CSIR
Touching lives through innovation

purco
PURCHASING CONSORTIUM SOUTHERN AFRICA NPC
ISO 9001:2015 certified company

INVITATION TO TENDER

THE COUNCIL FOR SCIENTIFIC AND INDUSTRIAL RESEARCH (CSIR) IN SOUTH AFRICA INVITES EXPERIENCED SERVICE PROVIDERS TO BID FOR THE FOLLOWING SERVICE:

TENDER NO.	**TENDER DESCRIPTION**	**CLOSING DATE AND TIME**
RFP No. **3551/15/12/2022**	Network: The Design, Provision of Network Equipment, Implementation, Maintenance and Support for a Period of Five (5) Years	15 December 2022 at 23:30pm

Please refers to Annexure A of this Invitation to Tender for detailed specification and bid requirements

Tender documents can be purchased at a non-refundable fee of R1150.00 (VAT included) on the PURCO SA website. All participated bidders on RFP 3551/15/12/2022 are allowed to re-tendering without paying PURCO participation fee. Visit www.purcosa.co.za.

Any queries must be in writing to tender@csir.co.za , Mr Tshepo Mampuru at tshepo.mampuru@purcosa.co.za.

All tender document availability and tender submission related queries must be sent to pozisa.makonco@purcosa.co.za, contact number 011 545 0940**.**

Submission for the tender is online via the PURCO SA website (link for submission is in the tender document).

Annexure A

Detailed Specification and Requirements

REQUEST FOR PROPOSAL SPECIFICATIONS (OVERVIEW OF REQUIREMENTS)

Date of Issue	Monday, 21 Novemebr 2022	
Closing Date for registration to attend the compulsory briefing session	Friday, 21 November 2022 and 23:30pm	Link: https://purcosa.co.za/webform/rfp-no-3551-15-12-2022-network-implementation-and-support-csir-pu4322-019
Date of Briefing Session	Wednesday, 30 November 2022 and 10:00am	Venue: Gauteng

Closing Date for Clarifying Questions	Tuesday, 05 December 2022 and 16:00pm	E-mailtshepo.mampuru@pursosa.co.za;
		tender@csir.co.za;
		pozisa.makonco@purcosa.co.za

Response Date for Clarifying Questions	Thursday, 08 December 2022 and 16:00pm	
Closing Date for Submission of Proposals	Day, 15 December 2022 and 23:30pm	Link: https://purcosa.co.za/webform/rfp-no-3551-15-12-2022-network-implementation-and-support-csir-pu4322-019
CSIR business hours	08h00 – 16h30	

1. INVITATION FOR PROPOSAL

Proposals are hereby invited from suitably qualified service providers for the design of the network, provision of network equipment for the replacement of the end-of-life, end-of-support, and end-of-sale CSIR network equipment, implementation according to a phased implementation plan and maintenance and support for a period of five (5) years as specified in this RFP to the CSIR. This implies that prospective bidders must have experience in similar scope and sized networks and customers operations.

The CSIR will host a compulsory briefing session, with the intent to create a dialogue to equip the Bidders with all the relevant information to enable them to submit a complete Bid. Also, the CSIR will allow additional time to ask clarification questions, and a consolidated briefing pack will be circulated to all Bidders who attended the briefing session. Furthermore, the briefing information pack will include details pertaining to the High-level design, support teams, and 3rd parties within the Networking ecosystem. Consequently, the Bidder shall submit OEM certifications and financial guarantees appropriate to cover the Bid value/ project value.

1.1. CRITERIA FOR PARTICIPATION IN THE COMPULSORY BRIEFING SESSION

The bidder must meet the following mandatory criteria for participation in the compulsory briefing session:

- Submit a fully completed and signed Expression of Interest Form. Annexure AA.
- Submit a fully completed and signed NDA (Non-Disclosure Agreement). Annexure C.
- Submit the company registration of the main bidder and the commercial agreements with all sub-contractors (Joint-venture agreement where applicable).
- Provide the names and identity numbers of the representatives who will be attending the compulsory briefing session.
- It is essential for the team (e.g. Bid manager and Solutions Architect), who will compile the bid, to attend the briefing session, as the bid is highly technical.
- Status as Vendor/OEM channel partner in the Top 2 tiers as specified by the OEM.

2. PROPOSAL SPECIFICATION

The CSIR requests bidders to provide a proposal in response to the CSIR's requirements as stated in the following proposal specification sections**.** In addition to the introduction and background to the project, the ecosystems and respective technologies mentioned, our aim is to simplify, support, modernise features, and reduce costs across the life cycle of our network.
Also, the solution must comply with all governing laws and acts related to, but not limited to, POPIA, PAIA, and electronic communications act.

2.1. Legislation

- The Regulation of Interception of Communications and Provision of Communication-related Information Act (Act No. 70 of 2002) ("RICA")
- Promotion of Access to Information Act (Act No.2 of 2000)
- Electronic Communications and Transactions Act (Act No 25 of 2002)
- Protection of Personal Information Act 4 of 2013 (POPIA)

2.2. Project phasing

The project phases are informed by the availability of budget, risks, and the unfolding of the re-configuration of the CSIR footprint over the next three years. Therefore, the deployment of the access layer and Wireless will be deferred to the last phase.

Table 1: Project phasing must be studied with the population and distribution of the networking hardware, as articulated in Table 2: Networking hardware population which will also be used to inform pricing as part of **PART 2: PRICING PROPOSAL.**

Table 1: Project phasing

Phases and deliverables	**Year**	**Training**	**Design**	**Hardware**	**Licensing**	**Implementation (all associated cost)**	**Year 1 to 5 Maintenance and support of hardware and software**
Phase 1							
Low-level design, depicting the configuration of all infrastructure hardware and software	2023/2024 Q1		🟨				
Core, Internet, and Data centre. (Proposed)	2022/2023			🟨	🟨	🟨	🟨
Training (Basic), covering design, configuration, implementation, support, and troubleshooting (based on 5 Network Engineers). (Proposed)	2023/2024 Q1-Q4	🟨					
Phase 2							
Regional core switches and distribution/aggregation layer. (Proposed)	2023/2024 Q1-Q4			🟨	🟨	🟨	🟨

Phases and deliverables	Year	Training	Design	Hardware	Licensing	Implementation (all associated cost)	Year 1 to 5 Maintenance and support of hardware and software
Training (Intermediate), covering design, configuration, implementation, support, and troubleshooting (based on 5 Network Engineers). (Proposed)	2023/2024 Q1-Q4	🟨					
Phase 3							
Access layer and/or Wireless. (Proposed)	2024/2025 Q1-Q4			🟨	🟨	🟨	🟨
Training (Advanced), covering design, configuration, implementation, support, and troubleshooting (based on 5 Network Engineers). (Proposed)	2024/2025 Q1-Q4	🟨					

Table 3 below provides an indication of the network hardware population and distribution across the CSIR offices.

