Al-hussien bin talal University Network Infrastructure

REQUEST FOR PROPOSAL (RFP)

Table of Contents

1. Introduction

1.1 Purpose

This Request for Proposal (RFP) invites qualified bidders to submit proposals for the design, supply, implementation, and support of a modern network infrastructure for State University's campus. The goal is to replace the aging network with a secure, high-performance, and scalable solution that enhances user experience for students, faculty, and staff.

1.2 Background

State University operates a multi-building campus serving a diverse population of students, faculty, and staff. The current network, a multi-vendor setup with outdated hardware, struggles with bandwidth demands, security, and management complexity.

1.3 Objectives

- Provide high-performance connectivity with minimal latency for campus users.
- Enhance security through integrated access control, real-time threat detection, and policy enforcement.
- Simplify management with a unified, AI-driven platform for the wired & wireless network
- Optimize cost efficiency with energy-efficient hardware and streamlined operations.

2. Project Overview

2.1 Current Environment

The university operates a multi-vendor network with limited visibility, disparate management systems, and legacy hardware. It supports diverse devices, including IoT, and requires enhanced security and bandwidth for academic and administrative functions.

2.2 Project Scope

The selected Bidder will:

- Design and deploy a campus-wide network infrastructure.
- Implement an integrated security and networking solution.
- Migrate from existing systems with minimal disruption.
- Provide training and knowledge transfer to IT staff.

3. Scope of Work

3.1 Hardware and Software

The Bidder must supply:

- **Network infrastructure**
  - **Active Components (Networking Equipment)**
    - ✓ **Core Layer Switches (redundant, high availability, 48-port)**
    - ✓ **Aggregation Layer Switches (24-port)**
    - ✓ **Access Layer Switches (Non-PoE units, accepting 24 and/or 48-port)**
    - ✓ **Access Layer Switches (PoE units accepting 24 and/or 48-port)**
    - ✓ **Wireless Access Points for campus-wide coverage**
    - ✓ **Network Access Control Requirements**
    - ✓ **Centralized management platform**
  - **Passive Components (Structured Cabling)**
    - ✓ **Fiber Optic Cabling**
    - ✓ **Copper Cabling (UTP)**
    - ✓ **Direct Attach Copper (DAC) Cables**
- **Security**
  - **WAF -Web Application Firewall**
  - **PAM - Privileged Access Management.**
  - **SSL certification**
- **IT Infrastructure**
  - **Server**
  - **Storage**
  - **Backup software**

3.2 Implementation Services

- Solution design and architecture
- Hardware installation and configuration
- Migration with minimal disruption
- Testing, validation, and knowledge transfer

3.3 Support Services

- Limited Lifetime Hardware Warranty support
- Software updates
- 24x7 technical support with defined SLAs

4. Network infrastructure Technical Requirements

The solution must be as a Leader in the Gartner Magic Quadrant for Wired and Wireless LAN Access Infrastructure
Bidder must indicate "Comply" or "Not Comply" for each requirement and provide comments if and where applicable.

4.1 Networking Equipment

4.1.1 General Requirements

- Unified management platform with single-pane-of-glass visibility for all components
- Zero-touch provisioning for all network devices
- Role-based access control with multi-factor authentication
- API support for third-party integrations
- Native network access control without additional licensing
- Solution must support mesh architecture connecting network and security components

4.1.2 Core Layer Switch Requirements — Quantity: 2 units

Description	Comply Yes/No	Comments
Should be fully managed Layer 3 switches with advanced IPv4/v6 Layer 3 routing (OSPF, BGP, VRRP, PIM, PBR, VRF) and all features enabled and QoS.		
The Switch shall support virtual switching to work the two switches as one virtual switch with high redundancy and availability		
Each core switch should have minimum of : 48x 1/10/25GbE SFP28 8x 40/100 QSFP28 ports		
The switch should support minimum of Two hot swap redundant power supplies		
Should support High speed non-blocking ports		
Should support high performance switching capacity with minimum of 4 Tbps		
Should support MAC authentication		
Should support minimum Forwarding capacity of 1.7 Bpps		
Support for 3 years from the vendor and local partner.		
Must be manageable via the same platform		

