Data Centre environment. This resource will be provided office space and communication devices to enable them to meet the Service Level requirements as outlined in this document. This resource will need to ensure all proposed management platforms are always accurately configured and updated. This resource must be onsite from 07:45 to 16:00 daily from Monday to Friday, but also be available after hours based on the requirements.

12.2 Access Layer: Wide Area Network (WAN) and Local Area Network (LAN)

The hybrid cloud deployment presents an opportunity for Unisa to redesign the WAN and LAN (Wired and Wireless) environment Software defined capabilities. Unisa currently makes use of the South African National Research Education Network (SANREN) to provide a layer 2 communication services between the Data Centre and remote sites. The SANReN also provides internet related services (as an ISP) to the Muckleneuk and Florida Science Campuses that are the two-internet landing/breakout points and serves all remote sites. Service providers must include in their proposal a complete Software Defined Wide Area Network (SDWAN) and Software Defined Access (SD-Access) solution that will enable seamless provisioning of on-premise and cloud services both the two Data Centres and remote sites.

13.2.1 LAN / WAN - High Level As-Is

Unisa WAN comprises of thirty-seven (37) regional offices, excluding Muckleneuk and Florida Science campuses. These offices range from a deployment of two (2) to more than twenty (20) network access switches, four (4) of these offices require fibre distribution devices. The details of each site network access required can be found in **Annexure B2 – Wide Area Network Topology.** The current wide area network has bandwidth speeds of between 30Mbp/s and 1Gbp/s with latency varying from 3ms to 30ms.

The proposed solution must cater for:

13.2.1.1 Modularity of campus top level switches and support at least 6 service slots.

13.2.1.2 Campus top level switches must support the VXLAN protocol.

13.2.1.3 Campus top level switches must have separate management, switching forwarding cards, data plane service cards and control plane service cards.

13.2.1.4 Backplane bandwidth that is 10Tbps or greater

13.2.1.5 Campus top level switches must natively manage the wireless network with a minimal value of 1000 access points and 10 000 users, without the need for an additional independent WLAN service blade.

13.2.1.6 The ability to configure QoS feature on campus top level switches.

13.2.1.7 Campus middle level switch needs to support a backplane bandwidth that is 2 Tbps or greater

12.2.1.8 Campus middle level switch must have the capability to natively manage the wireless network.

12.2.1.9 Campus middle level switch must natively manage configuration of all switches from a master switch within the network, without the need for a controller.

12.2.1.10 Campus middle level switch must cater for uplinks with capacity to handle 6 X 40GE or 6 X 100GE while downlinks should cater for 24 X 10GE.

12.2.1.11 Campus middle level switch must be able to detect abnormal encrypted and un-encrypted traffic.

12.2.1.12 Campus access switch msut support a backplane bandwidth of 200Gbps or greater.

12.2.1.13 Access switches must provide capacity of 4 X 10GE uplinks.

12.2.1.14 Access layer switches must provide capability to support a minimum of 3000 route entries, to cater for cellphone, tablets, IoT devices, etc.

12.2.1.15 Access layer switches must have capability to support uninterrupted POE

12.2.1.16 POE capability must supported over copper cable over a maximum distance of 150m

12.2.1.17 The proposed solution must cater for layer 3 functionality such as OSPF, ISIS and RIP should be supported access layer.

With the migration to a hybrid application service delivery model the Wide Area Network will need to provide Unisa with the ability to define intent based networking to all sites with low latency, high throughput and agile configuration of the WAN.

Service providers must ensure that the proposed solution provides the ability to intelligently route traffic to both on premise and cloud-based applications regardless of the geographical location of a Unisa site.

The proposed WAN solution must allow for traffic analysis, ease of management and a single platform for the management and reporting for LAN, WAN and Wireless environment. Service providers must propose how traffic analysis will be performed on these platforms.

The proposed design must ensure that Unisa can deploy and support applications with predictable end-user experience, and adequate security controls for any user or application.

The proposed solution must support the current cloud and application Software as a Service (SaaS) applications. The proposed solution must seamlessly extend the WAN to multiple public clouds with real-time optimization to improve performance for cloud-based applications such as Office365.

The proposed solution must provide costing for 1000 HPC hours for a 128 cores.

Service providers must ensure that the proposed design caters for increased network service agility as more of processing intelligence is moved from the data plane into the more abstract and programmable control plane.

Muckleneuk and Florida campuses (LAN) comprise of numerous buildings which requires distribution and core infrastructure. This requirement must be included in the proposed design.

The details of each site network access required can be found in **Annexure B3 – LAN / WAN Current.**

With the migration to a hybrid application service delivery model the Wide Area Network will need to provide Unisa with the ability to define intent based networking to all sites with low latency, high throughput and agile configuration of the WAN.

Service providers must ensure that the proposed solution provides the ability to intelligently route traffic to both on premise and cloud-based applications regardless of the geographical location of a Unisa site.

The proposed WAN solution must allow for traffic analysis, ease of management and a single platform for the management and reporting for LAN, WAN and Wireless environment. Service providers must propose how traffic analysis will be performed on these platforms.

The proposed design must ensure that Unisa can deploy and support applications with predictable end-user experience, and adequate security controls for any user or application.