Table 2: Networking hardware population

Core and Data center switches				
Network infrastructure models	**QTY**	**Model numbers**	**To be replaced in Phase 1,2 or 3**	**Location**
Core switch (DC)	1	VSP 8284XSQ	Phase 1	Pretoria
Core switch (DR)	1	VSP 8284XSQ	Phase 1	Pretoria
Internet switch (DC)	1	VSP 7254XSQ	Phase 1	Pretoria
Internet switch (DR)	1	VSP 7254XSQ	Phase 1	Pretoria
Data Center	12	ERS 4826GTS-PWR	Phase 1	Pretoria
Data Center	31	VSP 7024XLS	Phase 1	Pretoria
Data Center	2	VSP 7254XSQ	Phase 1	Pretoria
Aggregation/Distribution Switch				
Core switch (region)	1	ERS 5530-24TFD	Phase 2	Durban
Core switch (region)	2	ERS 5530-24TFD	Phase 2	Cape Town
Core switch (region)	1	ERS 5632-FD	Phase 2	Stellenbosch
Core switch (region)	1	ERS 4524GT-PWR	Phase 2	Carlow Road
Core switch (region)	1	ERS 4850GTS-PWR	Phase 2	Cottesloe
Building 9	2	VSP 7024XLS	Phase 2	Pretoria
Building 14	1	ERS 5632FD	Phase 2	Pretoria
Building 16	2	VSP 7024XLS	Phase 2	Pretoria
Building 20	4	VSP 7024XLS	Phase 2	Pretoria
Building 35	2	VSP 7024XLS	Phase 2	Pretoria
Building 38	2	VSP 7024XLS	Phase 2	Pretoria
Building 43	1	ERS 5632FD	Phase 2	Pretoria
Building 44	2	ERS 5632FD	Phase 2	Pretoria
Entabeni	1	VSP 4450GSP-PWR	Phase 2	Pretoria

Access switches and Wireless				
Network infrastructure models	**QTY**	**Model numbers**	**To be replaced in Phase 1,2 or 3**	**Location**
All buildings	47	ERS 3510GT-PWR	Phase 3	Pretoria, Johannesburg, Durban, Cape Town
Building 9	1	ERS 3549GTS-PWR	Phase 3	Pretoria
All buildings	68	ERS 4524GT-PWR	Phase 3	Pretoria, Johannesburg, Durban, Cape Town, Stellenbosch
All buildings	14	ERS 4526GT-PWR	Phase 3	Pretoria
All buildings	182	ERS 4548GT-PWR	Phase 3	Pretoria, Johannesburg, Durban, Cape Town, Stellenbosch
All buildings	46	ERS 4850GTS-PWR	Phase 3	Pretoria, Johannesburg, Durban, Cape Town, Stellenbosch
Entabeni	1	ERS 4926GTS-PWR	Phase 3	Pretoria
All buildings	10	ERS 4950GTS-PWR	Phase 3	Pretoria
Building 9	5	MSM760	Phase 3	Pretoria

Access switches and Wireless				
Network infrastructure models	**QTY**	**Model numbers**	**To be replaced in Phase 1,2 or 3**	**Location**
Building 9	2	Aruba7010	Phase 3	Pretoria
Building 37	1	MSM430	Phase 3	Pretoria
Building 2 - 46	425	MSM460	Phase 3	Pretoria, Johannesburg, Durban, Cape Town, Stellenbosch
Building 50, Stellenbosch, ICC	3	MSM466-R	Phase 3	Pretoria, Stellenbosch
Building 2 - 46	25	HP560	Phase 3	Pretoria, Johannesburg, Durban, Cape Town, Stellenbosch
Building 1	1	Aruba IAP-325	Phase 3	Pretoria
Building 9	21	Aruba IAP-325	Phase 3	Pretoria
Building 3	20	Aruba IAP-325	Phase 3	Pretoria
Building 39	28	Aruba IAP-325	Phase 3	Pretoria
Building 43	41	Aruba IAP-325	Phase 3	Pretoria
Building 44	66	Aruba IAP-325	Phase 3	Pretoria
Entabeni	20	Aruba IAP-325	Phase 3	Pretoria
Carlow Road	14	Aruba IAP-325	Phase 3	Johannesburg
Paardefontein	3	Aruba IAP-325	Phase 3	Pretoria
Kloppersbos	6	Aruba IAP-325	Phase 3	Pretoria

Note: Further details pertaining to the Networking hardware, and model, fibre routes, will be provided at the briefing session.

Current Networking capabilities are insufficient to support the current and future CSIR requirements, which became evident through requests to create specific network configurations and capacity to support projects, lab work in the respective Impact areas, as the time it takes, informed by the limitations in the technology, supporting, for example, Software-Defined Networking and Security, prolong the fulfilment of such.

Through collaboration efforts, as part of the CSIR Strategy formulation, of the ICT and Network Strategies, interested Stakeholders provided the following high-level requirements, as critical **Networking capabilities** to pursue as part of this tender:

- **Network Access control**: Improving network security, by allowing only authorized devices on the network, blocking those that are not compliant with security policies.
- **Multi-tenancy** support is required to containerize networks of different tenants, separate from the CSIR, with the intent to isolate possible security breaches and network activity, which may negatively impact the CSIR reputation. The requirement for multi-tenants is on the increase, as Data Centre Hosting requirements and new tenants on campus grows. Although the CSIR will not necessarily provide data services to tenants, voice services are predominantly provided to all tenants, necessitating the requirement to cater for multiple tenants.
- **Support and Administration Simplicity:** The current capabilities do not support the agility to configure Software-Defined Configuration models to orchestrate network provisioning centrally. The time taken to create configurations via an SDN platform will reduce the time significantly.
- Support for **Internet of Things:** The proliferation of IoT devices on campus as well as research, necessitates the required network capabilities to support such, which is not possible with the current network hardware.
- Support for **Big data**: There has been an increasing need for the network to carry volumes of packets, generated by IoT devices and simulations, conducted in labs. The latter may not necessarily be in one geographical area and may span regional offices, hence the virtual lab configuration is required to support the transacting of large quantities of data. A second large data requirement is that of large datasets, which also need to be sent across CSIR offices and also internal to the Data Centre and LAN networks.
- **Wireless** connectivity: The CSIR currently has 412 HP wireless devices and 227 Aruba devices deployed. We are looking for a management capability for all wireless devices as well as a new Wireless technology, able to co-exist with the current models, whilst we are migrating.

- **Artificial Intelligence (AI):** Recent networking technologies deploys machine and deep learning capabilities to identify patterns in traffic patterns, with the intent to contain possible security related events and to deploy intelligent routing and self-healing capabilities.

Requirements are given a priority according to the **M**o**SC**o**W** method where:

- **M**: Is a 'Must Have' requirement. Requirements labelled as 'Must Have' are critical to the current delivery time frame in order for it to be a success.
- **S**: is a 'Should Have' requirement. Requirements labelled as 'Should Have' are important but not necessary for delivery in the current delivery time frame.
- **C**: is a 'could have requirement. Requirements labelled as 'Could Have' are desirable but not necessary and could improve user experience or customer satisfaction for little development cost.
- **W**: Requirements labelled as 'Won't Have', have been agreed by stakeholders as the least-critical, lowest-payback items, or not appropriate at that time.

2.3. Wired Network

2.3.1. Campus Networking

Access Switch / Core Switch / Aggregation/Distribution

Campus and branch office access networking is evolving to support better user experiences and use cases such as SDN and Edge networking. The Infrastructure Operations team within CSIR is tasked to identify vendors that are positioned to supply a SDN solution to meet changing requirements for access network connectivity, automation, and management.

The core capabilities of the enterprise wired local-area network should include the following technology hardware components:

(It should be noted that the requirements in section 2.3, are mandatory, and forms part of the elimination criteria).