4.1.3 Aggregation Layer Switch Requirements Quantity: 10 units (all 24-port models)

Description	Comply Yes/No	Comments
Should be fully managed Layer 3 switches with BGP, RIP v1&v2 and OSPF with and QoS with all features enabled and licensed (no extra license should be added)		
The Switch shall support virtual switching to work the two switches as one virtual switch with high redundancy and availability for the core		
Each core switch should have minimum of: 24 x 10GbE RJ45 && 2 x 40/100GE ports uplink/stacking ports		
Each core switch should support minimum of Two hot swap redundant power supplies		
Should be stackable switch and support minimum 9 switches per stack, also support long distance stacking.		
Should support High speed non-blocking ports		
Should support high performance switching with minimum of 1Tbps and forwarding rate 800 Mpps		
Should support MAC authentication		
Should be fully managed Layer 3 switches with BGP, RIP v1&v2 and OSPF with and QoS with all features enabled and licensed (no extra license should be added)		

4.1.4 Access Layer Switch Requirements (Non-PoE) Quantity: 80 units (40 x 48 ports + 40 x 24 ports)

Description	Comply Yes/No	Comments
Must be 24-port and/or 48-port models		
10GBASE-T uplink ports for copper connectivity to aggregation		
1 GE RJ45 ports for endpoint connectivity		
Support for 802.1X authentication and MAC-based authentication		
Support for dynamic VLAN assignment		
Advanced security features including DHCP snooping, ARP inspection, and IP source guard		
Must be centrally managed by the same platform as core and aggregation switches		
Built-in device identification and profiling capabilities		
Support for policy-based security enforcement		

4.1.5 Access Layer Switch Requirements (PoE) Quantity: 70 units (30 x 48 ports + 40x 24 ports)

Description	Comply Yes/No	Comments
Switches should be 1U rack mounted form factor		
Should support full Layer 2/3		

Description	Comply Yes/No	Comments
Should have 24-Port and/or 48-port x 10/100/1000BASE-T ports and shall have 2x1GE BASE-T & 2x10GE for copper connectivity to aggregation		
Should be stackable switch and support minimum 9 switches per stack		
Should support high performance switching with minimum of 130Gbps for 24-Port Switches and 180 Gbps for 48-Port switches		
Should support high performance forwarding capacity with minimum of 95 Mpps for 24-Port Switches and 130 Mpps for 48-Ports Switches		
Shall be non-Blocking architecture		
Shall support min one USB ports as console and for external file storage		
Shall support Dynamic VLAN assignment, including the type protocol (SSH + RADIUS CoA), port, username, password and enable password		
Shall support Open Flow		
Shall support both local management station and must support cloud managed from vendor's cloud, such as: • Switch configuration, including: ○ Switch Configuration profiles ○ Port settings ○ LAG management ○ VLAN interfaces ○ Client visibility Troubleshooting		
Switch Must be enterprise level switch (SMB not Approved)		

4.1.6 Wireless Requirements **Quantity:(200 indoor + 100 outdoor)**

Description	Comply Yes/No	Comments
Dual Radio and Dual Band Access Point with Weatherproof, temperature- Hardened, and rated IP-67 for outdoor AP.		
Support for 6 GHz band for future expansion && Support for Wi-Fi 6E (802.11ax) on both 2.4 GHz and 5 GHz bands		
Minimum 4x4 MU-MIMO support		
Support for 802.1X, WPA3, and Hotspot 2.0		
Built-in WIPS/WIDS capabilities		
Centralized RF management and optimization		
Must be managed through the same platform as the wired infrastructure		
Capable of multi-function services including data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical "touch"		
Internal Antenna, Omnidirectional radiation pattern capabilities		
Real time packet capture on the APs, without disconnecting clients, Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi- Fi 5 devices		

Description	Comply Yes/No	Comments
Should support for the latest Wi-Fi standard, IEEE's new 802.11ax specification.		
Should extend support to a new generation of Wi-Fi clients, such as smartphones, tablets, and high-performance laptops that have integrated 802.11ax support.		
Should support dual radio, Orthogonal frequency-division multiple access (OFDMA) and WPA3, Target Wake Time (TWT)		
Outdoor AP operating temperature of -20 °C to +65 °C.		
Support Power-over-Ethernet (PoE) 802.3at/bt standard with full capacity operation at full power of the radios		
Must support configurable split tunneling subnets per AP profile		
Must support configuration access via CLI on both, the controller and the individual AP		

