Republic of the Philippines
WESTERN MINDANAO STATE UNIVERSITY
Normal Road, Baliwasan Zamboanga City
www.wmsu.edu.ph
Telephone: 062-991-1771 LOC 1002

INVITATION TO BID

The Western Mindanao State University, through its Bids and Awards Committee (BAC), is inviting PhilGEPS registered suppliers to apply for eligibility and to submit bids for the item mentioned hereunder:

Name of Project: **ADOPTION OF DIGITAL LEARNING PLATFORM THROUGH ICT MODERNIZATION (CAMPUS NETWORK AND SECURITY)**
Approved Budget Cost: **Php 137,089,307.11**
Purchase Request No.: **PR 26-02-071**
Closing Date: **August 20, 2026 9:30 AM**
Delivery Period: **Sixty (60) Calendar Days**
Bid Docs: **Php 50,000.00**

1.) One (1) lot Adoption of Digital Learning Platform through ICT Modernization
- Campus Network and Security
The project covers the supply, delivery, installation, configuration, integration, testing, commissioning, and
support of a Smart Campus Network and Security Infrastructure.
The solution shall provide:
. High-availability campus network backbone
. Secure wired and wireless access
. Centralized monitoring and command center operations
. Integrated physical and logical security systems
. Digital engagement and campus services platform
. Data governance and privacy compliance systems
All components must be fully interoperable, enterprise-grade, and manufacturer-supported.
1.0 GENERAL REQUIREMENTS
. All equipment shall be brand new, unused, and currently supported by the manufacturer.
. The solution shall be delivered as a fully integrated, end-to-end system.
. The bidder shall be responsible for design, supply, installation, configuration, integration, testing,
commissioning, and support.
. All necessary licenses, subscriptions, accessories, and tools shall be included.
. The system shall operate as a single unified Smart Campus platform.
2.0 SYSTEM ARCHITECTURE REQUIREMENTS
The bidder shall implement a three-tier hierarchical network architecture:
. Core Layer (High Availability)
. Distribution Layer
. Access Layer (Wired and Wireless)
The architecture shall support:
. VLAN-based segmentation
. IPv4/IPv6 dual-stack operation
. Redundant links and failover
. Centralized monitoring and control
3.0 NETWORK DESIGN AND ENGINEERING REQUIREMENTS
The bidder shall submit and implement the following:
. Logical network topology diagram
. Physical network topology diagram
. VLAN segmentation plan
. IP addressing scheme
. Redundancy and failover design
. Wireless heatmap and coverage plan
All designs shall be approved by the End-User prior to implementation.
4.0 BILL OF QUANTITIES (BOQ) - BASIS OF DESIGN
The quantities are based on:
. Estimated 5,000-10,000 concurrent users
. Full campus wireless coverage
. Multi-building deployment
. Smart Campus security integration
Minimum Deployment:
. Core Switch: 3 units
. Distribution Switch: 2 units

. Access Switch: 12 units
. Indoor AP: 120 units
. Outdoor AP: 20 units
. CCTV DOME: 120 units
. IP PHONE: 64 units
. NVR-HDD: 10 units
. NGFW: 3 units
. NMS: 10,000 devices

5.0 STRUCTURED CABLING SYSTEM

The bidder shall supply and install a complete structured cabling system:

Copper Cabling
. Minimum: Category 6A
. Standards: ANSI/TIA-568

Fiber Cabling
. Backbone: Single Mode Fiber (OS2)
. Horizontal (if applicable): OM3/OM4

Requirements
. All cables shall be tested using certified cable analyzer (e.g., Fluke)
. 100% test results shall be submitted
. Proper labeling and documentation shall be mandatory

A. CORE SWITCH (3 units)

The winning bidder shall supply, deliver, install, configure, integrate, test, and commission:
. Three (3) units Core Switch
o Two (2) units - Main Campus (configured in High Availability mode)
o One (1) unit - Campus B (standalone or stackable, HAready)

Specifications:

GENERAL REQUIREMENTS

The Core Switch shall:
. Be enterprise-grade, brand new, and currently supported by the manufacturer
. Be designed for campus core / aggregation layer deployment
. Support non-blocking architecture with fully distributed forwarding
. Support automation and programmability via:
o REST API
o Python scripting (native or supported)
. Include built-in intelligent monitoring and analytics for:
o Traffic visibility
o Performance monitoring
o Network insights

PERFORMANCE

The switch must meet or exceed:
. Switching Capacity: ? 1.76 Tbps
. Forwarding Rate: ? 1,300 Mpps
. Fully distributed architecture with wire-speed forwarding
. Support for future scalability and high-bandwidth applications

INTERFACES

Each switch shall provide:
. Minimum 48 × 1G/10G SFP/SFP+ ports
. Minimum 4 × 40G QSFP+ OR 2 × 100G QSFP28 uplink ports
. Support for breakout cables (e.g., 40G to 4×10G)
. Support for Jumbo Frames (? 9,000 bytes)

LAYER 2 / LAYER 3 CAPABILITIES

- Layer 2 Features:
. VLAN support: ? 4,000 VLANs (IEEE 802.1Q)
. STP, RSTP, MSTP, or equivalent
. Link Aggregation (IEEE 802.3ad LACP)
. LLDP (IEEE 802.1AB)
. IGMP Snooping (v1/v2/v3)
. BPDU Guard / Filtering / Tunneling

- Layer 3 Features:
. Static Routing (IPv4/IPv6)
. OSPFv2 and OSPFv3
. BGP-4 (minimum support)
. VRF (Virtual Routing and Forwarding)
. ECMP (Equal-Cost Multi-Path)
. Policy-Based Routing (PBR)
. DHCP Server, Relay, and Client
. DNS Client

MULTICAST SUPPORT

The switch must support:
. IGMP v1/v2/v3 (IPv4)
. MLD v1/v2 (IPv6)
. Protocol Independent Multicast (PIM-SM) for IPv4 and IPv6

QUALITY OF SERVICE (QoS)

The switch shall support:
. Traffic classification (DSCP and 802.1p)
. Congestion avoidance mechanisms
. Queue management and scheduling
. Packet storm control (broadcast, multicast, unknown unicast)

Advanced QoS (Preferred but not restrictive):
. Priority Flow Control (PFC)
. Enhanced Transmission Selection (ETS)

HIGH AVAILABILITY

The solution must support:
. Virtual Switching / MLAG / VSX or equivalent technology
. Hitless failover / Non-stop forwarding
. Virtual Router Redundancy Protocol (VRRP) or equivalent
. Redundant, hot-swappable:
o Power supplies
o Fan modules
. Separation of control plane and data plane

SECURITY

The switch must include:
. Layer 2-4 Access Control Lists (IPv4/IPv6)
. 802.1X authentication support
. TACACS+ and RADIUS integration
. Role-based access control (RBAC)
. Secure management:
- SSHv2
- SFTP / Secure file transfer
. SNMP access control
. Syslog logging for audit trail
. Control Plane Policing (CoPP)

MANAGEMENT and MONITORING

The switch shall support:
. CLI (Command Line Interface)
. SNMP v2c and v3
. sFlow or NetFlow
. Remote Monitoring (RMON)
. IP SLA or equivalent performance monitoring
. Dual firmware images
. Configuration backup and rollback
. Diagnostic tools:
o Ping
o Traceroute
o Debug utilities