Hardware — The core capabilities of physical network elements include:

- Ethernet network switches suitable for deployment at the network access, distribution, and core network layers

Software — Network service applications that are cloud-, appliance- or virtual-appliance-based. The core capabilities include, but are not limited to:

- Network management
- Network monitoring
- Guest access portals
- Self-service device onboarding services
- Network security integration (e.g., IPS, IDS, 802.1X, DNS security, Anomaly detection, etc.)
- Network policy enforcement/integration
- Application visibility and/or performance management
- AI- and ML-enabled network assurance tools
- Network automation tools
- Must provide Micro segmentation for granular security
- Access solution that is SDN enabled
- Must provide full network access-control (NAC), client posture assessment and validation
- Provide single policy for both wired and wireless solution

The proposed Switch solution should adapt to the fast-changing digital landscape while protecting the CSIR network from security attacks. When modern technologies, applications, and devices emerge, the network needs to be ready to handle these changes. Users demand more network capabilities and convenience and therefore the proposed solution should include the following benefits related to security, mobility, and IoT:

- **Hybrid:** Ensure a more secure experience and bring exceptional speed and scale. Leveraging enhanced power and advanced AI/ML for continuous zero-trust security and deploy a powerful platform that can support today's hybrid work.
- **Mobility:** Fabric-enabled appliance-based end-to-end security, simplified guest and mobility segmentation, distributed data plane optimized for roaming, and compatible with future versions, supporting 1G, 2.5G, 5G and 10G for Wi-Fi 6 and 802.11ac Wave 2 access point deployment
- **IoT:** Automated IoT device segmentation and protocol recognition, simple device provisioning with Zero-touch provisioning (ZTP), strict timing synchronization for distributed IoT device deployment, segment users and devices on a common network based on policy, and industry-leading UPOE+ features

- **Cloud:** Single pane of glass management for Software Defined-Networking, refined intelligence, and programmability, simple QoS policy management, complete enterprise IT control for cloud access, and on-box application performance analytics

Please refer to Tables 4, 5 and 6 below for all Access Switch, Core Switch, and Aggregation/Distribution requirements.

2.3.2. Access Switch Mandatory Requirements (AS_MAN)

Table 3: Access Switch Mandatory Requirements (AS_MAN)

Req No	**Requirement Description**	**Must meet criteria**
AS_MAN_01	Switch must be built on x86 CPU for compute-intensive applications, enabling them to host containers and run third-party applications and scripts **natively** within the switch	Yes
AS_MAN_02	Switch must support the last power drawn from a particular PSE port and switches on power the moment AC power is plugged in without waiting for OS to boot up	Yes
AS_MAN_03	Switch must support Network automation & programmability with RESTCONF, NETCONF, YANG, and APIs	Yes
AS_MAN_04	Switch must support macsec (128 or 256 bit encryption) on all downlink and uplink ports	Yes
AS_MAN_05	Switch must provide 420Gbps or higher Dedicated (Physical) Stacking Bandwidth	Yes
AS_MAN_06	Switch must support field replicable redundant power supplies and fans.	Yes
AS_MAN_07	Switch must provide USB 3.0 interface for external SSD pluggable storage slot to host containers/application hosting	Yes
AS_MAN_08	Switch must support at least 24 x multi-rate (1/2.5/5G) ethernet ports for rich multi-media content delivery applications	Yes
AS_MAN_09	Switch must offer complete Wireless Controller functionality that handles management, control and data plane of AP	Yes
AS_MAN_10	Switch must support accelerated upgrade of software with less than 30sec of impact to traffic in a stacked deployment	Yes

Req No	Requirement Description	Must meet criteria
AS_MAN_11	Switch must provide an option of mGig port density for all 48 ports of 10 Gbps connectivity in a 1RU form factor	Yes
AS_MAN_12	Switch must support NAT features on a fixed platform	Yes
AS_MAN_13	Switch must support hot patching for software upgrades without any reboot cycles required	Yes
AS_MAN_14	Switch must support 10G, 25G and 40G QSFP+ modular uplinks for seamless migration to higher speed	Yes
AS_MAN_15	Switch must support MPLS and L3 VPN	Yes
AS_MAN_16	Switch must support IEEE 802.1ba AV Bridging (AVB)	Yes
AS_MAN_17	Switch must provide SFP (24/48 1G fiber) downlink ports and support modular uplinks	Yes
AS_MAN_18	Switch must provide SFP (24/48 1G fiber) downlink ports and stacking Bandwidth greater than 420Gbps with embedded synchronization for Layer 2 & Layer 3 protocols	Yes
AS_MAN_19	Switch must provide malware detection and traffic analysis without decrypting the encrypted traffic	Yes
AS_MAN_20	Switch should have option for 90W POE.	Yes
AS_MAN_21	Switch must support configuration of application-aware classification using deep packet inspection techniques on wired ports	Yes
AS_MAN_22	Switch must support application visibility for custom applications	Yes
AS_MAN_23	Switch stack must be able to aggregate all of the available power and manage it as one common power pool for the entire stack.	Yes
AS_MAN_24	Switch must support on-box Wireshark packet capturing	Yes

2.3.3. Core Switch Mandatory Requirements (CS_MAN)

Table 4: Core Switch Mandatory Requirements (CS_MAN)

Req No	Requirement Description	Must meet criteria
CS_MAN_01	Switch must support embedded Intel x86 architecture with up to 120GB of USB 3.0 SSD storage for container-based application hosting	Yes
CS_MAN_02	Campus Core Must Support 256-bit Macsec encryption for switch-switch links	Yes
CS_MAN_03	Campus Core Must Support multi-level segmentation over SDN fabric.	Yes
CS_MAN_04	Campus Core Must Support ability to automate on group-based policy in hardware	Yes
CS_MAN_05	Campus Core Must Support Full NetFlow based Behaviour Analytics for both ipv4 and IPv6	Yes
CS_MAN_06	Campus Core Must Support Malware detection in encrypted traffic and Distributed Security Anomaly Detection	Yes
CS_MAN_07	Switch must support IEEE 1588v2 to provide accurate clock synchronization with sub-microsecond accuracy	Yes
CS_MAN_08	Campus Core must support Hot patching to minimize traffic impact	Yes
CS_MAN_09	Campus Core must support MPLS, EoMPLS, MPLS over GRE, VPLS and L3 VPN	Yes
CS_MAN_10	Campus core should support traditional NAT and PAT	Yes
CS_MAN_11	switch must support NETCONF, RESTCONF, gRPC, YANG, ZTP, GuestShell (On-Box Python) for programming & Automation	Yes
CS_MAN_12	Campus Core must support customizable ASIC templates	Yes

2.3.4. Aggregation/Distribution Switch Mandatory Requirements (ADS_MR)

Table 5: Aggregation/Distribution Switch Mandatory Requirements (ADS_MR)

Req No	**Requirement Description**	**Must meet criteria**
ADS_MR_01	Switch must support up to 192 non-blocking 10 Gigabit Ethernet / 5 Gigabit Ethernet / 2.5 Gigabit Ethernet / 1 Gigabit Ethernet / 100 Megabit / 10 Megabit RJ45 copper ports	Yes
ADS_MR_02	Switch must support MACsec encryption on Ethernet over Multiprotocol label switching based VLANs	Yes
ADS_MR_03	Switch must support hitless software upgrade for control and data plane	Yes
ADS_MR_04	Switch must be a centralized architecture platform with dual control plane and dual data plane for zero to sub-sec failover	Yes
ADS_MR_05	Switch Must support multi-level segmentation over SDN fabric architecture.	Yes
ADS_MR_06	Switch Must support ability to automate on group-based policy	Yes
ADS_MR_07	Switch Must support Full NetFlow based Behaviour Analytics on both IPV4 & IPv6 traffic.	Yes
ADS_MR_08	Switch Must support detection of malware in encrypted traffic and Distributed Security Anomaly Detection	Yes
ADS_MR_09	Switch must support L2 and L3 MPLS VPNs	Yes
ADS_MR_10	Switch must support customizable ASIC templates	Yes

2.4. Data Center SDN

CSIR is looking for a solution that will transform its traditional data center network into a simplified, flexible, and highly scalable next-generation SDN architecture that delivers innovative network services at a low TCO. CSIR is looking to benefit from a network infrastructure solution that offers the following advantages:

(It should be noted that the requirements in section 2.4, are mandatory, and forms part of the elimination criteria).