4.1.7 wireless controller **Quantity: 2**

Description	Comply Yes/No	Comments
Single-pane-of-glass management for all network and security components		
Controller must support automatic discovery and authorization of newly connected APs & Switches.		
Unified policy management across network and security components		
LLM & AI/ML-powered analytics and chat by simply adding a license		
Zero-touch provisioning capabilities for all devices		
Automated network and security health assessments		
Centralized firmware management and updates		
Role-based access control with multi-factor authentication		
Built-in compliance reporting and audit logging		
Real-time monitoring and alerting		
Support for licensed extension for applications that can run within the platform		
API support for third-party integrations		
Support for security automation with customizable playbooks using license external applications		
Automatically recognize the type (e.g., Apple iOS) and model (e.g., iPhone, iPad) of the mobile device connecting to the network		
RADIUS support, ability to utilize RADIUS attributes to assign users or devices to specific roles/VLANs		
The controller shall be manageable using CLI, Telnet/SSH, HTTP based GUI and SNMPv2/v3 and console		
Controller shall support integrated and External AAA server and Database for user Authentication		
Support for 3 years from the vendor and local partner.		

4.1.8 Management software **Quantity: 1**

Description	Comply Yes/No	Comments
Single pane of glass on the Wired and Wireless components with Unified Network Management System for Switching and Wireless LAN.		
Support multiple generations of hardware infrastructure from the same console.		
enable end-to-end troubleshooting and root-cause analysis, the operations solution should monitor components of the wired network infrastructure that have a direct impact on the performance of the wireless network		
Ability to detect new and existing wireless APs and controllers are automatically discovered anywhere on the network.		
The solution will be used to discover existing access points and controllers as well as new "out-of-the-box" devices.		
The solution should provide a network "dashboard'', providing up-to-date network-wide information on key usage and performance metrics		
For faster problem resolutions, the operations solution should provide easy-to-use, real-time monitoring views of every device (i.e., access points and switches) under management.		
Operations staff should be able to search for users based on readily available attributes, e.g., username rather than MAC or IP address.		
The solution should provide easy-to-use, real-time monitoring views of every end-user device connected to the wireless network (i.e., laptops, phones, barcode scanners, printers).		
The operations solution should monitor and manage edge, distribution and core switches in the network.		
The solution should provide historical information (bandwidth, CPU utilization, memory, errors).		
The solution should provide easy-to-read graphs and reports showing how user signal quality, throughput, and other usage statistics		
The solution will be the primary tool used to diagnose and alert the IT staff when problems may impact users or network performance. It must provide a comprehensive set of configurable alerts that provide sufficient information for IT staff to assess and resolve these issues efficiently		
Alerts must be capable of being sent Alarms via email, NMS or using SNMP traps		
Ability to tag devices location and the system should be able visually display these maps.		
The solution must be able to apply configuration changes to be implemented globally to all APs/Switches, to a specified subset of devices, or to an individual device.		
The solution should have the ability to automatically create a configuration "template" from an existing AP or controller with a "known good" configuration. The occur during pre-defined maintenance windows to avoid downtime when network usage is high.		
The solution should include a standard set of reports for improved visibility and control across the entire wireless network		
The solution should report on daily/weekly/monthly usage of Aps in different format CSV and PDF		
The solution should provide a browser-based graphical user interface The solution should support all major commercial browsers.		
The solution can manage minimum 500 devices (Switches and Access Points), The licenses should be activated for 300 devices from the first day and for 3 years.		
The solution accepted: on-premise, virtual based on VMware / Hyper-V/KVM or H.W.		
In case (VM) is required, physical H.W machine should be included to proposal.		
Support 3 years from the vendor and local partner.		
Single pane of glass on the Wired and Wireless components with Unified Network Management System for Switching and Wireless LAN.		
Support multiple generations of hardware infrastructure from the same console.		

4.1.9 Network Access Control Requirements

Description	Comply Yes/No	Comments
Built-in network access control capabilities without requiring additional license		
Automated device discovery and profiling		
Support for agent-less posture via an onboarding application at the authentication level		
Support differentiated policies and workflows for each user group		
Upfront posture check with remediation support		
Guest management and onboarding		
BYOD onboarding and management		
Integration with third-party security systems		
Centralized policy management for both wired and wireless clients		
Device profiling must be integrated with switch port security		
The BYOD/NAC solution must allow for host quarantine to non-compliant devices on the Switches		
Support for 3 years from the vendor and local partner.		

