TECHNICAL SPECIFICATIONS
Solicitation No. RSU-2023-10-079
ABC: PhP1,250,000,000.00
QTY: 1 Lot

Intelligent Campus Enhancement Program for Romblon State University System (ABC: PhP1,250,000,000.00, QTY: 1 Lot)

ITEM NO.	UNIT	ITEM DESCRIPTION	QTY	Statement of Compliance
1	Lot	**1. Smart Agriculture System** Software that will automate processes for the agriculture research program of Romblon State University. 1.1.1. Components 1.1.1.1. Devices Management & Tracking Module 1.1.1.1.1. Device Templates Module 1.1.1.1.2. Devices Registration Module 1.1.1.1.3. Devices Enrollment Module 1.1.1.1.4. Devices Security (Whitelisting, Certificate Management, User Association) Module 1.1.1.1.5. Devices List / Reports Module (Based on state, property) 1.1.1.1.6. Devices Unenroll Module 1.1.1.2. Metrics Module 1.1.1.2.1. Devices Metrics Definition Module 1.1.1.2.2. Metrics View / Graphs Module 1.1.1.3. Connectivity Management Module 1.1.1.3.1. Devices Connectivity Module 1.1.1.3.2. Sensors / Devices Adapters 1.1.1.4. Updates Management Module 1.1.1.4.1. Secure Packages Creation Module 1.1.1.4.2. Secure Approval based Updates Campaign Management Module 1.1.1.4.3. Updates Campaign Run / Scheduling Management Module 1.1.1.4.4. Updates Campaign Start / Stop / Delete – Stages Management Module 1.1.1.4.5. Updates Campaign Status Monitoring & Reporting Module 1.1.1.4.6. Updates Modules for OS	1	

		1.1.1.4.7. Update Modules for Applications 1.1.1.5. Alerts Management Module 1.1.1.5.1. Alerts Creation / Management by Metrics 1.1.1.5.2. Alerts Creation / Management by Properties 1.1.1.6. Notifications Management Module 1.1.1.6.1. Notification Creation / Management 1.1.1.6.2. Notifications Integrations – 2 End-point REST System 1.1.1.7. Cyber-Security Management Module 1.1.1.7.1. Certificate management for supported devices 1.1.1.7.2. User / password policy management for devices 1.1.1.8. Log Management & Reporting Module 1.1.1.8.1. Uploading of Logs from Edge device to server 1.1.1.8.2. Reporting based on Log events 1.1.1.9. RSU System Management 1.1.1.9.1. Organizations Management Module 1.1.1.9.2. Users Management Module 1.1.1.9.3. Groups Management Module 1.1.1.10. RSU Integrations 1.1.1.10.1. RSU Ticketing System 1.1.1.10.2. SMS 1.1.1.10.3. RSU Email 1.1.1.10.4. Slack / MS Teams 1.1.1.10.5. RSU ERP 1.1.1.11. Data Management & Analytics 1.1.1.11.1. Data Warehouse 1.1.1.11.2. Data Management 1.1.1.11.3. Analytics Dashboards 1.1.1.11.4. Periodic Reports 1.1.1.12. Sensors and Miscellaneous Equipment 1.1.1.12.1. SAP Flow Meter 1.1.1.12.2. Heat Ration Sensor 1.1.1.12.3. Stem Increment Borer		

		1.1.1.12.4. Bark Depth Gauge 1.1.1.12.5. 20W Solar Panel 1.1.1.12.6. Integrated dendrometry monitoring station (includes 1 s-nodes & DBS60) 1.1.1.12.7. Dendrometer stainless steel band tape 1.1.1.12.8. Integrated crop water stress index station 1.1.1.12.9. Soil moisture probe 1.1.1.12.10. Wireless Node for SDI12 analogue and digital sensors 1.1.1.12.11. Integrated mounting system for 10W (SP10) or 20W (SP20) solar panel and wireless node 1.1.1.12.12. 20-Watt solar panel with cable 1.1.1.12.13. All-in-one 5 parameter weather station, SDI12 1.1.1.12.14. Silicon-cell pyranometer – SDI-12 Leaf and Bud Temperature Sensor 1.1.1.12.15. Leaf grid/Bird spikes for PRP-02 1.1.1.12.16. Professional Rain Gauge 1.1.1.12.17. RAK7249 WisGate Edge Prime Gateway LTE AS923 1.1.1.12.18. MP406 Moisture Sensor – Soil Moisture Instant Reading Kit 1.1.1.12.19. Plant Canopy Image 1.1.1.12.20. Handheld Laser Leaf Area Meter 1.1.1.12.21. Handheld Photosynthesis System		