The proposed solution must support the current cloud and application Software as a Service (SaaS) applications. The proposed solution must seamlessly extend the WAN to multiple public clouds with real-time optimization to improve performance for cloud-based applications such as Office365.

Service providers must ensure that the proposed design caters for increased network service agility as more of processing intelligence is moved from the data plane into the more abstract and programmable control plane.

Muckleneuk and Florida campuses (LAN) comprise of numerous buildings which requires distribution and core infrastructure. This requirement must be included in the proposed design. The details of each site network access required can be found in **Annexure B3 – LAN / WAN Current.**

12.2.2 LAN / WAN – Design Requirements

The proposed design must factor in all elements outlined in this specification document including all the information contained in the referenced and related Annexures to provide a fully managed Software Defined platform for communications.

Service providers must include in their proposal the Smart Campus requirements and components that will allow for various devices to be deployed seamlessly throughout the network. The inclusion of Internet of Things (IoT), mobile devices, and media-rich applications, on both cloud and on-premises require predictable and fast network performance. Unisa staff, students and visitors are using advanced smartphones requiring the network to be optimized to handle video and multimedia content for an enriched end user experience. Characteristics and functionality of the required SD-WAN/LAN must include, amongst others:

a. Centralized management of the SD-Access and SD-WAN platform.
b. Application layer policy enforcement and intelligent path control so that cloud optimized traffic can be routed straight to the Internet.
c. The ability to proactively manage network traffic at scale.
d. Improved security that will allow consistent application of policies.
e. Visibility of all devices that are connected to the network, as well as the end-user experience through traffic analysis on the access switches.
f. Reliable application performance and availability monitoring.
g. Re-use of existing cabling infrastructure, i.e. CAT5e and CAT6e.
h. Support for Multi-Gigabit Technology or 1Gb, 2,5Gb and 5Gb on CAT5e and CAT6e cables.
i. Traffic Analysis - Inspect traffic and application flows to help enforce network access policy and protect against attacks.
j. Consistent automation across WAN, WLAN, and wired networks. An example of this would be a new branch online deployment or roll out a new application policy within minutes using a single control pane and true network convergence.

k. Monitor and classify behaviors of devices and data that are critical to identifying problems using analytics and traffic analysis to classify traffic on the edge and inside the network.
l. Support new capabilities without major upgrades by leveraging existing infrastructure.
m. Support redundancy for business resiliency with switches that offer hot-standby N+1 redundancy in stacks, as well as redundant power and fans.
n. Consistent application performance across the network including Video through the application of Quality of Service (QoS).
o. Detect and set features to new devices such as IP phones, cameras, access points, or other devices. Automatically configurations such as QoS, VLAN, and security.
p. Power resiliency for IoT and other devices that are powered via PoE, even when the switch reboots.
q. The ability to provide advanced security features, Network as a Service (NaaS), Network Security Analytics, Identity Services, Encrypted Traffic Analytics, Network as an Enforcer (NaaE), mDNS gateway, and MACsec-256 link encryption.
r. Rapidly eliminate threats across the entire network (SD-WAN, SD-Access, wired and wireless) from a single dashboard/console.
s. Provide for Intent based networking for availability, agility, and policy segmentation to improve network availability and agility. The ability streamlines end-to-end network lifecycle management through automated design, implementation, and operation and advanced network assurance.
t. The ability to centralize and automate network design, policy, and provisioning of all wired and wireless networks.
u. Provide advisory services monitoring, SD-WAN & SD-Access to enable Implementation.
v. Provide cross-architecture capabilities that incorporate Network Optimization Services for SD-Access.
w. Provide both power and network access to a range of devices through a single standard CAT5e ethernet cable of 60 watts.
x. Redundant modular power supplies minimum 1100W.
y. Redundant modular fans.

z. 1Gb PoE interfaces on the entire network access switch.
aa. 4 X 1Gb / 10Gb LR (Single Mode) uplinks.
bb. Stackable data within a minimum throughput of 160Gbps throughput
cc. Stackable power.

Service providers must take note of the current hardware components that make up the entire WAN and LAN infrastructure currently at Unisa in Annexure B3 **12.2.3 Network LAN /WAN – Build / Implementation Requirements**

The verified, vetted and completed HLD and LLD of SD-Access and SD-WAN (including wired and wireless) by Service Providers will allow for the commencement of the build / implementation phase of the project. It will be the service providers responsibility to ensure that the entire build, testing and commissioning of the proposed data center is completed as per the agreed HLD and LLD.

Service providers must ensure that the proposed build / implementation includes elements, i.e. implementation plans and/or transitioning plans that will have minimal impact to staff and students through effective change management, service transition and awareness campaigns.

All solution builds and implementations must be jointly vetted and certified by own equipment manufactures and implementation partners that will be provided to Unisa for deliverable sign-off.

12.2.3 Network LAN / WAN – Managed Service

Service providers must ensure that the Network LAN / WAN is fully managed and supported through the duration of the entire engagement. Service providers must indicate and propose platforms, tools and applications that are required to fully manage and support the proposed environment. Service providers must also indicate where existing platforms and licenses can be utilised in the provisioning of solutions that would be utilized to provide a managed service. The proposal should allow for a 24/7 managed service that will provide Unisa the functionality to:

a. Improve security that will allow consistent application of policies across the entire network.
b. Have visibility of all devices that are connected to the network, as well as the end-user experiences.
c. Perform network wide data collection and analysis.
d. Optimize cloud access to enhance the hybrid cloud environment.
e. Ensure reliable application performance and availability.
f. Provide visibility of customer experiences/trends, allowing for analysis.
g. Implement automated fault identification, fault prediction and analysis.
h. Do reporting based detailed management information for availability, capacity management and inventory.

