

SCOPE OF WORK

ICT CISCO PANEL OF PROVIDERS

FOR

SUPPLY AND INSTALL CISCO NETWORK INFRASTRUCTURE

&

MAINTENANCE AND SUPPORT OF THE CURRENT CISCO INFRASTRUCTURE

TABLE OF CONTENTS

1.	BACKGROUND AND PURPOSE.....	3
2.	OVERVIEW OF THE SERVICES.....	4
3.	PROJECT DEFINITION	8
4.	HIGH-LEVEL PROJECT PLAN	9
5.	SUPPORT AND MAINTENANCE	11
6.	SERVICE LEVEL AGREEMENTS.....	11
7.	VENDOR MANAGEMENT	12
8.	RISKS, ASSUMPTIONS, DEPENDENCIES & EXCLUSIONS (RADE).....	12
9.	STANDARDS AND SPECIFICATIONS	14

1. BACKGROUND AND PURPOSE

Wits ICT will appoint a panel of service providers to deliver projects that may vary in complexity, quantity, and size. The increase in future projects will impact the capacity of the networking team, and the demand for these projects is likely to remain high in the next five (5) years.

To appoint a panel of service providers that will assist with the future sourcing of equipment, installation, implementation, support (third line), maintenance, and management of a Cisco network environment and related professional services (such as technical consulting services and projects)

Management of services for the University's future requirements will be for five (5) years and must be reviewed annually.

The appointed panel of the service provider(s) is required to assist Wits ICT in delivering network and security-related projects of various sizes and complexity. The projects range from medium to large-scale ICT infrastructure installations and maintenance. This will include networking and hardware equipment (Cisco wired and wireless networks, security, load balancing, and network services). The projects may run up to 24 months, depending on the size and agreed-upon timelines.

Wits University ICT infrastructure consists of Data Switching: Core Switches, Distribution Switches, Firewalls, Mini Distribution Switches, Wireless Controllers, Access Switches, and Access Points. These devices interconnect the entire Wits network as follows:

- Data Switching for the Wits Data Network
- The Wits Data Network consists of WAN Links and Cisco infrastructure
- The network topology is Cisco's three-tier model, Core, Distribution, and Access Layer, including mini routers at various sites.

The interconnection between Wits campuses and remote sites is through the ICLU (Inter-Campus Link Upgrade) Fiber optic ring, and the internal buildings connect via the Fiber backbone. ICLU is the primary connection for the main campuses, and the TENET Fiber ring is secondary. Hospital connectivity, including Chris Hani-Baragwanath, Helen Joseph, Sterkfontein Campus, Tara Hospital, Wits Research Biohub, and Rahima Moosa hospitals, TENET (via SANREN) Fiber ring is the primary link, and point-to-point is secondary for Helen Joseph and Rahima Moosa.

There are two point-to-point links from Solomon Mahlangu House (SMH) to the Medical School, one point-to-point from CLM to the Business School, and one point-to-point from the Medical School to the Business School. Lastly, there are two point-to-point links from the Essellen building to Forensics and NHLS (National Health Laboratory Services), which is the third level of redundancy between campuses.

There are two main data centres: the primary data centre is at East Campus, and the secondary data centre is at West Campus. The link between the two cores is 2x 100Gbps with a point-to-point configuration. There are three firewalls per data centre for intrusion prevention types, as well as external and internal services.

There are 8 Cisco distribution switches, with dual 100Gbps connections to the core switches. Then, 26 Cisco mini distributions all have dual 40Gbps connections to the Distributions.

The Access Layer 2157 Cisco Access Layer switches, stackable and stand-alone with uplinks, are 10Gbps and connect to the distribution and mini distribution switches.

Approximately 80,000 network wired connections, based on switch port utilization across all Wits campuses.

There are 16 Cisco Wireless Controllers with approximately 9000 Cisco Wireless Access Points, including indoor and outdoor Wireless Access Points.

This document also outlines the scope of work required to acquire CISCO maintenance and support for five (5) years, which will be awarded to one of the successful bidders. The contract will cover essential services, including hardware and software support, troubleshooting, system updates, regular maintenance, and annual review of the total CISCO network equipment due for maintenance, to ensure the optimal performance of all CISCO network equipment within the organization.