		1.1.1.12.22. Miniature Leaf Spectrometer with integrated Leaf Probe 1.1.1.13. Area of Agriculture and Orchard Farms 1.1.1.13.1. Area #1: approx. 130m x 150m 1.1.1.13.2. Area #2: approx. 300m x 30m 1.1.1.13.3. Area #3 is L-shape, with approx. 450m in length, 150m and 300m in width respectively. 1.1.1.14. Included Services 1.1.1.14.1. Application and Platform Installation 1.1.1.14.2. User workflow integration 1.1.1.14.3. SSL and DNS Configuration 1.1.1.14.4. Network Configuration 1.1.1.14.5. Integration to RSU RDBMS Database 1.1.1.14.6. IOT Sensors Installation and Configuration 1.1.1.14.7. Project Management Services 1.1.1.14.8. User Training 1.1.1.15. Technical Requirements - The proposed solution must support the following features: 1.1.1.16. Smart Agriculture Management Requirement. 1.1.1.16.1. Real time agriculture quality Measurement 1.1.1.16.2. Soil, Humidity and Environmental Quality key metrics Storage for historical analysis 1.1.1.16.3. Smart Connectors to interface with the devices 1.1.1.16.4. Analytics - Data Summarization for identifying trends 1.1.1.16.5. Trend Analysis & Anomaly detection 1.1.1.16.6. Data Ingestion for surface environmental data 1.1.1.16.7. Data export API module from		

		devices and surface environmental data 1.1.1.16.8. Securing the data end-to-end 1.1.1.16.9. Open APIs for authenticated Research and Student Community module 1.1.1.16.10. Tracking module - system metrics of the IoT sensors used 1.1.1.16.11. Reporting 1.1.1.16.12. Mobile Application 1.1.1.16.13. Web Application and Administration Console 1.1.1.17. Smart Orchard Management Requirement - Smart Orchards management should have the following modules: 1.1.1.17.1. Plant Monitoring, Measurement, Analysis & Correlation 1.1.1.17.1.1. Industrial, Orchard grade IoT sensors/devices used to precisely measure Plant Water Relations (SAP flow, Dendrometry), Plant Water potential (Stem, leaf, & root Psychometry), Plant Light Relations (PAR, Controlled Environment, Canopy Conditions), Infrared Bud Temperature, Canopy Temperature, Crop Water Stress Index, Leaf Area, Photosynthesis, etc. 1.1.1.17.1.2. Capability to log the data locally (on the machine) or a storage system or through a connection for data capture and backend processing. 1.1.1.17.1.3. Secure data transmission from devices to the backend systems 1.1.1.17.1.4. Capability to monitor the devices for system health 1.1.1.17.1.5. Authenticate the devices to maintain data integrity		

		1.1.1.17.1.6. Capability to support collection of the data on LoRaWAN/ Cellular protocols supported by the sensors/ devices 1.1.1.17.2. Irrigation 1.1.1.17.2.1. Connected devices/sensors which measure & control water flow, spray, duration, schedules, etc. 1.1.1.17.2.2. Control modules which are connected for remote actions & management 1.1.1.17.2.3. Capability to capture Past & Realtime Irrigation Drainage Data 1.1.1.17.3. Real time Soil, Water & Environment Measurement Module 1.1.1.17.3.1. Industrial, Agriculture grade IoT sensors/devices used to measure precisely the soil, humidity and environmental quality metrics. The metrics would be what's mentioned in the earlier sections. 1.1.1.17.3.2. Capability to log the data locally before being transmitted across the network for backend processing. This is to bring data transmission resiliency and redundancy 1.1.1.17.3.3. Secure data transmission from devices to the backend systems 1.1.1.17.3.4. Capability to monitor the devices for system health 1.1.1.17.3.5. Authenticate the devices to maintain data integrity 1.1.1.17.3.6. Capability to support collection of the data on LoRaWAN/ Cellular protocols supported by the sensors/ devices		