The proposed solution must assist in defining adequate roles and responsibilities to provide and fully managed and supported environment.

The proposed solution must cater for a requirement of an SLA for an on-site mid-level qualified resource that will be responsible to provide support (including troubleshooting) for the SD-WAN and SD-Access platform. This resource will be provided office space and communication devices to enable them to meet the Service Level requirements as outlined in this document. This resource will need to ensure all proposed management platforms are always accurately configured and updated. This resource must be onsite from 07:45 to 16:00 daily from Monday to Friday, but also be available after hours based on the requirements.

12.3 Wireless

12.3.1 Wi-Fi High Level As-Is

Service providers must propose a Wireless infrastructure solution that is designed to be scalable, secure and reliable. Unisa offers many services and has many clients that make use of the current wireless network infrastructure. The current solution allows for multiple SSID’s that provide access to various user groups through access control lists based on various types of authentication including MAC, PSK and Cisco Identity Services linked to Microsoft Active Directory.

See Figure 1 for an illustration of a high-level proposed design of the wireless network.

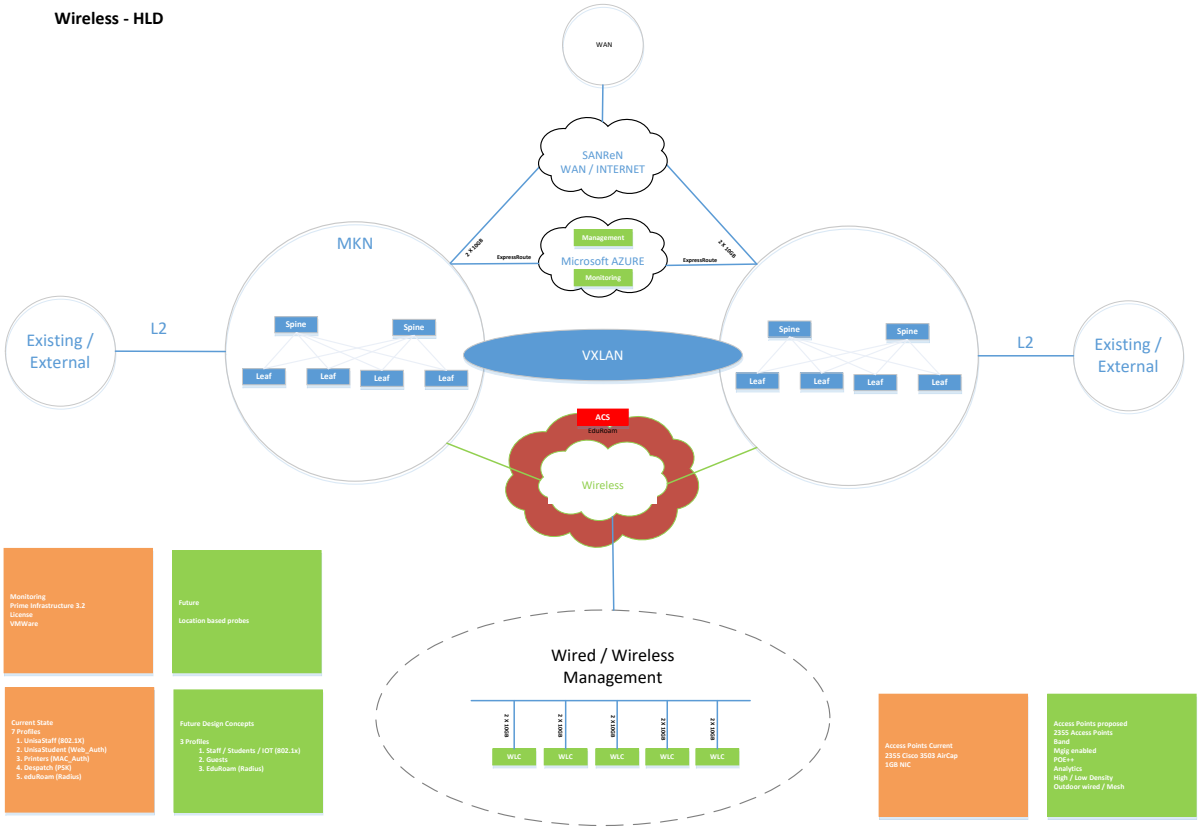

Figure 1: Wireless network – Proposed high-level design

Service providers must propose a Wireless infrastructure that is designed to be scalable, secure and reliable.

Wireless access controller:

The wireless controller must have capacity to manage 4000 access points while simultaneously supporting 64 000 users.

The backplane capacity of the wireless controller must be equal to or greater than 40Gbps and must support 2 X 40GE and a minimum of 8 X 10GE interfaces.

The power redundancy on the wireless controller must support an arrangement of 1+1. and access points must support at least 4X4 MU-MIMO mode and 802.11ax.

