ANNEXURE A2

Pre-Qualifying Criteria

CSIR Network upgrade (design, provisioning, implementation, maintenance and support) for Five (5) Years

RFP No. 3551.1/29/09/2023

*Note: Proposals with less than the minimum score of 1120 out of 1360 points for Pre-Qualifying Criteria will be disqualified from further evaluation on technical evaluation.

1. Purpose

The purpose of this document is to list the CSIR technical requirement specification as part of RFP No. 3551.1/29/09/2023 to allow the bidder to respond to the tender with their proposal, measured against the CSIR requirement.

2. Instruction

The bidder must complete the table in section 4 of this document and return the completed and signed Annexure A2 with the bid submission. The bidder is required to indicate where the technology of their proposal will satisfy each of the CSIR requirements and provide the relevant confirmation by either providing an internet link, pointing to a section or paragraph in the documentation included in the proposal and inserting captures (images) confirming the fulfilment of the requirement. Bidder must also indicate where an OEM-specific name replaced an open standard, e.g., S-Flow, NetFlow, NetStream.

3. Evaluation

Each of the criteria listed in the requirements specification of section 4 of this Annexure will be evaluated and scored as follows:

Non-compulsory items:

- Meets = 10
- Partially Meet = 5
- Does not Meet = 0

Compulsory items (Indicated with an *):

- Meets = 10
- Does not Meet = 0

The minimum score to pass the pre-qualifying evaluation is 1120 out of 1360.

Moreover, each of the requirements in section 4 carries equal weight.

Please note the following explanation about “Meets” requirements, “Partially meets” requirements and “Does Not Meet” requirements:

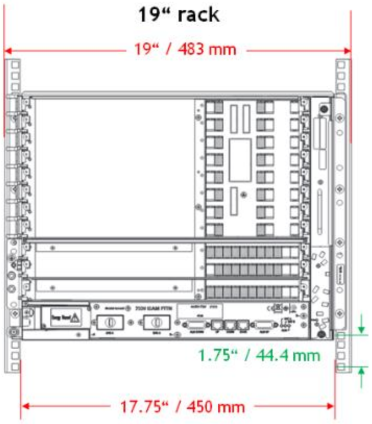
- **Does not meet requirements**: This outcome indicates that the bidder has failed to meet one or more of the specified networking requirements. The bidder's proposed solution or offer does not fulfil the minimum criteria outlined in the tender. It signifies that the bidder's submission does not comply with the essential aspects of the networking requirements, and therefore, a score of 0 will be attained.

- **Partially meets requirements:** This outcome suggests that the bidder has partially addressed the networking requirements but has not fully satisfied all of them. The bidder's proposed solution or offering falls short in some aspects, either in terms of functionality, performance, scalability, security, or other specified criteria. While the bidder has tried to meet some requirements, further evaluation and clarification may be necessary to determine whether the partial fulfilment is acceptable or if the deficiencies outweigh the strengths. Therefore, a score of 5 will be attained.
- **Meets requirements:** This outcome indicates that the bidder has fulfilled all the specified networking requirements outlined in the tender. The bidder's proposed solution or offering aligns with the desired outcomes and complies with the stated criteria. It demonstrates that the bidder thoroughly understands the requirements and has presented a comprehensive solution that meets all the necessary aspects. In this case, the bidder's submission is considered compliant, and therefore, a score of 10 will be attained.

4. Requirement Specification

The table below references the requirement specification for RFP No. 3551.1/29/09/2023 to be completed and returned with the bidder’s response per the instruction in section 2 of this document. The Request for Proposal (RFP) document aims to establish requirements without showing a preference for any particular Original Equipment Manufacturer. However, some descriptions may accidentally use language from specific vendors. We encourage vendors to suggest alternative technologies or solutions from their product range that can achieve similar results. In such cases, we request bidders to present a detailed functional comparison between their proposed technology and adequate requirements to ensure a just and impartial evaluation of all possible solutions.