		1.1.1.17.4. Soil, Humidity & Environmental Quality key metrics Storage for historical analysis 1.1.1.17.4.1. Capabilities to store data in a structured format for analytical needs 1.1.1.17.4.2. Built-in support for data storage redundancy 1.1.1.17.4.3. Data archival support 1.1.1.17.4.4. Support to store data for more than 10 years for historical analysis & for research purposes 1.1.1.17.4.5. Data could be retrieved and exported to multiple formats such as csv, tsv, JSON, xml, etc. 1.1.2. Common Platform and Module Requirement 1.1.2.1. Real time Soil & Environment Measurement Module for Smart Agriculture 1.1.2.1.1. Industrial, Agriculture grade IoT sensors/devices used to measure precisely the soil, humidity and environmental quality metrics. The metrics would be what's mentioned in the earlier sections. 1.1.2.1.2. Capability to log the data locally before being transmitted across the network for backend 1.1.2.1.3. Processing. This is to bring data transmission resiliency and redundancy 1.1.2.1.4. Secure data transmission from devices to the backend systems 1.1.2.1.5. Capability to monitor the devices for system health 1.1.2.1.6. Authenticate the devices to maintain data integrity 1.1.2.1.7. Capability to support collection of the data on LoRaWAN/ Cellular protocols supported by the sensors/ devices		

		1.1.2.2. Soil, Humidity & Environmental Quality key metrics Storage for historical analysis 1.1.2.2.1. Capabilities to store data in a structured format for analytical needs 1.1.2.2.2. Built-in support for data storage redundancy 1.1.2.2.3. Data archival support 1.1.2.2.4. Support to store data for more than 10 years for historical analysis & for research purposes 1.1.2.2.5. Data could be retrieved and exported to multiple formats such as csv, tsv, JSON, xml, etc. 1.1.2.3. Real time Water quality Measurement Module 1.1.2.3.1. Industrial, aquaculture grade IoT sensors/devices used to measure precisely the water quality metrics. The metrics would be what's mentioned in the earlier sections. 1.1.2.3.2. Capability to log the data locally before being transmitted across the network for backend processing. This is to bring data transmission resiliency and redundancy 1.1.2.3.3. Secure data transmission from devices to the backend systems 1.1.2.3.4. Capability to monitor the devices for system health 1.1.2.3.5. Authenticate the devices to maintain data integrity 1.1.2.3.6. Capability to support collection of the data on LoRaWAN/ Cellular protocols supported by the sensors/ devices 1.1.2.4. Water Quality key metrics Storage for historical analysis 1.1.2.4.1. Capabilities to store data in a structured format for analytical needs		

		1.1.2.4.2. Built-in support for data storage redundancy 1.1.2.4.3. Data archival support 1.1.2.4.4. Support to store data for more than 10 years for historical analysis & for research purposes 1.1.2.4.5. Data could be retrieved and exported to multiple formats such as csv, tsv, JSON, xml, etc. 1.1.2.5. Video capture 1.1.2.5.1. Cameras are used as the eyes for AI / Machine Vision projects as well as live human and recorded observations 1.1.2.5.2. Underwater cameras powered on a 12-volt power supply and is ideal for remote applications in conjunction with a battery and solar panel 1.1.2.5.3. The camera could capture real-time video, which will be stored on a hard disk. The system was designed to be used for a long period of time up to three months continuously without maintenance. 1.1.2.5.4. It's used to monitor changes in fish abundance with respect to time of day and among months. The present results thus showed two major behavioral patterns of fish 1.1.2.5.5. The primary camera that has been adapted for this use is the SAIS IP HD CAM. The mechanical design has been refined to make it robust and corrosion proof. The cables that we use have been refined and redesigned over many years to be robust and reliable. 1.1.2.5.6. The content from the camera is captured through ONVIF and IP based protocols 1.1.2.6. Video/ Image Storage 1.1.2.6.1. Devices have capability to stream		

		the data to Recorders using dedicated radio transceivers or cellular provided network 1.1.2.6.2. Data is compressed and secured with encryption 1.1.2.6.3. Archival capabilities for older content provided 1.1.2.7. Smart Connectors to interface with the devices 1.1.2.7.1. Connectivity to sensors/ devices and assets at the Edge via purpose-built adaptors. 1.1.2.7.2. Support both agent-based & agent-less ways of onboarding, collecting data, sending commands and OTA updates (for applicable devices) 1.1.2.8. Image Classification - Computer Vision Modules 1.1.2.8.1. Fish detection 1.1.2.8.2. Behavior detection 1.1.2.8.3. Identifying and clustering frames which have the relevant information about the fishes used for disease detection analysis 1.1.2.9. Reports with classified Images 1.1.2.9.1. Ability to measure multiple dimensions and time series data. 1.1.2.9.2. Capability to address the key areas to consider when summarizing a set of readings from the sensors/devices 1.1.2.9.3. Centrality – the middle value or average. 1.1.2.9.4. Dispersion – how spread out the values are from the average. 1.1.2.9.5. Replication – how many values there are in the sample. 1.1.2.9.6. Shape – the data distribution, which relates to how “evenly” the		