4.1.10 Integration Requirements

Description	Comply Yes/No	Comments
The solution must support mesh architecture		
End-to-end visibility of traffic flows through the network		
Policies must be consistently enforceable across the entire network		
Wireless APs must support latest security standards including WPA-3 Encryption		
The solution must take automated measures to protect against Wireless Intrusions including DOS, MITM attacks		
All components must share a common logging and reporting infrastructure		
The solution must provide a unified approach to network segmentation		
All components must support configuration backup and restore through the central management platform		
The solution must support applications recognition and control features, in addition to role-based access controls across the wireless network		

4.2. Network infrastructure Passive Components

4.2.1 General Requirements

- All cabling (fiber, Cat6a, cat7, DAC) must be **certified and tested** (OTDR for fiber, Fluke for Cat6a, vendor testing for DAC).
- DAC cables must meet IEEE 802.3by/bz/cu standards for 10G/25G/40G Ethernet.

4.2.2 Fiber Optic Cabling **Quantity:(per unit or meter approximately table 9.2)**

Description	Comply Yes/No	Comments
Installation of new single-mode/multi-mode fiber optic cables (specify required core count).		
Fiber patch panels (LC/SC/ST connectors as required).		
Fiber splicing and termination.		
Fiber patch cords (OM3/OM4/OS2 as applicable).		

4.2.3 Copper Cabling (UTP): **Quantity:(per unit or point approximately table 9.2)**

Description	Comply Yes/No	Comments
Replacement of existing Cat5/Cat5e cabling with Cat6a/cat7 for future-proofing. Proper cable management, labeling, and compliance with TIA/EIA-568 standards.		
Cat6a UTP patch panels (shielded/unshielded as per requirements).		
Cat6a UTP patch cords (certified for 10Gbps performance).		
cabinet 9U or 12U or 14U		

4.2.4 Direct Attach Copper (DAC) Cables **Quantity:(per unit approximately table 9.2)**

- ✓ 10G/25G/40G DAC cables for short-distance, high-speed connections .
- ✓ Compatibility with proposed core/aggregation switches (SFP+/QSFP+ ports).

4.2.5 Surveillance System License **Quantity:(per unit approximately table 9.2)**

- ✓ Nuuo main console
- ✓ Model type : SBC-IP+

5. Security Technical Requirements

5.1 WAF -Web Application Firewall Quantity: 2

Description	Comply Yes/No	Comments
Deployment		
The WAF must be deployable in full reverse proxy mode		
The System must support passive & Active Security mode operations		
The system must Support high availability (HA) configuration		
The system must support multiple load server balancing algorithm (not limited to round robin, Weighted round robin, Least Requests,etc.)		
The system must support Auto-Learning Mode		
The system must support HTTP/HTTPS/FTP/FTPS, & Custom Protocols		
The System must support multiple Web Protocols (not limited to HTTP/S 0.9/1.0/1.1/2.0, WebSocket, XML)		
The System must have built-in load balancing (ADC) web caching and compression		
The System must support content routing		
The System must be able to provide Secure traffic to a database server		
The System must support all security models		
The Deployment must support hardware, virtual and containerized		
Hardware		
2x1Gb RJ45 or SFP Ports		
Dedicated 1Gb Ethernet Port for Management		
The system must support at least 30,000 HTTP Transactions per second		
The system must support at least 12,000 HTTPS Transactions per second		
The system must support at least 500,000 Concurrent Connections		
The system must support at least 200Mbps HTTP/HTTPS L7 throughput		
1U Full size form factor		
Single Power Supply		
Solution must be replaced every 4 years for free under instant replacement program		
Web Application Security		
OWASP top 10 protection		
Protection against common attacks (not limited to SQL Injection, Cookie and forms tampering, cross-site scripting,…etc.)		
HTTP Protocol Checks , Data Leak Prevention		
Brute Force protection		
CSRF Protection (random token injection), Integrated Malware Protection (File Upload Extensions filter control)		
Integrated Advanced Threat Protection (ATP)		
True File Type Detection (regardless of extn.)		
Dynamic URL Encryption		
Cloaking detection and protection capability		
Clickjacking Protection		
XML Firewall and DoS checks		
SOAP Validation and security		
JSON Inspection and Validation		
Anti Defacement and Smart Signatures issuing for better cookie protection		

