BIDS AND AWARDS COMMITTEE

SUPPLEMENTAL BID BULLETIN NO. 2025-011

August 13, 2025

Attention:

All prospective bidders for the project: **E-LEARNING PLATFORM DEVELOPMENT WITH INTEGRATED DATA AND COMMUNICATIONS SYSTEM**

This supplemental bid bulletin is issued to clarify, modify, or amend the duration and specification for the following project as discussed during the pre-bid conference of the said project:

E-LEARNING PLATFORM DEVELOPMENT WITH INTEGRATED DATA AND COMMUNICATIONS SYSTEM	
Particulars/ Concerns	
Section VII. Technical Specifications pages 78-135 without number referencing.	
Amendments/ Clarifications/ Response	
1	**Project Summary** This project encompasses a wide range of technological aspects, from high-level AI tools and robust security measures to the fundamental IT equipment. It covers the entire spectrum of technological needs, from the cutting-edge advancements of artificial intelligence to the essential hardware components that underpin digital operations. Driven by the recent elevation of MPSPC status as a state university, this project aims to modernize the current digital infrastructure to cater the growing needs in network connectivity, data management and resiliency, and smart classrooms. Prospective bidders should possess a valid Business Permit applicable to the contract and have completed a similar contract with a value of at least 50% of the ABC, and the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law. The BAC will use non-discretionary pass/fail criteria in the Eligibility Check/Screening as well as the Preliminary Examination of Bids. The BAC will conduct post qualification of the lowest calculated bid.
2	**Project Description** 2.1 Purpose As part of the continuous effort of MPSU to deliver quality education, this project aims to enhance, scale and strengthen the IT infrastructure including the university information systems. 2.2 Key Elements of the Project 2.2.1 Virtualized Infrastructure 2.2.1.1 A new datacenter that can house all of the university systems and applications as well as data backups will be built as part of MPSU's redundancy initiative. 2.2.2 Core Network and Security 2.2.2.1 Continuous enhancement of the MPSU university requires

additional network and security equipment. These shall strengthen the cybersecurity and scale the network to cover new facilities.

2.2.3 Multimedia Conference Room

2.2.3.1 Conference rooms should be designed to accommodate both in-person and virtual meetings. They should be equipped with modern technology, such as high-speed internet, video conferencing systems, and large display screens. Additionally, comfortable seating arrangements and appropriate lighting should be provided to create a productive and inviting atmosphere for both in-person and remote participants.

2.2.4 Administrative and Educational Systems

2.2.4.1 A modernized digital tool with a focus on centralizing and streamlining both administrative and educational systems that will enhance productivity efficiency, and improve resource allocation. This ensures that MPSU staff and educators can focus more on their students

2.2.5 Computer Laboratory

2.2.5.1 The university shall have dedicated spaces equipped with computers and essential software, providing a platform for learning, research, and creative exploration. These labs offer access to technology and resources that empower individuals to develop digital skills, solve problems, and innovate.

2.2.6 Computer e-Laboratory

2.2.6.1 The university shall have dedicated spaces equipped with high-spec computers and dedicated software for multimedia, CAD, and animation.

2.2.7 E-classrooms

2.2.7.1 Equipped Visual representations and interactive elements significantly enhance information comprehension and retention. By presenting information visually, complex ideas can be simplified and made more accessible to a wider audience. Additionally, interactive features allow users to actively engage with the content.

2.2.8 University Productivity

2.2.8.1 University staff and offices shall be provided with digital equipment to aid with their functions and improve efficiency.

2.2.9 Other Peripherals

2.2.9.1 To further enhance the learning environment and support the IT infrastructure, additional equipment will be provided. These supplementary tools will facilitate a more comprehensive and engaging learning experience for students and faculty alike.

3 General Scope of Works

3.1 Requirement Analysis

3.1.1 Project key elements shall undergo requirement analysis with all the stakeholders.

3.2 Detailed Business User Requirements, Technical Design Requirements, Implementation Plan, and System Manuals

The winning bidder must submit the Detailed Business User Requirements, Technical Design Requirements, Implementation Plan, and System Manuals
A comprehensive business user requirement, technical design requirements, implementation plan and system manuals. The implementation plan will show the

details of the project's timeline, milestones, deliverables, and resources required for the successful execution.

3.3 Infrastructure Setup

The project team will install and set up the necessary digital infrastructure required for the project, including servers, routers, switches, and related equipment.

3.4 Software Implementation

Based on the business user requirements and technical design requirements, installation, customization, and testing of all software and applications shall be performed to ensure full integration of all systems that form part of this project.

3.5 Testing and Quality Assurance

3.5.1 The project team will perform individual component testing, and system integration testing for all components to ensure that they meet the specified requirements and are free from defects and errors.

3.5.2 Test scripts and user acceptance testing (UAT) documents should be provided for a smoother handover to end users.

3.6 Training

Facilitate the delivery of knowledge transfer through technical orientation and training sessions.

4 Command and Control Center Equipment Requirements (Main Datacenter)

The Command-and-Control Center is to be located at the main office. Components to be included in this project includes the following:

4.1 Auxiliary Works and Services

4.1.1 The winning bidder must provide all essential works to prepare the area nominated by for MPSU to be its Command-and-Control Center. At a minimum, it must include the following:

4.1.1.1 Wall, ceiling, and floor finish
4.1.1.2 Lighting works
4.1.1.3 Electrical works
4.1.1.4 2 Units 2.5 HP Air Conditioner Split Type
4.1.1.5 Provision of network nodes
4.1.1.6 2 Units Dome Camera
4.1.1.7 Door Access System
4.1.1.8 Provision of furnishings and other fixtures necessary for a Command Center
4.1.1.9 Provision of 6 x 55” Display Monitor (Video Wall 3 x 2 Setup)
4.1.1.10 Electrical Works for connecting electricity supply wiring to electrical equipment.
4.1.1.11 Fixtures, Tables and Chairs for the Command Center

4.2 Provision of 6 Units Desktop Computers

4.2.1 The winning bidder must provide the following desktops to MPSU for its Command-and-Control Center. At a minimum, it must include the following:

4.2.1.1 Minimum of 10 Core Processor with 20MB Cache Memory
4.2.1.2 16GB Memory
4.2.1.3 512GB SSD Storage
4.2.1.4 34” curved Monitor
4.2.1.5 Keyboard
4.2.1.6 Mouse
4.2.1.7 UPS 650 VA
4.2.1.8 Windows Operating System (Version 11 or better)

BIDS AND AWARDS COMMITTEE

4.2.1.9 Office Productivity Software (Word Processor, Spreadsheet, Slide Presentation)

4.3 Security Surveillance System

4.3.1 TCP/IP Based CCTV Cameras

4.3.2 Should support 12 VDC or 24 VAC.

4.3.3 Should support 1920 x 1080 Resolution.

4.3.4 Should support 25/30/50/60 fps.

4.3.5 Should be at least IP66 Ingress protection.

4.3.6 CCTV System is going to be installed in the NOCs of the different sites of MPSU

4.4 All In One Rack

4.4.1 Server Racks

The 5 racks will be located in MPSU Datacenter:

4.4.1.1 Rack configuration

4.4.1.1.1 Power input should be 220Vac, single phase, 50/60Hz.

4.4.1.1.2 Enclosure type should be fully enclosed hot and cold aisles(glass front door plus sold sheet metal rear door)

4.4.1.1.3 Available unit space shall be 29U

4.4.1.1.4 Single rack configuration

4.4.1.1.5 Rack size: (WxDxH) 600*1200*2000

4.4.1.1.6 Enclosure protection shall be IP50 rating.

4.4.1.1.7 Shall have an electronic door lock.

4.4.1.1.8 Rack enclosure is earthquake-resistant w/ seismic level 8 capability.

4.4.1.1.9 LED lighting shall be included in racks.

4.4.1.2 UPS

4.4.1.2.1 Shall have 1 unit of 6kVA UPS

4.4.1.2.2 UPS effeciency should be not less than 95%

4.4.1.2.3 Power meter included in UPS

4.4.1.2.4 UPS shall be capable for cloud monitoring through mobile phones or desktop

4.4.1.2.5 UPS shall have ethernet port for IoT connections

4.4.1.2.6 UPS shall have email and mobile notification.

4.4.1.3 PDU

4.4.1.3.1 With at least 2 unit of PDU.

4.4.1.3.2 Each PDU has 20*C13+4 *C19 sockets

4.4.1.3.3 PDU shall be CE certified.

4.4.1.4 Cooling

4.4.1.4.1 Cooling type is Split DX system

4.4.1.4.2 Cooling capacity shall be 4.2kW

4.4.1.4.3 Cooling air volume shall be 800m³/h

4.4.1.4.4 Cooling refrigerant is R410a

4.4.1.4.5 Condensate pump shall be included

4.4.1.5 Miscellaneous Rack Requirement

4.4.1.5.1 User interface: 10.1-inch touch screen LCD

4.4.1.5.2 Connectivity: SNMP/HTTP

4.4.1.5.3 Smoke sensor included

4.4.1.5.4 Shall have temperature and humidity sensor.

4.4.1.5.5 Pop-up front and rear doors for emergency plans.

4.4.1.5.6 Water leakage sensors included.

4.4.1.6 Certification
4.4.1.6.1 MDC distributor shall have ISO 9001 certification
4.4.1.6.2 MDC distributor shall have ISO 27001 certification

5 Virtualized Infrastructure

The winning bidder shall provide virtualized infrastructure for the university applications and other essential IT systems, and database.

5.1 Server Switch

The winning bidder shall supply 2 Leaf switch where the server computers will be directly connected and 2 Spine switch for university elected by MPSU to house its disaster recovery infrastructure It shall include 56 pcs SR transceivers and services for configuration and integration.

5.1.1 Must have high-performance of at least:
5.1.1.1.1 1.28Tbps and 952 Mpps for Spine
5.1.1.1.2 1.76Tbps and 1,309 Mpps for Leaf
5.1.1.2 Must have intelligent monitoring and visibility with network analytics
5.1.1.3 Must have high availability with industry leading VSX redundancy, and redundant power supplies and fans
5.1.1.4 Must be designed for core/aggregation in the Top of Rack or End of Row in data center environments
5.1.1.5 Must have automation and programmability using built-in REST APIs and Python scripts
5.1.1.6 Must be capable of advanced Layer 2/3 feature set includes BGP, OSPF, VRF, and IPv6

5.1.2 Quality of Service (QoS)
5.1.2.1 Must be capable of enabling congestion avoidance
5.1.2.2 Must support lossless Ethernet networking standards to eliminate packet loss due to queue overflow
5.1.2.3 Must have Priority Flow Control (PFC) 2 priorities per port
5.1.2.4 Must have Enhanced Transmission Service (ETS)
5.1.2.5 Must be able to prevent accumulation of excessive congestion with periodic flushing. Avoids packets buffering for an extended time period

5.1.3 Resiliency and high availability
5.1.3.1 Must be redundant and have load-sharing fans and power supplies -Increases total performance and power availability while providing hitless, stateful failover
5.1.3.2 Must have hot swappable power supply and fan modules - Allows replacement of accessory modules without any operational impact on other modules nor the switch operations
5.1.3.3 Must have separate data and control paths - Separates control from services and keeps service processing isolated; increases security and performance
5.1.3.4 Must be capable of Virtual Router Redundancy Protocol (VRRP)-VRRP allows a group of switches to dynamically back each other up to create highly available routed environments
5.1.3.5 Must have IEEE 802.3ad LACP - Supports up to 52 LAGs, with up to 8 members per LAG with a user-selectable L1- 4 hashing algorithm

5.1.4 Performance

BIDS AND AWARDS COMMITTEE

5.1.4.1 Must have scalable system design - Provides investment protection to support future technologies and higher-speed connectivity

5.1.4.2 Must have high-speed fully distributed architecture - Provides up to 1.76Tbps for bidirectional switching and 1,309 Mpps for forwarding to meet the demands of bandwidth- intensive applications today and in the future