2. OVERVIEW OF THE SERVICES

The scope of the work includes site surveys, supply, setup, installation, testing, monitoring, maintenance, support, and integration. The panel of service providers should be able to conduct site assessments, implementation, maintenance, and support, to assist the University with the latest (must not reach the end of life within five (5) years after installation) ICT networking solutions. The network switches and APs (wireless access points) must include the OEM warranty of 5 years as required. Proper end-to-end network connectivity to the University's infrastructure is needed to ensure no distractions in the day-to-day operation of current and future solutions.

Scoping will be conducted for ad-hoc and future network projects related to Cisco's wired, wireless, and security infrastructure. The future project requirements of the goods and/or services that the successful panel will deliver to service providers must, at a minimum, contain the following:

- Cisco network and security equipment and licensing.
- The solution must have a 5 (five) year full support and maintenance plan.
- The solution and equipment must not reach the end of life within the next 5 (five) years.
- The solution and equipment must have the capability of PoE (Power over Ethernet).

- The solution and equipment must be scalable to new technologies, including SDN technology.
- The successful panel of service providers must supply all required infrastructure, including network devices, and related software.
- The original equipment manufacturer (“OEM”) must cover all vendor-supplied equipment with a minimum of a 5 (five) year warranty.
- Successful service provider

The successful panel of service providers must install all equipment, including but not limited to the following:

- Cisco networking devices such as switches and wireless access points
- Network configurations for wired, wireless, and related solutions
- OEM Support (Smartnet Support), including installation and configuration
- Future Network Design and Architecture Requirements
- Future Firewall and Other Security Device Requirements
- Upgrade of Cisco network when required
- Upgrade and update Cisco software and licensing when required

Network Switches: Installation and Configurations

- Access layer switches must have Fiber modules, which will connect at a minimum of 10 Gbps to all mini-distribution switches
- Access layer switch ports must be scalable and support connections from 1 to 1000Gbps
- Access layer switches must have redundant power suppliers to provide for sufficient POE+ and POE++
- Access layer switches must support secure access to LAN & WLAN and Network Access Control (NAC) with integration to identity management that is Identity Services Engine (Cisco ISE)
- Access layer switches must support aggregation and power stacking, and switch aggregation must allow stacked switches to be managed as one logical switch.

Configuration

- The Interface configurations across switches deployed in all the Mini distributions & Access layers must be Consistent to ensure reliable network services across all Wits Campuses via LAN & WLAN
- Unified Access switch configurations must include:
 - The 99% high-availability connection
 - Support policy-based configuration
 - Support centralized management
 - Support one logical network, LAN & WLAN
 - Support roaming and device mobility
- Switch management configurations include the following, but are not limited to:

- Naming convention - Building Name_Floor_Type-Device
- Secure Shell (SSH) remote administration protocol should be used to access all switches.
- VTY lines to control inbound telnet connections on legacy devices if needed
- To control access to the switches, authentication, Authorization, and Accounting (AAA) access must be implemented.
- Identity Services Engine (ISE) for policy enforcement and security across all access layer switches.
- Spanning tree protocol is used to manage and optimize virtual local area networks (VLANs)
- The non-routable VLAN must be assigned to inactive switch ports. Shut the ports
- Access switch consists of Fiber modules, stacking cable where necessary, and dual power suppliers.
- Switch stacking is to be implemented to enable multiple switches to be aggregated and managed as a stack.

Installation

A Wi-Fi network installation and configuration:

- Must be carried out to enable the total production of the University's wireless network on agreed project milestones and dates.
- Must carry out RF scanning to determine the number of APs and installation layouts that have editable recommendations with approval from the University's representative before the installation. All wireless access installations must be as per the Site Survey and Wi-Fi RF scanning report.
- Ensure that Access Points are mounted on the ceiling with secure and lockable brackets

Wireless network configuration

- Naming convention - Building Name_Floor_Type-Device_Room Number
- Wireless access points must connect automatically to the controller. No stand-alone wireless access points
- Channel configuration must allow roaming and ensure non-interference
- The Wits wireless access group must be configured to allow roaming between wireless access points.
- The wireless network must be added to the existing Wits management and monitoring tools

The following Wits standard SSIDs must be configured:

- Wits SSID, a guest SSID, and eduroam SSID.
- Configurations must allow seamless MAC address authentication for legacy devices such as security cameras, mobile phones, laptops, etc.
- Quality of Service (QoS) must be provisioned and configured where needed
- The wireless connection must have adequate capacity and throughput for voice and video, such as Wi-Fi HD cameras.
- Provide a NAC (Network Access Control) Solution for user authentication on both wired and wireless users against the Active Directory (AD)

Delivery and storage of equipment

Successful service providers must meet storage and office requirements. The successful service provider covers the required cost and must secure equipment when in transit and before installation, once removed from the ICT storage area. The University will be liable for the equipment only when delivered to the specified location at Solomon Mahlangu House from OEM, and following the University delivery process:

University ICT delivery process

The vendor needs to communicate 3 days in advance by providing an inventory of the goods to be delivered on an Excel spreadsheet that includes the following details: delivery date, Purchase order, item description, serial number, quantity, warranty, unit cost, and total cost.

All goods will be delivered to East Campus, Solomon Mahlangu House, 1st Floor, Room SH1015.

Pick up for the installation process

The panel of service providers must complete the paperwork for equipment to be released, which includes item description, serial number, quantity, installation area, estimated date of installation, and an estimated date for installation sign-off. Wits will communicate with the successful service providers once the equipment is ready to be picked up. The successful service provider's project team leader will sign for the release upon pickup. Wits ICT and the service provider's team leader will complete the installation sign-off.

Reporting

The panel of service providers must alert the University within 5 (five) business days:

- a) On Cisco field notices, bugs, and issues that may impact service availability, provide a report on the nature of the bug and provide a solution based on the University's environment
- b) On new software releases that will improve network service availability, suitable software for the University, tested for tenacity.

Training and skills transfer

The panel of service providers must provide skills transfer for administration and technical support on all implemented solutions, such as (but not limited to) wireless, access switching, and monitoring tools skills:

- a) Transfer business and technical knowledge of the Network and Security Infrastructure through training the relevant University staff during the solution planning, configuration, deployment, and implementation. The competency of the University's Network staff following the training must be:
 - Competent at a level that will enable Wits ICT to be certified in the relevant technologies at an accredited institution approved by the University.

- Competent in the management, maintenance, planning, additions, changes, troubleshooting, and all other aspects of the day-to-day running of the network and security infrastructure.
- Specify the various means of knowledge transfer, e.g., workshops, expert panels, training, custom training, etc.
- Suggest progress through the levels of the various courses.

3. PROJECT DEFINITION

The Enabling Agreement for the CISCO Panel of Suppliers establishes a structured framework for the supply, maintenance, and support of CISCO network infrastructure. This agreement ensures seamless procurement, competitive pricing, and reliable technical support from pre-qualified Cisco-certified suppliers. It enables Wits to maintain a secure, scalable, high-performing network environment, ensuring business continuity, operational efficiency, and compliance with industry standards.

CISCO Panel of Suppliers objectives

The Enabling Agreement for the CISCO Panel of Suppliers aims to achieve the following key objectives:

- **Streamlined Procurement Process:** Establish a qualified panel of Cisco-certified suppliers to ensure efficient acquisition of networking equipment and services and reduce procurement lead times and administrative overhead.
- **Cost Optimization and Budget Control:** Secure competitive pricing through a structured agreement. Minimize ad-hoc procurement costs and optimize total cost of ownership (TCO).
- **Enhanced Network Reliability and Business Continuity:** Ensure timely maintenance and proactive support to reduce downtime and service disruptions. Establish clear SLAs for incident resolution and performance monitoring.
- **Access to Certified CISCO Expertise:** Engage Cisco-certified partners to ensure compliance with best practices and security standards. Leverage expert support for network upgrades, troubleshooting, and lifecycle management.
- **Security and Regulatory Compliance:** Maintain a secure IT environment by implementing regular updates, patch management, and cybersecurity best practices. Ensure compliance with industry regulations and internal IT policies.
- **Scalability and Futureproofing:** Ensure network infrastructure can adapt to organizational growth and emerging technology trends. Support cloud integration, digital transformation, and hybrid IT strategies.
- **Performance Management and Accountability:** Establish KPIs and service benchmarks to monitor supplier performance. Foster accountability through regular performance evaluations and audits.