ENVIRONMENTAL AND PHYSICAL REQUIREMENTS

. Rack-mountable (19-inch standard rack)
. Operating temperature: 0°C to 45°C
. Power input: 100-240V AC
. Redundant power supply support
Hot-swappable fans

B. DISTRIBUTION SWITCH (2 units)
The winning bidder shall supply, deliver, install, configure, integrate, test, and commission:
. Two (2) units Distribution Switch
o To be deployed at the Main Campus
o Configured in High Availability (HA) mode (stacking / MLAG / equivalent)
The Distribution Switch shall serve as the aggregation layer between Core and Access switches and must be fully interoperable with all network components.
Specifications:
GENERAL REQUIREMENTS
The Distribution Switch shall:
. Be enterprise-grade, brand new, and manufacturersupported
. Be designed for campus aggregation / distribution layer deployment
. Support non-blocking architecture and wire-speed forwarding
. Support centralized management and monitoring integration
. Support automation and programmability via REST API
Switching Performance
Each switch must meet or exceed:
. Switching Capacity: ? 480 Gbps
. Forwarding Rate: ? 350 Mpps
. Wire-speed performance across all ports
. Low-latency forwarding suitable for high-density campus traffic
INTERFACES AND CONNECTIVITY
Each switch shall provide:
. Minimum 24 × 1G/10G SFP+ ports
. Minimum 4 × 10G SFP+ uplink ports OR 2 × 40G QSFP+ uplink ports
. Support for fiber and copper SFP modules
. Support for link aggregation (LACP)
Included Accessories:
. Minimum 4 units 10G SFP+ SR optical transceivers per switch
LAYER 2 CAPABILITIES
The switch must support:
. VLAN support: ? 2,000 VLANs (IEEE 802.1Q)
. STP, RSTP, MSTP (IEEE 802.1s/w)
. Link Aggregation (IEEE 802.3ad LACP)
. IGMP Snooping (v1/v2/v3)
. Jumbo frames (? 9,000 bytes)
. Storm control (broadcast, multicast, unknown unicast)
. LLDP (IEEE 802.1AB)
LAYER 3 CAPABILITIES
The switch must support:
. Static routing (IPv4/IPv6)
. OSPFv2 and OSPFv3
. Inter-VLAN routing
. VRRP or equivalent redundancy protocol
. Equal-Cost Multi-Path (ECMP)
. Policy-Based Routing (PBR)
Optional (for future scalability):
. BGP support (preferred but not mandatory)
QUALITY OF SERVICE (QoS)
The switch shall support:
. Minimum 8 hardware queues per port
. DSCP classification and marking
. IEEE 802.1p prioritization
. Traffic shaping and policing
. Weighted scheduling (WRR or equivalent)
. Strict priority queuing

SECURITY FEATURES
The switch must include:
. 802.1X port-based authentication
. RADIUS and TACACS+ support
. Dynamic VLAN assignment
. DHCP snooping
. Dynamic ARP inspection
. IP Source Guard
. Layer 2-4 ACLs (IPv4/IPv6)
. Control Plane Policing (CoPP)
HIGH AVAILABILITY AND RESILIENCY
The switch must support:
. Stacking or MLAG / Virtual Switching (or equivalent)
. Dual hot-swappable power supplies
. Hot-swappable fan modules
. Stateful failover in HA configuration
. Link aggregation across stacked units
MANAGEMENT AND MONITORING
The switch shall support:
. CLI access via SSHv2
. Web-based GUI (optional but preferred)
. SNMP v1/v2c/v3
. NetFlow or sFlow
. Syslog logging
. NTP synchronization
. REST API support
. Role-based access control (RBAC)
. Dual firmware images
. Configuration backup and rollback
ENVIRONMENTAL AND PHYSICAL REQUIREMENTS
. Rack-mountable (19-inch standard rack)
. Operating temperature: 0°C to 45°C
. Power input: 100-240V AC
. Front-to-back airflow preferred
C. 10G SFP+ OPTICAL TRANSCEIVERS
The bidder shall supply, deliver, install, test, and certify all 10G SFP+ optical transceivers required for the complete operation of the campus network, including:
. Core Layer interconnections
. Distribution uplinks
. Access uplinks
. Firewall interfaces
All modules shall be fully integrated, tested, and operational.
The bidder shall supply 88 units of 10G SFP+ optical transceivers for use across the campus network infrastructure.
TYPES AND QUANTITIES
. Access & intra-building links
o 10GBASE-SR Short Range (Multimode) - 52 units
. Backbone & inter-building
o 10GBASE-LR Long Range (Single-mode) - 36 units
1. TECHNICAL SPECIFICATIONS:
A. 10GBASE-SR (SHORT RANGE)
Optical & Physical
. Form Factor: SFP+ (Hot-pluggable)
. Standard: IEEE 802.3ae 10GBASE-SR
. Wavelength: 850 nm VCSEL laser
. Fiber Type: OM3 / OM4 multimode fiber
. Connector: Duplex LC
Distance Support
. ? 300 m (OM3)
. ? 400 m (OM4)
. Must support auto-adaptation across MMF grades
Performance Data Rate: 10.3125 Gbps full duplex
. Bit Error Rate: ? 1 × 10?¹²
. Low latency, wire-speed performance

Advanced Features
. Digital Optical Monitoring (DOM/DDM) with:
o Temperature
o Voltage
o TX/RX optical power
o Laser bias current
. Link diagnostics and alarm thresholds
. Soft TX disable / enable support
. EEPROM with module identification
B. 10GBASE-LR (LONG RANGE)
Optical & Physical
. Standard: IEEE 802.3ae 10GBASE-LR
. Wavelength: 1310 nm DFB laser
. Fiber Type: Single-mode (OS2)
. Connector: Duplex LC
Distance Support
. ? 10 km standard reach
. Stable operation up to 12 km typical (non-restrictive)
Performance
. Data Rate: 10.3125 Gbps
. Bit Error Rate: ? 1 × 10?¹²
. High optical sensitivity for long-distance stability
Advanced Features
. Full DOM/DDM monitoring
. Optical power margin monitoring
. Fault detection and reporting
2. GENERAL TECHNICAL REQUIREMENTS:
All transceivers must:
. Be compliant with:
o SFP+ MSA (Multi-Source Agreement)
o IEEE 802.3ae
. Support:
o Plug-and-play interoperability
o Automatic configuration with host devices
o Error detection and link diagnostics
3. COMPATIBILITY
The modules shall:
. Be OEM-certified OR guaranteed fully compatible with:
o Core switches
o Distribution switches
o Access switches
o Firewall systems
. Must:
o NOT disable ports or trigger vendor lock restrictions
o NOT void OEM warranty
. Bidder must provide:
o Compatibility declaration
o Vendor certification OR test validation
4. RELIABILITY AND DURABILITY
. MTBF: ? 1,000,000 hours
. Industrial-grade components preferred
. Resistant to:
o Temperature variation
o Optical degradation over time
5. ENVIRONMENTAL REQUIREMENTS
. Operating Temperature: 0°C to 70°C
. Storage Temperature: -40°C to 85°C
. Compliance:
o RoHS
o CE / FCC