Indoor Wireless Access Point:

Must support a maximum of at least 5Gbps bandwidth

Access points must support an intendent scan feature, which can be used to shield the noise and optimize the wireless signal.

Access Points must have the ability to bind two radios, providing more bandwidth to end points

Access Points must have the ability to support IOT protocols.

Access Points must support at least 2 ports with the feature to logically binding these ports.

Access Points must support at least 4X4 MU-MIMO mode and 802.11ax.

Outdoor Wireless Access Point:

Outdoor wireless access points must support a maximum bandwidth of 5Gbps

Outdoor wireless access points must carry an IP68 rating.

Outdoor wireless access points must support at least 2 physical ports with the capability to logically bind these ports.

12.3.2 Network Wireless / Wi-Fi – Design Requirements

Service providers must propose a wireless network design that will allow Unisa to leverage the current and future use of the wireless network effectively and seamlessly as would be the case of the wired network as outlined in Section 12.2 – LAN / WAN.

The proposed solution should cater for as few as possible SSIDs to be broadcasted to allow for the secure, simple and managed wireless network required to continue providing services currently available on the Unisa Wireless Network. These include:

- Staff (Unisa Device): Provides full access to all Unisa services.
- Staff (Staff Device): Provides limited access to Unisa services.
- Student (Student Device): Provides limited access to Unisa services.
- Printers: Makes use of MAC authentication to deliver printing services to staff.
- Dispatch: Makes use of PSK for limited access to Unisa services.
- Council (Non Unisa Devices): Provides full access to all Unisa services.
- Guest (Non Unisa Devices): Provides limited access to Unisa services.

Service providers must provide a solution that is Wi-Fi 6 ready to deliver high data rates more consistently in typical Wi-Fi environments, with the focus on key performance indicators that improve Quality of Experience (QoE).

The solution must provide for Ultra-High-Density (UHD) environments with 200-500 users each carrying or wearing three or four 802.11 clients that all require network resources concurrently. With the increased adoption of real-time applications such as 4K video and augmented or virtual reality (AR/VR) being the foundation of digital transformation, the solution must be capable of incorporating all these requirements.

In the IoT space where devices are converging with low-complexity and low-power devices such as HVAC, asset tags, and cameras to support a Smart Campus in the future, the solution must provide for ultra-reliable, low-latency communications.

The proposed solution for wireless must ensure that the devices support more clients in dense environments and must provide a better experience for typical wireless LAN networks. The proposed solution must provide a more predictable performance for advanced applications such as 4K or 8K video, high-density high-definition collaboration apps, all-wireless offices, and the Internet of Things (IoT).

The proposed solution must ensure that the solution is backward compatible to ensure support for all the mandatory 802.11a, b, g, n, and ac modes of operation. The

proposed solution must ensure that Wi-Fi 6 Access Points and clients are backward compatible with legacy APs and clients.

Unisa currently has 2600 wireless access points nationally and the proposed solution must be based on this current deployment.

The proposed design must cater for the following minimum requirements:

a. In order to modernize the wireless LAN, it must be upgraded from 802.11n to 802.11ac Wave 2 that will enable wireless APs that can support connectivity of up to 2.5Gbps, i.e. 1.7 Gbps of effective throughput.
b. Next-generation programmable wireless LAN controllers (WLC) must be able to support up to 64K concurrent users and 40G per WLC.
c. Leverage existing authentication servers to handle increased capacity (CISCO Identify services engine).
d. Scalable Wi-Fi provisioning, e.g. for high-density and traffic burst scenarios.
e. Current solution offers rich-content media communication with devices every 20 meters. All proposals must include the ability to identify coverage, densification and latency issues. There are currently 2600 wireless access point deployed at Unisa.
f. Connection must be scalable from current 10Gb to 40Gb in the future and eventually to 100Gb on the wireless controller environment.
g. A single SSID that provides functionality for profile/identity management.
h. Refined policy control e.g. types of user, hours of access, type of connection, type of device used to connect.

12.3.3 Network Wireless – Build / Implementation Requirements

The successful completion of the HLD and LLD of the Network Wireless Infrastructure by Service Providers will allow for the build / implementation phase of the project. It will be the service provider’s responsibility to ensure the entire build, test and commissioning of the proposed wireless network infrastructure is completed as per the agreed HLD and LLD.

Service providers must ensure that the proposed build / implementation includes elements that will minimize the impact to staff and students through effective change management, service transition and awareness campaigns.

12.3.4 Network Wireless – Managed Service Requirements

Service providers must ensure that the Network Wireless solution is fully managed and supported through the entire engagement. Service providers must ensure that the wired and wireless infrastructure platforms, tools and applications are the same and that multiple management solutions will not be allowed as part of the proposed solution. The proposal should allow for a 24/7 managed service that will provide Unisa the functionality to:

a. Improve security that will allow consistent application of policies across the entire network.
b. Provide visibility of all devices that are connected to the network, as well as the end-user experiences.
c. Perform network wide data collection and analysis.
d. Optimize cloud access to enhance the hybrid cloud environment.
e. Ensure reliable application performance and availability.
f. Allow for visibility of customer experiences/trends, allowing for analysis.
g. Implement automated fault identification, fault prediction and analysis.
h. Do reporting based detailed management information to cater for
    i. Availability
    ii. Capacity management (including throughput)
    iii. Inventory
    iv. Coverage
    v. End user experience
    vi. Support

The proposed solution must assist in defining adequate roles and responsibilities to provide a fully managed and supported environment.