5.1.5 Connectivity

5.1.5.1 Must support port configuration below.

5.1.5.1.1 Spine. 24 ports of 1GbE/10GbE (SFP/SFP+) 4 ports of 40GbE/100GbE (QSFP+/ QSFP28)

5.1.5.1.2 Leaf. 48 ports of 1GbE/10GbE (SFP/SFP+) 4 ports of 40GbE/100GbE (QSFP+/ QSFP28)

5.1.5.2 Must support Jumbo frames - Allows high-performance backups and disaster-recovery systems; provides a maximum frame size of 9K bytes

5.1.5.3 Must have Loopback - Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility

5.1.5.4 Must have packet storm protection - Protects against unknown broadcast, multicast, or unicast storms with user-defined thresholds

5.1.6 Management

5.1.6.1 Must have management interface control - Enables or disables each of the following interfaces depending on security preferences: console port or reset button

5.1.6.2 Must have industry-standard CLI with a hierarchical structure - Reduces training time and expenses, and increases productivity in multivendor installations

5.1.6.3 Must have management security - Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; local and remote Syslog capabilities allow logging of all access

5.1.6.4 Must have IP SLA - Monitors the network for degradation of various services, including voice. Monitoring is enabled via the NAE for history and for immediate automated gathering of additional information when anomalies are detected

5.1.6.5 Must support SNMP v2c/v3 - Provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions

5.1.6.6 Must support sFlow (RFC 3176) - Provides scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes

5.1.6.7 Must have Remote Monitoring (RMON) - Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups as well as a private alarm extension group

5.1.6.8 Must support TFTP and SFTP - Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows

bidirectional transfers over a TCP/ IP network ; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security

5.1.6.9 Must have debug and sampler utility - Supports ping and traceroute for IPv4 and IPv6

5.1.6.10 Must support Network Time Protocol (NTP) - Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock- dependent devices within the network; Can serve as the NTP server in a customer network

5.1.6.11 Must have IEEE 802.1AB Link Layer Discovery Protocol (LLDP) - Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications

5.1.6.12 Must have dual flash images - Provides independent primary and secondary operating system files for backup while upgrading

5.1.6.13 Must support multiple configuration files - Stores files easily to the flash image

5.1.7 Layer 2 Switching

5.1.7.1 Must have VLAN that supports up to 1,024 port-based or IEEE 802.1Q-based VLANs

5.1.7.2 Must have Bridge Protocol Data Unit (BPDU) tunneling - Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs

5.1.7.3 Must support port mirroring - Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports 4 mirroring groups, with an unlimited number of ports per group

5.1.7.4 Must support STP - standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)

5.1.7.5 Must support Internet Group Management Protocol (IGMP) - Controls and manages the flooding of multicast packets in a Layer 2 network

5.1.7.6 Must support Rapid Per-VLAN spanning tree plus (RPVST+) - Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs

5.1.8 Layer 3 Services and Routing

5.1.8.1 Must support Address Resolution Protocol (ARP) - Determines the MAC address of another IP host in the same subnet; supports static ARPs ;Gratuitous ARP allows detection of duplicate IP addresses; Proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

5.1.8.2 Must support Dynamic Host Configuration Protocol (DHCP) - DHCP services are offered within a client network to simplify network management. DHCP Relay enables DHCP operation across subnets

5.1.8.3 Must support Domain Name System (DNS) - Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server

5.1.8.4 Must support Policy Based Routing (PBR) - Enables use of a classifier to select traffic that can be forwarded based on policy set by the network administrator

5.1.8.5 Must support Static IPv6 routing - Provides simple

BIDS AND AWARDS COMMITTEE

manually configured IPv6 routing

5.1.8.6 Must support Open shortest path first (OSPF) - Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

5.1.8.7 Must support Border Gateway Protocol 4 (BGP-4) - Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks

5.1.8.8 Must support 6in4 tunnels - tunneling of IPv6 traffic in an IPv4 network

5.1.8.9 Must support IP performance optimization - Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities

5.1.8.10 Must support Static IPv6 routing - Provides simple manually configured IPv6 routing

5.1.8.11 Must support OSPFv3 - Provides OSPF support for IPv6

5.1.8.12 Must support Equal-Cost Multipath (ECMP) - Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

5.1.8.13 Must support Generic Routing Encapsulation (GRE) - enables tunneling traffic from site to site over a Layer 3 path

5.1.9 Security

5.1.9.1 Must support Access Control List (ACL) Features - powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses. For instance, IT management devices could be grouped in this way; ACLs can also protect control plane services such as SSH, SNMP, NTP or web servers

5.1.9.2 Must support Remote Authentication Dial-In User Service (RADIUS) - Eases security access administration by using a password authentication server

5.1.9.3 Must support Terminal Access Controller Access Control System (TACACS+) - Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security

5.1.9.4 Must support management access security - provides both on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication; Additionally, TACACS+ can also provide user authorization, services

5.1.9.5 Must support Secure shell (SSHv2) - Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers

5.1.10 Multicast

5.1.10.1 Must support Multicast Internet Group Management Protocol (IGMP) - Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3

5.1.10.2 Must support Multicast Listener Discovery (MLD) - Enables discovery of IPv6 multicast listeners; supports MLDv1 and v2

5.1.10.3 Must support Protocol Independent Multicast (PIM) - Protocol Independent Multicast for IPv4 and IPv6 supports one-to-many and many-to-many media casting use cases such as IPTV over IPv4 and IPv6 networks. Support for PIM Sparse Mode (PIM-SM, IPv4 and IPv6)

5.1.11 56 units of Short Range 10G Transceivers

5.2 50TB Enterprise NAS with the minimum following specifications:

The NAS must provide 50TB of storage and adhere to the specified technical parameters. The Winning Bidder have the flexibility to configure the NAS as long as it meets these requirements:

5.2.1 NAS Scale-out of up to 12 arrays

5.2.1.1 Maximum Drives (HDD/SSD) of up to 864 or higher

5.2.1.2 Maximum Raw Capacity of up to 13.8PB or higher

5.2.1.3 Maximum onboard Flash Cache Based on NVMe Technology of up to 12TB or higher

5.2.1.4 Maximum Flash Pool of up to 144TB or higher

5.2.1.5 Maximum Memory of up to 768GB or higher

5.2.1.6 Maximum Drives (HDD/SSD) of up to 72 or higher

5.2.1.7 Maximum Raw Capacity of up to 1PB or higher

5.2.1.8 Maximum Onboard Flash Cache Based on NVMe Technology of up to 1TB or higher

5.2.1.9 Maximum Flash Pool of up to 12TB of higher

5.2.1.10 Minimum of ECC Memory of up to 64GB

5.2.1.11 At least NVRAM 4GB

5.2.1.12 Minimum of 4 x 25GbE Ports

5.2.1.13 Minimum of 4 x 10GbE BASE-T Ports (1GbE autoranging) (maximum)

5.2.1.14 With 12Gb / 6Gb SAS Ports (maximum)

5.2.1.15 With Protocols Supported FC, iSCSI, NFS, pNFS, CIFS/SMB, S3

5.2.1.16 With Host/Client Operating Systems Support for Microsoft Windows, Linux, VMware ESXi

5.2.1.17 3 Years Warranty and Maintenance with Implementation Services

5.3 Compute Nodes for HCI Environment consisting of Six (6) Rack mounted Servers with minimum specifications as follows:

5.3.1 Hardware

5.3.1.1 2 x Intel Xeon Gold processor

5.3.1.2 24 Core per processor

5.3.1.3 24 x 32G DDR4 RDIMM or similar type or equivalent per node

5.3.1.4 4 x Port 10GbE (SFP+)

5.3.1.5 2 x 480 GB system disk per node

5.3.1.6 Total of 60 TB storage capacity for the HCI stack

5.3.1.7 Redundant Power Supply

5.3.2 Software

5.3.2.1 Technology

5.3.2.1.1 Hyper-Converged Infra (HCI) is a software-defined IT infrastructure that virtualizes all the elements of conventional “hardware-defined” systems. HCI includes, at a minimum,

virtualized computing (hypervisor) and virtualized SAN (software-defined storage). The HCI must be also capable and ready for network virtualization, network virtual security (Virtual Firewall, Bandwidth Manager etc.) or virtual Load balancing.

5.3.2.1.2 The HCI solution should start with minimum two nodes, and still expandable from two nodes to more nodes directly without redo of implementation or reinitialization of HCI.

5.3.2.1.3 The management platform is integrated and distributed, not relied on a certain virtual machine or physical machine, which is more reliable.

5.3.2.1.4 Do not require installing additional management software after deployment of the hypervisor to achieve basic web-based access to GUI, granular management and easy operation.

5.3.2.1.5 The crucial components for virtualization of compute, storage, networking, network functions, application firewall, application delivery controller, are provided by the same vendor, to ensure scalability and compatibility

5.3.2.1.6 Support correlated security service with intelligent threat detection and response platform to automatically take actions (such as quarantine VM by distributed firewall, take snapshot for VM, etc.,) against malicious activities that are detected by the security platform.

5.3.3 Compute Virtualization

5.3.3.1 Should have High-Availability. In case host fails, all the VMs running on that host can be recovered to another clustered host to ensure business continuity.

5.3.3.2 Backup is built-in by default and support agent-less incremental VM-level backup. For Windows VMs, filelevel recovery must be supported.

5.3.3.3 Should have built-in back-up and support agent-less incremental VM-level back-up. For Windows VMs, file level recovery must be supported without using 3rd Party solutions.

5.3.3.4 Support snapshot consistent group and scheduled snapshots.

5.3.3.5 Able to evaluate performance of virtual machines and hot-add resources (vCPU and vRAM) when they are running out of CPU or memory, minimizing business downtime.

5.3.3.6 Must be ready support module Activated CDP

5.3.3.7 (Continues Data Protection) capable of recording VMs' IOs at an interval as minimum as 1 second, data can be restored at any point of time in the past 3 days for both clusters.

5.3.3.8 AI-Enhanced database performance optimization with built-in self-adaptive performance optimization engine.

5.3.3.9 Support host health monitoring, when a host is deemed

5.3.3.10 unhealthy, it will be put in an unhealthy host list, VM placement and HA failover will avoid using the unhealthy host as a destination. When the host is back to normal, it can be taken out of the unhealthy host list automatically.

5.3.4 Storage Virtualization

5.3.4.1 Support striping function, and support setting different number of strips in units of virtual disks.

5.3.4.2 Support data reconstruction priority adjustment, users able to view the data reconstruction task list information and can click the priority in the operation to prioritize data reconstruction.

5.3.4.3 A full copy of VM's data should be existed on the node where the VM is running on to facilitate faster read and write.

5.3.4.4 Support striping function, and support setting different number of strips in units of virtual disks.

5.3.4.5 Support disk bad sector prediction, scanning and repair to maximize data security.

5.3.4.6 Support storage capacity prediction based on historical usage statistics and consumption behavior.

5.3.4.7 Support disk remaining lifecycle prediction.

5.3.5 Network Virtualization

5.3.5.1 Natively Support deploying virtual routers, virtual switches and firewalls.

5.3.5.2 Built-in distributed firewall to apply granular access control policy between VMs, securing east-west traffic (also known as Micro-segmentation).

5.3.5.3 The virtual router supports high availability. A failed virtual router can be automatically recovered upon host failure, to ensure high availability of routing service.

5.3.5.4 Visualized Network topology can be completed simply by dragging objects and drawing connections via a visualized web-based management panel

5.3.5.4.1 CDP Function

5.3.5.4.1.1 CDP must support recording VMs' IOs at an interval as minimum as 1 second, data can be restored at any point of time in the past 3 days.

5.3.5.4.1.2 CDP must be integrated without additional 3rd party software.

5.3.5.4.1.3 The CDP must be agent-less to avoid any negative impact on VMs' stability and performance.

5.3.5.4.1.4 Support fast browsing files from CDP backups, able to fast retrieve data or files from CDP backups.

5.3.5.4.2 Warranty and support

5.3.5.4.2.1 At least three (3) years software license subscription & upgrade, and technical support 7*24.

5.3.5.4.2.2 Vendor must have direct local support in the Philippines.

5.3.5.4.3 Certification

5.3.5.4.3.1 To ensure the maturity of Hyper-converged Infrastructure solution, the vendor must be CMMI L5 certified.

6 Core Network and Security

6.1 3 units of Next Generation Firewall / SDWAN for Satellite Campuses

The winning bidder shall supply, install and configure 3 units of NGFW / SDWAN with the specifications described below:

6.1.1 Performance and Hardware specifications

6.1.1.1 The system must have the minimum throughput capacity

listed below.