Measurements of Success

- To ensure the success of the CISCO Panel of Suppliers Enabling Agreement, the following metrics will be used:
- Procurement Efficiency: Reduction in procurement processing time and supplier onboarding lead times. Number of successful acquisitions completed within agreed timelines.
- Cost Savings and Budget Adherence: Reduced total cost of ownership (TCO) through negotiated pricing. Increased percentage of spend optimization compared to previous procurement models.
- Network Uptime and Service Availability: 99.9% or higher network uptime minimizes disruptions. The mean time to repair (MTTR) for network-related incidents is reduced.
- Supplier Performance and SLA Compliance: SLA adherence rate (e.g., response and resolution times met as per contract). Number of service requests completed within SLA terms.
- Security and Compliance Metrics: The number of security patches and updates applied within prescribed timelines, and compliance with internal and external audit standards.
- Scalability and Technology Readiness: Percentage of infrastructure upgraded or modernized through the agreement. Ability to seamlessly integrate new technologies and services.
- Stakeholder Satisfaction: Feedback from IT teams and end-users on network performance and reliability. Supplier rating and evaluation scores based on periodic reviews.

Maintenance and support

- Ensure the continuous and optimal operation of CISCO network equipment.
- Minimize downtime through prompt and efficient support services.
- Maintain up-to-date software and firmware on all CISCO devices.
- Provide preventive maintenance to avoid potential issues.
- Facilitate access to CISCO's technical resources and expertise.

Wits ICT will ensure a resilient, cost-effective, and future-ready network infrastructure by meeting these objectives and success measures.

4. HIGH-LEVEL PROJECT PLAN

The panel of service providers must provide the University with a comprehensive Project Plan for each project, based on recognized best practice IT project management methodology for the following:

- a) Implementation, configuration, installation, support, maintenance, deployment, knowledge, and skills transfer
- b) Support and maintenance after the Implementation Period
- c) The Project Plan must include:

General

- Graphical representation of the project timeline showing key Milestones and payment Milestones
- The successful service provider's resources required, their number, role, and duration of involvement
- University resources required, their number, role, and duration of involvement
- Lead times for management system integration with the University's infrastructure
- Lead times for ordering and installation of components
- Production of a comprehensive risk register and risk management plan (covering both Supplier and Purchaser risks)

Deployment planning

- Workshops for the Network and Security Infrastructure
- Deployment Planning
- Low-level (comprehensively detailed) documentation relating to Workshops detailing installation and configuration tasks and technical requirements for deployment
- Change management plan, which includes how to communicate with users and university technical resources
- Test plan of the solution with details such as setup, commands, results expected, and the duration
- Milestones for User Acceptance Testing during the Implementation Period
- Configuration and Installation
- Configuration of Network and Security Infrastructure
- Documentation relating to all configurations done on the Network and Security Infrastructure
- Physical installation of the Network and Security Infrastructure, where necessary or as per the university directive
- Documentation relating to all installations done on the Network and Security Infrastructure,
- The project plan and milestones should follow the standard model as shown in Table 4.1

Table 4.1 High-level example of a Project Plan

Milestone 1: Pilot	<ul style="list-style-type: none"> i. Sign off the contract and service level agreement (SLA) ii. Site visit and introduction iii. Technical scoping and initial planning iv. Ordering equipment
Milestone 2: Transition and asset verification period	<ul style="list-style-type: none"> i. Delivery of equipment ii. Requests for building access iii. All equipment will be asset-tagged and registered with the University iv. Delivery of equipment to the site
Milestone 3: Implementation phase	<ul style="list-style-type: none"> i. Installation of equipment ii. Configuration of equipment iii. Testing of equipment functionality

Milestone4: Sign-Off	iv.	Tidying Up
	i.	Documentation
	ii.	Quality assurance and fixing snags
	iii.	Skills Transfer
	iv.	Final site visits
	v.	Full end-to-end testing
	vi.	Handover to operations

5. SUPPORT AND MAINTENANCE

The University has transitioned from Partner Support Service (PSS) to SmartNet Cisco technical support services. Therefore, the university is expecting the successful service provider to have the capabilities to work with the OEM (CISCO) for the Smartnet maintenance and support of the current network and security infrastructure.