The proposed solution must cater for a requirement of an SLA for an on-site mid-level qualified resource that will be responsible to provide support (including

troubleshooting) for the Wireless Network platform. This resource will be provided office space and communication devices to enable them to meet the Service Level requirements as outlined in this document. This resource will need to ensure all proposed management platforms are always accurately configured and updated. This resource must be onsite from 07:45 to 16:00 daily from Monday to Friday, but also be available after hours based on the requirements.

First time authorizations and authentications should be stored in a central database, containing unique device and network topology information. This pre-evaluated information will be used to onboard users faster during future authentications.

12.4 Network Cabling Infrastructure

The successful service provider will be required to provide all network cabling including, but not limited to CAT5, CAT6 and Fibre infrastructure nationally at all offices for the duration of the contract. The service needs to adhere to the following high-level services nationally as outlined below:

- Repair of network cables – 3 days
- Installation of network points (1-20) – 5 days
- Installation of network points (21-100) – 15 days
- Projects to be determined based on requirements

Unisa based its current infrastructure on the Krone cabling technology and service providers will be required to ensure that all costing supplied in this process is based on this. Based on the averages or the last few years it is estimated that 1000 new network points are required and 1000 network points are repaired per year.

Baseline costing (unseen) provided through this process will be used for the first years of the contact where after inflation linked increases as agreed upon will be used.

Bidders can quote on 50 man hours for cabling.

12.5 Monitoring and management

Unisa has implemented a Technical Operations Center, however network specific management and monitoring tools must be part of the proposed solution. Service providers must indicate whether different tools will be required for data center, WAN, LAN and Wireless.

The proposed management solution must ensure that Unisa can see the entire network as a whole. To ensure automation the solution must allow for the future provisioning and devices based on pre-determined policies across the wired and wireless network. The management system must enable the simplification of the design, provisioning, and configuration management of the entire network from a centralized policy-based dashboard.

The purpose of the management platform is to optimize end user and application experience in a hybrid cloud model securely with integrated comprehensive security. The proposed solution must provide a complete view of users, devices and applications to enable end-to-end management of the network infrastructure. The management platform must enable faster troubleshooting of problems using analytics.

Service providers must ensure that Unisa is able to route traffic between source and destination efficiently across LAN and WAN to leverage our hybrid cloud delivery model of software and applications. It is essential that a consistent user experience is achieved with insights and analytics into user and application behavior

The proposed solution must ensure and provide the ability to report certain levels of compliance and regulatory requirements.

The tool must provide the following:

- Capacity planning to provide visibility on how devices within the network are being utilized.

- The ability to track how usage pattern trends change on the network. Usage pattern trends may include clients, devices, bands, or applications.
- The ability to provide reports about network operations, such as upgrade completions or provisioning failures.
- Reports that provide the overall health of the network through reports.
- The ability to create custom dashboards for monitoring the network infrastructure. The dashboards should be able to contain one or more dashboard widgets, that include charts, tables, geographic maps, and other types of information.
- Inventory management.
- Change and configuration management (hardware, firmware, OS).
- Visibility of customer experiences and analysis per access wireless point.
- As wireless network traffic increases, traffic forwarding without bottlenecks must be ensured.
- Simplification of Wi-Fi management.
- Implement plug-and-play of switches and APs to reduce deployment costs.
- Automated fault identification, fault prediction and analysis.
- All management and monitoring tools must support deployment on a virtualized and /or cloud platform.

Service providers must ensure that all proposed onsite resources are responsible for accuracy and updating of all management platforms provided through this process to ensure proper network management is achieved.

Section B: Data Centre Infrastructure

12.6 Compute

The current compute (servers) are connected with 10GB network interfaces including Fabric Extenders, short and long-range network interfaces. The proposed solution must able to:

a) Support the short and long-range network interfaces, and no Fabric Extenders will be accepted.

b) Be compatible with the Hybrid (private and public) cloud model.
c) Move workloads to and from the cloud and on-premises environments.
d) Move workloads to any cloud services or on-premises.
e) Must be able to provide equipment above the CPU industry average capacity as per the response template.
f) able to support the latest Microsoft, Linux environment.

The proposed solution should cater for demand and scalability, provide equipment for growth for the next 5 years, and allow Unisa to come back on-premises anytime. Furthermore, it must:

g) Ensure that Unisa ICT Infrastructure always integrate with the current Unisa application systems and future new applications.
h) Must be compatible with the current version of VMWare ESXi (6.5).
i) Must be able to cater for VMWare Licensing limited to 298 processors.