6. TESTING AND ACCEPTANCE (STRONGER)
The bidder shall:
. Perform:
o Optical signal testing (TX/RX levels)

o Link validation per segment
o End-to-end connectivity testing
. Submit:
o Optical test results
o Link performance report
o Acceptance certification
7. SPARE STRATEGY
. Approx. 15% spare units (12 modules) shall be maintained
. Stored on-site for:
o Immediate replacement
o Maintenance operations
o Network expansion
8. WARRANTY AND SUPPORT
. Minimum 3 years warranty
. Advance replacement (within 7 days max)
. Access to:
o Firmware compatibility updates
o Technical support
D. NEXT-GENERATION FIREWALL (3 units)
The bidder shall supply, deliver, install, configure, integrate, test, and commission:
. Three (3) units Next Generation Firewall (NGFW)
o Two (2) units - Main Campus (configured in High Availability mode)
o One (1) unit - Campus B (standalone deployment)
The NGFW shall provide comprehensive network security, threat prevention, VPN connectivity, and centralized management for the campus network.
Specifications:
1. PERFORMANCE AND HARDWARE REQUIREMENTS
1.1 Throughput Capacities
The NGFW shall meet or exceed:
. Firewall Throughput: ? 18 Gbps
. Threat Prevention Throughput: ? 9.5 Gbps
. Application Inspection Throughput: ? 11 Gbps
. Intrusion Prevention System (IPS): ? 10 Gbps
. Anti-malware Inspection: ? 9.5 Gbps
. TLS/SSL Decryption & Inspection: ? 5 Gbps
. IPSec VPN Throughput: ? 11 Gbps
1.2 Session and Connection Handling
. New Connections per Second: ? 115,000 CPS
. Maximum Concurrent Sessions (SPI): ? 4,000,000
. Maximum DPI Connections: ? 2,000,000
. Maximum SSL Inspection Sessions: ? 350,000
1.3 Interface Requirements
. Minimum 6 × 10G SFP+ ports (supporting multi-speed where applicable)
. Minimum 24 × 1GbE RJ45 ports
. Minimum 1 × dedicated management port
. Minimum 1 × console port
. Minimum 2 × USB ports
1.4 Storage
. Internal storage: ? 128 GB
. Expandable storage support
2. SECURITY ARCHITECTURE AND FEATURES
2.1 Traffic Inspection and Threat Detection
The NGFW shall:
. Perform deep packet inspection (DPI) on all traffic
. Support bi-directional inspection (inbound and outbound)
. Support application identification and control across all ports and protocols
. Utilize single-pass or equivalent multi-function inspection engine
. Provide real-time threat detection with minimal latency
2.2 Advanced Threat Protection
The NGFW shall include:

. Cloud-based or on-premise sandboxing (or equivalent)
. Detection of:
o Advanced persistent threats (APT)
o Encrypted malware
o Zero-day attacks
. Ability to:
o Analyze suspicious files
o Block threats based on sandbox verdict
2.3 Intrusion Prevention System (IPS)
. Signature-based and behavior-based detection
. Automatic signature updates
. Bi-directional inspection
. Granular rule configuration
. GeoIP-based filtering
. Botnet detection and blocking
2.4 Anti-Malware Protection
. Gateway anti-virus and anti-spyware
. Real-time scanning of files and traffic
. Detection of known and unknown threats
. Continuous updates for emerging threats
2.5 Denial-of-Service (DoS/DDoS) Protection
. SYN flood protection
. UDP/ICMP flood protection
. Connection rate limiting
. Anomaly detection
3. APPLICATION AND WEB CONTROL
Application Control
. Identification and control of applications using signature database
. Ability to block, allow, or prioritize applications
Web Filtering
. URL filtering (HTTP/HTTPS)
. Content categorization
. Keyword-based filtering
. Policy-based access control
4. NETWORKING CAPABILITIES
. Policy-Based Routing (PBR)
. WAN Load Balancing (e.g., round-robin, spillover, weighted)
. Support for:
o VLAN trunking
o NAT (static, dynamic, PAT)
o DHCP server
. Routing Protocols:
o OSPF
o BGP
o RIP
5. VPN CAPABILITIES
The NGFW shall support:
. IPSec VPN (site-to-site)
. SSL VPN (remote access)
. Client VPN for:
o Windows
o macOS
o Linux
. Bandwidth management
o iOS / Android
. Redundant VPN gateway
. Secure SD-WAN capability (built-in, no additional license required)
6. HIGH AVAILABILITY AND RESILIENCY
The NGFW shall support:
. Active/Passive High Availability (HA)
. Stateful failover with session synchronization
. Shared licensing between HA units
. Hardware redundancy (dual PSU if applicable)

7. MANAGEMENT, MONITORING, AND REPORTING
The NGFW shall provide:
. Web-based GUI
. Command Line Interface (CLI via SSH)
. SNMP v2/v3 support
. Centralized management platform (on-premise or cloud)
. NetFlow/IPFix export
Visualization:
. User activity monitoring
. Application usage
. Real-time threat analytics
Additional Features:
. Zero-touch provisioning
. Configuration backup (local/cloud)
. Audit logs and reporting
8. LICENSING REQUIREMENTS
The solution must include:
. Minimum three (3) years subscription/license for:
o Intrusion Prevention (IPS)
o Anti-malware / Anti-virus
o Web filtering
o Application control
o Sandbox / advanced threat protection
9. COMPATIBILITY REQUIREMENTS
. Must be fully compatible with:
o Core network switches
o Distribution switches
o Network management system
. Must support:
o Open standards
o Interoperability with third-party systems
10. TESTING AND ACCEPTANCE
The bidder shall:
. Perform:
o Security validation
o Performance testing
o Failover testing
. Submit:
o Test reports
o Configuration documentation
o Acceptance certificates
11. WARRANTY AND SUPPORT
. Minimum 3 years warranty
. 24×7 technical support
. Firmware and software updates
. Advanced hardware replacement
E. 12- PORT POE ACCESS SWITCH (12 units)
The bidder shall supply, deliver, install, configure, integrate, test, and commission:
. Twelve (12) units 12-Port PoE Access Switch
The switches shall be deployed at the access layer to provide connectivity for:
. End-user devices (PCs, printers)
. Wireless access points
. IP phones and IoT devices
Specifications:
GENERAL REQUIREMENTS
The Access Switch shall:
. Be enterprise-grade, brand new, and manufacturersupported
. Be designed for access layer deployment in campus networks
. Support non-blocking switching architecture
. Support centralized management (on-premise or cloud)
. Support zero-touch provisioning or equivalent automated deployment