6. SERVICE LEVEL AGREEMENTS

a) Provide the process and plan, including your approach with detailed steps, including, but not limited to, indicating resources to be used, equipment to be installed, and timelines to ensure that the approach submission is within 24 hours (one business day) after the scoping session.

b) Once the final BOQ has been determined and communicated to panel providers, quotations should be sourced within seven (7) working days.

c) The pricing/quotation should be valid for 30 calendar days. Project implementation should commence five business days after the equipment is delivered to Wits' premises.

d) The service provider shall deliver all required equipment per SOW within 6-12 weeks of placing an order.

e) All elements of the solution must be proven to function correctly, integrated with the existing University systems and infrastructure, and must comply with the sign-off process in Table 4.1, and according to the following procedure, and as per Wits ICT standard document:

- Core switches must have the latest IOS software and be configured with all applicable routing protocols, VLANs for specific data channelling, management IP addresses, and appropriate interface configurations.
- Distribution switches must have the latest IOS software and be configured with all applicable routing protocols, including the spanning-tree protocol on interfaces, management IP addresses, and appropriate interface configurations.
- Switches must have OEM-approved IOS software, all required VLANs, management IPs, switch access security features, port security, spanning tree protocol, and be discoverable on monitoring devices.

- Wireless controllers have OEM-approved IOS software, configured with wireless VLANs, AP grouping functionality, RF management, load balancing, SSID, and AP power management functionality
- Access Points have OEM-approved IOS software and are configured with a wireless SSID, power setting, channels, and coverage.
- All network devices to be tested and fine-tuned for high availability and Functionality:
- Testing LAN and wireless user connectivity.
- Testing all wireless SSIDs.
- Logging on to the intranet and the internet.
- Logging on to learning management systems
- Test the University's applications, such as MS Teams and e-mails.

7. VENDOR MANAGEMENT

Full contractual management details are on the drafted contract, and below is basic vendor management information:

- Weekly meetings must be held. The University's project manager will chair meetings and take minutes; regular performance reviews will be based on compliance with the University's ICT standards, SLA, and scope of work.
- All payments will be according to project deliverables and milestone percentages. Payment will be according to the agreed milestones/deliverables. Payment will be withheld if the service or installation regarding testing and skills transfer has not been delivered.
- The panel of service providers must provide all incidents and ad-hoc consultation reports. The reports must include, but are not limited to, the following: Description of the incident, start time and end time, cause, resolution, recommendation, and additional information. A consultation report will include information per the agreed scope, recommendations, and additional information.

8. RISKS, ASSUMPTIONS, DEPENDENCIES & EXCLUSIONS (RADE)

The following risks, assumptions, dependencies, and exclusions will have the following effect on the contract and project delivery:

Risk (R)	Effect on the project
Power failures	Equipment and tools that need power to operate might delay the project.
Sub-Contractors	No subcontracting will be allowed and not form part of the main contract.

Properties not owned by the University.	There could be delays while waiting for installation permission and access to non-Wits University property.
Sensitive areas, for example, mortuaries, X-Rays, theatres, and ICUs	The protocol needs to be observed, which can limit access to these areas.
Heritage Buildings	Protocols need to be observed, i.e., a qualified team from a successful panel of service providers will execute installations.
Storage	All equipment will be delivered at SMH; there could be delays as it will not be delivered directly to the site but picked up by a panel of service providers for installation. A panel of service providers will carry the liability from SMH to the site. Wits will have the liability once the equipment is delivered to SMH and when it is installed at the project site.

Assumption
All equipment must be Cisco standard and meet the University's needs.
Software Licenses and Equipment must have relevant Academic Discounts and New Version Rights.
Equipment must come with a minimum of 12 months of functionality guarantee.
Equipment pricing must include software licensing, installation, media converters, relevant power cables, stacking cables, power stacking cables, dual power supply, fibre modules, and configuration for Cisco equipment.
For the security component, the expansion pricing must be calculated per item based on the technical specifications and design principles.