		values are spread either side of the average. 1.1.2.9.7. The solution should support multiple use cases of visualization software including reporting, interactive analysis and business intelligence. 1.1.2.10. Anomaly detection for aqua organisms using machine learning modules 1.1.2.10.1. Ability to determine baseline signals. Ability to statistically model the characteristics of normalcy 1.1.2.10.2. System has ability to ingest internal or external data signals or features for the ML models 1.1.2.10.3. To track gradual drift, cyclical rhythms such as seasonality, and abrupt phase changes. 1.1.2.10.4. Make this data available for University's researchers to use normalcy models to make predictions, describe expectations about future events, and accurately estimate the probability that new or past observations are anomalous. 1.1.2.10.5. The platform monitors millions of time series data and identifies drifts from baseline and suspicious trends. 1.1.2.10.6. Platform's ML models to detect notable changes from normal behavior after accounting for typical change patterns, volatility, and seasonal trends triggering alerts and notifications to the users 1.1.2.11. Smart Connectors to interface with the devices 1.1.2.11.1. Connectivity to sensors/ devices and assets at the Edge via purpose-built adaptors. 1.1.2.11.2. Support both agent-based & agent-less ways of onboarding, collecting		

		data, sending commands and OTA updates (for applicable devices) 1.1.2.12. Analytics - Data Summarization for identifying trends 1.1.2.12.1. The product must provide native functionality to store XML, JSON within the database and support search, query functionalities 1.1.2.12.2. The product must support provide both Row-Store and Column-Store (columnar) in the same table 1.1.2.12.3. The product must provide federated query options from multiple sources. 1.1.2.12.4. The product must support machine learning, text/graph/geo-spatial analytics out of box. 1.1.2.12.5. The product must support GPU's. 1.1.2.12.6. The product must support real-time event processing/streaming. 1.1.2.12.7. The product must support data backups locally, on external systems (such as S3 file system) 1.1.2.13. Trend Analysis & Anomaly detection 1.1.2.13.1. Ability to determine baseline signals. Ability to statistically model the characteristics of normalcy 1.1.2.13.2. System has ability to ingest internal or external data signals or features for the ML models 1.1.2.13.3. To track gradual drift, cyclical rhythms such as seasonality, and abrupt phase changes. 1.1.2.13.4. Make this data available for University's researchers to use normalcy models to make predictions, describe expectations about future events, and accurately estimate the probability that new or past observations are anomalous.		

		1.1.2.13.5. The platform monitors millions of time series data and identifies drifts from baseline and suspicious trends. 1.1.2.13.6. Platform's ML models to detect notable changes from normal behavior after accounting for typical change patterns, volatility, and seasonal trends triggering alerts and notifications to the users 1.1.2.14. Data Ingestion for surface environmental data 1.1.2.14.1. This module provides ability to ingest external data sources such as weather APIs 1.1.2.14.2. The smart connectors would be used to connect to these sources either through RESTful APIs or MQTT protocols 1.1.2.15. Data export API module from devices and surface environmental data 1.1.2.15.1. Data export capabilities to enable running co-relation & ML models/algorithms with real-time sensor and Environmental data 1.1.2.15.2. Enabling the IoT data as Tensorflow dataset format supported for ingestion into multiple ML frameworks 1.1.2.15.3. Supported ML frameworks for the data format compatible with PyTorch, Tensorflow, Numpy or Pandas libraries 1.1.2.16. Securing this data 1.1.2.16.1. End-to-end encryption to protect data streaming between devices, applications 1.1.2.16.2. Token-based access control, which grants access to specific data channels to the relevant devices instead of overwhelming all of the end devices with every signal – this also eliminates the inefficiency and insecurity of asking all end devices to just filter out irrelevant topics		