- Accelerated application deployment through fully automated and programmatic infrastructure for application provisioning and placement
- Scalability and performance to meet both virtualized and bare-metal application deployments
- An open, programmable solution through a comprehensive published set of APIs and orchestration tool support
- Investment protection through a network foundation that supports evolution to a Software Defined Network
- Achieve resource elasticity with automation through common policies for data center operations.
- Extend consistent policy management across multiple on-premises and cloud instances for security, governance, and compliance.
- Get business continuity, disaster recovery, and highly secure networking with a zero-trust security model.

The proposed SDN should deliver an agile data center with simplified operations and increased application responsiveness to support a new generation of distributed applications while accommodating existing virtualized and non-virtualized environments. This SDN solution must be hypervisor independent and works cohesively with all types of workloads including virtual machines, physical bare-metal servers, containers, and public clouds. The SDN solution must extend capabilities to any location: small and large, on-premises and remote, private, and public cloud, satellite data centers, and 5G-enabled telecom edges.

Key Points

- **Network availability:** The SDN solution should provide highly available networks with minimal to no outages, adequate for real-time and latency-sensitive applications.
- **Micro segmentation across and between data centers:** In addition to supporting a Whitelist Policy model, the SDN solution should support and protect heterogeneous workloads including physical servers (bare metal), virtual machines, and containers across multiple data centers using micro segmentation.
- **Better automation:** The SDN solution should integrate and automate both the physical (underlay) and overlay network without requiring additional virtual resources, while providing intent-based APIs that are friendly for DevOps environments.

Optimized network

- Operational simplicity, with common policy, management, and operation models across application, network, and security resources both on premises and within an enterprise hybrid cloud environment
- A flexible and yet highly available network that allows agile application deployment within a site, across sites, and across global data centers, while removing the need for complex Data Center Interconnect (DCI) infrastructure
- Centralized network management and visibility with full automation and real-time network health monitoring
- Seamless integration of underlay and overlay networks
- Open northbound APIs creating an ideal development platform to provide flexibility for DevOps teams and ecosystem partner integration
- Common platform for managing physical and virtual environments
- Automation of workflows related to cloud management, orchestration, monitoring, and network services
- Better alignment with the strategic objectives of the organization and delivery of ongoing benefits through automation and modernization

Protecting business

- Business continuity and disaster recovery
- Inherent security with a zero-trust whitelist model and innovative features in policy enforcement, micro segmentation, and analytics
- Security at cloud scale with hardware performance

- Highly available networks with minimal to zero outages, suitable for real-time and latency-sensitive applications
- Integrated security with ecosystem partners
- Consistent security posture at scale across a multiload environment

Accelerate to multicloud

- Single policy and seamless connectivity across any data center and public cloud
- Any hypervisor, any workload, any location, any cloud
- Cloud automation enabled by integration with vRealize, AzurePack, OpenStack, OpenShift and Kubernetes

Accelerate network operations

- Operational simplicity, with common policy, management, and operation models across application, network, and security resources
- Centralized network management and visibility with full automation and real-time network health monitoring
- Seamless integration of underlay and overlay
- Open northbound APIs to provide flexibility for DevOps teams and ecosystem partner integration
- A cloud ready SDN solution
- Common platform for managing physical and virtual environments
- Automation of IT workflows and application deployment agility

Deliver superior application experience

- Single policy and seamless connectivity across any data center and public cloud
- Through any hypervisor, for any workload, at any location, using any cloud
- Cloud automation enabled by integration with vRealize, Azure Pack, OpenStack, OpenShift and Kubernetes
- Open APIs and a programmable SDN fabric

2.4.1. Data Center switch Mandatory Requirements (DC_SW_MAN)

Please refer to Table 7 below for all Data Center requirements.

Table 6: Data Center switch Mandatory Requirements (DC_SW_MAN)

Req No	Requirement Description	Must meet criteria
DC_SW_MAN_01	Must support a Clos Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol	Yes
DC_SW_MAN_02	Full cross-sectional bandwidth (any- to- any) – all possible equal paths between two endpoints are active	Yes
DC_SW_MAN_03	Must have Switch and Optics from same OEM.	Yes
DC_SW_MAN_04	The SDN solution should support all the forms of Virtualization like ESXi, KVM, Hyper-V and RHEV	Yes
DC_SW_MAN_05	Must support hardware telemetry from ASIC - Flow path trace (ingress to egress switch) Per Flow Hop by Hop packet drop with reason of drop Per Flow latency (per switch and end to end)	Yes
DC_SW_MAN_06	Must provide open scripting interface using Bash, PowerShell, NetConf, YANG from the central management appliance / SDN Controller for configuring the entire fabric.	Yes
DC_SW_MAN_07	Must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc.	Yes
DC_SW_MAN_08	Must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man – in – the – middle – attack, Replay Attack, Data Disclosure, Denial of Service.	Yes
DC_SW_MAN_09	Must support Micro Segmentation for the Virtualize and Non – Virtualize environment	Yes
DC_SW_MAN_10	Must act as a State-less distributed firewall with the logging capability	Yes
DC_SW_MAN_11	Multi DC fabric solution should provide encryption between sites using 256-bits AES	Yes

Req No	Requirement Description	Must meet criteria
DC_SW_MAN_12	Must support 500 VRF/Private network without any additional component or upgrade or design change	Yes
DC_SW_MAN_13	Must scale from 100 to 500 Tenants without any additional component or upgrade or design change	Yes
DC_SW_MAN_14	Must integrate with minimum 3 Virtual Machine Manager (i.e., vCenter, SCVMM, OpenStack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator	Yes
DC_SW_MAN_15	Must be capable of connecting 2500 physical servers and scale to 5000 physical servers	Yes
DC_SW_MAN_16	SDN Fabric must be capable of inserting physical and virtual L4 - L7 (FW, LB, IPS) services dynamically between multiple segment using policy-based traffic redirect.	Yes
DC_SW_MAN_17	Must support a minimum of 4 Leaf switches and scale up to 250 Leaf switches without any design change	Yes
DC_SW_MAN_18	Must provide Centralized management or SDN Controller must manage and provision L4 – L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager	Yes
DC_SW_MAN_19	Centralized management appliance or SDN Controller must provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity	Yes
DC_SW_MAN_20	Centralized management appliance or SDN Controller must run in “N + 1 or N + 2” redundancy to provide availability as well as function during a split-brain scenario	Yes
DC_SW_MAN_21	Must provide Uniformed Policy anywhere/everywhere across the on-prem and public cloud	Yes
DC_SW_MAN_22	Must be well integrated with most of the L4-7 vendors	Yes
DC_SW_MAN_23	Must provide fabric-wide visibility of VMware vCenter, Microsoft SCVMM, OpenStack, OpenShift, Red Hat Virtualization, Cloud Foundry, and Kubernetes	Yes