6.1.1.1.1 Firewall Inspection at 5.2 Gbps
6.1.1.1.2 Threat Prevention at 3 Gbps
6.1.1.1.3 Application inspection at 3.6 Gbps
6.1.1.1.4 IPS at 3.4 Gbps
6.1.1.1.5 Anti-malware inspection at 2.9 Gbps
6.1.1.1.6 TLS/SSL decryption and inspection (DPI SSL) at 800 Mbps
6.1.1.1.7 VPN at 2.10 Gbps

6.1.1.2 The system must be capable of handling:
6.1.1.2.1 At least 21,000 Connections per second
6.1.1.2.2 Max connections (SPI) of 1,500,000
6.1.1.2.3 Max DPI-SSL Connections of 125,000
6.1.1.2.4 Max connections (DPI) of 500,000

6.1.1.3 The system's interface must include the following interfaces.
6.1.1.3.1 16 x 1GbE
6.1.1.3.2 3 x 10G SFP+
6.1.1.3.3 2 USB 3.0
6.1.1.3.4 1 Console
6.1.1.3.5 1 Management port

6.1.1.4 Storage of at least 64GB M.2 that is expandable up to 256GB

6.1.2 Capabilities and features

6.1.2.1 Must perform stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.

6.1.2.2 Must scan for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.

6.1.2.3 Must have proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.

6.1.2.4 Must have a single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

6.1.2.5 Must have an engine with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.

6.1.2.6 Must identify and mitigate even the most insidious modern threats, including future Meltdown exploits. Detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption.

6.1.2.7 Must prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.

6.1.2.8 Must have multi-engine sandbox platform, which includes

virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.

6.1.2.9 Must have a Secure SD-WAN that enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public Internet services without additional license cost.

6.1.2.10 Must have a wizard to automatically configure SDWAN Policy on the firewall.

6.1.2.11 Must displays SD-WAN Performance probes and top connections.

6.1.2.12 All network traffic must be inspected, analyzed and brought into compliance with firewall access policies.

6.1.2.13 Must supports Active/Passive (A/P) with state synchronization. The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance

6.1.2.14 Must have block until verdict to prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.

6.1.2.15 Must have zero-day protection to protect the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.

6.1.2.16 Must have Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats.

6.1.2.17 Must have application control that controls applications, or individual application features that are identified by the engine against a continuously expanding database of over thousands of application signatures. That increases network security and enhances network productivity.

6.1.2.18 Must have DDoS/DoS attack protection. SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.

6.1.2.19 Must be capable of load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. Policy-based routing creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage

6.1.2.20 Must display rules which are actively used or not being used.

6.1.2.21 Must be able to simplify and reduce complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between firewalls while security and connectivity occurs instantly and automatically.

6.1.2.22 Must guarantee critical communications with 802.1p, DSCP tagging and remapping of VoIP traffic on the network.

6.1.2.23 The system Intrusion Prevention System must be capable

of Signature-based scanning, Automatic signature updates, Bi-directional inspection, Granular IPS rule capability, GeoIP enforcement, Botnet filtering with dynamic list, Regular expression matching.

6.1.2.24 The Anti-Malware System must be capable of Stream-based malware scanning, Gateway anti-virus, Gateway anti-spyware, Bi-directional inspection, No file size limitation

6.1.2.25 The system must have traffic visualization that can monitor User activity, application, bandwidth, and threat.

6.1.2.26 Must have a HTTP/HTTPS Web content filtering that is capable of URL filtering, Proxy avoidance, Keyword blocking, Policy-based filtering (exclusion/inclusion), HTTP header insertion, Bandwidth manage, and rating categories.

6.1.2.27 Must have a VPN that is capable of Secure SD-WAN, Auto-provision VPN, IPSec VPN for site-to-site connectivity, SSL VPN and IPSec client remote access, Redundant VPN gateway, and Mobile client for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire.

6.1.2.28 Must have networking capabilities such as Port Shield, Path MTU discovery, Enhanced logging, VLAN trunking, Layer-2 QoS, Port security, Dynamic routing (RIP/OSPF/BGP), Policy-based routing (ToS/metric and ECMP), NAT, DHCP server, Bandwidth management, A/P high availability with state sync, Inbound/outbound load balancing, L2 bridge, wire/virtual wire mode, tap mode, NAT mode, Asymmetric routing, and Common Access Card (CAC) support.

6.1.2.29 The system management and monitoring must have Web GUI, Command Line Interface (CLI), SNMP v2/v3 support, centralized management and reporting, NetFlow/IP Fix exporting, cloud-based configuration back up, and Zero-Touch registration & provisioning.

6.1.2.30 Must be certified with ICSA labs Advance Threat Defense certified with 100% unknown threat detection for 7 consecutive quarters from Q1-Q4, 2021 & Q1-Q3, 2022.

6.1.2.31 Must have 24x7 support that includes firmware updates and hardware replacement. Support includes around-the-clock access to telephone and web-based support for basic configuration and troubleshooting assistance, as well as hardware replacement in the event of failure.

6.1.3 12 pcs. of Short Range 10G Transceivers

6.2 Next-Generation Firewall / SDWAN for Bontoc Main Campus

The winning bidder shall supply, install and configure 2 units of NGFW with the specifications described below:

6.2.1 Performance and Hardware specifications

6.2.1.1 The system must have the minimum throughput capacity listed below.

6.2.1.1.1 Firewall Inspection at 18 Gbps

6.2.1.1.2 Threat Prevention at 9.5 Gbps

6.2.1.1.3 Application inspection at 11 Gbps

6.2.1.1.4 IPS at 10 Gbps

6.2.1.1.5 Anti-malware inspection at 9.5 Gbps

6.2.1.1.6 TLS/SSL decryption and inspection (DPI SSL) at 5 Gbps

6.2.1.1.7 VPN at 11 Gbps

6.2.2 The system must be capable of handling:

BIDS AND AWARDS COMMITTEE

6.2.2.1.1 At least 115,000 Connections per second
6.2.2.1.2 Max connections (SPI) of 4,000,000
6.2.2.1.3 Max DPI-SSL Connections of 350,000
6.2.2.1.4 Max connections (DPI) of 2,000,000

6.2.3 The system's interface must include the following interfaces.
6.2.3.1.1 6 x 10G/5G/2.5G/1G SFP+
6.2.3.1.2 24 x 1GbE Cu
6.2.3.1.3 2 USB 3.0
6.2.3.1.4 1 Console
6.2.3.1.5 1 Management port

6.2.4 Storage of at least 128 GB that is expandable up to 1 TB

6.2.5 Capabilities and Features

6.2.5.1 Must perform stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.

6.2.5.2 Must scan for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.

6.2.5.3 Must have proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.

6.2.5.4 Must have a single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

6.2.5.5 Must have an engine with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.

6.2.5.6 Must identify and mitigate even the most insidious modern threats, including future Meltdown exploits. Detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption.

6.2.5.7 Must prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.

6.2.5.8 Must have multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.

6.2.5.9 Must have a Secure SD-WAN that enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using readily-available, low-cost public Internet services without additional license cost.

6.2.5.10 Must have a wizard to automatically configure SDWAN Policy on the firewall

6.2.5.11 Must displays SD-WAN Performance probes and top connections.

BIDS AND AWARDS COMMITTEE

6.2.5.12 All network traffic must be inspected, analyzed and brought into compliance with firewall access policies.
6.2.5.13 Must supports Active/Passive (A/P) with state synchronization. The proposed solution should support Hardware redundancy using only single security license in both primary & secondary appliance
6.2.5.14 Must have block until verdict to prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
6.2.5.15 Must have zero-day protection to protect the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
6.2.5.16 Must have Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats.
6.2.5.17 Must have application control that controls applications, or individual application features that are identified by the engine against a continuously expanding database of over thousands of application signatures. That increases network security and enhances network productivity.
6.2.5.18 Must have DDoS/DoS attack protection. SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.zdfbn cx
6.2.5.19 Must be capable of load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods. Policy-based routing creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage
6.2.5.20 Must display rules which are actively used or not being used.
6.2.5.21 Must be able to simplify and reduce complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between firewalls while security and connectivity occurs instantly and automatically.
6.2.5.22 Must guarantee critical communications with 802.1p, DSCP tagging and remapping of VoIP traffic on the network.
6.2.5.23 The system Intrusion Prevention System must be capable of Signature-based scanning, Automatic signature updates, Bi-directional inspection, Granular IPS rule capability, GeoIP enforcement, Botnet filtering with dynamic list, Regular expression matching.
6.2.5.24 The Anti-Malware System must be capable of Stream-based malware scanning, Gateway anti-virus, Gateway anti-spyware, Bi-directional inspection, No file size limitation
6.2.5.25 The system must have traffic visualization that can monitor User activity, application, bandwidth, and threat.
6.2.5.26 Must have a HTTP/HTTPS Web content filtering that is capable of URL filtering, Proxy avoidance, Keyword blocking, Policy-based filtering (exclusion/inclusion), HTTP header insertion, Bandwidth manage, and rating categories.

6.2.5.27 Must have a VPN that is capable of Secure SD-WAN, Auto-provision VPN, IPSec VPN for site-to-site connectivity, SSL VPN and IPSec client remote access, Redundant VPN gateway, and Mobile client for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire.

6.2.5.28 Must have networking capabilities such as PortShield, Path MTU discovery, Enhanced logging, VLAN trunking, Layer-2 QoS, Port security, Dynamic routing (RIP/OSPF/BGP), Policy-based routing (ToS/metric and ECMP), NAT, DHCP server, Bandwidth management, A/P high availability with state sync, Inbound/outbound load balancing, L2 bridge, wire/virtual wire mode, tap mode, NAT mode, Asymmetric routing, and Common Access Card (CAC) support.

6.2.5.29 The system management and monitoring must have Web GUI, Command Line Interface (CLI), SNMP v2/v3 support, centralized management and reporting, NetFlow/IP Fix exporting, cloud-based configuration back up, and Zero-Touch registration & provisioning.

6.2.5.30 Must be certified with ICSA labs Advance Threat Defense certified with 100% unknown threat detection for 7 consecutive quarters from Q1-Q4, 2021 & Q1-Q3, 2022.

6.2.6 Must have 24x7 support that includes firmware updates and hardware replacement. Support includes around-the-clock access to telephone and web-based support for basic configuration and troubleshooting assistance, as well as hardware replacement in the event of failure.

6.2.7 8 pcs. of Short Range 10G Transceivers

6.3 Core Switch

The winning bidder shall supply, install and configure 2 units of Core Switch with a total of 26 pcs SR transceivers for the 2 switches. Please see the specifications as described below.