12.7 Storage

The current SAN (Storage Area Network) comprises of:

12.7.1 Compellent Solution

This solution was procured in 2013

MKN & FLO: 4 x SC8000 controllers with a combination of SC220 & SC200 Arrays with is tiered
MKN 500TB (Tiered)
FLR 280TB (Tiered)

12.7.2 HP Nimble Solution

This solution was procured in 2018 with 3-year maintenance and support

HF60(100TB Usable - MKN) + 2 x FC Switches SN6000B / 16gb x 48 port
HF40(100TB Usable - FLO) + 2 x FC Switches SN6000B / 16gb x 48 port

12.7.3 Backups

Backup Tape Libraries - MKN: (TL 4000 x 2) with 4 x LTO-6 Drives each / FLO: (TL4000 x 1) with 4 x LTO-4 Drives

12.7.4 Storage

The solution was procured in 2013

Muckleneuk 150TB

Florida 80TB

POWERVAULT MD3600F
POWER VAULT MD1200
POWER VAULT MD1200
POWER VAULT MD1200
POWERVAULT MD3600F
POWER VAULT MD1200
POWER VAULT MD3660F

12.7.5 StorSimple 8600

The solution was procured in 2017:

Muckleneuk 30TB

12.8 Virtualization Platform

12.8.1 VMWare 6.5

UNISA VMWare HDWare environment overview					
Location	**Cluster Name**	**No. of Host Servers**	**Dell Server Type**	**Number of VM's(Pwr ON)**	**Storage (Connected to)**
Pretoria - Muckleneuk	Production	22	M820	511	1. DELL Compellent and HP Nimble SAN via Fibre Channel switches 2. StorSimple Hybrid Device via iSCSi
	DMZ	8	M820	167	
	AVAYA	6	R720	28	Internal Server Storage
	Library	1	R720	3	Internal Server Storage

	Proxy	2	R720	9	Internal Server Storage
	Network Security	1		?	Internal Server Storage
Roodepoort Florida	Production	8	M820	104	1. DELL Compellent and HP Nimble SAN via Fibre Channel switches
	DMZ	4	M820	7	
	DEV	2	M820	43	
	AVAYA	3	M820	19	
	Proxy	1	R520	4	Internal Server Storage
NB: 1. There is One Virtual VCenter per site. 2. There is a 10GB backbone between the 2 sites					

12.9 Technical Operations Center

Service providers must propose a technical operations center solution that must provide the following functionality

12.9.1 Provide end to end monitoring of all infrastructure components stipulated in this specification document

12.9.2 Provide end to end monitoring of all applications within the environment

12.9.3 Provide end to end monitoring and reporting of the health of both infrastructure and applications

12.9.4 Provide end to end trend analysis and capacity planning

12.9.5 Provide end to end monitoring and reporting of end user experience

12.9.6 Provide capability and functionality to monitor real user usage trends and KPI's

12.9.7 Provide capability and functionality to visualize end user transactions in real time

12.9.8 Provide capability and functionality to monitor end user experience of cloud hosted applications

12.9.9 Provider end to end monitoring and reporting on a web driven application that shows performance indicators, system and application health on an executive level

12.9.10 Provide end to end monitoring and reporting on a web driven application that shows performance indicators, system and application health on an operational level

12.9.11 Provide an end to end application centric infrastructure monitoring

12.9.12 Provide visibility of all problems and events associated with an application or set of applications

12.9.13 Provide ability to visualize and easily drill into any tier (web, database, application, network, etc.)

12.9.14 Provide ability to visualize information about the underlying infrastructure affecting a particular tier of the application

12.9.15 Provide an end to end capability and functionality to simulate user experience

12.9.16 Provide capability and functionality to test mobile and web application performance

12.9.17 Provide capability and functionality to isolate and resolve performance problems in cross platform systems

12.9.18 Provide capability and functionality to test a range of enterprise environments without changing test scripts

12.9.19 Provide end to end deep dive diagnostics

12.9.20 Provide capability and functionality to automatically discover and map application topology

12.9.21 Provide capability and functionality to monitor key business transactions for each defined or discovered application

12.9.22 Provide capability and functionality to drill down to view trace details of the application flow as well as the code level stack at run time

13 SERVICE LEVEL AGREEMENT

The service level agreement (SLA) covers all the equipment that will be deployed within Unisa offices, i.e. Muckleneuk and Florida Science Campus and regional offices.

SLA performance will be measured in accordance with the service provider's ability to restore service within the allocated and agreed upon time.

To eliminate ambiguity, mean time to restore (MTTRv) will be defined as follows:
the mean time taken from when the call is logged, to when the fault is cleared on a permanent basis.

13.1.1 Network Infrastructure

#	Layers	Office Location	SLA Requirement
1	Data Centre and Core	Muckleneuk Campus Florida Science Campus	4 hours
2	Access Layer	All Unisa offices	6 hours
3	Wireless	All Unisa offices	6 hours

****SLA requirement – Maximum time allowed to restore services***

13.1.2 Data Center

#	Layers	Location	SLA Requirement
1	Compute	Muckleneuk Campus Florida Science Campus	4 hours
2	Storage	Muckleneuk Campus Florida Science Campus	4 hours
3	Backup	Muckleneuk Campus Florida Science Campus	4 hours
4	High Performance Computing	Muckleneuk Campus Florida Science Campus	4 hours

****SLA requirement – Maximum time allowed to restore services***

13.1.3 Network Cabling

#	Scope description	Location	SLA Requirement
1	0 – 10 network points	All campuses	40 hours
2	11 -50 network points	All campuses	80 hours
3	50+ network points	All campuses	240 hours

****SLA requirement – Maximum time allowed to complete installation***

13.1.4 Operational effectiveness

The successful service provider must adhere to the operational service level agreements for both the data center and network infrastructure.
The prioritization of calls will be based on the Information Technology Service Management (ITSM) process that will classify calls according to priority and severity.