Req No	Requirement Description	Must meet criteria
DC_SW_MAN_24	Must have integration to AWS and Azure	Yes
DC_SW_MAN_25	Solution should be able to store historical data to provide anomalies and trending information of each resource (environment, configuration & operational) and graphical representation of parameters to help debug.	Yes
DC_SW_MAN_26	Solution should provide an automated mechanism to find configuration deviations, security risks & non-compliances against segmentation rules by assessing current configuration, network security policies and generate alert for any deviation to provide assurance.	Yes
DC_SW_MAN_27	Solution should provide network visibility and historical analysis between any two timeframes to identify any issues and changes including user information	Yes
DC_SW_MAN_28	The spine switch must be able to provide the following chassis options - 4 Slot, 8-Slot, and 16-Slot.	Yes
DC_SW_MAN_29	Switch must have the following interfaces: 36 line rate and Non – Blocking 40/100G ports	Yes
DC_SW_MAN_30	Switch must support a minimum of 1000 VRF instances	Yes
DC_SW_MAN_31	Must be able to provide MACsec enabled line-cards	Yes
DC_SW_MAN_32	Must support FT, FTE, SSX	Yes
DC_SW_MAN_33	Must support NetFlow and Sflow	Yes
DC_SW_MAN_34	Switch must support multi-OEM hypervisor environment and should be able to sense movement of VM and configure network automatically	Yes
DC_SW_MAN_35	Switch must support BFD For Fast Failure Detection as per RFC 5880 and RFC-7419, 3618, 7296, 7427, 7296	Yes
DC_SW_MAN_36	Switch system must support 802.1P classification and marking of packet using DSCP (Differentiated Services Code Point), Source physical interfaces, Source/destination IP subnet, Protocol types (IP/TCP/UDP), Source/destination TCP/UDP ports	Yes

Req No	Requirement Description	Must meet criteria
DC_SW_MAN_37	Switch must trust the QoS marking/priority settings of the end points as per the defined policy	Yes
DC_SW_MAN_38	Switch must support MOTD banner displayed on all connected terminals at login and security messages can be flashed	Yes
DC_SW_MAN_39	Switch must support predefined and customized execution of script for device management, automatic and scheduled system status update, monitoring and management	Yes
DC_SW_MAN_40	The solution should provide pre-change analysis of the configuration to highlight any challenges and issues before pushing the configuration within the fabric to reduce the risk of network failures and human errors for a robust change management.	Yes
DC_SW_MAN_41	Switch must support real time Packet Capture using Wireshark for traffic analysis and fault finding	Yes
DC_SW_MAN_42	Switch must support multicast routing for IPv6 network using PIMv2 Sparse Mode	Yes

2.5. NAC Mandatory Requirements (NAC_MAN)

Generally, network access control (NAC) refers to a technology that controls access to corporate infrastructure from both user-oriented devices and Internet of Things devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity. Even though NAC can integrate with other security products, post-connect policies can also be implemented. Examples are:

- Based on an alert from a SIEM, NAC could enforce a policy to contain an endpoint.
- In addition to device visibility and profiling, organizations should think about access control, security posture checks, guest management, and bidirectional integration with other security products.
- Wireless management

(It should be noted that the requirements in section 2.5, are mandatory, and forms part of the elimination criteria).

Please refer to Table 8 below for all NAC requirements.

Table 7: NAC Mandatory Requirements (NAC_MAN)

Req No	Requirement Description	Must meet criteria
NAC_MAN_01	Each policy server should be able to support up to 100000 Maximum Concurrent Sessions	Yes
NAC_MAN_02	Vendor must provide in-house NAC solution (same OEM manufactured)	Yes
NAC_MAN_03	Must support AAA, BYOD, Onboarding, Guest access, and profiling capability (DNS, Active Directory, DHCP, HTTP, RADIUS)	Yes
NAC_MAN_04	Must support compliance capabilities with posture visibility and enforcement	Yes
NAC_MAN_05	Must support device health checks with endpoint posture assessments over wireless, wired and VPN connections	Yes
NAC_MAN_06	Must offer flexible deployment options including agentless and agent-based configuration	Yes
NAC_MAN_07	NAC solution must be integrated with the centralized management platform for policy automation.	Yes
NAC_MAN_08	Must provide full endpoint visibility across the network to provide the right context of all connected devices, giving comprehensive policy control and real time enforcement	Yes
NAC_MAN_09	NAC solution must support AI based endpoint analytics	Yes
NAC_MAN_10	Must allow for manually or automatically changing the users' access privileges when there's suspicious activity, a threat or vulnerabilities discovered	Yes
NAC_MAN_11	Must provide Anomalous Endpoint Detection or anomalous network activity for threat containment	Yes
NAC_MAN_12	NAC solution must provide user identity based micro-segmentation regardless of MAC address, IP, VLAN and Subnet ID.	Yes
NAC_MAN_13	Support at least 1600 Built-in/Add-on Profile Dictionaries	Yes

Req No	Requirement Description	Must meet criteria
NAC_MAN_14	Supplicant provisioning without MDM	Yes
NAC_MAN_15	Centralized customizable dashboard allowing the view of specific kinds of information needed to monitor and understand what is occurring on the network, as to track detailed authentication records, audit trails, and details on network-access trends.	Yes
NAC_MAN_16	Should use Artificial Intelligence (AI) and machine learning capabilities to intuitively group endpoints that have common attributes and accurately identify those.	Yes

2.6. Wireless Technology Requirement (WL_TECH)

Wi-Fi has evolved from 2Mbps to 1Gbps and most recently to 10Gbps speeds. The standard has continuously advanced itself by introducing new protocols such as 802.11n, 802.11ac, 802.11ax (Wi-Fi 6) and 801.11be (Wi-Fi 7). The Wi-Fi 7 standard supports higher order of modulation and transmission of multiple streams to a single client or multiple clients simultaneously.

In addition to increasing peak data rates, spectral efficiency has been improved which characterizes how well the wireless infrastructure uses the available spectrum. Multi-user techniques such as multi-user multiple-input-multiple-output (MU-MIMO) and orthogonal frequency division multiple access (OFDMA) have been introduced to improve network efficiency and network capacity.

802.11be is the next enhancement to the 802.11 Wi-Fi series beyond 802.11ax and is call Wi-Fi 7. The maximum data rate of "ac" is 7Gbps for a Wave 2 device and the maximum data rate for "ax" is 10 Gbps, and this may be seen as only a slight increase for the next generation of Wi-Fi. This will be superseded by Wi-fi 7 with approximate rates of 30-40Gbs "EHT" for Extremely High Throughput wireless. However, the aim of IEEE 802.11ax/be is not just the headline speed, but a much better experience for users in all environments, especially where there are high user density levels on a wireless LAN. Here previous generations often struggled and in places like airports, large offices, events and the like, Wi-Fi could be terribly slow when large numbers of devices were connected.

IEEE 802.11ax, Wi-Fi 6 seeks to resolve these issues and provide a much better level of service for large numbers of users of wireless networks. Some of the key performance indicators for 802.11ax are the average per station throughput, area throughput and power efficiency. Wi-Fi 7 standards must be used if it is available when phase 3 starts. A minimum of Cat 6a Ethernet access cabling and multigig switching should be taken into consideration. NBASE-T is part of the IEEE 802.3bz specification. The specification allows for up to 10 Gbp/s over unshielded (UTP) Cat6 Ethernet cable. These speeds are possible out to the maximum allowed distance of 55 meters. Respectively, these two new port speeds are 2.5GBASE-T and 5GBASE-T or full 10GBASE-T port.