PERFORMANCE REQUIREMENTS
Each switch must meet or exceed:
. Switching Capacity: ? 68 Gbps
. Forwarding Rate: ? 45 Mpps
. Wire-speed forwarding across all ports
INTERFACES AND CONNECTIVITY
Each switch shall provide:
Downlink Ports
. Minimum 12 × 10/100/1000BASE-T PoE+ ports
. PoE Standard:
o IEEE 802.3af / 802.3at
. Power per port: ? 30W
Uplink Ports
. Minimum 4 × 1G/10G SFP/SFP+ uplink ports
Additional Interfaces
. Minimum 1 × console port (USB or RJ45)
. Minimum 1 × dedicated management port (OOBM)
. Minimum 1 × USB port (for storage/logs)
LAYER 2 FEATURES
The switch must support:
. VLAN support: IEEE 802.1Q (? 4,000 VLANs)
. STP, RSTP, MSTP
. Link Aggregation (IEEE 802.3ad LACP)
. LLDP (IEEE 802.1AB)
. IGMP Snooping (v1/v2/v3)
. Jumbo frames (? 9,000 bytes)
. Storm control (broadcast, multicast, unknown unicast)
BASIC LAYER 3 CAPABILITIES
The switch shall support:
. Static routing (IPv4/IPv6)
. Inter-VLAN routing
QUALITY OF SERVICE (QoS)
The switch shall support:
. IEEE 802.1p prioritization
. DSCP classification and marking
. Minimum 4-8 hardware queues per port
. Traffic shaping and rate limiting
. Priority queuing (strict priority or equivalent)
SECURITY FEATURES
The switch must include:
. IEEE 802.1X port-based authentication
. MAC-based authentication
. RADIUS and TACACS+ support
. DHCP snooping
. Dynamic ARP inspection
. IP Source Guard
. Layer 2-4 ACLs (IPv4/IPv6)
. Port security (MAC limiting, sticky MAC)
. Control Plane Policing (CoPP)
HIGH AVAILABILITY AND RESILIENCY
The switch must support:
. Stacking or virtual switching (or equivalent technology)
. Link redundancy using LACP
. Loop prevention mechanisms (STP/RSTP/MSTP)
MANAGEMENT AND MONITORING
The switch shall support:
. CLI access (via SSHv2)
. Web-based GUI (optional but preferred)
. SNMP v1/v2c/v3
. Syslog logging
. sFlow or NetFlow
. NTP synchronization
. REST API (preferred)
. Configuration backup and restore
. Dual firmware images

ENVIRONMENTAL AND PHYSICAL REQUIREMENTS
. Rack-mountable (19-inch standard rack)
. Operating Temperature: 0°C to 45°C
. Power input: 100-240V AC
. Fixed or modular power supply
TESTING AND ACCEPTANCE
The bidder shall:
. Perform:
o Functional testing
o Connectivity testing
o PoE load testing
. Provide:
o Test reports
o Configuration documentation
WARRANTY AND SUPPORT
. Minimum 3 years warranty
. Advance hardware replacement
. Firmware and software updates
. Technical support
F. INDOOR ACCESS POINT (120 units)
The bidder shall supply, deliver, install, configure, integrate, test, and commission:
. One hundred twenty (120) units Indoor Wireless Access Points
The Access Points shall provide secure, high-performance wireless connectivity for:
. Classrooms and laboratories
. Offices and administrative areas
. Common indoor spaces
Specifications:
GENERAL REQUIREMENTS
The Access Point shall:
. Be enterprise-grade, brand new, and manufacturersupported
. Be designed for indoor deployment in campus environments
. Support centralized management (cloud-based or controller-based)
. Support zero-touch provisioning or equivalent automated deployment
. Support high-density client environments
WIRELESS STANDARDS AND PERFORMANCE
The Access Point must support:
. IEEE 802.11ax (Wi-Fi 6)
. Dual-band operation:
o 2.4 GHz
o 5 GHz
Radio Specifications:
. Minimum 2×2 MIMO per radio
. Maximum aggregate throughput: ? 1.4 Gbps
CLIENT CAPACITY
. Minimum 256 associated clients per radio
. Ability to support multiple concurrent users with optimized performance
. Automatic RF optimization (channel and power adjustment)
. Interference detection and mitigation (or equivalent technology)
SECURITY FEATURES
The Access Point must support:
. WPA3 Enterprise and WPA3 Personal
. WPA2 backward compatibility
. IEEE 802.1X authentication
. RADIUS integration
. Guest access with isolation
. Rogue AP detection and mitigation
. Secure boot or equivalent device integrity mechanism

INTERFACES AND CONNECTIVITY
Each Access Point shall provide:
. Minimum 1 × 10/100/1000BASE-T Ethernet port. Automatic RF optimization (channel and power adjustment)
. Interference detection and mitigation (or equivalent technology)
SECURITY FEATURES
The Access Point must support:
. WPA3 Enterprise and WPA3 Personal
. WPA2 backward compatibility
. IEEE 802.1X authentication
. RADIUS integration
. Guest access with isolation
. Rogue AP detection and mitigation
. Secure boot or equivalent device integrity mechanism
INTERFACES AND CONNECTIVITY
Each Access Point shall provide:
. Minimum 1 × 10/100/1000BASE-T Ethernet port
RF AND PERFORMANCE FEATURES
The Access Point shall support:
. Orthogonal Frequency Division Multiple Access (OFDMA)
. Multi-user MIMO (MU-MIMO)
. Band steering (2.4 GHz to 5 GHz optimization)
. Load balancing across access points
. Fast roaming support:
o 802.11k
o 802.11v
o 802.11r
. Automatic RF optimization (channel and power adjustment)
. Interference detection and mitigation (or equivalent technology)
SECURITY FEATURES
The Access Point must support:
. WPA3 Enterprise and WPA3 Personal
. WPA2 backward compatibility
. IEEE 802.1X authentication
. RADIUS integration
. Guest access with isolation
. Rogue AP detection and mitigation
. Secure boot or equivalent device integrity mechanism
INTERFACES AND CONNECTIVITY
Each Access Point shall provide:
. Minimum 1 × 10/100/1000BASE-T Ethernet port
. Support for:
o Auto MDI/MDX
o Auto-negotiation
POWER REQUIREMENTS
. Power over Ethernet (PoE):
o IEEE 802.3af / 802.3at compliant
. Maximum power consumption: ? 15W-20W
ANTENNA
. Integrated omnidirectional antennas
. Optimized for ceiling-mounted indoor deployment
. Support for dual-band operation
MANAGEMENT AND MONITORING
The Access Point shall support:
. Centralized management via:
o Cloud platform OR
o On-premise controller
. Web-based GUI
. SNMP v2/v3
. Syslog
. Real-time monitoring:
o Client usage
o Traffic analytics