		1.1.2.16.3. Device status monitoring so for alerts whenever a sensor or device disappears or stops 1.1.2.16.4. Sending or receiving data, which could mean tampering, an outage or another issue 1.1.2.16.5. User-friendly setup and upgrades so it's simple and quick to keep all devices up to date on software and firmware 1.1.2.17. Open APIs for authenticated Research and Student Community module 1.1.2.17.1. The Platform API offers a way for Students and Researchers to interact with the Platform and leverage the rich real-time data from the devices and various systems which are integrated. 1.1.2.17.2. These are programmable REST APIs to integrate with your existing research applications and tools. 1.1.2.17.3. The APIs, enable teams to create, view, edit, and build ML models using various 1.1.2.17.4. Platform entities such as Devices, Campaigns, Alerts, Notifications, Groups, and Users, programmatically. 1.1.2.18. Tracking module - system metrics of the IoT sensors used 1.1.2.18.1. Platform offers out-of-box discoverability and visibility to all devices in your edge environment with zero disruption to your operations. 1.1.2.18.2. AI allows analysis & categorization of devices, properties, settings and vulnerabilities, across diverse protocols, thereby helping you gain a comprehensive understanding of your IT/OT network topology 1.1.2.18.3. Enables entire lifecycle -		

		Discover, Plan, Onboard, Configure, Monitor, Manage, Secure & End of Life of Devices and Sensors. 1.1.2.18.4. Provides capabilities like advanced authentication, onboarding, preconfigured templates, campaigns, AI-alerts, workflows, adapters, Identity & Access management, security management. 1.1.2.19. Analytics & Dashboards and Reporting 1.1.2.19.1. Ability to measure multiple dimensions and time series data. 1.1.2.19.2. Capability to address the key areas to consider when summarizing a set of readings from the sensors/devices 1.1.2.19.3. Centrality – the middle value or average. 1.1.2.19.4. Dispersion – how spread out the values are from the average. 1.1.2.19.5. Replication – how many values there are in the sample. 1.1.2.19.6. Shape – the data distribution, which relates to how "evenly" the values are spread either side of the average. 1.1.2.19.7. The solution should support multiple use cases of visualization software including reporting, interactive analysis and business intelligence. 1.1.2.20. Design Storage and Reusability 1.1.2.20.1. The solution should enable the design and content of a table or graph (the query and the visualization) to be stored once and re-used for multiple purposes, for example when users want to see it from different perspectives like month, year, customer, product et cetera. The reusability is within the tool or the reusables can be used		

		across BI applications 1.1.2.21. Authentication 1.1.2.21.1. The solution should support different ways of authentication - native, database, windows, LDAP etc. 1.1.2.22. Role-Based Reporting 1.1.2.22.1. The solution should support the concept of role-based reporting, dash boarding and analysis. For example, when a user logged on, he sees only the information (portlets, graphs, tables, gauges, data) he is authorized for 1.1.2.23. Sharing and collaboration 1.1.2.23.1. The solution should contain drill-down ways that users can share analysis and collaborate on the same visual interface. 1.1.2.24. SQL Support 1.1.2.24.1. The solution should support SQL SELECT supported Is the full syntax of the SELECT statement supported (for example inner joins, outer joins, unions, sub queries, group by) and execute in an in memory or in-database fashion 1.1.2.25. Analytics Engine 1.1.2.25.1. The solution should come with an embedded enterprise grade analytics engine. 1.1.2.26. Standard expressions 1.1.2.26.1. The solution should support calculation and math expressions on the fly 1.1.2.27. Machine Learning 1.1.2.27.1. The solution should have out of the box support for various ML algorithms such as clustering and		

		regression 1.1.2.28. Real-time streaming support 1.1.2.28.1. The solution should include real-time message visualization. 1.1.2.29. Mobile Application 1.1.2.29.1. Get soil, humidity and environmental quality data, accessible at a finger's touch 1.1.2.29.2. Easily view the status of your tanks with color-coded icons 1.1.2.29.3. Alerts or alarms can be sent via email, text and notifications to ensure you are alerted when alarm conditions are met 1.1.2.29.4. Data is saved on a remote server at a configurable frequency, providing backup of historical information that is easily accessible 1.1.2.29.5. Easily view historical data 1.1.2.29.6. Greater flexibility to display data with responsive pages that adapt to the size of your screen (mobile-friendly) 1.1.2.29.7. Easy to use with simple menu structure 1.1.2.30. Common Web Application and Administration Console 1.1.2.30.1. The common platform should have the Devices Management & Tracking, Metrics, Connectivity 1.1.2.30.2. Management, OTA Updates Management, Alerts Management, Notifications Management, Cyber- Security Management, Log Management & Reporting, System Management, Integrations, Data Management & Analytics, Users, Groups and Organization Management 1.1.2.30.3. Onboarding, enrollment of existing and new devices in an		