13.1.4.1 Incident Support – MUKN & FLO Data Center

Service provider must make available skilled resources in all layers that must be available 24 hours a day, 7 days a week for the two (2) data centers (MUKN &FLO).

Service provider must adhere and meet the following response times for incidents categorized under the different levels of severity and priority.

- Priority 1, respond within 30 minutes,
- Priority 2 calls, respond within 60 minutes,
- Priority 3 calls, respond within 2 hours and
- Priority 4 calls respond within next business day (NBD).

13.1.4.2 Incident Support – Remote offices

Service provider must have a resource that can be dispatched to remote offices 8 hours a day, 5 days a week.

Service provider must adhere and meet the following response times for incidents categorized under the different levels of severity and priority.

- Priority 1, respond within 30 minutes,
- Priority 2 calls, respond within 60 minutes,
- Priority 3 calls, respond within 2 hours and
- Priority 4 calls respond within next business day (NBD).

13.2 Office locations

Unisa has 39 campuses and regional offices nationally that will form part of this contract. Service Providers must take cognizance of the geographical dispersion of the various offices when determining the response to the service level agreements.
Below is a list of all Unisa Offices, addresses – and where available GPS Coordinates°– of all Unisa offices and campuses that are referenced within this document. The service provider must support all the offices and pricing must be provided based on location and service level agreement.

#	Regional Site	Address	GPS Co-ordinates:
	Limpopo		
1	Makhado	87 Krogh Street, Louis Trichardt	-23.040621, 29.907403
2	Giyani	Office no 11, Masingita Complex, Giyani Road	-23.31098, 30.694711
3	Polokwane Registration	23 Landros Mare Street, Polokwane	23°54'53.05"S 29°27'12.52"E
4	Polokwane Library	29 Landros Mare Street, Polokwane	23°54'58.28"S 29°27'13.67"E
	Mpumalanga		
5	Middelburg	Town Square Building, Cnr Walter Sisulu and Bhimy Damane Streets, Middelburg	-25.764081, 29.456202
6	Nelspruit	31 Brown Street, Nelspruit	-25.471527, 30.977441
	KZN		
7	Durban Registration	230 Stalwart Simelane Street, Durban	-29.84978, 31.030093
8	Durban Boland Bank	221 Dr Pixley Kaseme Street, Durban	-29.856901, 31.028287
9	Durban Bright Side	251 Mahatma Ghandi Road, Point, Durban	-29.867934, 31.041154
10	Pietermaritzburg	1 Langalibalele Street, Pietermaritzburg	-29.610658, 30.370776
11	Richards Bay	Block C, Via Verbana, Veldenvlei, Richards Bay	-28.754548, 32.043686
12	Newcastle	Cnr Sutherland & Harding Streets, Newcastle	-27.759944, 29.931744
13	Wild Coast	Unisa - Wild Coast Sun	-31.051042, 30.210881
	Eastern Cape		
14	Mthatha	32 Victoria Street, Mthatha	-31.592683, 28.788332
15	East London	10 St Lukes Road, Southernwood, East London	-33.001119, 27.896932
16	Port Elizabeth	Greyville House, Cnr Cape Road, Ring Road and Greyville Street, Green Acres, PE	**-33.951957, 25.578253**
	Western Cape		
17	Parow	15 Jean Simmons Street, Parow	-33.908017, 18.593835

#	Regional Site	Address	GPS Co-ordinates:
18	George	1 Joubert Plaza, 100 Meade Street, George	-33.96285, 22.45878
	Midlands		
19	Bloemfontein	2nd Floor NRE Building, 161 Zastron Street, Westdene, Bloemfontein	
20	Kroonstad	1st Floor NFS Building, 36 Brand street, Kroonstad	-27.663627, 27.232854
21	Kimberley	Northern Cape Mall, Suite 62, Memorial Road, Kimberley	-28.756886, 24.764135
22	Potchefstroom	20 Auret Street, Potchefstroom	-26.70498, 27.090762
23	Mafikeng	29 Main Street, Mafikeng	-29.110748, 26.20677
24	Rustenburg	Forum Building, C/O Steen and oliver Tambo Roads, Rustenburg	-25.67814, 27.235236
	Gauteng		
25	Midrand SBL	Cnr Janadel and Alexandra Avenue, Midrand	-25.991021, 28.120869
26	Florida	Phapha Building, 5th Floor, Science Campus, Florida	-26.158842, 27.904002
27	Johannesburg	Bram Fischer Building, 29 Rissik Street	-26.206313,28.042324
28	Ekurhuleni	Corner R51 and Brazil Roads	-26.144247, 28.397491
29	Vereeniging	Hangar Building, First floor, corner of Rhodes and Voortrekker streets, Vereeniging	-26.668141, 27.932761
30	Sunnyside North	Building 13 and 14, Sunnyside Campus, Corner of Justice Mahomed and Steve Biko Streets, Sunnyside	-25.758764,28.200398
31	Muckleneuk Campus	Preller street, Muckleneuk Ridge, 0002	-25.76776, 28.199158
32	Skinner East	360 van der Walt Street, Pretoria 0002	-25.750915, 28.193683
33	Skinner West	263 Nana Sita Street, Pretoria 002	-25.750773, 28.191602
34	Sunny side Registration	139 Joubert Street, Pretoria 0002	-25.757991, 28.197623
35	Unisa Little Theatre	287 Nana Sita Street, Pretoria 002	-25.750822, 28.192342
36	Brooklyn	342 Giovanetti Street, Pretoria 0181	-25.773893, 28.236051
38	Lenasia	House 1, South East Metro Complex, Route K43, Lenasia	-26.355611, 27.851667
39	Honeydew		
40	Ormonde	2 Vinton Road, Ormonde, Johannesburg	-26.243058, 27.997156

Service providers must provide a list of the companies points of presence nationally, which will assist in determining its ability to comply with the proposed service level agreements stated within this document.