o RF performance
. Firmware upgrades (centralized)
. Configuration backup and restore
IoT AND ADDITIONAL FEATURES (PREFERRED)
. Bluetooth Low Energy (BLE) support (optional)
. Zigbee or IoT radio support (optional)
ENVIRONMENTAL REQUIREMENTS
. Operating temperature: 0°C to 45°C
. Designed for indoor ceiling or wall mounting
LICENSING REQUIREMENTS (MANDATORY)
The solution must include:
. Minimum three (3) years license/subscription for:
o Centralized management
o Monitoring and analytics
o Firmware and feature updates
TESTING AND ACCEPTANCE
The bidder shall:
. Perform:
o Wireless coverage testing
o Connectivity and roaming validation
o Performance testing
. Provide:
o Test reports
o Deployment documentation
WARRANTY AND SUPPORT
. Minimum 3 years warranty
. Advance hardware replacement
. Technical support and firmware updates
G. OUTDOOR ACCESS POINTS (20 units)
The winning bidder shall supply, deliver, install, configure, integrate, test, and commission:
. Six (6) units Outdoor Wireless Access Points
The Access Points shall provide reliable, high-performance wireless connectivity in outdoor areas.
Specifications:
GENERAL REQUIREMENTS
The Access Point shall:
. Be enterprise-grade, brand new, and manufacturersupported
. Be designed for outdoor deployment in campus environments
. Support centralized management (cloud-based or controller-based)
. Support zero-touch provisioning or equivalent automated deployment
. Support high-density user environments
WIRELESS STANDARDS AND PERFORMANCE
The Access Point must support:
. IEEE 802.11ax (Wi-Fi 6)
. Dual-band operation:
o 2.4 GHz
o 5 GHz
Radio Specifications:
. 5 GHz: 4×4 MIMO (minimum)
. 2.4 GHz: 2×2 MIMO (minimum)
. Maximum aggregate throughput: ? 3 Gbps
RF AND PERFORMANCE FEATURES
The Access Point shall support:
. Orthogonal Frequency Division Multiple Access (OFDMA)
. Multi-user MIMO (MU-MIMO)
. Band steering (2.4 GHz to 5 GHz optimization)
. Load balancing across access points
. Fast roaming support:
o 802.11k
o 802.11v
o 802.11r

. Automatic RF optimization (channel and power adjustment)
. Interference detection and mitigation (or equivalent technology)
. Beamforming for improved signal quality and range
CLIENT CAPACITY
. Minimum 256 associated clients per radio
. Capable of supporting high-density outdoor environments
SECURITY FEATURES
The Access Point must support:
. WPA3 Enterprise and WPA3 Personal
. WPA2 backward compatibility
. IEEE 802.1X authentication
. RADIUS integration
. Rogue AP detection and mitigation
. Secure boot or equivalent device integrity protection
INTERFACES AND CONNECTIVITY
Each Access Point shall provide:
. Minimum 1 × 1/2.5GBASE-T Ethernet port (multi-gig)
. Optional secondary Ethernet port (for redundancy or link aggregation)
. Support for:
o Auto MDI/MDX
o Auto-negotiation
. Support for Link Aggregation (LACP) (if dual ports available)
POWER REQUIREMENTS
. Power over Ethernet:
o IEEE 802.3at or 802.3bt compliant
. Maximum power consumption: ? 30W
OUTDOOR HARDENING (MANDATORY)
The Access Point must:
. Be weatherproof with minimum IP67 rating
. Be resistant to:
o Dust
o Rain and moisture
o UV exposure
. Support:
o Pole and wall mounting (mounting kit included)
o Operating temperature: -20°C to 55°C (or better)
. Include:
o Surge and lightning protection
ANTENNA
. Integrated or external antennas (omnidirectional or sectorized)
. Optimized for outdoor coverage
. Support dual-band operation
MANAGEMENT AND MONITORING
The Access Point shall support:
. Centralized management via:
o Cloud platform OR
o On-premise controller
. Web-based GUI
. SNMP v2/v3
. Syslog
. Real-time monitoring:
o Client usage
o Traffic analytics
o RF conditions
. Firmware upgrades (centralized)
. Configuration backup and restore
IoT AND ADDITIONAL FEATURES
. Bluetooth Low Energy (BLE) support (optional)
. Zigbee or equivalent IoT radio (optional)
LICENSING REQUIREMENTS (MANDATORY)
The solution must include:
. Minimum three (3) years license/subscription for:

o Centralized management
o Monitoring and analytics
o Firmware and feature updates
TESTING AND ACCEPTANCE
The bidder shall:
. Perform:
o Outdoor wireless coverage testing
o Connectivity and roaming validation
o Performance testing
. Provide:
o Test reports
o Deployment documentation
WARRANTY AND SUPPORT
. Minimum 3 years warranty
. Advance hardware replacement
. Technical support and firmware updates
H. OUT-OF-BAND MANAGEMENT SWITCH (3 units)
The bidder shall supply, deliver, install, configure, integrate, test, and commission:
. One (1) unit Out-of-Band (OOB) Management Switch / Console Server
The solution shall provide secure, centralized remote management access to:
. Network devices (core, distribution, access switches, firewalls)
. Servers and compute nodes
Specifications:
GENERAL REQUIREMENTS
The solution shall:
. Be enterprise-grade, brand new, and manufacturersupported
. Be designed for out-of-band management and remote access
. Support secure remote administration independent of the production network
. Provide centralized console and management access
HARDWARE REQUIREMENTS
The device must include:
Console Ports
. Minimum 24 × RJ45 serial console ports (RS-232)
Network Interfaces
. Minimum 2 × 10/100/1000BASE-T Ethernet ports (for management and redundancy)
. Minimum 1 × dedicated management port
System Specifications
. Multi-core processor (? 1.4 GHz equivalent)
. Memory: ? 8 GB RAM
. Storage: ? 64 GB internal storage (SSD or equivalent)
Additional Interfaces
. Minimum 1 × USB port for storage or backup
. Console access via:
o RJ45 or USB console port
CORE FUNCTIONALITY
The solution shall support:
. Centralized access to all connected devices via:
o Serial console
o Network management interfaces
. Secure remote access via:
o SSH (mandatory)
o HTTPS (mandatory)
. Ability to:
o Remotely monitor devices
o Access device consoles during outages
o Perform troubleshooting and recovery
SECURITY FEATURES
The solution must support:

. Role-Based Access Control (RBAC)
. Authentication via:
o RADIUS
o TACACS+
o Local authentication (fallback)
. Secure communication:
o SSHv2
o HTTPS (SSL/TLS)
. Audit logging:
o User activity logs
o Session tracking
o Event logs
MANAGEMENT AND MONITORING
The solution shall support:
. Web-based management interface
. Command Line Interface (CLI)
. SNMP v2/v3
. Syslog integration
. Configuration backup and restore
HIGH AVAILABILITY AND RESILIENCY
The solution must support:
. Dual Ethernet ports for redundancy
. Automatic failover between management interfaces (preferred)
. Reliable operation during production network outages
OTHER FEATURES
The solution may support:
. Secondary WAN or cellular failover (optional)
. Environmental monitoring integration (optional)
COMPATIBILITY REQUIREMENTS
The solution must:
. Be fully compatible with:
o Core switches
o Distribution switches
o Access switches
o Firewall systems
. Support:
o Standard serial console interfaces
o Multi-vendor environments
TESTING AND ACCEPTANCE
The bidder shall:
. Perform:
o Connectivity testing (console and network access)
o Remote access validation
o Failover testing
. Provide:
o Test reports
o Configuration documentation
WARRANTY AND SUPPORT
. Minimum four (4) years warranty
. Firmware and software updates
. Technical support
. Advance hardware replacement (RMA)

. 137,089,307.11/LOT. Total of 137,089,307.11
of I. ENTERPRISE NETWORK MANAGEMENT SYSTEM (License and Deploy for Minimum 10,000 Devices , 3years Subscription)
General Features and Capabilities
. The solution must support installation on both physical and virtual servers/environment.
. The solution must support installation with industry recognized operating systems.
. The installation process should provide an option to automatically install (WhatsUp Gold or SolarWinds