Description	Comply Yes/No	Comments
URL and Response Body Rewrites and Web scraping protection		
SSL Capabilities		
SSL Offloading with Hardware Accelerator		
HTTP Links to HTTPS rewrite		
Custom SSL Ciphers including PFS		
Client Certificate Validation		
Custom Cipher list per SSL/TLS version		
Redirection for unsupported ciphers		
OCSP and CRL support		
HTTP/2 and WebSockets		
Application DDoS and Client Controls		
Application DDoS Attack Protection		
Geolocation based blocking		
Slowloris, RUDY, Slow Read Attacks Protection		
Blacklist Known Attack Sources		
CAPTCHA Challenge to Suspicious sources		
Client Fingerprinting		
Blocking TOR nodes		
XML DOS protection		
Support SMS PASSCODE		
The solution should provide a comprehensive “profile learning"		
Authentication and Authorization		
Authentication Proxy, including SSO		
LDAP, RADIUS support		
NTLM Support , Two-Factor Authentication		
Kerberos Support , Federated Authentication and SSO (e.g. SAML)		
Management and Integrations		
Automated Virtual Patching aka Vulnerability Remediation Service (VRS)		
Custom Notifications		
Management Via REST API		
Custom Syslog upstream and SIEM Integration		
Assign user roles with variable permissions		
Support for Centralized Management		
Licensing & Support		
Three Years Subscription and Support.		
Implementation provided by OEM		
Training Provided by OEM		
A license may be included as requirement when needed. Advance bot protection and volumetric DDos attack		
Certifications		
ICSA Certified		
FIPS Certified Must be Listed in leaders or strong performers forester wave for Web Application Firewall in last published years.		

5.2 PAM - Privileged Access Management **Quantity: 1**

Description	Comply Yes/No	Comments
Architecture		
The solution should have multi-tenant architecture compatible with service providers' environments, with a complete isolation of instances		
The solution must have minimum 3 layers of scalability like primary, HA & DR		
The solution must have inbuilt capability – HA/load balancing, - Disaster recovery, Backup and restore, Management API's & should not rely on any third party DB like MSSQL or Oracle		
The solution must have Easy and efficient deployment toward quickly attainable milestones resulting in better control over implementation and cost, while also optimizing the Total Cost of Ownership		
The solution should have custom Linux based OS & DB in an hardened appliance form		
The solution should be available as On Premise for all the modules including remote access		
The solution should have only proxy-based architecture for connections to RDP, SSH		
The solution should also work without a bowser using native applications like putty & mstsc		
The solution should support remote access to target devices over internet without use of VPN using single port 443 from end user to web portal and web portal to internal network on internet		
The solution Should support full customization of logo, fonts, text, disclaimer on login page, Background Images, Names etc.		
The solution must only use RDS server to host web applications & thick clients		
Solution should not install any ActiveX, Java, Plugins, registry entries in the browser or end user machine		
The Solution should support Active-Active Configuration		
The solution vendor must provide OS & Database updates & Patches for solution in future		
The solution should provide the flexibility to push all the logs to an external storage automatically without any human intervention		
The solution should have all the configuration options only from the front end of the application		
The solution should log all activities, issues, errors in the front end in the form of syslog's		
The Solution should support Active-Active Configuration		
The solution vendor must provide OS & Database updates & Patches for solution in future		
Session Management		
The solution should record all videos on the PAM server		
The solution should gather metadata to supply dashboards with detailed and context-relevant information		
The solution should have feature to OCR through sessions to read the meta data of a privileged session		
The solution must have Complete audit logs and advanced searches(Global Search) to isolate incidents		
Video recorded should be downloadable only in MP4 format		
The solution should allow auditors to monitor privileged users on demand real-time		
The solution audit logs should clearly show who accessed which target device with duration (start time & end time)		
The solution should automatically connect disconnected sessions		
The solution should also have flexibility to maintain & share sessions with auditors for interaction		
The solution should allow flexibility for users to automatically login to target devices with primary accounts		
The solution should provide high quality resolution video logs with the flexibility of increasing & decreasing resolution		
The solution should have flexibility to disable video logs for selected servers		
The Solution should restrict hop on feature – block mstsc at port level		
Access Management		