The solution must also integrate seamlessly with the software defined network protocols of the wired network to enable network access control and other security functionality such as isolated guest networks.

(It should be noted that the requirements in section 2.6, are mandatory, and forms part of the elimination criteria).

Please refer to Table 9 below for all Wireless Technology requirements.

Table 8: Wireless Technology Requirement (WL_TECH)

Req No	**Requirement Description**	**Must meet criteria**
WL_TECH_01	Support 802.11b/g/n (2.4 GHz) and 802.11a/n/ac/ax (5 GHz) on the same access point i.e. multiple radios	Yes
WL_TECH_02	Access point should be 4x4 on both radios (2.4Ghz and 5Ghz)	Yes
WL_TECH_03	Access point should be WiFI 6 certified from Wi-Fi Alliance organisation	Yes
WL_TECH_04	Support DFS channels (Std, Dual DFS, Zero-Wait DFS)	Yes
WL_TECH_05	Support manual and dynamic packet captures for wireless assurance	Yes
WL_TECH_06	Auto Radio Resource Management (RRM) - Automatically detect interference and change channels to least affected channels to provide real-time RF management.	Yes
WL_TECH_07	Must support Layer 3 roaming without adding any additional appliance.	Yes
WL_TECH_08	Support 40-, 80-, 160 MHz channels	Yes
WL_TECH_09	Support WPA2 and WPA3 enterprise	Yes

Req No	Requirement Description	Must meet criteria
WL_TECH_10	Support multi gigabit uplinks i.e. NBASE-T 2.5|5G	Yes
WL_TECH_11	Access Point shall support Off channel RRM using dedicated radio without compromising client serving radios	Yes
WL_TECH_12	Access Point shall support containers to host applications	Yes
WL_TECH_13	Access Point shall support Dual 5GHz without band locking to certain channels	Yes
WL_TECH_14	Access Point shall be able to support full radio features at 802.3at	Yes
WL_TECH_15	Support internal only and external antennae (not on the same ap)	Yes
WL_TECH_16	Access Point shall support dedicated radio for spectrum monitoring capabilities without compromising client serving radios	Yes
WL_TECH_17	Access Point contain 2GB or higher-sized DRAM for capacity	Yes

2.6.1. Wireless Security Requirements (WL_SEC)

Security was an IT manager's main concern in the past and the reason WLANs were not implemented. However, as the ubiquity of wireless devices drove demand from end users, evolving wireless standards have solved these security issues to the point where a properly implemented wireless network is more secure than most wired networks.

The original standard for wireless security was proven to be insecure but the problem has been solved by the IEEE802.1x protocol. 802.1X is the strongest form of Wi-Fi authentication, but it is more expensive and difficult to set up and maintain.

Rogue APs have long been a headache to IT managers. Network admins waste countless hours tracking down unauthorized devices. Two fundamental issues drove rogue AP's: (1) lack of corporate Wi-Fi and (2) cheap home APs that required little network knowledge to install and configure.

The later made it simple for employees to bring rogue APs to the workplace and are possibly the first case of consumer products critically impacting tightly controlled corporate networks. Rogue AP detection and location services in modern enterprise-class Wi-Fi systems have given IT powerful tools to combat these devices.

Wireless Client Isolation plays a key role in modern day Wi-Fi networks. End users usually do not have any need to directly access each other's machines. The 802.11i standard defines two authentication methods - WPA2-Enterprise and WPA2-. WPA2-Enterprise is extremely secure and is built around the 802.1X port authentication standard. The proposed Wireless solution should be based on IEEE802.11i standards. A minimum of WPA-2 and WPA-3 should be supported, with the ability to integrate with RADIUS or 802.11x services.

Please refer to Table 10 below for all Wireless Security requirements.

Table 9: Wireless Security Requirements (WL_SEC)

Req No	Requirement Description	Must meet criteria
WL_SEC_01	Wireless Intrusion Prevention System to protect against DoS attacks, management frame attacks, tool-based attacks etc	Yes
WL_SEC_02	Customizable WIPS detection rules via simple workflows i.e. no coding required	Yes
WL_SEC_03	Support forensic packet capture per signature	Yes
WL_SEC_04	Detect threats using signature-based techniques	Yes
WL_SEC_05	Use network intelligence and analytics to detect threats	Yes
WL_SEC_06	Radios can serve clients and scan for possible threats simultaneously	Yes
WL_SEC_07	Detect and alert on rogue or unknown access points	Yes
WL_SEC_08	Support isolation of client devices	Yes
WL_SEC_09	Support posture verification before clients may connect	Yes
WL_SEC_10	Support for Network access control and a management console to quarantine and update devices before authorising access to the network	Yes

2.6.2. Deployment Requirements (WL_DEP)

Accurate network planning is one of the most critical steps in a successful Wi-Fi deployment, as poor planning can result in best effort coverage, unhappy users, and over-spending on infrastructure.

The following design considerations need to be considered:

- Application planning: triple play, bandwidth
- Capacity planning: connections per AP, physical size of building(s) and wall construction materials
- Coverage planning: indoor, outdoor
- Deployment planning: physical layout of building(s), optimum AP deployment, mounting options, aesthetics
- RF planning: active & passive reports

A robust, ubiquitous, and high-performance WLAN can deliver a quality connection comparable to like a wired network if “Best Practices” are followed during the design phase.

The proposed Wireless solution must take all above planning into consideration. Active and passive RF reports need to be generated pre and post Wi-Fi design, and in accordance with the required services to be facilitated by the Wi-Fi solution.

Please refer to Table 11 below for all Wireless Deployment requirements.

Table 10: Wireless Deployment Requirements (WL_DEP)

Req No	**Requirement Description**	**Must meet criteria**
WL_DEP_01	Support tunnelling data via controllers or direct to VLAN	Yes
WL_DEP_02	Provide on-premise deployment support	Yes
WL_DEP_03	Provide multiple access point types for normal, outdoor, and high-density high throughput conference areas	Yes
WL_DEP_04	Able to deploy countrywide to all regional offices with central management	Yes
WL_DEP_05	Support of HA/clustering on controllers without adding additional hardware	Yes
WL_DEP_06	Access points support POE power delivery	Yes
WL_DEP_07	External Antennas must be OEM manufactured.	Yes
WL_DEP_08	Support ceiling and wall mounting options	Yes

2.6.3. Wireless Management Requirements (WL_MAN)

Network management is an important component of modern IT operations and service delivery. As networks grows, new devices, applications and services are added. As requirements and landscape changes occur, there can be a knock-on effect on the network. Network management enables administrators to manage and monitor the network, ensuring overall reliability, availability, and performance. Wireless network management enables IT admin staff with greater control and flexibility in the day-to-day management of their Wi-Fi network. A modern-day network management solution provides a single-pane-of-glass visibility for superior AP inventory monitoring and management, and AP health visibility.

Ideally, a Wireless network management solution should provide the following:

- Global Wireless network visibility
- Wireless network health monitoring & reporting
- AP monitoring & reporting
- Controller monitoring & reporting
- Wireless client analytics
- Incident tracking

The proposed Wireless solution must include a Wireless monitoring service that provides comprehensive monitoring, reporting and analytics services as stipulated above.

Please refer to Table 12 below for all Wireless Management requirements.