TABLE 1: REQUIREMENTS SPECIFICATION AND BIDDER RESPONSE

Number	Requirement	Bidder Response (Confirm Fulfilment)
EXAMPLE	Support standard 19-inch data centre rack technology.	Our technology will satisfy the requirements as indicated below:  19“ rack 19“ / 483 mm 1.75“ / 44.4 mm 17.75“ / 450 mm Weblink: [Wikipedia]()
Wired network requirements		
WN_01*	The switch should have a centralised management platform for wired analytics, configuration templates and anomaly detection.	
WN_02*	Network security integration (e.g., IPS, IDS, 802.1X, Cloud-based DNS security, Anomaly detection, etc.).	
WN_03*	Network automated policy enforcement from a centralised management platform.	
WN_04	AI- and ML (or equivalent) -enabled network assurance tools from the Centralised management dashboard.	
WN_05	Must provide user identity-	

	based Micro-segmentation regardless of VLAN, Subnet ID, and Mac address for granular security.	
WN_06*	Access solution that is SDN enabled and supports VXLAN, EVPN or similar IEEE standard virtualisation protocol.	
WN_07*	Provide a single policy for both wired and wireless solutions.	
Access layer switch requirements		
AS_01*	The switch must support Network automation & programmability.	
AS_02	The switch must support MACsec (128- or 256-bit encryption) on all downlink and uplink ports.	
AS_03*	The switch should support field-replaceable redundant power supplies and fans.	
AS_04*	The solution must provide the ability to support all connectivity, ranging from low-end (10Mbps) to high-speed (10Gbps) connectivity for network endpoints, by offering a range of port speeds, including multi-gigabit speeds. The solution should support a range of form factors and port densities, including those suitable for small, medium, and large-scale networks, preferably in the 1RU form factor.	

AS_05	Switch must provide (24/48 1G copper) downlink ports and support 10G, 25G and 40G modular SFP/QSFP+ uplinks for seamless migration to higher speeds.	
AS_06*	The switch must support at least 30W POE (POE+ or 802.3at).	
AS_07	The switch must support the configuration of application-aware classification using deep packet inspection techniques on wired ports.	
AS_08	The switch must support application visibility for custom applications.	
Core switch requirements		
CS_01	Campus Core must support 256-bit MACsec encryption for switch-switch links.	
CS_02*	Campus Core must support multi-level segmentation over SDN fabric.	
CS_03*	Campus Core must support the ability to automate a group-based policy in hardware.	
CS_04*	Campus Core must support NetFlow/Sflow or similar industry standard Behaviour Analytics for IPv4 and IPv6.	
CS_05*	The switch must support programmability & automation.	
Aggregation/Distribution switch requirements		
ADS_01*	The switch must support non-	

	blocking, wire speed architecture.	
ADS_02*	The solution must provide the ability to secure traffic flows between endpoints over the network by using encryption technology. The solution should support a range of encryption technologies and VLAN types, including those based on MACsec encryption and Multiprotocol label switching-based VLANs. The solution should be able to interoperate with the existing network infrastructure and be flexible enough to adapt to changing business requirements.	
ADS_03*	The switch must support multi-level segmentation over SDN fabric architecture.	
ADS_04*	The switch must support the ability to automate a group-based policy.	
ADS_05*	The switch must support NetFlow/Sflow or similar-based Behaviour Analytics on both IPv4 & IPv6 traffic.	
Data Centre switch requirements		
DC_SW_01*	The solution must provide the ability to support a scalable and resilient network architecture that can handle the required traffic flows and provide high availability. The solution should support a range of network	

	architectures and protocols, including those based on Spine-Leaf topology and VXLAN encapsulation. The solution should be able to interoperate with the existing network infrastructure and be flexible enough to adapt to changing business requirements.	
DC_SW_02	Full cross-sectional bandwidth (any- to- any) – all possible equal paths between two endpoints are active.	
DC_SW_03*	It is preferred that the solution provide the ability to support the same brand optic components, ensuring compatibility with the chosen switches. Alternatively, the solution should be flexible enough to allow for optics from multiple vendors as long as they meet the required specifications and are compatible with the switches. Using different vendors for switches and optics should not compromise the functionality or performance of the network.	
DC_SW_04*	The SDN solution should support all the forms of Virtualization like ESXi, KVM, Hyper-V and RHEV.	
DC_SW_05*	Must provide an open scripting interface using Bash, PowerShell, NetConf, and YANG from the central	

	management appliance / SDN Controller for configuring the entire fabric.	
DC_SW_06	Must have zero trust policy model for connected systems or hosts to help protect against attacks like Unauthorized Access, Man-in-the-middle-attack, Replay Attack, Data Disclosure, and Denial of Service.	
DC_SW_07*	Must support Micro-Segmentation for the Virtualized and Non–Virtualized environment.	
DC_SW_08*	Multi DC fabric solution should provide encryption between sites using 256-bit AES.	
DC_SW_09*	The solution must support at least 500 VRFs or private networks to meet the organisation's current and future needs without requiring additional components or significant design changes. The solution should provide scalability and flexibility in the number of VRFs or private networks supported to ensure that it can adapt to changing requirements and growth.	
DC_SW_10	Must be able to scale from 100 to 500 Tenants without any additional component, upgrade, or design change.	
DC_SW_11*	Must integrate with a minimum	