6.3.1 Must have high-performance of at least:

6.3.1.1 1.76Tbps and 1,309 Mpps

6.3.1.2 Must have intelligent monitoring and visibility with network analytics

6.3.1.3 Must have high availability with industry leading VSX redundancy, and redundant power supplies and fans

6.3.1.4 Must be designed for core/aggregation in the Top of Rack or End of Row in data center environments

6.3.1.5 Must have automation and programmability using built-in REST APIs and Python scripts

6.3.1.6 Must be capable of advanced Layer 2/3 feature set includes BGP, OSPF, VRF, and IPv6

6.3.2 Quality of Service (QoS)

6.3.2.1 Must be capable of enabling congestion avoidance

6.3.2.2 Must support lossless Ethernet networking standards to eliminate packet loss due to queue overflow

6.3.2.3 Must have Priority Flow Control (PFC) 2 priorities per port

6.3.2.4 Must have Enhanced Transmission Service (ETS)

6.3.2.5 Must be able to prevent accumulation of excessive congestion with periodic flushing. Avoids packets buffering for an extended time period

6.3.3 Resiliency and high availability

6.3.3.1 Must be redundant and have load-sharing fans and power supplies -Increases total performance and power availability while

providing hitless, stateful failover

6.3.3.2 Must have hot swappable power supply and fan modules - Allows replacement of accessory modules without any operational impact on other modules nor the switch operations

6.3.3.3 Must have separate data and control paths - Separates control from services and keeps service processing isolated; increases security and performance

6.3.3.4 Must be capable of Virtual Router Redundancy Protocol (VRRP)-VRRP allows a group of switches to dynamically back each other up to create highly available routed environments

6.3.3.5 Must have IEEE 802.3ad LACP - Supports up to 52 LAGs, with up to 8 members per LAG with a user-selectable L1- 4 hashing algorithm

6.3.4 Performance

6.3.4.1 Must have scalable system design - Provides investment protection to support future technologies and higher-speed connectivity

6.3.4.2 Must have high-speed fully distributed architecture - Provides up to 1.76Tbps for bidirectional switching and 1,309 Mpps for forwarding to meet the demands of bandwidth- intensive applications today and in the future

6.3.5 Connectivity

6.3.5.1 Must support port configuration below.

6.3.5.2 48 ports of 1GbE/10GbE (SFP/SFP+) 4 ports of 40GbE/100GbE (QSFP+/ QSFP28)

6.3.5.3 Must support Jumbo frames - Allows high-performance backups and disaster-recovery systems; provides a maximum frame size of 9K bytes

6.3.5.4 Must have Loopback - Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility

6.3.5.5 Must have packet storm protection - Protects against unknown broadcast, multicast, or unicast storms with user-defined thresholds

6.3.6 Management

6.3.6.1 Must have management interface control - Enables or disables each of the following interfaces depending on security preferences: console port or reset button

6.3.6.2 Must have industry-standard CLI with a hierarchical structure - Reduces training time and expenses, and increases productivity in multivendor installations

6.3.6.3 Must have management security - Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; local and remote Syslog capabilities allow logging of all access

6.3.6.4 Must have IP SLA - Monitors the network for degradation of various services, including voice. Monitoring is enabled via the NAE for history and for immediate automated gathering of additional information when anomalies are detected

6.3.6.5 Must support SNMP v2c/v3 - Provides SNMP read and trap support of industry standard Management Information Base (MIB), and

private extensions

6.3.6.6 Must support sFlow (RFC 3176) - Provides scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes

6.3.6.7 Must have Remote Monitoring (RMON) - Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups as well as a private alarm extension group

6.3.6.8 Must support TFTP and SFTP - Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network ; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security

6.3.6.9 Must have debug and sampler utility - Supports ping and traceroute for IPv4 and IPv6

6.3.6.10 Must support Network Time Protocol (NTP) - Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock- dependent devices within the network; Can serve as the NTP server in a customer network

6.3.6.11 Must have IEEE 802.1AB Link Layer Discovery Protocol (LLDP) - Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications

6.3.6.12 Must have dual flash images - Provides independent primary and secondary operating system files for backup while upgrading

6.3.6.13 Must support multiple configuration files - Stores files easily to the flash image

6.3.7 Layer 2 Switching

6.3.7.1 Must have VLAN that supports up to 1,024 port-based or IEEE 802.1Q-based VLANs

6.3.7.2 Must have Bridge Protocol Data Unit (BPDU) tunneling - Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs

6.3.7.3 Must support port mirroring - Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports 4 mirroring groups, with an unlimited number of ports per group

6.3.7.4 Must support STP - standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)

6.3.7.5 Must support Internet Group Management Protocol (IGMP) - Controls and manages the flooding of multicast packets in a Layer 2 network

6.3.7.6 Must support Rapid Per-VLAN spanning tree plus (RPVST+) - Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs

6.3.8 Layer 3 Services and Routing

6.3.8.1 Must support Address Resolution Protocol (ARP) - Determines the MAC address of another IP host in the same subnet; supports static ARPs ;Gratuitous ARP allows detection of duplicate IP

addresses; Proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

6.3.8.2 Must support Dynamic Host Configuration Protocol (DHCP) - DHCP services are offered within a client network to simplify network management. DHCP Relay enables DHCP operation across subnets

6.3.8.3 Must support Domain Name System (DNS) - Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server

6.3.8.4 Must support Policy Based Routing (PBR) - Enables use of a classifier to select traffic that can be forwarded based on policy set by the network administrator

6.3.8.5 Must support Static IPv6 routing - Provides simple manually configured IPv6 routing

6.3.8.6 Must support Open shortest path first (OSPF) - Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

6.3.8.7 Must support Border Gateway Protocol 4 (BGP-4) - Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks

6.3.8.8 Must support 6in4 tunnels - tunneling of IPv6 traffic in an IPv4 network

6.3.8.9 Must support IP performance optimization - Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities

6.3.8.10 Must support Static IPv6 routing - Provides simple manually configured IPv6 routing

6.3.8.11 Must support OSPFv3 - Provides OSPF support for IPv6

6.3.8.12 Must support Equal-Cost Multipath (ECMP) - Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

6.3.8.13 Must support Generic Routing Encapsulation (GRE) - enables tunneling traffic from site to site over a Layer 3 path

6.3.9 Security

6.3.9.1 Must support Access Control List (ACL) Features - powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses. For instance, IT management devices could be grouped in this way; ACLs can also protect control plane services such as SSH, SNMP, NTP or web servers

6.3.9.2 Must support Remote Authentication Dial-In User Service (RADIUS) - Eases security access administration by using a password authentication server

6.3.9.3 Must support Terminal Access Controller Access Control System (TACACS+) - Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security

6.3.9.4 Must support management access security - provides both

on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication; Additionally, TACACS+ can also provide user authorization, services

6.3.9.5 Must support Secure shell (SSHv2) - Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers

6.3.10 Multicast

6.3.10.1 Must support Multicast Internet Group Management Protocol (IGMP) - Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3

6.3.10.2 Must support Multicast Listener Discovery (MLD) - Enables discovery of IPv6 multicast listeners; supports MLDv1 and v2

6.3.10.3 Must support Protocol Independent Multicast (PIM) - Protocol Independent Multicast for IPv4 and IPv6 supports one-to-many and many-to-many media casting use cases such as IPTV over IPv4 and IPv6 networks. Support for PIM Sparse Mode (PIM-SM, IPv4 and IPv6)

6.3.11 26 units of Short Range 10G Transceivers

6.4 Distribution Switch

The winning bidder shall supply, install and configure 2 units of Distribution Switch and a total of 22 pcs SR transceivers for all 2 switches with the specifications described below:

6.4.1 Must have high-performance of at least:

6.4.1.1 1.76Tbps and 1,309 Mpps

6.4.1.2 Must have intelligent monitoring and visibility with network analytics

6.4.1.3 Must have high availability with industry leading VSX redundancy, and redundant power supplies and fans

6.4.1.4 Must be designed for core/aggregation in the Top of Rack or End of Row in data center environments

6.4.1.5 Must have automation and programmability using built-in REST APIs and Python scripts

6.4.1.6 Must be capable of advanced Layer 2/3 feature set includes BGP, OSPF, VRF, and IPv6

6.4.2 Quality of Service (QoS)

6.4.2.1 Must be capable of enabling congestion avoidance

6.4.2.2 Must support lossless Ethernet networking standards to eliminate packet loss due to queue overflow

6.4.2.3 Must have Priority Flow Control (PFC) 2 priorities per port

6.4.2.4 Must have Enhanced Transmission Service (ETS)

6.4.2.5 Must be able to prevent accumulation of excessive congestion with periodic flushing. Avoids packets buffering for an extended time period

6.4.3 Resiliency and high availability

6.4.3.1 Must be redundant and have load-sharing fans and power supplies -Increases total performance and power availability while providing hitless, stateful failover

6.4.3.2 Must have hot swappable power supply and fan modules - Allows replacement of accessory modules without any operational impact on other modules nor the switch operations

BIDS AND AWARDS COMMITTEE

6.4.3.3 Must have separate data and control paths - Separates control from services and keeps service processing isolated; increases security and performance

6.4.3.4 Must be capable of Virtual Router Redundancy Protocol (VRRP)-VRRP allows a group of switches to dynamically back each other up to create highly available routed environments

6.4.3.5 Must have IEEE 802.3ad LACP - Supports up to 52 LAGs, with up to 8 members per LAG with a user-selectable L1- 4 hashing algorithm

6.4.4 Performance

6.4.4.1 Must have scalable system design - Provides investment protection to support future technologies and higher-speed connectivity

6.4.4.2 Must have high-speed fully distributed architecture - Provides up to 1.76Tbps for bidirectional switching and 1,309 Mpps for forwarding to meet the demands of bandwidth- intensive applications today and in the future

6.4.5 Connectivity

6.4.5.1 Must support port configuration below.

6.4.5.2 48 ports of 1GbE/10GbE (SFP/SFP+) 4 ports of 40GbE/100GbE (QSFP+/ QSFP28)

6.4.5.3 Must support Jumbo frames - Allows high-performance backups and disaster-recovery systems; provides a maximum frame size of 9K bytes

6.4.5.4 Must have Loopback - Supports internal loopback testing for maintenance purposes and increased availability; loopback detection protects against incorrect cabling or network configurations and can be enabled on a per-port or per-VLAN basis for added flexibility

6.4.5.5 Must have packet storm protection - Protects against unknown broadcast, multicast, or unicast storms with user-defined thresholds

6.4.6 Management

6.4.6.1 Must have management interface control - Enables or disables each of the following interfaces depending on security preferences: console port or reset button

6.4.6.2 Must have industry-standard CLI with a hierarchical structure - Reduces training time and expenses, and increases productivity in multivendor installations

6.4.6.3 Must have management security - Restricts access to critical configuration commands; offers multiple privilege levels with password protection; ACLs provide SNMP access; local and remote Syslog capabilities allow logging of all access

6.4.6.4 Must have IP SLA - Monitors the network for degradation of various services, including voice. Monitoring is enabled via the NAE for history and for immediate automated gathering of additional information when anomalies are detected

6.4.6.5 Must support SNMP v2c/v3 - Provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions

6.4.6.6 Must support sFlow (RFC 3176) - Provides scalable ASIC-based wire-speed network monitoring and accounting with no impact on network performance; this allows network operators to gather a variety

of sophisticated network statistics and information for capacity planning and real-time network monitoring purposes

6.4.6.7 Must have Remote Monitoring (RMON) - Uses standard SNMP to monitor essential network functions and supports events, alarms, history, and statistics groups as well as a private alarm extension group

6.4.6.8 Must support TFTP and SFTP - Offers different mechanisms for configuration updates; trivial FTP (TFTP) allows bidirectional transfers over a TCP/ IP network ; Secure File Transfer Protocol (SFTP) runs over an SSH tunnel to provide additional security

6.4.6.9 Must have debug and sampler utility - Supports ping and traceroute for IPv4 and IPv6

6.4.6.10 Must support Network Time Protocol (NTP) - Synchronizes timekeeping among distributed time servers and clients; keeps timekeeping consistent among all clock- dependent devices within the network; Can serve as the NTP server in a customer network

6.4.6.11 Must have IEEE 802.1AB Link Layer Discovery Protocol (LLDP) - Advertises and receives management information from adjacent devices on a network, facilitating easy mapping by network management applications

6.4.6.12 Must have dual flash images - Provides independent primary and secondary operating system files for backup while upgrading

6.4.6.13 Must support multiple configuration files - Stores files easily to the flash image

6.4.7 Layer 2 Switching

6.4.7.1 Must have VLAN that supports up to 1,024 port-based or IEEE 802.1Q-based VLANs

6.4.7.2 Must have Bridge Protocol Data Unit (BPDU) tunneling - Transmits STP BPDUs transparently, allowing correct tree calculations across service providers, WANs, or MANs

6.4.7.3 Must support port mirroring - Duplicates port traffic (ingress and egress) to a local or remote monitoring port; supports 4 mirroring groups, with an unlimited number of ports per group

6.4.7.4 Must support STP - standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)

6.4.7.5 Must support Internet Group Management Protocol (IGMP) - Controls and manages the flooding of multicast packets in a Layer 2 network