Platform).
. The software must be capable of monitoring a vast number of devices.
. The solution must be installed in an environment with a dedicated database server instance.
. The solution must be able to run in the following minimum specifications:
- Processor: CPU: 8 Cores / vCPUs, 2.6 GHz
- RAM: 32GB
- Hard Drive: 15 GB in RAID 1 for OS/Application, 4 x 100 GB in RAID 10 for database files
- Network Interface: 1 Gbps
- Licenses should be perpetual and based on the number of devices monitored, independent of the number of components monitored.
- The solution must have the capability to integrate separate add-on modules to unlock additional features as needed.
- The solution must not require the installation of agents on the servers to be monitored; all discovery and monitoring should be done through standard network protocols like SNMP, SSH, WMI, ping, etc.
- The architecture must support active/passive failover with the necessary licensing.
- The solution should allow for customization of the graphical web interface, including adding an organization logo.
- The solution must support different methods of user authentication, including:
-- Local users
-- LDAP, including Active Directory
-- Cisco ISE
-- OpenID Connect
Device Discovery
. The software must support device discovery through IP address ranges.
. The solution should support discovery of devices associated with cloud accounts (e.g., AWS, Azure).
. The software should support discovery of devices in both Hyper-V and VMWare virtual environments.
. The software must support discovery of wireless infrastructure devices from major vendors.
. The software should support discovery via multiple industry standard credential types, including SNMP versions 1-3, WMI, ADO, Telnet, SSH, VMWare, JMX, SMIS, AWS, Azure, Meraki Cloud and REST API credentials.
. The solution should allow scheduling automatic discovery of new devices and assign corresponding monitors to device components.
Device Monitoring
. The solution must continuously monitor the availability and performance of all infrastructure components, including routers, switches, firewalls, servers, and storage devices. It should support monitoring of any IP-enabled device using standard protocols such as ICMP, SNMP, WMI, and SSH.
. The solution should provide notifications when performance monitors exceed configured thresholds.
. The solution must be capable of discovering, mapping, and monitoring cloud environments such as Amazon Web Services (AWS) and Microsoft Azure. It should track cloud resource usage, performance, and billing, with the ability to store data for long-term trend analysis
Alerting and Automated Actions
. The solution must provide real-time alerts via email, SMS, Slack, and logging when devices change state or

performance thresholds are exceeded. The alerting system should minimize alert storms by utilizing network dependencies identified during the discovery process.
. The solution should support the creation of action policies for alerts, including automated responses such as service restarts or custom PowerShell scripts to mitigate issues without manual intervention.
Network Mapping and Visualization
. The solution must automatically identify and map all devices within the network, including routers, switches, servers, access points, and other connected devices. It should utilize Seed Scan technology to discover network topology and support IP Range Scanning.
. The solution must generate and display Layer 2/3 network maps that provide a comprehensive view of core infrastructure, Windows infrastructure, wireless devices, and cloud resources. The map should offer end-to-end visibility, enabling quick status checks and drilldowns for detailed performance data.
Dashboard and Reporting
. The solution should offer a user-friendly reporting environment, allowing for the creation of customizable dashboards and real-time performance monitors. Reports should cover hardware inventory, installed software, updates, warranty status, and other critical metrics.
. The solution should simplify IT asset management by providing comprehensive inventory reports that identify underutilized hardware, unlicensed software, and other actionable insights.
Configuration Management
. The software must have an add-on feature to allow backup and monitoring of network device configurations, including compliance checking with industry standards (e.g., PCI, HIPAA, SOX).
. The solution should notify when configurations deviate from the previous backup and display configuration differences.
Virtual Infrastructure Monitoring
. The software must have an add-on feature to support monitoring of virtual environments, including Hyper-V and VMWare.
. The solution should provide dashboards and maps detailing virtualization environments.
Integration and APIs
. The solution must include a REST API to facilitate integration with other systems and applications. It should support both inbound and outbound API calls to enable automated workflows, device management, and data exchange with third-party applications such as Salesforce and Office 365.
. The solution should be able to integrate with network traffic analytics platforms, support real-time traffic flow monitoring, and offer advanced anomaly detection.
. Documentation, Support and Services
- The software provider must offer public access to tool manuals, user community forums, and a knowledge base.
- The software provider must offer 8x5 and 24x7x365 support options for critical issues, with support channels including phone, web, and email.
- The vendor must provide installation and configuration services for the solution, ensuring full deployment and integration with existing infrastructure.
- The vendor must offer training services for administrators and users, covering all aspects of the solution's operation, including device discovery, monitoring, dashboard creation, and reporting.
- The vendor must offer maintenance and support services,

including software updates, troubleshooting, and assistance with system optimization.

J. BOOM BARRIERS (3 units)

. Barrier Arm Length: 3 to 6 meters (adjustable based on site requirements)
. Operation Type: Automatic (Motorized) with manual override option
. Opening/Closing Time: Adjustable, 1.5 to 6 seconds
. Control Modes: Remote control, push button, loop detector, RFID access, timer
. Motor: DC Brushless motor / AC motor with frequency conversion
. Power Supply: 220V AC ±10%, 50/60 Hz
. Power Consumption: Max 60-100 W
. Duty Cycle: Continuous operation capable (24/7 use)
. Ingress Protection : IP54 or higher (weatherproof for outdoor use)
. Material & Finish: Steel enclosure with powder coating (rust & corrosion resistant)
. Safety Features: Infrared safety sensors, emergency stop button, auto-reverse on obstacle detection
. Communication Interfaces: Relay output, dry contact, RS485, optional integration with access control systems
. Mounting: Floor mounted, bolt-down base plate

K. 2-PATHWAY TURNSTILE (4 units)

. Number of Lanes: 2 separate pathways, bidirectional or unidirectional options
. Type: full-height turnstile
. Material: Stainless steel 304 or 316 (rust and corrosion resistant)
. Dimensions (per lane): Approx. 1200mm (L) × 300mm (W) × 1000mm (H)
. Operation Mode: Motorized with electromagnetic or mechanical locking
. Access Control Integration: Supports RFID card readers, biometric scanners (fingerprint/face), QR code, barcode readers
. Control System: Microprocessor-based control with fail-safe mechanism
. Throughput Capacity: Up to 30-40 persons per minute per lane
. Power Supply: AC 220V ±10%, 50/60 Hz; Power consumption approx. 30-50 W
. Backup Power: with battery backup for 4-6 hours during power failure
. Safety Features: Anti-tailgating sensors, emergency pushto-release button, obstacle detection
. Ingress Protection: IP54 or higher for indoor/outdoor installation
. Communication Interface: RS-485, TCP/IP, dry contacts for integration with building management systems
. Indicators: LED directional indicators, audio alarms
. Mounting: Floor mounted with anchor bolts
. Finish Brushed or polished stainless steel
. With Remote control, visitor management software compatibility, anti-panic mode