	of 3 Virtual Machine Managers (i.e., vCenter, SCVMM, OpenStack, etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without a common orchestrator.	
DC_SW_12	Must be capable of connecting 2500 physical servers and scale to 5000 physical servers.	
DC_SW_13	SDN Fabric must be capable of inserting physical and virtual L4 - L7 (FW, LB, IPS) services dynamically between multiple segments using policy-based traffic redirect.	
DC_SW_14	The solution must provide the ability to manage centrally, provision L4-L7 services, including physical or virtual appliances, and integrate with virtual machine management systems. The management and provisioning functionality should be agnostic to the specific vendor or technology used for the L4-L7 services or virtual machine management, allowing for flexibility and interoperability with a variety of solutions such as vSphere, Hyper-V, XenServer, Xen, and KVM.	
DC_SW_15	A centralised management appliance or SDN Controller must provide dynamic device inventory of the Fabric as well as the current network topology	

	of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.	
DC_SW_16*	A centralised management appliance or SDN Controller must run in “N + 1 or N + 2” redundancy to provide availability and function during a split-brain scenario.	
DC_SW_17*	The solution must support consistent policy management across all environments, including on-premises and public cloud environments, to ensure uniformity and ease of management. The solution should provide a flexible policy management framework that allows policies to be applied consistently across multiple environments without being tied to any specific cloud provider or technology.	
DC_SW_18	The solution must be designed to integrate with a wide range of Layer 4-7 networking products, such as load balancers, firewalls, content switches, and application delivery controllers. The integration should be seamless, with no dependency on any particular vendor's solution, allowing for flexible deployment options and future-proofing. The solution should	

	provide comprehensive documentation and support for integration with various Layer 4-7 vendors to ensure successful implementation and optimal performance.	
DC_SW_19	Must provide fabric-wide visibility of VMware vCenter, Microsoft SCVMM, OpenStack, OpenShift, Red Hat Virtualization, Cloud Foundry, and Kubernetes.	
DC_SW_20*	The solution must be capable of integrating with public cloud platforms, but at the minimum, Amazon Web Services (AWS) and Microsoft Azure. This feature should be a standard system function, allowing for efficient and secure integration with cloud resources. The implementation should comply with industry-standard specifications to ensure compatibility with a wide range of public cloud providers.	
DC_SW_21	The solution should be able to store historical data to provide anomalies and trending information of each resource (environment, configuration & operational) and a graphical representation of parameters to help debug.	
DC_SW_22	The 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 generating alerts for any deviation to provide assurance.	
DC_SW_23	The solution should provide network visibility and historical analysis between two timeframes to identify issues and changes, including user information.	
DC_SW_24	Switch must have the following interfaces: 30-line rate and Non – Blocking 40/100G ports.	
DC_SW_25*	The switch must support NetFlow/Sflow or similar based Application Analytics for both IPV4 & IPv6 traffic.	
DC_SW_26	Switches must support failure detection on uplinks and downlinks.	
DC_SW_27	The switch system must support 802.1P classification and marking of packets using DSCP (Differentiated Services Code Point), Source physical interfaces, Source/destination IP subnet, Protocol types (IP/TCP/UDP), Source/destination TCP/UDP ports.	
DC_SW_28	The switch must trust the end points' QoS marking/priority	

	settings as per the defined policy.	
DC_SW_29	Switch must support the MOTD banner displayed on all connected terminals at login, and security messages can be flashed.	
DC_SW_30	The switch must support predefined and customised execution of scripts for device management, automatic and scheduled system status updates, monitoring, and management.	
DC_SW_31	The switch must support multicast routing for the IPv6 network using PIMv2 Sparse Mode.	
NAC requirements		
NAC_01*	The NAC solution must support at least a maximum of 100,000 concurrent sessions per policy server to provide sufficient capacity for the organisation's needs.	
NAC_02*	The NAC solution must be an integrated, in-house solution fully supported by the vendor to ensure seamless integration and ongoing support.	
NAC_03*	Must support AAA, BYOD, Onboarding, Guest access, and profiling capability (DNS, Active Directory, DHCP, HTTP, RADIUS).	
NAC_04*	Must support compliance	