6.4.7.6 Must support Rapid Per-VLAN spanning tree plus (RPVST+) - Allows each VLAN to build a separate spanning tree to improve link bandwidth usage in network environments with multiple VLANs

6.4.8 Layer 3 Services and Routing

6.4.8.1 Must support Address Resolution Protocol (ARP) - Determines the MAC address of another IP host in the same subnet; supports static ARPs ;Gratuitous ARP allows detection of duplicate IP addresses; Proxy ARP allows normal ARP operation between subnets or when subnets are separated by a Layer 2 network

6.4.8.2 Must support Dynamic Host Configuration Protocol (DHCP) - DHCP services are offered within a client network to simplify network

management. DHCP Relay enables DHCP operation across subnets

6.4.8.3 Must support Domain Name System (DNS) - Provides a distributed database that translates domain names and IP addresses, which simplifies network design; supports client and server

6.4.8.4 Must support Policy Based Routing (PBR) - Enables use of a classifier to select traffic that can be forwarded based on policy set by the network administrator

6.4.8.5 Must support Static IPv6 routing - Provides simple manually configured IPv6 routing

6.4.8.6 Must support Open shortest path first (OSPF) - Delivers faster convergence; uses link-state routing Interior Gateway Protocol (IGP), which supports ECMP, NSSA, and MD5 authentication for increased security and graceful restart for faster failure recovery

6.4.8.7 Must support Border Gateway Protocol 4 (BGP-4) - Delivers an implementation of the Exterior Gateway Protocol (EGP) utilizing path vectors; uses TCP for enhanced reliability for the route discovery process; reduces bandwidth consumption by advertising only incremental updates; supports extensive policies for increased flexibility; scales to very large networks

6.4.8.8 Must support 6in4 tunnels - tunneling of IPv6 traffic in an IPv4 network

6.4.8.9 Must support IP performance optimization - Provides a set of tools to improve the performance of IPv4 networks; includes directed broadcasts, customization of TCP parameters, support of ICMP error packets, and extensive display capabilities

6.4.8.10 Must support Static IPv6 routing - Provides simple manually configured IPv6 routing

6.4.8.11 Must support OSPFv3 - Provides OSPF support for IPv6

6.4.8.12 Must support Equal-Cost Multipath (ECMP) - Enables multiple equal-cost links in a routing environment to increase link redundancy and scale bandwidth

6.4.8.13 Must support Generic Routing Encapsulation (GRE) - enables tunneling traffic from site to site over a Layer 3 path

6.4.9 Security

6.4.9.1 Must support Access Control List (ACL) Features - powerful ACLs for both IPv4 and IPv6. Supports creation of object groups representing sets of devices like IP addresses. For instance, IT management devices could be grouped in this way; ACLs can also protect control plane services such as SSH, SNMP, NTP or web servers

6.4.9.2 Must support Remote Authentication Dial-In User Service (RADIUS) - Eases security access administration by using a password authentication server

6.4.9.3 Must support Terminal Access Controller Access Control System (TACACS+) - Delivers an authentication tool using TCP with encryption of the full authentication request, providing additional security

6.4.9.4 Must support management access security - provides both on-box as well as off-box authentication for administrative access. RADIUS or TACACS+ can be used to provide encrypted user authentication; Additionally, TACACS+ can also provide user authorization, services

BIDS AND AWARDS COMMITTEE

6.4.9.5 Must support Secure shell (SSHv2) - Uses external servers to securely log in to a remote device; with authentication and encryption, it protects against IP spoofing and plain-text password interception; increases the security of Secure FTP (SFTP) transfers

6.4.10 Multicast

6.4.10.1 Must support Multicast Internet Group Management Protocol (IGMP) - Enables establishing multicast group memberships in IPv4 networks; supports IGMPv1, v2, and v3

6.4.10.2 Must support Multicast Listener Discovery (MLD) - Enables discovery of IPv6 multicast listeners; supports MLDv1 and v2

6.4.10.3 Must support Protocol Independent Multicast (PIM) - Protocol Independent Multicast for IPv4 and IPv6 supports one-to-many and many-to-many media casting use cases such as IPTV over IPv4 and IPv6 networks. Support for PIM Sparse Mode (PIM-SM, IPv4 and IPv6)

6.4.11 22 units of Short-Range Transceivers

6.5 Supply and Installation of 5 units 32 Ports Aggregation Switch with a total of the following specifications on the IDFs per building of 5 target buildings with 1 switch per building.

6.5.1 Performance

6.5.1.1 The switch must have a switching capacity of at least 760 Gbps or equivalent.

6.5.1.2 The switch must have a total non-blocking throughput of at least 380 Gbps or equivalent.

6.5.1.3 The switch must have a forwarding rate of at least 565.44 Mpps or equivalent.

6.5.1.4 The switch must have an operating temperature range of -5 to 40° C (23 to 104° F).

6.5.1.5 The switch must have an operating humidity range of 10 to 90% non-condensing.

6.5.2 Connectivity

6.5.2.1 Must support below configuration

6.5.2.1.1 28 1/10 Gbps SFP+ Ethernet ports

6.5.2.1.2 4 1/10/25 Gbps SFP+ Ethernet ports

6.5.3 Power

6.5.3.1 The switch must be able to support a universal input of 100-240V AC, 50/60 Hz.

6.5.3.2 The switch must be able to support a USP RPS DC input.

6.5.3.3 The switch must have an internal AC/DC power supply of 100W.

6.5.4 Management

6.5.4.1 The switch must have a 1.3" touchscreen LCM display for AR Switch Management.

6.5.5 Layer 2 Switching

6.5.5.1 Must support the layer 2 features listed but not limited to the following:

6.5.5.2 IGMP snooping

6.5.5.3 STP / RSTP with priorities and port-level disable

6.5.5.4 Port isolation

6.5.5.5 Storm control

6.5.5.6 Voice VLAN

6.5.5.7 Port mirroring

BIDS AND AWARDS COMMITTEE

6.5.5.8 LACP port aggregation
6.5.5.9 Multicast / broadcast rate limiting
6.5.5.10 MAC address blocking
6.5.5.11 Flow control
6.5.5.12 802.1X control
6.5.5.13 Jumbo frames
6.5.5.14 DHCP snooping / guarding
6.5.5.15 Egress rate limit
6.5.5.16 LLDP-MED
6.5.5.17 Port restricted by MAC
6.5.5.18 Device isolation with ACLs

6.5.6 Layer 3 Switching

6.5.6.1 Must support the layer 3 features listed but not limited to the following:

6.5.6.1.1 DHCP for locally-managed networks
6.5.6.1.2 DHCP relay
6.5.6.1.3 Inter-VLAN routing between networks on same switch
6.5.6.1.4 Static routing between local networks

6.5.7 Performance

6.5.7.1 The switch must have a switching capacity of at least 176 Gbps or equivalent.
6.5.7.2 The switch must have a total non-blocking throughput of at least 88 Gbps or equivalent.
6.5.7.3 The switch must have a forwarding rate of at least 130.944 Mpps or equivalent.
6.5.7.4 The switch must have an operating temperature range of -5 to 40° C (23 to 104° F).
6.5.7.5 The switch must have an operating humidity range of 10 to 90% non-condensing.

6.5.8 Connectivity

6.5.8.1 Must support below configuration

6.5.8.1.1 48 Gigabit Ethernet RJ45 ports
6.5.8.1.2 40 PoE/PoE+ (Pins 1, 2+, 3, 6-)
6.5.8.1.3 8 60W PoE++; PoE/PoE+ (Pins 1, 2+: 3,6-)
6.5.8.1.4 PoE++ (Pair A 1, 2+; 3, 6-) (Pair B 4, 5+, 7, 8-)

6.5.9 Power

6.5.9.1 The switch must be able to support a universal input of 100-240V AC, 50/60 Hz.
6.5.9.2 The switch must be able to support a USP RPS DC input of 52V DC, 11.54A/11.5V DC, 5.22A.
6.5.9.3 The switch must have an internal AC/DC power supply of 660W.

6.5.9.3.1 The switch must have a total PoE power budget of 600W.
6.5.9.3.2 The switch must be able to provide a maximum PoE wattage per port of the following:

6.5.9.3.2.1 32W for PoE+
6.5.9.3.2.2 64W for PoE++.

6.5.9.3.3 The switch must have a voltage range in PoE mode of the following:

6.5.9.3.3.1 44V - 57V for PoE
6.5.9.3.3.2 50V - 57V for PoE+.
6.5.9.3.4 48 Gigabit Ethernet RJ45 ports
6.5.9.4 The switch must have a maximum power consumption of 60W (excluding PoE output).
6.5.10 Management
6.5.10.1 The switch must have a 1.3" touchscreen LCM display for AR Switch Management.
6.5.11 Layer 2 Switching
6.5.11.1 Must support the layer 2 features listed but not limited to the following:
6.5.11.1.1 IGMP snooping
6.5.11.1.2 STP / RSTP with priorities and port-level disable
6.5.11.1.3 Port isolation
6.5.11.1.4 Storm control
6.5.11.1.5 Voice VLAN
6.5.11.1.6 Port mirroring
6.5.11.1.7 LACP port aggregation
6.5.11.1.8 Multicast / broadcast rate limiting
6.5.11.1.9 MAC address blocking
6.5.11.1.10 Flow control
6.5.11.1.11 802.1X control
6.5.11.1.12 Jumbo frames
6.5.11.1.13 DHCP snooping / guarding
6.5.11.1.14 Egress rate limit
6.5.11.1.15 LLDP-MED
6.5.11.1.16 Port restricted by MAC
6.5.11.1.17 Device isolation with ACLs
6.5.12 Layer 3 Switching
6.5.12.1 Must support the layer 2 features listed but not limited to the following:
6.5.12.1.1 DHCP for locally-managed networks
6.5.12.1.2 DHCP relay
6.5.12.1.3 Inter-VLAN routing between networks on same switch
6.5.12.1.4 Static routing between local networks
6.5.12.1.5 Network isolation with ACLs
6.5.12.1.6 DHCP snooping / guarding
6.5.12.1.7 Egress rate limit
6.5.12.1.8 LLDP-MED
6.5.12.1.9 Port restricted by MAC

6.6 Supply and Installation of 170 Indoor Access Points across several campuses with the following specifications:
6.6.1 Quantity and Location: in-building installation, Main Campus
6.6.1.1 Access Point shall support an aggregate radio rate of up to or equivalent or higher of the following:
6.6.1.1.1 6 Ghz (2x2 DL/UL MU-MIMO)
6.6.1.1.2 5 GHz (4x4 DL/UL MU-MIMO)
6.6.1.1.3 2.4 GHz (2x2 DL/UL MU-MIMO)
6.6.1.2 Access Point shall support the following data rates for Wifi 7:

6.6.1.2.1 802.11be (Wifi 7)
6.6.1.2.2 802.11ax (WiFi 6/6e)
6.6.1.2.3 802.11ac (WiFi 5)
6.6.1.2.4 802.11n

6.6.1.3 The Access point shall be able to have a Maximum Transmit of the following:
6.6.1.3.1 2.4 Ghz: 23dBm
6.6.1.3.2 5 Ghz: 29dBm
6.6.1.3.3 6 Ghz: 23dBm

6.6.1.4 Access Point shall be able to power up using the following methods
6.6.1.4.1 PoE
6.6.1.4.2 Power supply: PoE switch and PoE adapter with supported voltage of 44-57V DC and power consumption of 13W
6.6.1.4.3 The Access Point shall have the following features:
6.6.1.4.3.1 BSSID: 8 per radio
6.6.1.4.3.2 VLAN: 802.1Q
6.6.1.4.3.3 Advanced QoS: Per-user rate limiting
6.6.1.4.3.4 Guest Traffic Isolation
6.6.1.4.3.5 Concurrent Clients: 350 or equivalent

6.6.1.5 The Access Point shall have the following features:
6.6.1.5.1 Max BSSID: 8 per radio
6.6.1.5.2 VLAN: 802.1Q
6.6.1.5.3 Advanced QoS: Per-user rate limiting
6.6.1.5.4 Guest Traffic Isolation
6.6.1.5.5 Concurrent Clients: 350 or higher

6.6.1.6 Access Point shall support the following data rates:
6.6.1.6.1 802.11n (WiFi 4)
6.6.1.6.1.1 6.5 Mbps to 300 Mbps (MCS0 - MCS15, HT 20/40)
6.6.1.6.2 802.11ac (WiFi 5)
6.6.1.6.3 6.5 Mbps to 1.7 Gbps (MCS0 - MCS9 NSS1/2, VHT 20/40/80/160)
6.6.1.6.4 802.11ax (WiFi 6/6e)
6.6.1.6.4.1 7.3 Mbps to 4.8 Gbps (MCS0 - MCS11 NSS1/2/3/4, HE 20/40/80/160)
6.6.1.6.5 802.11be (Wifi 7)
6.6.1.6.5.1 5 GHz: 7.3 Mbps to 8.6 Gbps (MCS0 - MCS13 NSS1/2/3/4, EHT 20/40/80/160/240)
6.6.1.6.5.2 6 GHz: 7.3 Mbps to 5.7 Gbps (MCS0 - MCS13 NSS1/2, EHT 20/40/80/160/240/320)

6.7 Network Controller

Winning bidder shall supply one (1) network controller for the Bontoc campus.