Description	Comply Yes/No	Comments
The solution must have Automatic session termination based on actions interception: blacklist, widget event, reports, process sequences, keyboard traffic plus the user executing malicious command should be blocked from PAM on such activity		
The solution should support workflows designed with context relevant access configurations		
The solution must identify sleeping accounts at risk as well as devices through discovery feature		
The solution must enforce regulatory requirements through traceable audit trails and separation of operational tasks from administrative Perimeter		
The solution should support checkout \ Check-in of passwords		
The solution should support quota on approvers for instance if 2 out of 3 approvers approve, request for access is approved		
The solution must support auto approvals within specified time approvals		
The workflow server access request should have flexibility to increase \ decrease time for requested session		
The workflow request for users should have free text field to write reason for access \ justification		
The workflow feature should have the flexibility of deleting an existing approved request		
The solution should provide a web portal for users and administrators to track operations more efficiently and in real-time		
The solution should have Global search across your entire Bastion infrastructure		
The solution should Protect assets and systems through set rules that can automatically authorize or revoke user access		
The solution should provide logs for approval history for privileged sessions		
The solution must provide authentication history for all users logged within a specified time		
The solution must provide flexibility to assign multiple approvers at each level for request-based access to target devices		
Password Management		
The solution should be agentless in true sense in performing the following Session recording, Session recording, Command process restriction, Password management		
The solution should have dedicated plugin library for target password management		
The solution should support Enforce periodic change and rotation of passwords		
The solution should store all passwords in a secured vault with encryptions like AES 256 bit		
The solution should auto change the passwords if not checked in with in the specified time limit		
The solutions should only support Application to application password management using comprehensive agent-based application fingerprinting technology		
The solution must be capable of changing passwords in text files, configuration files, scripts, schedulers scripts etc.		
The solution should support Break the glass feature in case of emergency or outage of PAM servers		
The solution must be capable of changing passwords for service account OOTB		
Integration		
Solution must bulk onboarding feature for users, servers, domains, restrictions, groups etc.		
The solution should support access to Consoles, business web applications, and fat clients (e.g.: firewall management, Salesforce, or Sage)		
He solution must have Bi-directional SIEM integration for advanced reporting and real-time processing of malicious behavior detection		
The solution should have Open architecture to enable integration with third party vaults		
The solution should support Unix or Windows operating systems, network devices, databases, mainframes, virtual infrastructures, or SU/SUDO injection		
The solution must support following protocols for integration like HTTP/HTTPS, RDP/TSE, SSH, Internet, SFTP.		
The solution should support following authentication methods like Identifier, LDAP, Active Directory, Radius,TACAS+, Kerberos, X509, OTP, Web SSO,		
The solution must have capability to integrate SNMP & e-mail monitoring tools, ticketing tools and workflows for administrator notifications.		
The solution should support Easy provisioning and synchronization with central Identity Access Management solutions within the REST API.		