	capabilities with posture visibility and enforcement.	
NAC_05*	Must support device health checks with endpoint posture assessments over wireless, wired and VPN connections.	
NAC_06*	Must offer flexible deployment options, including agentless and agent-based configurations.	
NAC_07*	NAC solution must be integrated with the centralised management platform for policy automation.	
NAC_08*	Must provide complete endpoint visibility across the network to provide the right context of all connected devices, giving comprehensive policy control and real-time enforcement.	
NAC_09*	The NAC solution must be capable of providing detailed endpoint profiling and application analytics. This feature should be included as a standard system function, allowing for accuracy and efficiency.	
NAC_10*	Must allow for manually or automatically changing the users' access privileges when suspicious activity, a threat or vulnerabilities are discovered.	
NAC_11*	NAC solution must provide user identity-based micro-segmentation regardless of MAC address, IP, VLAN and	

	Subnet ID.	
NAC_12	Support at least 1600 Built-in/Add-on Profile Dictionaries.	
NAC_13*	Supplicant provisioning without mobile device management MDM (Supplicant = endpoint device communicating with the NAC).	
NAC_14	A centralised customisable dashboard allows the view of specific kinds of information needed to monitor and understand what is occurring on the network and track detailed authentication records, audit trails, and details on network-access trends.	
NAC_15*	The NAC solution should support endpoint grouping and attribute identification using advanced analytics capabilities based on next-generation technologies.	
NAC_16	The system must support guest management with various self-registration options for up to 2000 guests. The solution should not require additional licensing or systems to manage 2000 guests beyond the number of CSIR user devices. The implementation should comply with industry-standard specifications to ensure compatibility with a wide range of network devices.	

NAC_17*	Must support at least 5000 devices for CSIR users without purchasing extra licensing, excluding guest devices.	
Wireless Technology requirements		
WL_TECH_01*	Wi-Fi 6E - must support 802.11b/g/n/ac/ax (2.4 GHz), 802.11a/n/ac/ax (5 GHz) and 802.11ax (6 GHz).	
WL_TECH_02	The access point should be 4x4 on three radios (2.4Ghz, 5Ghz and 6Ghz) - MU-MIMO.	
WL_TECH_03*	The access point should be Wi-Fi 6 certified from the Wi-Fi Alliance organisation.	
WL_TECH_04*	Support DFS channels (Std, Dual DFS, Zero-Wait DFS).	
WL_TECH_05	The system must be capable of capturing data packets manually or dynamically. This feature should be included as a standard system function, allowing the capture of data packets as needed. The implementation should comply with industry-standard specifications to ensure compatibility with a wide range of network devices.	
WL_TECH_06*	The system must automatically detect and mitigate interference by identifying the least affected channels and changing to them in real time to ensure efficient RF management. The implementation should comply	

	with industry-standard specifications to ensure compatibility with a wide range of network devices.	
WL_TECH_07*	Must support Layer 3 roaming without adding any additional appliance.	
WL_TECH_08*	Support 20-, 40-, 80- and 160 MHz channels.	
WL_TECH_09*	Support WPA2 Enterprise and WPA3 Enterprise.	
WL_TECH_10*	The equipment must support dual multi-gigabit uplinks, including NBASE-T 2.5|5G (mGig) or 802.11bz technology where high throughput is required. The implementation should comply with industry-standard specifications to ensure compatibility with a wide range of network devices.	
WL_TECH_11*	The access point must support Off-channel Radio Resource Management (RRM) using a dedicated radio without affecting the performance of client-serving radios. This capability should be included as a standard feature of the access point.	
WL_TECH_12*	Access Point shall support software programmable radio modes to support client performance.	
WL_TECH_13*	Access Point shall be able to support full radio features at	

	30W POE (POE+ or 802.3at) or higher.	
WL_TECH_14*	Support internal antennae.	
WL_TECH_15*	Provide spectrum monitoring capabilities that do not affect the quality of service for client devices. The solution should conform to industry-standard techniques for spectrum monitoring and provide the ability to perform spectrum monitoring, preferably using a dedicated radio, without affecting the performance of client-serving radios.	
Wireless Security requirements		
WL_SEC_01*	Wireless Intrusion Prevention System to protect against DoS attacks, management frame attacks, tool-based attacks, etc.	
WL_SEC_02	Customisable WIPS detection rules via simple workflows, i.e., no coding required.	
WL_SEC_03*	Provide threat detection capabilities incorporating various techniques, including signature-based methods, behavioural analysis, and machine learning. The solution should provide robust threat detection capabilities that can identify known and unknown threats and provide alerts and remediation guidance as needed.	
WL_SEC_04*	Use network intelligence and	