6.7.1 General Features and Capabilities
6.7.1.1 The network controller must have the following specifications:
6.7.1.1.1 Processor: Quad-core ARM® Cortex®-A57 at 1.7 GHz or equivalent
6.7.1.1.2 System memory: 4 GB DDR4 or equivalent
6.7.1.1.3 On-board storage: 16 GB eMMC

6.7.2 Connectivity

BIDS AND AWARDS COMMITTEE

6.7.2.1 The network controller must support below configuration:
6.7.2.1.1 8 Gigabit Ethernet RJ45 ports
6.7.2.1.2 1 10G SFP+ port
6.7.2.1.3 SDWAN
6.7.2.1.3.1 1 Gigabit Ethernet RJ45 port
6.7.2.1.3.2 1 10G SFP+ port

6.7.3 Power
6.7.3.1 The network controller must be able to support a universal input of 100-240V AC, 50/60 Hz and 1 DC input.
6.7.3.2 The switch must be able to support a USP RPS DC input
6.7.3.3 The switch must have an internal AC/DC power supply of 50W.
6.7.3.4 The switch must have a maximum power consumption of 33W of and ESD/EMP protection of Air: ± 15kV, contact: ± 8kV

6.7.4 Management Tools
6.7.4.1 The controller must have the following management interfaces:
6.7.4.1.1 Ethernet port
6.7.4.1.2 Bluetooth

6.7.5 Performance
6.7.5.1 The controller must have the following features:
6.7.5.1.1 Redundant WAN with failover and load balancing WiFi QoS for the following:
6.7.5.1.1.1 Access points
6.7.5.1.2 Internet quality reporting
6.7.5.1.3 Outage reporting
6.7.5.1.4 Internet failover with LTE Backup

6.7.6 Security
6.7.6.1 The controller must have the following security features:
6.7.6.1.1 Application-aware firewall
6.7.6.1.2 Signature-based IPS/IDS threat detection
6.7.6.1.3 Content/country/domain/ad filtering
6.7.6.1.4 VLAN/subnet-based traffic segmentation
6.7.6.1.5 Full-stateful firewall

6.7.7 Security
6.7.7.1 The controller must support the following advanced networking features:
6.7.7.1.1 License-free SD-WAN
6.7.7.1.2 WireGuard
6.7.7.1.3 L2TP
6.7.7.1.4 OpenVPN server and client
6.7.7.1.5 IPsec site-to-site VPN
6.7.7.1.6 Policy-based WAN and VPN routing
6.7.7.1.7 DHCP relay
6.7.7.1.8 Customizable DHCP server
6.7.7.1.9 IGMP proxy
6.7.7.1.10 IPv6 ISP support

6.7.8 The switch must have an operating humidity range of 10 to 90% non-condensing.

6.8 Other SR transceiver requirements:
6.8.1 50 pcs transceivers for distribution switches proposed for the purposes

of connecting the aggregate switch to the distribution switch.

6.8.2 40 pcs transceivers for access switches for the purpose of connecting the aggregate switch to the access switch.

6.8.3 2 pcs transceiver from Ubiquiti Dream Machine to Core Switch

6.9 Out-Of-Band Switch

Winning bidder shall supply, install and configure 1 unit of Out-Of-Band switch for the network equipment and servers.

6.9.1 Console and Interface

6.9.1.1 24 x Selectable RJ45 RS-232 Ports and 24 x Managed 10/100/1000 Base-T Switched Ethernet Ports

6.9.1.2 2 x 10/100/1000 Ethernet/SFP Fiber auto-media ports (1GbE chassis)

6.9.1.3 2 x SFP+ (10G only) Fiber and 1 x 10/100/1000 Base-T Ethernet (10 GbE chassis)

6.9.1.4 1 x micro USB 2.0 Console Port and 1 x RJ45 Serial (Straight Pinout)

6.9.1.5 16, 32, or 48 x RJ45 RS-232 Software Selectable 50 to 230,400 bps Console Ports

6.9.1.6 1 x Internal V.92 modem with RJ11 Socket

6.9.1.7 2 x USB 3.0 Host Ports for storage and 8 x USB 2.0 ports for device console management

6.9.1.8 24 x managed 10/100/1000 Base-T switched Ethernet Ports

6.9.2 Power

6.9.2.1 Dual IEC 60320 Socket Universal 100-240V AC 50/60Hz and IEC C14 side connectors

6.9.3 Memory and CPU

6.9.3.1 4-core CPU

6.9.3.2 8 GB DDR3 RAM

6.9.3.3 16 MB SPI with password protection

6.9.3.4 M.2 SATA III 64 GB SSD

6.9.4 Security, Encryption & Authentication

6.9.4.1 Trusted Platform Module 2.0

6.9.4.2 AAA - TACACS+, RADIUS, Active Directory/OpenLDAP, Kerberos, with local fallback

6.9.4.3 Embedded Firewall

6.9.4.4 IPSec and OpenVPN

6.9.5 Automation & Scalability

6.9.5.1 Docker support

6.9.5.2 Python

6.9.5.3 Perl and bash support

6.9.5.4 ZTP

6.9.5.5 SNMP-Standard MIBs

6.9.6 Global LTE Cellular Interface

6.9.6.1 Coverage Global LTE-A Support

6.10 University Internet

Winning bidder shall provide internet subscription for the main campus under the university with 1 Gbps speed.

7 Systems

7.1 Administrative Systems

BIDS AND AWARDS COMMITTEE

Winning bidder shall develop, install and configure the following systems for MPSU.

7.1.1 Integrated Student Information System

7.1.1.1 Student Information Management

7.1.1.1.1 Must maintain accurate and up-to-date student records, including personal information, contact details, emergency contacts, and academic history.

7.1.1.1.2 Must track student demographics, such as age, gender, and nationality.

7.1.1.2 Enrollment Management

7.1.1.2.1 Must manage the entire enrollment process, from application submission to admission decisions and registration.

7.1.1.2.2 Must track student enrollment status, course registration, and fee payments.

7.1.1.3 Academic Records Management

7.1.1.3.1 Must maintain accurate academic records, including grades, transcripts, and degree audits.

7.1.1.3.2 Must calculate GPAs and generate academic reports.

7.1.1.3.3 Must manage course schedules, room assignments, and instructor assignments.

7.1.1.4 Financial Management

7.1.1.4.1 Must track student fees, payments, and refunds.

7.1.1.4.2 Must generate invoices and receipts.

7.1.1.4.3 Must integrate with the financial system to ensure accurate financial reporting.

7.1.1.5 Scholarship Management

7.1.1.5.1 Must manage student discounts and other scholarship grants

7.1.1.6 Attendance Management

7.1.1.6.1 Must track student attendance, including class attendance and event attendance.

7.1.1.6.2 Must generate attendance reports to monitor student engagement.

7.1.1.7 Access Rights Management

7.1.1.7.1 Must allow administrators to define roles and permissions, ensuring secure access to sensitive information.

7.1.1.8 Data Migration

7.1.1.8.1 Must provide a secure migration of existing data into the new system in ensuring a smooth transition.

7.1.1.9 User Training

7.1.1.9.1 Must provide end-user training, knowledge transfer, administrator training, user management, reports creation, and site administration.

7.1.1.10 Generation of Reports

7.1.1.10.1 Must generate reports such as Transcript of Records, Student Evaluation, Grades, and others

7.1.1.10.2 Must generate reports required by oversight agencies

7.1.2 Human Resource Management System

7.1.2.1 Employee Information Management

7.1.2.1.1 Must maintain accurate and up-to-date employee

records, including personal information, contact details, emergency contacts, and employment history.

7.1.2.1.2 Must manage the organizational structure, including departments, job titles, and reporting hierarchies.

7.1.2.2 Performance Management

7.1.2.2.1 Must allow for the creation, distribution, and completion of performance review forms.

7.1.2.2.2 Must track employee performance and provide feedback.

7.1.2.3 Payroll Processing

7.1.2.3.1 Must calculate salaries, wages, and deductions accurately.

7.1.2.3.2 Must generate payslips and other payroll reports.

7.1.2.3.3 Must comply with tax laws and regulations.

7.1.2.4 Benefits Administration

7.1.2.4.1 Must manage employee benefits, such as health insurance, retirement plans, and leave entitlements.

7.1.2.4.2 Must track benefit eligibility and deductions

7.1.2.4.3 Must track leave balances

7.1.2.5 Time and Attendance Tracking

7.1.2.5.1 Must track employee attendance, including time-in, time-out, and overtime hours.

7.1.2.5.2 Must generate attendance reports and calculate overtime pay.

7.1.2.6 Items (Plantilla) Management

7.1.2.6.1 Must manage employee positions, designations, and other employee agency profile

7.1.2.7 Generation of Reports

7.1.2.7.1 Must generate reports required by oversight agencies

7.1.3 Financial System

7.1.3.1 General Ledger

7.1.3.1.1 Must maintain a comprehensive general ledger, including a chart of accounts.

7.1.3.2 Financial Reporting

7.1.3.2.1 Must generate various financial reports, such as income statements, balance sheets, and cash flow statements.

7.1.3.3 User Access Control

7.1.3.3.1 Must implement strong access controls to protect sensitive financial information.

7.1.3.3.2 Must assign roles and permissions to different users to limit access to specific functions.

7.1.3.4 Procurement Module Vendor Management

7.1.3.4.1 Must allow for the creation and maintenance of a vendor database, including vendor information, contact details, and payment terms.

7.1.3.5 Procurement Module Purchase Order Management

7.1.3.5.1 Must track student attendance, including class attendance and event attendance.

7.1.3.5.2 Must generate attendance reports to monitor student engagement.

7.1.3.6 Financial Management

7.1.3.6.1 Must generate purchase orders, track order status, and manage purchase order approvals.

7.1.3.6.2 Must integrate with the inventory system to update stock levels upon receipt of goods.

7.1.3.7 Procurement Module Receiving and Inspection

7.1.3.7.1 Must facilitate the process of receiving goods, verifying quantities, and inspecting quality.

7.1.3.8 Procurement Module Accounts Payable

7.1.3.8.1 Must process vendor invoices, match them with purchase orders and receiving documents, and generate payment vouchers.

7.1.3.8.2 Must manage vendor payments and reconcile accounts.

7.1.3.9 Point-of-Sale (POS) Module Product and Service Catalog

7.1.3.9.1 Must maintain a comprehensive product and service catalog, including pricing, taxes, and discounts.

7.1.3.10 Point-of-Sale (POS) Module Sales Transactions

7.1.3.10.1 Must process sales transactions, including cash, credit card, and other payment methods.

7.1.3.10.2 Must generate sales receipts and invoices.

7.1.3.11 Point-of-Sale (POS) Module Inventory Management

7.1.3.11.1 Must track inventory levels, manage stock replenishment, and generate inventory reports.

7.1.3.11.2 Must integrate with the procurement module to initiate purchase orders when stock levels fall below a certain threshold.