		easy and secure mode 1.1.2.30.4. Management of devices in groups or clusters through device templates or defined query set 1.1.2.30.5. Management and Collection of metrics from devices, show aggregate and node data in different dashboards for OT and IT stakeholders (including management, teachers, researchers, students and commercial partners) 1.1.2.30.6. Management of metrics for different org / by groups 1.1.2.30.7. Inventory of devices, including firmware, properties (settable by customers or pre-defined) 1.1.2.30.8. Management and updates of such firmware and properties 1.1.2.30.9. Setting up threshold-based alerts, notifications for users internal and external users 1.1.2.30.10. Location setting and advanced location definitions on GUI for different devices 1.1.2.30.11. Security in terms of monitoring devices for configuration, settings changes, and alerts. 1.1.2.30.12. Troubleshooting and log management for service providers 1.1.2.30.13. Rich data analytics, reports and AI/ML for analyzing captured data and images. 1.1.2.30.14. Flexible organizations setup including RBAC, users, groups and device templates under each of org / groups 1.1.3. Supply of Drone for Smart Agriculture application, compliant with the following minimum requirements: 1.1.3.1. 90 kg maximum takeoff weight for spraying (at sea level)		

		1.1.3.2. 101 kg maximum takeoff weight for spreading (at sea level) 1.1.3.3. Hovering Accuracy Range: 1.1.3.3.1. Real-time Kinetic Positioning (RTK) enabled: ±10 cm horizontal, ±10 cm vertical 1.1.3.3.2. Real-time Kinetic Positioning (RTK) disabled: ±60 cm horizontal and ±30 cm vertical (radar enabled: ±10 cm) 1.1.3.4. Hovering Time: 1.1.3.4.1. Hovering without payload: 18 min (@30000 mAh & takeoff weight 50 kg) 1.1.3.4.2. Hovering and spraying with full payload: 7 min (@30000 mAh & takeoff weight 90 kg) 1.1.3.4.3. Hovering and spreading with full payload: 6 min (@30000 mAh & takeoff weight 101 kg) 1.1.3.5. Motor KV value of at least 48/RPM/ V 1.1.3.6. Motor power of at least 4000W/ rotor 1.1.3.7. Rotor quantity of at least eight (8) 1.1.3.8. Must be equipped with Dual Atomized Spraying System 1.1.3.8.1. with Operation Box: Capacity of 40 L (Full load) 1.1.3.8.2. Sprinkler Quantity: 2 1.1.3.8.3. with Magnetic Drive Impeller Pump 1.1.3.9. Must include an Intelligent Remote Controller compliant with the following, at a minimum: 1.1.3.9.1. Operating frequency of 2.4000 to 2.4835 GHz and 5.725 to 5.850 GHz 1.1.3.9.2. Signal Effective Distance of at least 4 kms 1.1.3.9.3. WIFI 6 WiFi Protocol		

		1.1.3.9.4. WiFi Operating frequencies: 2.4000 to 2.4835 GHz; 5.150 to 5.250 GHz; 5.725 to 5.850 GHz 1.1.3.9.5. Equipped with Bluetooth 5.1. Bluetooth protocol 1.1.3.9.6. Bluetooth Operating Frequency of 2.4000-2.4835 GHz 1.1.3.9.7. Display screen of at least 7-inches touch LCD 1.1.3.9.8. Internal battery life of at least 3 hours 1.1.3.9.9. External battery life of at least 2.5 hours 1.1.4. Supply of drone for Immersive Site Survey applications, compliant with the following minimum requirements: 1.1.4.1. Equipped with Normalized Difference Vegetation Index (NDVI) imaging that indicates plant health 1.1.4.2. Able to monitor field conditions and soil health 1.1.4.3. Flight time duration of approximately 41 minutes on a single battery charge 1.1.4.4. Dual max ascent speed mode with 6ms and 8 ms respectively 1.1.4.5. Dual max descent speed mode with 6ms and 6 ms respectively 1.1.4.6. Triple max speed with 75 kph, 72 kph and 68kph respectively 1.1.4.7. Omnidirectional vision system 1.1.4.8. Vision altitude range of at least 0-30m 1.1.4.9. Equipped with Infrared Sensing System 1.1.4.10. Effective camera pixel of at least 20MP 1.1.4.11. Maximum video bit rate of 4K: 130Mbps, FHD: 70Mbps 1.1.4.12. Supported File System: exFAT 1.1.4.13. Support photos in JPEG, DNG (raw) and		