Description	Comply Yes/No	Comments
The solution should support Delegation to third-party systems for user authentication and identification (SAML 2.0)		
The solution should have capability to create connectors on the fly to meet needs to technology products at the client end		
The solutions support Direct access to resources using native clients (PuTTY, WinSCP, MSTC, OpenSSH, etc.) with connection rules embedded directly into the Bastion		
The Solution should support X509 Certificate based Authentication for users.		
He solution must have Bi-directional SIEM integration for advanced reporting and real-time processing of malicious behavior detection		
The solution should support remote app management		
The Solution should not use any vendor provided thick client application; it should work seamless with all major browser & Native applications		
The solution should have universal web app integration gateway which is capable to integrate all web apps on the go		
The solution should have capability to integrate all leading MFA's with SAML & RADIUS. Optionally should have MFA of their own		
Security		
The solution should possess certifications like ANSII & FSTEK		
The Solution should only have custom Linux OS like Debian with GRSecurity patch		
The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)		
The solution should only support authentication for target devices on the Privileged Access management server and not on the user's machine		
The solution should have high encryptions standards like AES 256bit encryption		
The PAM Server must be hardened with GRSecurity Patch for Memory Corruption Defenses, Filesystem Hardening, Miscellaneous Protections, Role Based Access Control (RBAC), GCC Plugins		
Hardening of PAM server will be done by the vendors with DDOS protection		
Solution should use State of the art cryptography protections are used to secure the PAM users & target devices for privileged access		
The solution must support transparent mode		
The solution should not provide direct access to PAM Database in any case		
The Solution should be capable to install TLS Certification of the devices on the PAM server for security		
The solution must have multiple levels of authentication to reach to the PAM database logs		
The solution should have video logs which cannot be tampered along with the flexibility to delete additional logs by only means of a custom command		
The solution should only be connected using a custom port. The default ports like 22 & 3389 should not be used to connect to PAM servers		
Reporting		
The solution should have reporting feature for meaningful use		
The solution should have reports like • Unused users & resources • Top target connection by device • Top target connections by target account • Primary connections by User • Parallel target connections by date • Target connection duration by a user		
Reports should be downloadable in csv format		
The solution should have dashboard to show currently logged in users		
The solution should contain enterprise dashboard with real time information on users, servers, services, anomalies etc.		
The Solution should inbuilt customizable dashboards giving business critical information like: - 1. Longest sessions 2. Sessions during abnormal hours		

Description	Comply Yes/No	Comments
3. Sessions during normal hours 4. Failed sessions along with reason of failure 5. Inventory information such as users, devices, user groups, target groups		
6. Subscription and Support for 3 years from the vendor and local partner.		

5.3 SSL certification

Feature	Minimum Requirements	Comply Yes/No	Comments
SSL Certificate	Wildcard SSL certificate to secure Al Hussein bin Talal University website URL and an unlimited number of its sub domains.	**valid for three years**	
	The certificates are needed for Al-Hussein Bin Talal University website identity and domain ownership, Microsoft Exchange & all services and sub domains. ✓ Up to 256-bit encryption ✓ Daily website malware scanning ✓ Free 24/7 support, express renewal, and a 30-day money back guarantee ✓ SSL Installation Checker ✓ Generic Apache SSL Certificate and Domain certificate		

6 IT Infrastructure

6.1 SAN Storage — Quantity: 2

Feature	Minimum Requirements	Comply Yes/No	Comments
Storage Architecture	• The proposed Storage solution must be based on All-Flash SSD.		
	• Must be same company as the compute nodes		
	• Servers & Storage must be from the same Vendor.		
Type	• Rack industry-standard rack		
Storage Controllers	• Dual controller active/active design • RAID offload ASIC and updated CPUs		
System memory	• 48 GB system cache		
Row Capacity	• Min 32TB Useable Capacity • RAID-6 with 1 hot spare • Using 3.84TB Read Intensive vy6lSSD		
Host Interface	• 8-port 10GB Base-t iSCSI Per Array		
Operating System	• The storage array should support industry-leading Operating System platforms & clustering including Windows Server 2022 / 2025, VMware ESXI 7/8, Red hat enterprise Linux and SUSE Enterprise Server (SLES) etc		

Feature	Minimum Requirements	Comply Yes/No	Comments
Active Feature and licensed	• All the below licenses should be licensed and included for storage proposed for maximum capacity: • Snapshot and clone • Thin provisioning • QOS		
Cables	• All Required cables and SFP's should be provided.		
Warranty	• Warranty from Mother Company (Parts/Labor/On-Site) With (24/7) support		

6.2 TOR SAN Switch **Quantity: 2**

Feature	Minimum Specification	Comply (Yes/No)	Comments
Ports	• 24 x 100/1000/2.5G/ 5G/10G BASE-T ports, supporting 2 x 100GE/40GE QSFP28/QSFP+ ports		
Module slot	• 2 x power module slots 3 x fan module slots		
System switching capacity	• 880 Gbps • 1300 Mpps		
Power supply	• 2 x pluggable power modules		

6.3 server **Quantity: 4**

Feature	Minimum Specification	Comply (Yes/No)	Comments
Processor Type	2 x Intel Xeon-Silver 4514Y 2.0GHz 16-core 150W Processor		
Memory	128 GB DDR5-5600 Memory.		
Hard Drives	2 x 480 GB NVMe boot drives with RAID-1		
Network Connectivity	2 x Dual Ports 10GB Base-t 1 x Quad Ports 1GB Base-T		
Power Supply & Fan	Dual, Hot plug, Power Supply Redundant.(1000W) Redundant hot plug Fans.		
Drivers and Utilities	All Drivers and Full Management Utilities must be Included.		