7.1.4 Records Management System

7.1.4.1 Centralized Document Repository

7.1.4.1.1 Must provide a centralized repository for storing and organizing electronic documents.

7.1.4.1.2 Must support various file formats, including documents, spreadsheets, presentations, and images.

7.1.4.2 Document Classification and Indexing

7.1.4.2.1 Must allow for the classification and indexing of documents based on metadata, such as subject, author, date, and keywords.

7.1.4.2.2 Must use a consistent classification system to ensure easy retrieval.

7.1.4.3 Document Security and Access Control

7.1.4.3.1 Must implement strong security measures to protect sensitive documents.

7.1.4.3.2 Must assign access permissions to different user groups to limit access to authorized personnel.

7.1.4.4 Document Retention and Disposal

7.1.4.4.1 Must establish and enforce document retention policies based on legal and regulatory requirements.

7.1.4.4.2 Must automate document disposal processes to avoid unnecessary storage.

7.1.4.5 Workflow Management

7.1.4.5.1 Must automate document workflows, such as

approval processes and routing.

7.1.4.5.2 Must track the status of documents and generate notifications.

7.1.4.6 Document Search and Retrieval

7.1.4.6.1 Must provide advanced search capabilities to quickly locate documents based on keywords, metadata, or full-text search.

7.1.4.6.2 Must support filtering and sorting options to refine search results.

7.1.4.7 Document Version Control

7.1.4.7.1 Must track changes to documents over time and maintain version history.

7.1.4.7.2 Must allow for easy comparison of different versions.

7.1.5 Campus-wide Online Portal (Web App and Mobile App)

7.1.5.1 Personalized Dashboard

7.1.5.1.1 Must display relevant information, such as announcements, notifications, and upcoming deadlines.

7.1.5.2 Student Services

7.1.5.2.1 Must provide access to student information systems, including academic records, course schedules, and financial aid.

7.1.5.2.2 Must enable online registration, fee payment, and other student-related transactions.

7.1.5.3 Campus News and Events

7.1.5.3.1 Must display the latest campus news, events, and announcements.

7.1.5.3.2 Must allow users to subscribe to relevant news and event notifications.

7.1.6 Asset and Fleet Management System

7.1.6.1 Asset Inventory and Tracking

7.1.6.1.1 Must maintain a comprehensive inventory of all MPSU assets, including IT equipment, furniture, laboratory equipment, and vehicles.

7.1.6.1.2 Must track asset information, such as purchase date, cost, and current location.

7.1.6.1.3 Must use barcode or RFID technology for efficient asset identification and tracking.

7.1.6.2 Asset Lifecycle Management

7.1.6.2.1 Must track the entire lifecycle of assets, from acquisition to disposal.

7.1.6.2.2 Must schedule preventive maintenance and repairs to extend the life of assets.

7.1.6.2.3 Must calculate depreciation and generate depreciation schedules.

7.1.6.3 Asset Utilization and Allocation

7.1.6.3.1 Must allocate assets to departments or individuals based on need and availability.

7.1.6.3.2 Must track asset usage and utilization rates.

7.1.6.4 Fleet Management

7.1.6.4.1 Must track vehicle information, including make, model, year, and mileage.

7.1.6.4.2 Must schedule vehicle maintenance and repairs.

7.1.6.4.3 Must monitor fuel consumption and track vehicle usage.

7.1.6.4.4 Must manage driver licenses and insurance information.

7.1.6.5 Asset Disposal

7.1.6.5.1 Must establish procedures for asset disposal, including surplus property and equipment.

7.1.6.5.2 Must ensure compliance with disposal regulations and guidelines.

7.1.6.6 Reporting and Analytics

7.1.6.6.1 Must generate reports on asset utilization, maintenance costs, and depreciation.

7.1.6.6.2 Must provide data-driven insights to optimize asset management.

7.1.6.7 Hardware Integration

7.1.6.7.1 Must integrate with barcode scanners and RFID readers to automate asset tracking and inventory management.

7.1.7 Executive Management System

7.1.7.1 Dashboard and Key Performance Indicators (KPIs)

7.1.7.1.1

7.1.7.1.2 Must provide a centralized dashboard with real-time key performance indicators (KPIs) to track the overall performance of the institution.

7.1.7.1.3 Must allow for customization of dashboards to suit individual preferences and roles.

7.1.7.2 Data Visualization and Reporting

7.1.7.2.1 Must offer powerful data visualization tools to represent complex data in easy-to-understand charts and graphs.

7.1.7.2.2 Must generate comprehensive reports on various aspects of the institution's operations, such as financial performance, student enrollment, and faculty productivity.

7.1.7.3 Decision Support Tools

7.1.7.3.1 Must provide decision support tools, such as forecasting, scenario analysis, and what-if analysis, to assist in strategic planning.

7.1.7.4 Collaboration Tools

7.1.7.4.1 Must facilitate collaboration among executives and other stakeholders through features like document sharing, messaging, and video conferencing.

7.1.7.5 Security and Access Control

7.1.7.5.1 Must implement robust security measures to protect sensitive information and ensure data privacy.

7.1.7.5.2 Must provide role-based access control to limit access to authorized users.

7.1.7.6 Attendance Management

7.1.7.6.1 Must track student attendance, including class attendance and event attendance.

7.1.7.6.2 Must generate attendance reports to monitor student engagement.

7.1.7.7 Integration with Other Systems

7.1.7.7.1 Must integrate with other campus systems, such as

the SIS, HRMS, and Financial System, to provide a unified view of institutional data.

7.2 Educational Systems

Winning bidder shall supply, install and configure the following systems for MPSU.

7.2.1 Library Management System

7.2.1.1 Catalog Management

7.2.1.1.1 Must allow for the creation, editing, and deletion of bibliographic records for books, journals, articles, and other library materials.

7.2.1.2 Item Management

7.2.1.2.1 Must track the physical items in the library, including their location, status (e.g., available, checked out, lost), and circulation history.

7.2.1.3 User Management

7.2.1.3.1 Must create and manage user accounts, including student, faculty, and staff accounts.

7.2.1.3.2 Must assign privileges and access rights to different user groups.

7.2.1.4 Circulation Management

7.2.1.4.1 Must allow for the automated checkout, return, and renewal of library materials.

7.2.1.4.2 Must generate overdue notices and fines.

7.2.1.5 Online Catalog

7.2.1.5.1 Must provide a user-friendly online catalog that allows users to search for library materials by keyword, author, title, subject, or other criteria.

7.2.1.5.2 Must enable users to place holds on items, request interlibrary loans, and save search results.

7.2.1.6 Digital Resources

7.2.1.6.1 Must support the management of electronic resources, such as e-books, databases, and online journals.

7.2.1.6.2 Must provide access to licensed databases and e-books through the library's website or a dedicated portal.

7.2.1.7 Attendance Management

7.2.1.7.1 Must track student attendance, including class attendance and event attendance.

7.2.1.7.2 Must generate attendance reports to monitor student engagement.

7.2.1.8 Reporting and Analytics

7.2.1.8.1 Must generate various reports, such as circulation statistics, usage reports, and inventory reports.

7.2.1.8.2 Must provide analytics tools to track library usage patterns and trends.

7.2.2 Learning Management System

7.2.2.1 Course Management

7.2.2.1.1 Must allow instructors to create and manage online courses, including organizing course content, setting deadlines, and assigning grades.

7.2.2.1.2 Must support various content formats, such as text, images, videos, and multimedia files.

7.2.2.2 Student Enrollment

7.2.2.2.1 Must allow students to enroll in courses and access course materials.

7.2.2.3 Communication Tools

7.2.2.3.1 Must provide tools for communication between instructors and students.

7.2.2.4 Assessment Tools

7.2.2.4.1 Must allow instructors to create and administer various types of assessments, including quizzes, exams, and assignments.

7.2.2.4.2 Must provide automated grading and feedback features.

7.2.2.5 Content Delivery

7.2.2.5.1 Must support various content delivery methods, such as streaming video, downloading files, and online lectures.

7.2.2.6 Progress Tracking

7.2.2.6.1 Must track student progress and provide timely feedback on assignments and assessments.

7.2.2.6.2 Must generate reports on student performance and course completion rates.

8 Auditorium

The winning bidder shall develop the existing audatorium MPSU university that should include the specifications below:

8.1 Wide LED Wall Display

8.1.1 Display

8.1.1.1 Dimension: ~8 ft. (vertical) x 11 ft. (horizontal) (Approximately)

8.1.1.2 Display area: ~97.59 ft2

8.1.1.3 Diagonal dimension: ~169.651 in.

8.1.1.4 Resolution of at least 1344 x 1080

8.1.2 Power requirement

8.1.2.1 Max: 3300 watts

8.1.2.2 Typical: 1100 watts

8.1.3 Heat generation

8.1.3.1 Max: 11260 BTU

8.1.3.2 Typical: 3755 BTU

8.2 1 Unit Mixer with the following specifications:

8.2.1 20-Channel Mixing Console

8.2.2 Max. 16 Mic / 20 Line Inputs (12 mono + 4 stereo)

8.2.3 4 GROUP Buses + 1 Stereo Bus

8.2.4 4 AUX (incl. FX)

8.2.5 “D-PRE” mic preamps with an inverted Darlington circuit

8.2.6 1-Knob compressors High-grade effects: SPX with 24 programs

8.2.7 24-bit / 192kHz 2in / 2out USB Audio functions

8.2.8 Works with the iPad (2 or later) through the Apple iPad Camera Connection Kit / Lightning to USB Camera Adapter

8.2.9 Includes Cubase AI DAW software download version

BIDS AND AWARDS COMMITTEE

8.2.10 Cubasis LE for iPad available at App Store
8.2.11 PAD switch on mono inputs
8.2.12 +48V phantom power
8.2.13 Internal Universal Power Supply for world-wide use
8.2.14 XLR balanced outputs
8.2.15 Rack Mount Kit included
8.2.16 Metal chassis

8.3 2 Units Speakers with the following specifications:
- 8.3.1 System Performance
  - 8.3.1.1 System Type Self-powered, 2-way
  - 8.3.1.2 Frequency Response (±3 dB) 55 Hz – 14 kHz
  - 8.3.1.3 Frequency Range (–10 dB) 48 Hz – 16 kHz
  - 8.3.1.4 Nominal Dispersion 100° H × 40° V (C-position)
  - 8.3.1.5 Maximum SPL @ 1 m 132 dB-SPL (peak)
  - 8.3.1.6 Crossover Frequency 600 Hz acoustic 4th-order Butterworth
- 8.3.2 Amplification
  - 8.3.2.1 System Power 1000 W
  - 8.3.2.2 Distortion at Rated Power 0.1% max (30 Hz – 15 kHz)
  - 8.3.2.3 System Limiter Dynamic limiter
  - 8.3.2.4 Power Indicator Blue LED (system on)
- 8.3.3 Transducers
  - 8.3.3.1 Driver Complement 8 × 21/4 in mid-high drivers; 1 × 12 in LF
- 8.3.4 Channels
  - 8.3.4.1 Signal Indicators Power/fault, limit, front LED, signal input
  - 8.3.4.2 Input Connections Channel 1: XLR balanced: Pin 1 (GND), Pin 2 (+), Pin 3 (–)

8.4 2 units Subwoofer Speakers with the following specifications:
- 8.4.1 System Performance
  - 8.4.1.1 System Type Self-powered
  - 8.4.1.2 Frequency Response (–3 dB) 40 Hz – 250 Hz
  - 8.4.1.3 Frequency Range (–10 dB) 38 Hz – 250 Hz
  - 8.4.1.4 Nominal Dispersion Omni-directional
  - 8.4.1.5 Maximum SPL @ 1 m 130 dB-SPL (peak 6 dB CF)
  - 8.4.1.6 Crossover Frequency 40 – 100 Hz Butterworth bandpass, 100 Hz 4th-order Butterworth HPF at Line Out
- 8.4.2 Amplification
  - 8.4.2.1 System Power 1000 W
  - 8.4.2.2 Distortion at Rated Power 0.1% max (30 Hz – 15 kHz)
  - 8.4.2.3 System Limiter Dynamic limiter
  - 8.4.2.4 Power Indicator Blue LED (system on)
- 8.4.3 Transducers
  - 8.4.3.1 Driver Compliment 2 × 10-in high-excursion drivers
- 8.4.4 Channels
  - 8.4.4.1 Channels 1/2
  - 8.4.4.2 Signal Indicators Power/fault, limit, front LED, signal input
  - 8.4.4.3 Input Connections 2 XLR-1/4-in combo
  - 8.4.4.4 Controls Volume level, front LED function select, power

on/off, polarity select, line output

8.5 3 Units Wireless PA System Bluetooth Speakers

8.6 3 Units Compact Loudspeakers with the following specifications:

8.6.1 Frequency Response (–3 dB) 1 80 Hz – 16,000 Hz

8.6.2 Frequency Range (–10 dB) 1 70 Hz – 18,000 Hz

8.6.3 Nominal Coverage Pattern AMU208: 90° × 60° in horizontal configuration (rotatable high-frequency horn)

8.6.4 AMU208-120: 120° × 60° in horizontal configuration (rotatable high-frequency horn)

8.6.5 Recommended High-pass Filter 70 Hz with minimum 12-dB/octave filter

8.6.6 Crossover Passive, separate bandpass filters per transducer (200 Hz & 1.2 kHz)

8.6.7 Transformer Taps 70V: 5, 10, 20, 40, 80 W, bypass

8.6.8 100V: 10, 20, 40, 80 W, bypass

8.7 1 Unit Amplifier

8.7.1 Power Rating

8.7.1.1 Amplifier Power 2 × 600 W (THD+N < 0.04%, 1 kHz, 4–8 Ω, 70/100V)

8.7.1.2 I-Share Mode Power 1 × 1200 W (2–4 Ω, 70/100V)

8.7.1.3 Gain (Low-Z mode) 35 dB

8.7.1.4 Gain (70V mode) 35 dB

8.7.1.5 Gain (100V mode) 38 dB

8.7.2 Audio Performance

8.7.2.1 Frequency Response 4–8 Ω: 20 Hz – 20 kHz (±1 dB @ 1 W)

8.7.2.2 70/100V: 20 Hz – 20 kHz (±1 dB @ 1 W) with 50 Hz high-pass filter

8.7.2.3 Channel Separation (Crosstalk) > 80 dB @ 1 kHz, > 65 dB @ 20 kHz

8.7.2.4 Dynamic Range ≥ 100 dBA (at rated power)

8.7.2.5 Audio Latency < 1 ms (any analog or AmpLink input to loudspeaker output)

8.8 6 pcs Wireless Microphone (with receiver and transmitter for the 6 units Wireless Microphones)

8.9 1 Unit Dual Band Equalizer to integrate with the sound system solution in this section

8.10 2 Units Live streaming mixer

9 Multimedia Conference Room

The winning bidder shall develop a total of 2 multimedia conference rooms for MPSU university. Each conference room should include quantities based on the specifications below:

9.1 Must include 1 unit Interactive Display of at least 75” with the specifications below:

9.1.1 Screen type resolution of 3,840 x 2,160 with 60Hz.

9.1.2 Brightness of 350cd/m2

9.1.3 Contrast ratio of 1200:1

9.1.4 Must have 10ms response time.

9.1.5 Speaker type: Built in Speaker (12W x 2CH);

9.1.6 External Control: RS232C In/Out, RJ45 In/Out

9.1.7 # of Touch 40 points

BIDS AND AWARDS COMMITTEE

9.1.8 Touch pen type - passive pen.
9.1.9 Object recognition range 5mm/ 10mm / 15mm.
9.1.10 Touch response time of 10ms.
9.1.11 Drawing speed (touch latency) of 45ms.
9.1.12 VESA Mount of 800 * 400.
9.1.13 Must be Wall Mounted
9.1.14 Hardware features Touch Overlay (IR), Front Connectivity, OPS I/F Support (w/OPS Box); WiFi/BT Module.

9.2 Conference table for 15 people
9.3 15 units of ergonomic office chair
9.4 2 units 2.5HP Split type Air-conditioning unit
9.5 1 unit of Digital Signal Processor (DSP) unit
9.6 1 unit of ceiling microphone
9.6.1 Must have automatic dynamic beamforming.
9.6.2 Must have 28 electret condenser capsules.
9.6.3 Must have perfect speech intelligibility.
9.6.4 Must be certified to work with MS Teams and Zoom.
9.6.5 Must have exclusion zones.
9.6.6 Must have priority zone.
9.6.7 Must have an audio output 1 x 3-pin terminal (fits Phoenix contact MCVW 1.5-3-ST-3.81); 2 x Digital Dante Network Audio (RJ-45 Primary and Secondary).
9.6.8 Must have a minimum latency of 4 ms
9.6.9 Must have max. sound pressure level 104 dB SPL.
9.6.10 Must have transducer principle of pre-polarized condenser microphone.
9.6.11 Must be integrated to the sound system solution.
9.7 1 unit of WiFi Access Point (See item 9.5 for specifications).

10 E-Classrooms

The winning bidder shall develop a total of 20 e-classrooms for MPSU main campus. Each conference room should include quantities based on the specifications below:

10.1 Must include 1-unit Interactive Display of at least 75” with the specifications below.
10.1.1 Must have screen size of 75"
10.1.2 Must have IPS panel technology
10.1.3 Must have direct type back light
10.1.4 Must have an aspect ratio of 16:09
10.1.5 Must have native resolution of 3,840 x 2,160 (UHD)
10.1.6 Must have 60 Hz Refresh Rate
10.1.7 Must have brightness of 440 nit (w/o Glass Max.) and 390 nit (w/o Glass Typ.)
10.1.8 Must have contrast ratio of 1,200: 1
10.1.9 Must have a color gamut of 72% NTSC
10.1.10 Must have a viewing angle (H x V) of 178 × 178
10.1.11 Must have a color depth of 16.7 Million colors
10.1.12 Must have a response time of 8ms
10.1.13 Must have a surface treatment (haze) of 25%
10.1.14 Must have Built-in OPS Slot
10.1.15 Must have an operation hour of 16 / 7 (Hours / Days)
10.1.16 Must include a wall mount kit

BIDS AND AWARDS COMMITTEE

10.1.17 Must have AC 100-240 V ~, 50/60 Hz power supply
10.1.18 Must have a touch screen response time of ≤ 5 ms
10.1.19 Must have a power consumption of 225 W / 430 W
10.1.20 Must have the following technical specifications
- 10.1.20.1 CPU - At least a Quad Core
- 10.1.20.2 RAM - At least 8GB
- 10.1.20.3 Storage – 64GB
- 10.1.20.4 WiFi – 802.11a/b/g/n/ac/ax (Wi-Fi 6)
- 10.1.20.5 LAN – Gigabit LAN
- 10.1.20.6 Bluetooth – 5.0
- 10.1.20.7 OS Ver – Android 13

10.1.21 Must have the following input/output connectivity
- 10.1.21.1 HDMI (3, HDCP 2.2)
- 10.1.21.2 RGB (VGA)
- 10.1.21.3 Audio In
- 10.1.21.4 RS-232C In
- 10.1.21.5 RJ45 (LAN),
- 10.1.21.6 USB 3.0 Type A (4),
- 10.1.21.7 USB 2.0 (Type A)
- 10.1.21.8 USB Type C (USB-PD, DP-Alt)

10.1.22 Must have the following video/audio input/output
- 10.1.22.1 HDMI Out
- 10.1.22.2 Audio Out (1, Optical 1 (SPDIF))
- 10.1.22.3 Touch USB (2)
- 10.1.22.4 RJ45 (LAN)

BIDS AND AWARDS COMMITTEE

E-LEARNING PLATFORM DEVELOPMENT WITH INTEGRATED DATA AND COMMUNICATIONS SYSTEM

Particulars/ Concerns	Amendments/ Clarifications/ Response
A. General Section page 20	
5.4 The Bidder must have completed, within a period of ten (10) years from the submission of the bid, unless a shorter period is indicated in the Invitation to Bid and BDS, a Single Largest Completed Contract (SLCC) that is similar to the procurement project to be bid, and whose value must be equivalent to at least fifty percent (50%) of the ABC, adjusted to current prices using the Philippine Statistics Authority (PSA) consumer price indices.	**5.4 The Bidder must have completed, within a period of five (5) years from the submission of the bid, unless a shorter period is indicated in the Invitation to Bid and BDS, a Single Largest Completed Contract (SLCC) that is similar to the procurement project to be bid, and whose value must be equivalent to at least fifty percent (50%) of the ABC, adjusted to current prices using the Philippine Statistics Authority (PSA) consumer price indices.**
Section II. Instruction to Bidders page 32	
Each Bidder shall submit one copy of the original component and 3 copies of the second components of its Bid.	**Each Bidder shall submit one copy of the original component and 3 copies of the first and second components of its Bid.**
Section II. Instruction to Bidders page 41	
31.3 The performance security shall be in any form selected by the Procuring Entity in the amount indicated in the BDS, which shall not be less than the percentage of the ABC in accordance with the following price schedule:	**31.3 The performance security shall be in any form selected by the Procuring Entity in the amount indicated in the BDS, which shall not be less than the percentage of the Contract Price in accordance with the following price schedule:**
Section II. Instruction to Bidders page 48	
31.3 The Performance Security shall be in the form: *[choose one from any of the following:]* 1) The amount of not less than **Php 45,000,000.00** [*5% of ABC],* if performance security is in cash. 2) The amount of not less than **Php 45,000,000.00** [*5% of ABC],* if performance security is in cashier's check. 3) The amount of not less than **Php 45,000,000.00** [*5% of ABC],* if performance security is in manager's check. 4) The amount of not less than **Php 45,000,000.00** [*5% of ABC]* if performance security is in bank draft. 5) The amount of not less than **Php 45,000,000.00** [*5% of ABC]* if performance security is in guarantee. 6) The amount of not less than **Php 45,000,000.00** [*5% of ABC]* if performance security is irrevocable LoC, Or 7) The amount of not less than **Php 270,000,000.00** [30% of ABC] if performance security is Surety Bond.	31.3 **The Performance Security shall be in the form: *[choose one from any of the following:]*** 1) **The amount of not less than *5% of Contract Price,* if performance security is in cash.** 2) **The amount of not less than *5% of Contract Price,* if performance security is in cashier's check.** 3) **The amount of not less than *5% of Contract Price,* if performance security is in manager's check.** 4) **The amount of not less than *5% of Contract Price* if performance security is in bank draft.** 5) **The amount of not less than *5% of Contract Price* if performance security is in guarantee.** 6) **The amount of not less than *5% of Contract Price* if performance security is irrevocable LoC, Or** 7) **The amount of not less than 30% of *Contract Price* if performance security is Surety Bond.**

BIDS AND AWARDS COMMITTEE

C. Preparation of Bids page 29	
d) Bid Securing Declaration	Not Applicable
d) Bid Securing Declaration	Applicable

Section VII. Technical Specifications	
6.2.5.18 Must have DDoS/DoS attack protection. SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.zdfbn cx	**6.2.5.18 Must have DDoS/DoS attack protection. SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.**
10.2. HDMI (3 (HDMI1/2: HDCP 2.2/1.4, HDMI3: HDCP 1.4)),	**10.2. HDMI (3 (HDMI1/2: HDCP 2.2/1.4, HDMI3: HDCP 1.4)or orequivalent or higher or latest specs.),**
6.9.1.6 1 x Internal V.92 modem with RJ11 Socket	**6.9.1.6 1 x Internal V.92 modem with RJ11 Socket** **or equivalent or higher or latest specs.**
6.5.12.1.5 Network isolation with ACLs 6.5.12.1.6 DHCP snooping / guarding 6.5.12.1.7 Egress rate limit 6.5.12.1.8 LLDP-MED 6.5.12.1.9 Port restricted by MAC	**(Removed)**
13.2.25.1 The solution must have a 2.8-inch (320x240) capacitive touch screen TFT LCD.	**13.2.25.1 The solution must have a 2.8-inch (320x240) capacitive touch screen TFT LCD or equivalent or higher or latest specs.**

This shall form an integral part of the Bidding Documents.

REYNALDO P. GAYO JR.
Chairperson, Bids and Awards Committee