		JPEG+DNG format 1.1.4.14. Supports videos in MP4 (MPEG-4 AVC/H.264) format 1.1.4.15. Must support microSD Cards 1.1.4.16. Must have Mini HDMI port 1.1.5. Maritime Drone 1.1.5.1. The drone system aims to help the university's push for innovation and applied technology for the advancement of its aquaculture and maritime research. 1.1.5.2. The use cases include fish density mapping, coral and sea-life inventory, shipwreck and diving spots exploration, rivers and lakes vegetation mapping, fishponds health check, mining-pit surveying, among others. 1.1.5.3. Supply of one (1) a luggable, autonomous drone boat for search and mapping with side-scan sonar and drop camera. 1.1.5.4. The autonomous drone boat should have the minimum specifications: 1.1.5.4.1. Front camera 1.1.5.4.2. Wi-Fi antenna that communicates with its base station 1.1.5.4.3. Underwater camera 1.1.5.4.4. 2x electric brushed on-board motors 1.1.5.4.5. Side-scan sonar sensor 1.1.5.4.6. Base station 1.1.5.4.7. Battery capacity of 40Ah, 12V 1.1.5.4.8. Operating speed of 4km/h 1.1.5.4.9. Switch to autonomous and manual drive modes 1.1.5.4.10. Data link range of 200m to base station 1.1.5.4.11. Directional antenna with automatic tracking system 1.1.5.5. The drone software should have at least the following features: 1.1.5.5.1. Define target area on the map for autonomous driving mode. 1.1.5.5.2. Playback captured camera video, sonar display, and side-scan down-scan sonar data. 1.1.5.5.3. Click anywhere on the drone route to see the data captured at that position.		

1.1.5.5.4. Measure location, water depth and distances on the map
1.1.5.5.5. Inspect point of interest with the drop camera
1.1.5.5.6. Export 3D-model of the scanned area

1.2. Animation Laboratory

The Animation laboratory shall be a dedicated facility equipped with tools, software, and resources for animators to develop and produce animated contents. In this facility, animators are able to explore various aspects of animation including character design, storyboarding, 2D or 3D animation techniques, special effects, and post-production editing.

1.2.1. Participating bidder must provide the following:

1.2.1.1. Perform fit out works for the existing facility designated by RSU as its Animation laboratory. It must include the following at a minimum:

1.2.1.1.1. Secured Door with Door Access System

1.2.1.1.2. Wall, floor and ceiling finishes

1.2.1.1.3. Provision of Cooling Equipment

1.2.1.1.4. Electrical Works

1.2.1.1.5. Provision of Network Nodes

1.2.1.2. Supply and installation of the following hardware:

1.2.1.2.1. Desktop computers with furnishing

1.2.1.2.2. Interactive Boards

1.2.1.2.3. Access Point (AP)

1.2.1.2.4. CCTV Camera

1.2.1.2.5. Three (3) streaming servers with the following minimum specifications or equivalent:

- Single Socket P (LGA 3647)
- Radeon RTX 5000 has 16GB
- 1U Rackmount
- PCI-E Gen 3 x16 Switch CPU-GPU Interconnect

		• 128 GB RAM • 1TB SSD • 2- RJ45 10GBase-T ports • 1- RJ45 Dedicated IPMI LAN port 1.2.1.2.6. Three (3) streaming servers with the following minimum specifications or equivalent: • Single Socket E (LGA-4677) • 1U Rackmount • 32 GB RAM • 1TB SSD • 2 RJ45 10GBase-T ports • 1 RJ45 Dedicated IPMI LAN port 1.2.1.3. Supply and installation of Animation Software: 1.2.1.3.1. 2D Animation Software to create two-dimensional animations. 1.2.1.3.2. 3D Animation Software to create three-dimensional animations 1.2.1.3.3. Motion Graphics Software to create animated graphics and visual effects for videos, presentations, and other multimedia projects. 1.2.1.3.4. Web Animation Software for creating animations that can be displayed on websites and web applications. 1.2.1.3.5. Streaming platform to deliver immersive 2D and 3D content on the internet using thin clients such as PC, tablet, and mobile phones. (3-year license) 1.2.1.3.6. Training of Unity3D Software for 2D and 3D content creation 1.2.1.3.7. Ten (10)-day on-site and online training on the use Unity3D for thirty (30) select students participating in the program **1.3. E-Classroom** Retrofitting traditional classrooms to a digitally enhanced facility that will allow learners to access course contents online, deliver lectures remotely and host productivity tools		