13.3 Quality standards

Due to the extensive requirements of this agreement all service providers must provide the quality standards they comply with, as well as proof thereof. Bidders must provide valid certificate(s) issued in the bidder's name containing accreditation Details and validity period.

The following standards must be submitted as part of the tender response:

- The bidder must be an accredited Cloud Service Provider and must have the ISO certification system of international standardization organizations.
- ISO 9001:2015 Quality management system.
- ISO 27001:2013 Information security management
- ISO 27018:2014 Personnel data protection
- ISO 22301:2012 Business continuity system standard

Note: All certificates must be in writing, dated, signed and on a letterhead of the entity that issued the letter.

13.4 Client / Service Provider SLA Meetings

Service providers must commit to monthly service level agreement meetings with Unisa where incidents, breaches of SLAs and any other matters related to this agreement must be discussed. This is essential to ensure accurate reporting and feedback mechanisms throughout the duration of the contract.

13.5 General Responsibilities of Service Provider

13.5.1 Service provider must implement the contract in line with the scope of work outlined in this document, taking into account necessary adjustments post the negotiation and contracting process.

13.5.2 Service provider will be accountable for the provision of an end to end solution including migration, implementation, quality assurance, change management, rollout, solution maintenance and support services.

13.5.3 Service Provider will be held responsible for the optimal functioning of the solution, including the high performance of the solution in line with service level standards.

13.5.4 Service Provider must ensure that, for the duration of the contract, adequate, certified and qualified resources – in line with the proposed implementation roadmap and appropriate functional requirements – are deployed to deliver the required functions within the stipulated service level standards, taking into consideration the expected business outcomes, the functional requirements, the size of the institution and industry best practices.

13.5.5 Service Provider may only change its core Service Delivery Management team assigned to the contract at inception, after consultation with the university.

13.5.6 Service Provider must provide in advance the details of its employees that will be working during the contract period for the purposes of enabling the necessary clearance and access (e.g. security clearance, non-disclosure agreements and access to premises).

13.5.7 The Service Provider may be required to be in possession of valid security clearances to the level determined by the University commensurate with the nature of the activities they are performing or involved in. The cost of obtaining suitable clearances is for Service Provider's account.

13.5.8 When requested upon to do so, the Service Provider must supply and maintain a list of personnel involved on the contract indicating their clearance status.

13.5.9 The service provider must ensure proper management of all documents related to the contract, for audit purposes. The service provider must ensure that documentation and/or reports submitted to the university are of good quality and includes relevant stakeholder consultations and communications during the documentation compilation.

13.5.10 The service provider must inform Unisa of changes in its ability to render services as defined in this document. This includes and is not limited to, changes in partner status that may compromise the service provider's ability to provide services as per the requirements of a back to back agreement with the own equipment manufacturer (OEM).

13.5.11 Although no employee-employer relationship exists between the university and the service provider's resources, the service provider and its resources must adhere to the university's policies (e.g. health and safety, physical security).

13.5.12 The service provider will be responsible for its own travelling, parking and accommodation costs incurred in the discharging of its services. The university will not accommodate any claims whatsoever for travelling, parking and accommodation.

13.5.13 The service provider must ensure the continuous transfer of knowledge and skills to the university resources in cases where the service provider and university resources work alongside each other collaboratively to ensure success.

13.5.14 Where required, services may be performed by the service provider and its partners after hours at no cost to the university (e.g. scheduled maintenance windows, resolutions of major incidents, etc.).

13.5.15 Service Provider must provide adequate toolsets to deliver the required functions within the stipulated service level standards, taking into consideration the expected business outcomes, the functional requirements, the size of the institution and industry best practices.

13.5.16 Service Provider must provide a knowledge transfer plan which shall include, but not limited to, the following:

13.5.16.1 Knowledge transfer of tasks / activities / actions taken during the project implementation.

13.5.16.2 Project timeline required by the university staff to work alongside service provider or its partners during the project.

13.5.16.3 Formal sign-off document from service provider that details monthly progress being made regarding knowledge transfer to university's resources during project implementation.

14 TENDER RESPONSE: SERVICE PROVIDER APPROACH AND CAPABILITY

A blank Tender Response Template containing the requirements listed above is contained in Annexure A9 and A10. All responses must be completed using these templates any other templates will be discarded.

15 ANNEXURES

Annexure A5:	Pricing Template
Annexure A6:	Reference Template
Annexure A9:	IaaS Specification and Response Template
Annexure A10:	SLA Response Template
Annexure A15:	Sub-Contracting Template
Annexure B1:	Current Data Center HLD
Annexure B2:	Wide Area Network Topology
Annexure B3:	Unisa WANLAN Current