Feature	Minimum Specification	Comply (Yes/No)	Comments
	Optional : Unified Management software to manage as a single pane of glass for all same hardware vendor infrastructure.		
From Factor	1U Rack Mount with all the needed accessories to install in a Rack cabinet with all needed cables		
System Security	The server must support the following • FIPS 140-3 validation • Secure erase of NAND/User Data • Support for Commercial National Security Algorithms (CNSA)		
OS	2xMicrosoft Windows Server 2025 16-core Standard		
Warranty	Support for 3 years from the vendor and local partner.		

6.4 Backup software

Feature	Minimum Specification	Comply (Yes/No)	Comments
Backup Capabilities	• Image-based backup for virtual, physical, and cloud workloads. • Incremental and full backups to optimize storage and performance. • Application-aware processing for Microsoft SQL Server, Exchange, SharePoint, and Active Directory		
Recovery Options	• Instant VM Recovery to minimize downtime. • Granular file-level recovery and application item recovery. • Bare-metal recovery for physical servers.		
Monitoring and Reporting	• Real-time monitoring with customizable dashboards. • Comprehensive reporting tools for backup performance and health.		
Supported Environments	• **Virtualization Platforms**: VMware vSphere, Microsoft Hyper-V. • **Physical Servers**: Windows and Linux operating systems. • **Cloud Services**: Support for SaaS applications like Microsoft 365		

7. Implementation and Support Requirements

7.1 Tender Training Programs — 4 employee

- ✓ **Training for of IT staff On-Site and from Mother Company**
- ✓ **Cover administrative/operational features**
- ✓ **Provide documentation and reference materials**

7.2 Training for Programmers — 2 employee

Full Stack Web Development Course with ASP.NET MVC, VB.NET, Python, and AI

- ✓ **Foundations of MVC with VB.NET**
- ✓ **Introduction to Python**
- ✓ **Creating Dynamic Web Pages**
- ✓ **Efficient Data Management**
- ✓ **Building Responsive User Interfaces**
- ✓ **API and Web Services Development**
- ✓ **Integrating AI Capabilities**
- ✓ **Professional Optimization Techniques**

8. Payment Terms

The bid shall be submitted as a single lot, and the payment shall be made in five installments as follows:

- The first installment shall be paid upon final delivery of the project.
- The remaining amount shall be paid in four equal annual installments, due at the beginning of each calendar year during the specified period.

9. Warranty and quantity

9.1 Warranty

Five years Warranty from Mother Company (Parts/Labor/On-Site) With (24/7) support for all of tender component.

9.2 Table of quantity

Item no	Item		Qty	Unit price	Total price
4 Netwok	4.1.2 Core switch		2		
	4.1.3 Aggregation		10		
	4.1.4 Access SW non-POE	24 port	40		
		48 port	40		
	4.1.5 Access SW POE	24 port	40		
		48 port	30		
	4.1.6 wireless	Indoor	200		
		outdoor	100		
	4.1.7 Wireless controller		2		
	Centralized management platform	4.1.8 Management soft	-		
		4.1.9 NAC	-		
	4.2.2 Fiber	Fiber cable	6K		
		Fiber testing	20		
		Fiber batch	20		

Item no	Item		Qty	Unit price	Total price
		Fiber cord	40		
		splicing	40		
		Sfp+	40		
	4.2.3 Cooper	cabinet	21		
		Cat6a replacement	1K		
		Cat6a batch panel	50		
		Patch cored	1K		
	4.2.4 Dac cable		50		
	4.2.5 nuuo license		40		
5 Security	1	5.1 WAF	2		
	2	5.2 PAN	1		
	3	5.3ssl	3 Y		
6 IT Infra	1	6.3 server	4		
	2	6.1 San storrage	1		
	3	6.2 San switch	2		
	4	6.4 Backup sw	1		
7 Training	-	Training	-		
Total Budget (…..JD)					