Table 11: Wireless Management Requirements (WL_MAN)

Req No	Requirement Description	Must meet criteria
WL_MAN_01	Provide full management console that allows management of all controllers, access points, and clients country wide	Yes
WL_MAN_02	Provide wireless SDN Fabric support (VXLAN) and integration with wired fabric.	Yes
WL_MAN_03	Support captive portals for guest management and posture assessment mitigation	Yes

Req No	Requirement Description	Must meet criteria
WL_MAN_04	Supports Cloud and on-premises wireless controllers with full wireless functionality.	Yes
WL_MAN_05	Automated load balancing of clients across access points	Yes
WL_MAN_06	Support scalability to 1500x APs	Yes
WL_MAN_07	Support guest management with various self-registering options up to 2000x guests	Yes
WL_MAN_08	Planning, Deployment and Maintenance support via gold or better partner is available locally	Yes
WL_MAN_09	Support software defined network integration between LAN and Wi-Fi	Yes
WL_MAN_10	The Wireless solution must fully integrate with the proposed wired SDN solution.	Yes
WL_MAN_11	The solution must provide a unified management solution for both the wired and wireless components.	Yes
WL_MAN_12	The solution must provide a consistent security policy and services across both wired and wireless networks.	Yes
WL_MAN_13	Management of wired and wireless networks and users from a single interface.	Yes

2.7. Information Security Business Requirements (ISO_BUS)

There are few business requirements regarding information security, but Policies and Standards must be adhered to. These include the following legislation:

(It should be noted that the requirements in section 2.7, are mandatory, and forms part of the elimination criteria).

- The National Key Point Act, 1980 (Act No. 102 of 1980)
- Public Finance Management Act (Act No.1 of 1999 as amended by Act 29 of 1999)
- The Regulation of Interception of Communications and Provision of Communication- related
- Information Act (Act No. 70 of 2002) (“RICA”)
- Promotion of Access to Information Act (Act No.2 of 2000)
- Electronic Communications and Transactions Act (Act No 25 of 2002)
- The National Strategic Intelligence Act (Act No. 39 of 1994)

- Protection of Personal Information Act 4 of 2013 (POPIA)
- Minimum Information Security Standards (MISS)

Please refer to Table 13 below for all IS Business requirements.

Table 12: Information Security Business Requirements (ISO_BUS)

Req No	**Requirement Description**	**Must meet criteria**
ISO_BUS_01	Implement controlled access to network resources in the organisation, including network access control (avoid unrestricted access to networks).	Yes
ISO_BUS_02	Where possible, implement role-based access for provisioning access to network resource. This ensures that access is normalised across the organisation.	Yes
ISO_BUS_03	Implement a network segmentation approach.	Yes

2.8. High-Level Design (HLD)

This is a global overview of the solution, with a basic description of all the modules and parts based on the below requirements. Some terms might include Zoning, Traffic flow, high-level connectivity, etc across the various elements of the solution. Please refer to Table 14 below for all HLD requirements.

(It should be noted that the requirements in section 2.8, are mandatory, and forms part of the elimination criteria).

Table 13: High-Level Design (HLD)

Req No	**High Level Design consisting of the following criteria**	**Must meet criteria**
HLD	Keep a revision history to track updates Describe the business goals the solution is addressing Provide high level estimated timelines of major phases Describe the Scope and Scale of the project e.g., number and types of site	Yes

Req No	High Level Design consisting of the following criteria	Must meet criteria
	Provide overview of the current network Provide overview of the new solution Provide high level network diagram(s) and topology information Describe individual components that make up the solution and design Describe redundancy and HA features of the design Describe any special requirements of the design if any Provide benefits of the solution Describe potential future expansion (e.g. Integration with cloud) Describe potential additional add-on features	

2.9. Low-Level Design (LLD)

The LLD is a follow-on and expands on the HLD that provides detailed and in-depth information on how the network will be configured. Also, it should include features such as VLAN, IP address, and port numbering, which will be developed during the planning, implementation, and post-implementation of the project. The LLD should be updated after the completion of each phase. Please refer to Table 15 below for all LLD requirements.

(It should be noted that the requirements in section 2.9, are mandatory, and forms part of the elimination criteria).

Table 14: Low-Level Design (LLD)

Req No	Low Level Design consisting of the following criteria	Must meet criteria
LLD	Keep a revision history to track updates Define the scope of the LLD List related documents associated with the LLD Overview of the HLD Overview of hardware and software used in the solution Detailed overview of the technology used in the solution List limitations and scalability Define device naming conventions and list device names	Yes

Req No	Low Level Design consisting of the following criteria	Must meet criteria
	Record device asset and serial numbers Describe how Out-of-band and/or in-band management will be configured List device management IP addresses Provide device administration access control Define and record IP address, subnet, VLAN allocations and assignments Provided detailed connectivity diagrams Describe firmware and/or software image management standards and procedures Define security policies and configuration Define solution policies Record cabling matrix, should include From_Device, From_Port, To_Device, To_Port, Transceiver, Cable Type, Rack_From, Rack_To Signed off by OEM and is in line with best practice	

2.10. Datacentre Technical Requirements (DC_REQ)

Please refer to Table 16 below for all Datacentre requirements.

(It should be noted that the requirements in section 2.10, are mandatory, and forms part of the elimination criteria).

Table 15 Datacentre Technical Requirements (DC_REQ)

Req No	Requirement Description	Must meet criteria
DC_REQ_01	Support standard 19-inch data centre rack technology	Yes
DC_REQ_02	Support redundant power supply, multiple power supplies to be fed from alternative Data Centre power sources	Yes
DC_REQ_03	Support IEC C13 power supply cable connection type	Yes
DC_REQ_04	Support rack mountable fitment into a standard 19-inch data centre rack	Yes
DC_REQ_05	Support standard data centre rack rail measurements (i.e. “U” placements)	Yes

2.11. Operational Business Requirements (OP_BUS)

Please refer to Table 17 below for all Operational Business requirements.

(It should be noted that the requirements in section 2.11, are mandatory, and forms part of the elimination criteria).

Table 16: Operational Business Requirements (OP_BUS)

Req No	Requirement Description	Must meet criteria
OP_BUS_01	Co-existence and interoperability with ALE, Checkpoint, Aruba, and Extreme Networks technologies	Yes
OP_BUS_02	Mobile enabled management console with scalable dashboarding and reporting	Yes
OP_BUS_03	Software Defined networking and orchestration	Yes
OP_BUS_04	Training and certification with multiple channel partners in South Africa (more than 5) and at least 3 in Gauteng.	Yes
OP_BUS_05	Models acquired by the CSIR, must be supported and maintained for a period of not less than 10 years by the OEM. This includes Hardware, software/firmware and peripherals	Yes
OP_BUS_06	Asset, configuration, and release management	Yes
OP_BUS_07	Local partners are to provide support to all CSIR offices	Yes

2.12. Legal/Regulatory requirements (L-LR)

Please refer to Table 18 below for all Legal/Regulatory requirements.

(It should be noted that the requirements in section 2.12, are mandatory, and forms part of the elimination criteria).

Table 17: Legal/Regulatory requirements (L-LR)

Req No	Requirement Description	Must meet criteria
L-LR_1	Regulation of Interception of Communications and Provision of Communication-related Information Act, 70 of 2002.	Yes
L-LR_2	Electronic Communications and Transactions Act 25 of 2002 (ECT).	Yes
L-LR_3	Protection of Personal Information Act 4 of 2013 (POPIA)/GDPR.	Yes

Req No	**Requirement Description**	**Must meet criteria**
L-LR_4	Scientific Research Amendment Act, No. 71 of 1990.	Yes
L-LR_5	ICASA amendment Act (Independent Communications Authority of South Africa Act, 2000 and Icasa Amendment Act 2006)	Yes

2.13. Training

Please refer to Table 19 below for all Training requirements.