	analytics to detect threats.	
WL_SEC_05*	Radios should be able to serve clients and scan for possible threats simultaneously.	
WL_SEC_06*	Detect and alert on rogue or unknown access points.	
WL_SEC_07*	Support isolation of client devices.	
WL_SEC_08	Support posture verification before clients may connect.	
WL_SEC_09*	Support for Network access control and a management console to quarantine and update devices before authorising access to the network.	
Wireless deployment requirements		
WL_DEP_01*	Support tunnelling data via controllers or direct to VLAN.	
WL_DEP_02*	Provide multiple access point types for normal, outdoor, and high-density high throughput areas, i.e., conference areas.	
WL_DEP_03*	Must be able to deploy countrywide to all regional offices with central management.	
WL_DEP_04*	Support of HA/clustering on controllers without adding additional hardware.	
WL_DEP_05	External antennas must be compatible and supported by OEM.	
WL_DEP_06*	Support ceiling and wall mounting options.	

Wireless management requirements		
WL_MAN_01*	Provide a full management console that allows management of all controllers, access points, and clients nationwide.	
WL_MAN_02*	Provide wireless SDN Fabric support and integration with wired fabric.	
WL_MAN_03*	Support captive portals for guest management and posture assessment mitigation.	
WL_MAN_04*	Supports Cloud and on-premises wireless controllers with full wireless functionality.	
WL_MAN_05*	Automated load balancing of clients across access points.	
WL_MAN_06*	Support scalability to 1500 Access Points.	
WL_MAN_07*	Support software-defined network integration between LAN and Wi-Fi.	
WL_MAN_08*	The solution must provide a unified management solution for wired and wireless components.	
WL_MAN_09*	The solution must provide a consistent security policy and services across wired and wireless networks.	
Datacentre Technical requirements		
DC_REQ_01*	Support standard 19-inch data centre rack technology.	
DC_REQ_02*	Support redundant power supply (multiple power supplies to be fed from alternative Data	

	Centre power sources).	
DC_REQ_03*	Support IEC C13 power supply cable connection type.	
DC_REQ_04*	Support rack mountable fitment into a standard 19-inch data centre rack.	
DC_REQ_05*	Support standard data centre rack rail measurements (i.e., “U” placements).	
High-Level Design		
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 project's Scope and Scale, e.g., number and types of sites. • Provide an overview of the current network • Provide an 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	*Name the document with “HLD” appended in the document name and reference the paper included in the bid submission here (ex: rfp_xyz_hld.pdf).*

	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	
Commitment to develop a Low-Level Design		
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. • Record device asset and serial numbers • Describe how Out-of-band and in-band	*Include a signed commitment to provide an LLD according to the criteria and reference the document here. Name the document with "LLD" appended to the document name. (ex:rfp_xyz_lld_commitment.pdf).*

	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	
Information Security Business requirements		
ISO_BUS_01*	Implement controlled access to network resources in the organisation, including network access control (avoid	

	unrestricted access to networks).	
ISO_BUS_02	Where possible, implement role-based access for provisioning access to network resources. This ensures that access is normalised across the organisation.	
ISO_BUS_03	Implement a network segmentation approach.	
Training		
W_TRAIN_01*	Provide certification training for planning, deployment, management, and maintenance on ALL supplied equipment and software (OEM certified training).	
W_TRAIN_02*	Provide integration training and support.	
Operational Business requirements		
OP_BUS_01	The solution must be compatible with various industry-standard technologies and protocols, allowing for seamless co-existence and interoperability with other network devices and systems, regardless of the vendor. Specifically, to be compatible with ALE, Checkpoint, Extreme Networks technologies, and HPE/ARUBA.	
OP_BUS_02	Mobile-enabled management console with scalable dashboarding and reporting.	
OP_BUS_03	Software Defined networking and orchestration.	