L. ELECTROMAGNETIC LOCK SYSTEM (26 units)

. Type: Fail-safe (unlocks when power is off)
. Holding Force: ??600?lb (270?kg) ideal; 1200?lb (545?kg) for heavy doors
. Voltage Input: 12?V DC or 24?V DC
. Current Draw: ~300-500?mA @12?VDC; bigger units at 24?V
. Finish & Material Steel or stainless steel; corrosion-resistant coating
. Mounting Standard surface-mount for swing door frames

. Door Type: Compatible with inswing, outswing, fire/swing doors
. Safety Features LED status indicator, door monitoring, surge protection
. Control Interface Dry contacts, relay, RS-485 (for access control tools)
. Fire/Alarm Support Integrates with fire panels for emergency release
. Ingress Rating: IP54 for outdoor-grade; IP65 models

M. ACCESS CONTROL TERMINAL (1 unit)
. Authentication Modes: Fingerprint, RFID card (13.56 MHz & 125 KHz), PIN code, facial recognition, QR code
. User Capacity: Minimum 10,000 users (scalable up to 100,000)
. Card Compatibility : MIFARE, HID, EM, or IC cards
. Identification Speed: ? 1 second for fingerprint/face/card scan
. False Acceptance Rate: (FAR) < 0.001% (biometric mode)
. False Rejection Rate: (FRR) < 1%
. Display: at least 2.4-5 inch TFT LCD or capacitive touchscreen
. Keypad Touch or physical numeric keypad
. Connectivity: TCP/IP, RS-485, USB Host, Wiegand Input/Output, Wi-Fi (optional), 4G LTE (optional)
. Relay Output: 1× Door Lock Relay Output (NO/NC), 1× Alarm Output
. Door Sensor Input: 1× Door Contact, 1× Exit Button, 1× Tamper Switch
. Built-in Features: Access logs storage (?100,000 logs), tamper alarm, access schedules, anti-passback
. Software Integration: Compatible with access control software (e.g., ZKTeco ZKBioSecurity, Suprema BioStar, HID)
. Power Supply: 12V DC ±10%, ?500mA
. Backup Optional battery or UPS power (for >2 hours)
. Housing: Vandal-resistant polycarbonate or metal alloy, IP65-rated
. Mounting: turnstile-mounted

N. RFID System
Centralized Access Management Software (CAMS)
Quantity: One (1) Package
Specifications:
. Dynamic Management Function for RFID
. Must be capable of student access, faculty access, and visitor access.
. Must support multiple access control systems.
. Must be capable of advanced online registration for visitors through the web.
. Must support both server and client network configuration.
. Must operate in real time with the ability to manage access control input and output up to 5 zones within a 24-hour period.
. Must be capable of filtering individual or group data based on the
. user's preferences.
. Multi-Mode Authentication for Enhanced Security and Flexibility
Note: The RFID system will also be integrated to the current university Academic Record and Information System (ARIS)
General Description:
. The Access Turnstile shall support dual-mode authentication using RF cards (e.g., MIFARE, NFC-compatible) and QR codes for seamless and secure user access.
. Must be capable of efficiently controlling the movement of individuals by installing turnstiles with rotating arms or barriers, allowing entry to one person at a time.

. Must have Anti-fraud measures with encrypted communication between readers and the central server using AES-256 to prevent cloning or unauthorized access.
Additional Features/Specifications:
. RF card reader: ISO/IEC 14443 Type A/B standards, with a reading range of at least 5 cm and a response time of ?0.2 seconds.
. QR code scanner: High-resolution optical scanner capable
. of reading dynamic and static QR codes from mobile devices or printed media, with a scanning speed of ?0.3 seconds.
. Turnstile Size: at least 1200*280*1000 mm (customizable)
. Lane width: at least 500 mm
. Passing speed: 35 person/min
. Casing Material: at least 304 stainless steel
. Emergency Function: The Arm drops automatically
. during power loss.
. Working Volt/Watt: at least 24V/ 20 Watts
. Power Input: at least 110-220VAC 50/60Hz
O. SMART ID THIN PVC CARD, 13.56Mhz
. 1K bytes EEPROM, ISO14443A
. Read/Writable
. PVC Material
. White Glossy surface
. Size: 85 x 54mm,
. Thickness: 0.8mm - 0.85mm
. ISO Standard
. Printable by following Thermal and Retransfer Printer; Magicard, Evolis Zebra, Hiti, Fargo, Smart, Data Card, Point man CIM, Hodoo, Etc.
P. RFID Printer (2 units)
Specifications:
. Print speed
- Up to 190 full colour cards per hour
- Up to 720 monochrome cards per hour
. Card capacities
- 100 card input
- 70 card output
. Visual security
. Electronic security
- Magnetic stripe encoding: HiCo and LoCo ISO 7811, JIS2 (Optional)
- Smart card encoding: Contact chip, MIFARE®, DESFire® and iClass® (Optional)
. Warranty: at least 2 years
. Print technology: 300dpi colour dye sublimation, monochrome thermal printing and rewritable technology.
. Feed system: Manual/automatic
. Connectivity: USB, Ethernet
. Compatibility: Windows, Mac, Linux with CUPS support.
. Card thickness: 0.50mm to 1.27mm / 20mil to 50mil
. Dimensions: mm 220 W x 250 H x 470 D, Inch 8.6 W x 9.8 H x 18.5 D
Q. 2GB Internet Leased Line (3 Years SLA) with 12 Public IP
R. 500MB Internet Leased Line (3 Years SLA) with 6 Public IP(ESU Diplahan,Ipil,Curuan,Pagadian,Tungawan Campus)
S. 3KVA UPS Racmount(6 units)
. Apparent Power Rating: 3000 VA (3kVA)
. Real Power Capacity: 2400 Watts (assuming a standard ??. ?? power factor) up to 2700 Watts.
. Topology: Double-Conversion Online. This is critical-it ensures zero transfer time (?? ms) between grid loss and battery backup because the inverter continuously runs off the DC bus.
. Output Waveform: Pure Sine Wave (essential for modern active PFC servers and sensitive enterprise

IT hardware).
. Efficiency: ~88% at full load under normal online mode.
. Nominal Input/Output Voltage: 230V AC standard (highly compatible with 220V/240V grids).
T. 5MP IP Dome/Bullet Cameras
o TCP/IP Based CCTV Cameras
o Should support 12 VDC or 24 VAC.
o Should support 25/30/50/60 fps.
o Should be at least IP66 Ingress protection
U. NVR-HDDs
Surveillance HDDs (10TB)
V. IP Phone
Display: 2.4" upto 2.8" Color LCD display
Built-in na Wi-Fi at Bluetooth
Installation Services(SLA)
Scope of Work
The winning bidder shall provide all labor, tools, equipment, supervision, testing instruments, consumables, and materials necessary for the complete installation of the Campus Network and Security Infrastructure.
Minimum Requirements
. Installation of all active network equipment including:
o Core Switches
o Distribution Switches
o Access Switches
o Next Generation Firewalls
o Outdoor and Indoor Access Points
o Out-of-Band Management Switch
o Network Management System servers/appliances
. Installation of RFID System components
. Installation of Turnstiles and Boom Barriers
. Installation of fiber optic and structured cabling accessories
. Rack mounting, grounding and power integration
. Equipment labeling and identification
. Cable management and routing
. Installation shall comply with:
o TIA/EIA Standards
o IEEE Standards
o Manufacturer installation guidelines
. Site restoration after installation
Deliverables
. Equipment installation report
. Cable and equipment labeling report
. As-built diagrams
. Site acceptance report
. Photographic documentation
Acceptance Criteria
. 100% equipment physically installed
. Equipment powered on and operational
. All ports and interfaces tested
. Acceptance signed by authorized university representatives
(Covers physical mounting, structured/fiber cabling integration, Fluke testing, turnstiles/barrier rollouts, CCTV,IP Phone, UPS, and deployment.)
Configuration Services
Scope of Work
The winning bidder shall perform complete configuration, integration, optimization, and security hardening of all supplied systems.
Minimum Configuration Requirements
Network Infrastructure
. VLAN design and implementation
. Layer 3 routing configuration
. OSPF and BGP configuration where required