(It should be noted that the requirements in section 2.13, are mandatory, and forms part of the elimination criteria).

Table 18: Training

Req No	**Training requirement description**	**Must meet criteria**	**Training provided to**
W_TRAIN_01	Provide training for planning, deployment, management, and maintenance on ALL supplied equipment and software (OEM certified training)	Yes	5 Network Engineers
W_TRAIN_02	Provide integration training and support	Yes	5 Network Engineers

3. EVALUATION CRITERIA

The CSIR has set minimum standards that a bidder needs to meet in order to be evaluated and selected as a successful bidder. The minimum standards consist of the following:

Pre-Qualification and Elimination Criteria (Phase 1)	**Technical Evaluation Criteria (Phase 2)**	**Preferrential Points (Phase 3)**

Only bidders that comply with ALL the criteria set on **Phase 1** below will proceed to Technical/Functional Evaluation (Phase 2).	Bidder(s) are required to achieve a minimum threshold of 80 points out of 100 points overall. Only bidder (s) who meet and/or exceed the minimum threshold points on Phase 2 will proceed to Phase 3.	Bidders will be evaluated on Prefferential Points system of 90/10
		Price = 90
		B-BBEE = 10

3.1. ELIMINATION CRITERIA

Proposals will be eliminated under the following conditions:

- Proposals received after the deadline,
- Proposals submitted at the incorrect location,
- Bidders that are listed on the National Treasury database of restricted suppliers,
- Bidders that are registered on the National Treasury Register of Tender Defaulters,
- Non-submission of any of the Annexures A-B D-M, and AB,
- Non-attendance of the compulsory briefing session,
- Failure to complete, sign and submit SBD 1 and SBD 4 forms,
- Failure to submit the tenderer's accreditation certificates on Partner documentation from OEM (Refer to Annexure F),
- **Failure to provide a signed letter of intent to obtain a financial guarantee before the contract is awarded**
- Bidders who fail to meet the Functional criteria, as specified in Annexure A Technical Requirements,
- Bidders who fail to submit their agreement with the OEM**.**

The CSIR will use the workbook Annexure AC: Elimination criteria, to record the outcome of the Elimination criteria.

3.2. FUNCTIONAL EVALUATION CRITERIA

The evaluation of the functional/technical criteria will be based on **PART 1 TECHNICAL PROPOSAL.xlsx**, which covers the following sections:

- Bidder to submit a comprehensive Annexure B: Project plan, which contributes 25% of the overall score.
- Bidder to submit an Annexure D: SLA Performance requirements, which contributes 20% of the overall score.
- Bidder to submit an Annexure AB, which will be used to conduct site visits, contributing 15% of the overall score
- Bidder to submit an Annexure E: Company related documents, which contributes 40% of the overall score.

The site visits will serve as confirmation that the Bidder has demonstrated the requisite capability to implement the required specification.

Error! Reference source not found., provides an indication of the Functional evaluation criteria to be used during the scoring process of each bid.

Table 19: PART 1 TECHNICAL PROPOSAL evaluation criteria and scoring matrix

Functional Factors	Proof Required	Weighting	Scoring Mechanism	Points achieved per section	Weighted score	Individual section result	Min score required
Project plan	Bidder to submit a comprehensive **Annexure B: Project plan**	25%	This section is scored in **PART 1 TECHNICAL PROPOSAL.xlsx workbook**, sheet **Annex B Project plan**				Overall: 80% Each of the individual criteria >=5
SLA Performance	**Annexure D: SLA Performance requirements**	20%	This section is scored in **PART 1 TECHNICAL PROPOSAL.xlsx workbook**, sheet **Annexure D: SLA Performance requirements**				Overall: 80% Each of the individual criteria >=5
Site evaluation	**Site evaluation**	15%	This section is scored in **PART 1 TECHNICAL PROPOSAL.xlsx workbook**, sheet **Site evaluation**				Overall: 80% Each of the individual criteria >=5
Company Experience	**Annexure E: Company related documents**: Company profile indicating the number of years the company has been in existence and actively operating in the Networking industry	40%	This section is scored in **PART 1 TECHNICAL PROPOSAL.xlsx workbook**, based on the company related documentation submitted, as articulated in **Annexure E: Company related documents**				Overall: 80% Each of the individual criteria >=5

Proposals with functionality / technical points of less than the predetermined **minimum overall percentage of 80%,** will not pass through the next step in the evaluation process.

In addition, the individual sections Annexure B: Project plan, Annexure D: SLA Performance requirements, and Site evaluation **must score 80% or more,** each, to pass to the next step in the evaluation process.

Annexure E: Company related documents: Company profile indicating the number of years the company has been in existence and actively operating in the Networking industry **must score 50% or higher**, to progress to the next step of evaluation.

4. ANNEXURE M: RETURNABLE DOCUMENTS CHECKLIST

This Annexure provides guidance to the Bidder to ensure all returnable documents are submitted.

Please complete **Annexure M Returnable documents checklist.docx**.

RETURNABLE DOCUMENTS –		
Electronic File 1: **PART 1: TECHNICAL PROPOSAL**		
Description and Bid submission structure reference	**Included**	
	Yes	**No**
A.1 Signed Declaration by Bidder (Section 26 of RFP document)		
A.2 Completed and duly signed Expressions of Interest Form (Annexure AA)		
A.3 Completed and signed PART 1 TECHNICAL PROPOSAL sections		
A.3.1 Annexure A: Technical requirements (this annexure will form part of the Elimination criteria)		
A.3.2 Annexure B: Project plan • Table 22: Project implementation schedule table • Table 23: Risk management table • Table 24: Table of assumptions • Table 25: Table of Inclusions and Exclusions • Table 26: Stakeholder management table • Table 27: Stakeholder classification categories		
A.3.3 Annexure C: Non-Disclosure Agreement		
A.3.4 Annexure D: SLA Perf requirements • Sample reports for the CORE, Distro, Access, and Wireless services • The reports should include at least: ○ Number of calls logged per month ○ MTTR ○ Root Cause Analysis report for all incidents/requests. ○ Summary of maintenance and support actions undertaken per month		
A.3.5 Annexure E: Company related documents (Holding company vs subsidiary, Company Profile, Joint venture, memorandum of understanding etc.) **Completed: Annexure E Company related documentation.xlsx**		
A.3.6 Annexure F: OEM assurance • Proof of certifications for the respective technical roles from the OEM • Proof of Tier level with OEM		
A.4 Any other information the bidder wishes to submit, e.g. marketing messages, sales executive messages, etc. This information must not contain any pricing information		
A.5 Any other technical information the bidder wishes to share as part of the technical submission, e.g. Network diagrams, SLA info, etc. This information must not contain any pricing information.		
A.6 Annexure AB: SCHEDULE OF BIDDER’S EXPERIENCE AND REFERENCE SITES • Table 29: Site visit reference list		

Electronic File 2: **PART 2: PRICING PROPOSAL**		
B.1 Annexure G: Pricing Proposal (PART 2: PRICING PROPOSAL.XLSX)		
B.1.1 PART 2 PRICING PROPOSAL		
B.1.2 Table 3 Network HW population		
B.2 Annexure I: Certified copy of valid B-BBEE Certificate or sworn affidavit		
B.3 Annexure H: Completed SBD1 Form		
B.4 Annexure J: Recent audited financial statements		
B.5 Annexure K: Pricing Guarantee		
B.6 Annexure L: Completed SBD4 Form		
B.6 Annexure M: Returnable documents checklist		