OP_BUS_04	Training and certification in South Africa/Gauteng or online virtual classroom training.	
OP_BUS_05	The proposed design and technology for the network infrastructure must be future-proof, with a lifespan of at least ten years. The design should be adaptable to emerging technologies and scalable to accommodate future growth. The technology should be energy-efficient and sustainable, using low-power hardware or renewable energy sources where possible. The proposed network infrastructure should include a comprehensive monitoring and management system to ensure optimal performance and proactively identify any issues. The tender should also have a detailed maintenance plan to ensure the infrastructure remains functional and up to date over the 10-year lifespan.	*The bidder is requested to provide a signed letter of intent supporting the proposed technology and design for the 10-year lifespan, demonstrating the long-term viability, energy efficiency, low power usage and sustainability of the proposed solution as per the requirement.* *(ex:rfp_xyz_letter_of intent.pdf).*
OP_BUS_06	Asset, configuration, and release management via the central management console.	
OP_BUS_07	Local partners are to support all CSIR offices (Gauteng, Western Cape, and KwaZulu-Natal) to minimise the risk of delayed resolution of problems.	
General Business Requirements		

GEN_BUS_01	The solution must provide support for the Internet of Things.	
GEN_BUS_02	The solution must provide support for Big data.	
GEN_BUS_03	The solution must provide Artificial Intelligence (AI) enabled capabilities for wired and wireless networks (campus networking).	
GEN_BUS_04	The solution must have the option of an On-Site Management dashboard that can provide unified policy automation and AI ML assurance for both wired and wireless networks.	
GEN_BUS_05	The solution must have the capability of providing End-to-end visualisation of the path from campus/branch to cloud/DC.	

5. Commitment from Bidder

On behalf of the Bidder:

____

Signature

Name and Surname: ____

Designation or Role: ____

6. Acronyms, Abbreviations, and definitions:

a. Acronyms

This section explains all shortened words, phrases, or statements, etc., used to represent concepts, ideas, or provisions of Annexure A2.

TABLE 2: LIST OF ACRONYMS

Abbreviation	Explanation
AAA	Authentication, authorisation, and accounting
AES	Advanced Encryption Standard
AI	Artificial intelligence
ALE	Alcatel-Lucent Enterprise
AP	Access Point
AV Bridging (AVB)	Audio Video Bridging
BYOD	Bring Your Own Device
DFS	Dynamic Frequency Selection
DNS	Domain Name System
DoS	Denial of Service
ESXi	Elastic Sky X integrated, VMware type-1 hypervisor.
EVPN	Ethernet VPN (technology for carrying layer 2 Ethernet traffic)
Gbps	Gigabits or Gigabytes per Second
HA	High Availability
HLD	High-Level Design
Hyper-V	Microsoft's virtualisation platform, or 'hypervisor.'
IEC C13	“kettle cord”, 10Amps male power connector
ID (Subnet)	Used by routers to determine the best route between subnetworks
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

Abbreviation	Explanation
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LLD	Low-Level Design
MAC	Media Access Control
MACsec	Media Access Control security
Mbps	Megabits per second
MDM	Mobile Device Management
ML	Machine Learning
MOTD	Message Of The Day
MU-MIMO	Multi-user, multiple-input, multiple-output technology (allows a Wi-Fi router to communicate with multiple devices simultaneously)
NAC	Network Access Control
OEM	Original Equipment Manufacturer
PIMv2	Protocol Independent Multicast v2
POE	Power over Ethernet
QoS	Quality of service
QSFP+	Quad Small Form-Factor Pluggable Plus
RF	Radiofrequency
RHEV	Red Hat® Virtualization
RRM	Radio Resource Management
RU	Rack Unit
SCVMM	System Centre Virtual Machine Manager
SDN	Software-Defined Networking
Sflow	Sampled flow (industry standard for packet export at Layer 2)
SFP	Small Form-factor Pluggable
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VRF	Virtual routing and forwarding
VXLAN	Virtual Extensible Local Area Network

Abbreviation	Explanation
Wi-Fi	Family of wireless network protocols based on the IEEE 802.11
WIPS	Wireless Intrusion Prevention System
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
YANG	Standardised data model to manage the network at the service level
Xen	Free and open-source type-1 hypervisor

b. Definitions

This section explains the meanings of words, expressions, jargon, etc., not fully explained elsewhere in Annexure A2.

TABLE 3: LIST OF DEFINITIONS

Keyword/ Term	Definition
Anomalous Endpoint Detection	It involves analysing data from various sources, such as system logs, network traffic, and user behaviour, to identify deviations from normal activity patterns. These anomalies may include unusual network connections, unauthorised access attempts, or unusual file access or modification patterns.
NBASE-T	Technology that enables higher speeds over existing Ethernet cabling beyond the traditional limits of 1 Gbps up to 10 Gbps and beyond, using advanced modulation techniques, and it offers several benefits for enterprise networks.