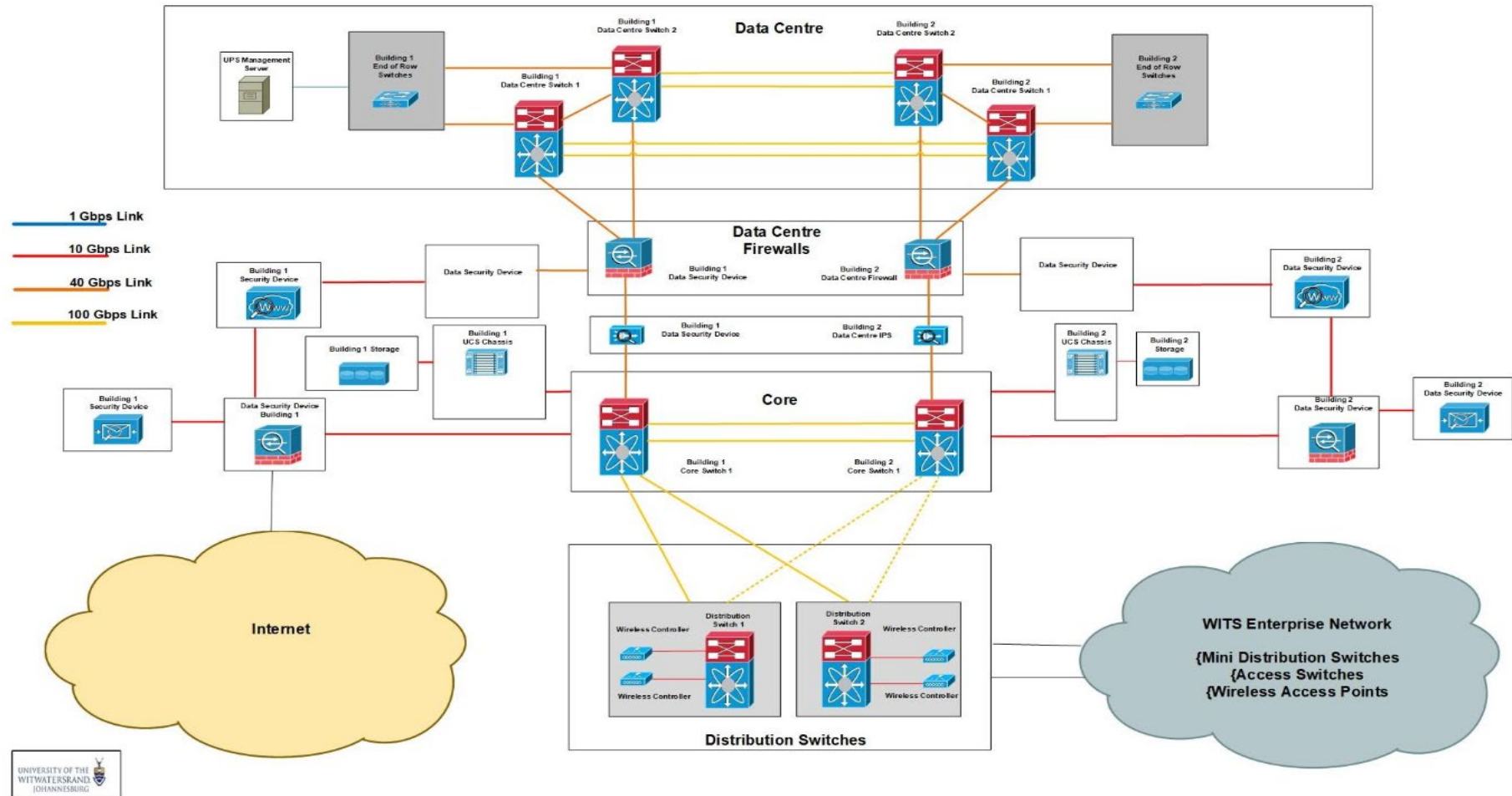
Exclusion
Cabling installation
UPS
Cabinet
All non-Cisco equipment

Dependency
Standardised panel contract
VAT
Project scope for ad-hoc request
Rate of exchange

9. STANDARDS AND SPECIFICATIONS

The Wits ICT standard document **Annexure E: WITS ICT Standards document** details the University's ICT installation standards for network-related infrastructure installation, configuration, and testing.

Below is a diagram depicting Cores, Distribution, Firewalls, etc.



Below is a diagram depicting Distributions, mini-distributions, access switches, wireless controllers, and wireless access points.