. IP addressing scheme implementation
. High Availability (HA) configuration
. VRRP configuration
. Link Aggregation (LACP)
. QoS implementation

Security Infrastructure
. Firewall policy creation
. IPS/IDS configuration
. Application control policies
. Web filtering policies
. VPN configuration
. Threat prevention activation
. User authentication integration
. Role-based access control
. CCTV
. IP PHONE

Wireless Infrastructure
. SSID creation
. WPA3 security configuration
. Guest access implementation
. Roaming optimization
. RF tuning and optimization

Network Management System
. Device onboarding
. Dashboard creation
. Alert and notification setup
. Reporting templates
. Performance monitoring policies

RFID and Access Control
. User enrollment system
. Access schedules
. Access zones
. Turnstile integration
. Boom barrier integration

Deliverables
. Complete configuration documentation
. Network topology diagram
. IP addressing plan
. Security policy documentation
. Backup copies of all configurations

Acceptance Criteria
. Successful end-to-end connectivity
. Successful failover testing
. Successful security policy testing
. Successful monitoring and alert testing

PROJECT MANAGEMENT

Scope of Work
The bidder shall provide overall project management throughout the implementation period.

Minimum Requirements
The bidder shall assign:
. One (1) Project Manager
. One (1) Network Architect
. One (1) Security Specialist
. Technical Implementation Team

Responsibilities
. Project planning
. Project scheduling
. Resource management
. Stakeholder coordination
. Risk management
. Change management
. Quality assurance
. Progress monitoring
. Issue escalation and resolution

. Documentation management
Deliverables
. Project Management Plan
. Detailed Implementation Schedule
. Weekly Progress Reports
. Risk Register
. Quality Assurance Reports
. Completion Report
Acceptance Criteria
. Project milestones achieved
. Progress reports submitted
. Successful completion of all project phases
The bidder shall submit a detailed implementation methodology, manpower deployment plan, work breakdown structure (WBS), project schedule, testing procedures, acceptance procedures, and complete turnover documentation. All services shall be included in the contract price and no additional costs shall be charged to the University.
DEPLOYMENT AND IMPLEMENTATION
Scope of Work
The bidder shall perform production deployment, migration, commissioning, testing, turnover, and operationalization of the complete Campus Network and Security Solution.
Minimum Requirements
System Deployment
. Migration from existing network infrastructure
. Production activation of network services
. Wireless deployment activation
. Security policy enforcement
. RFID activation
. Turnstile commissioning
. Boom barrier commissioning
. NMS production rollout
Testing and Validation
. Network connectivity testing
. Wireless coverage testing
. Performance testing
. Failover testing
. Security testing
. User Acceptance Testing (UAT)
Knowledge Transfer
. Administrator training (minimum 40 hours)
. Operations training (minimum 16 hours)
. Documentation turnover
Deliverables
. Commissioning Report
. UAT Report
. Training Completion Report
. Final Acceptance Report
. Operations Manual
. Maintenance Manual
. As-Built Network Diagram
. Asset Inventory
Acceptance Criteria
. Successful UAT
. Successful HA and failover testing
. Successful RFID and access control operation
. Successful NMS monitoring
. Final acceptance by the University
ABC:Php 137,089,307.11
The criteria to be used for the eligibility check of the prospective bidders, examination and evaluation of bids, post qualification and all matters relevant to this procurement shall be in accordance with Republic Act No. 12009 (New Government Procurement Act) and its Implementing Rules and Regulations.

Interested bidders may obtain further information from WMSU BAC Secretariat regarding the checklist of eligibility and technical requirements and Evaluation Criteria (Eligibility Checklist and Evaluation Criteria indicated in the Philippine Bidding Documents (PBDs) can be downloaded in the associated components of this Invitation to Bid).

IMPORTANT NOTICE FOR BIDDERS:
1. Bidding papers may be acquired starting July 25 to August 20, 2026, from the BAC Office or download from agency website (www.wmsu.edu.ph) and PhilGEPS website. The WESTERN MINDANAO STATE UNIVERSITY shall allow the bidder to present its proof of payment for the Bidding Documents fees before the submission of their bids, pursuant to the latest Guidelines issued by the GPPB, in the amount of Fifty Thousand Pesos (Php.50,000.00). (Please attached the machine copy of the Official Receipt)

2. All bidders are required to post a Bid Security, at least Two (2%) Percent of the ABC in the form of Cash, Cashier's Check or Manager's Check or may submit Bid Securing Declaration. Bids without Bid Security will not be considered.

3. The Bidder shall prepare an original of the Eligibility Documents & Technical Components and original of Financial Proposal and clearly mark each "ORIGINAL – ELIGIBILITY DOCUMENTS and TECHNICAL COMPONENTS", and "ORIGINAL – FINANCIAL PROPOSAL", respectively. Bidders shall submit one (1) set of the first and second components of its bid. State the unit price of each item and the total bid price and also state the shortest time of delivery and submit your proposal duly signed by your representative in a sealed envelope. Failure to submit any of the eligibility documents, technical components and financial proposal during bid opening will result in disqualification.

4.Pre-Bid Conference will be on August 6, 2026 9:30 AM at Procurement Conference Office, Ground Floor Administration Building, WMSU, Zamboanga City and/or through video conferencing or webcasting via Zoom, which shall be open to prospective bidders.

5. Bid Submission will be on or before August 20, 2026 9:30 AM. through Manual Submission.

6. Bid opening shall be on August 20, 2026 9:30 AM. at Procurement Conference Office, Ground Floor Administration Building, WMSU, Zamboanga City. Bids will be opened in the presence of the Bidders representatives who choose to attend at the address above. Late bids shall not be accepted.

7. The contract will be awarded to the bidder who submits the Most Economically Advantageous Responsive Bid (MEARB)

8. Price validity shall be for a period of 120 calendar days.

9. Bidders shall submit original brochures showing certifications of the product being offered.

10. Warranty shall be for a period of Six (6) months for supplies and materials. One (1) year for equipment, from date of acceptance by WESTERN MINDANAO STATE UNIVERSITY.

11. Bids received in excess of the ABC shall be automatically rejected at Bid Opening.

The WESTERN MINDANAO STATE UNIVERSITY reserves the right to reject any or all Bids and to accept the bid most advantageous to the government, and to award the contract by lot, if warranted.