		among others. 1.3.1. **Fit out works** 1.3.1.1. Lighting works 1.3.1.2. Wall finishing 1.3.1.3. Ceiling works 1.3.1.4. Cooling and Ventilation 1.3.1.5. Electrical works 1.3.1.6. 2 units of Dome Camera, 4MP or higher MP 1.3.1.7. Supply of Access Point for Wi-Fi access 1.3.1.8. Provision of furnishing 1.3.2. **Supply of Interactive Boards** The interactive board should be able to deliver the minimum following features and specifications listed. 1.3.2.1. Display 1.3.2.1.1. Must have at least Diagonal Size - 65" 1.3.2.1.2. Must have at least Resolution 3,840 x 2,160 1.3.2.1.3. Must have typical brightness of 350 cd/m (220cd/m with glass) 1.3.2.1.4. Should have viewing angle (H/V) of 178/178 degree 1.3.2.1.5. Should have at least Color Gamut 72% 1.3.2.1.6. Able to have H-Scanning Frequency of 30~81 kHz 1.3.2.1.7. Able to have V-Scanning Frequency of 48~75 Hz 1.3.2.1.8. Must be panel type of New Edge, 60 Hz 1.3.2.1.9. Should have Pixel Pitch (HxV) 0.372 x 0.372 mm 1.3.2.1.10. Be able to have contrast ratio 4,000:1 1.3.2.1.11. Should have response time of 8 ms 1.3.2.1.12. Glass Haze of 2% (without		

		glass) 1.3.2.1.13. Maximum pixel frequency of 594 MHz 1.3.2.2. Connectivity 1.3.2.2.1. HDMI in 2 1.3.2.2.2. Audio Output (Stereo Mini Jack) 1.3.2.2.3. RJ45 In 1.3.2.2.4. Bluetooth 1.3.2.2.5. USB 1.3.2.2.6. RS232 In 1.3.2.2.7. Wi-Fi 1.3.2.3. Power 1.3.2.3.1. Power Supply (AC 100~240 V 50/60 Hz 1.3.2.3.2. Power Consumption (Sleep Mode) 0.5 W 1.3.2.3.3. Power Consumption (on Mode) 181.5 W 1.3.2.4. Dimension 1.3.2.4.1. Set dimension (WxHxD) 1522.4 x 897.6 x 62.9 mm 1.3.2.4.2. Package dimension (WxHxD) 1691 x 1055 x 198 mm 1.3.2.5. Mechanical Specification 1.3.2.5.1. VESA Mount (400 x 400 mm) 1.3.2.5.2. Bezel Width (26.2 mm) 1.3.2.6. Operation Conditions 1.3.2.6.1. Touch screen display (InGlass) 1.3.2.6.2. Mount (WMN-WM65R) 1.3.3. **Computer Hardware supply** 1.3.3.1. **Desktop Computer** 1.3.3.1.1. CPU Intel i7-12700 2.1 Ghz (25MB cache, up to 4.9 GHz, 12 cores) 1.3.3.1.2. Intel B660 Chipset 1.3.3.1.3. 4GB Discrete GPU 1.3.3.1.4. With UHD Graphics 1.3.3.1.5. Memory 16GB DDR4 U-DIMM		

		(4xDIMM Slot, Dual Channel DDR4 3200 MHz up to 128GB) 1.3.3.1.6. Serial ATA (4xSerial ATA 6.0 Gb/s 1.3.3.1.7. Storage 1TB SSD 1.3.3.1.8. Wireless discrete Wi-Fi, Antenna Type; External 1.3.3.1.9. Rear I/O Port 1.3.3.1.9.1. 1x RJ45 Gigabit Ethernet 1.3.3.1.9.2. 1x HDMI 1.4 1.3.3.1.9.3. 1x VGA Port 1.3.3.1.9.4. 2x DisplayPort 1.2 1.3.3.1.9.5. 1x 7.1 Channel audio (3 port) 1.3.3.1.9.6. 2x PS2 1.3.3.1.9.7. 3x Audio jacks 1.3.3.1.9.8. 4x USB 2.0 Type-A 1.3.3.1.10. Front I/O Port 1.3.3.1.10.1. 1x Headphone 1.3.3.1.10.2. 1x 3.5mm combo audio jack 1.3.3.1.10.3. 2x USB 2.0 Type-A 1.3.3.1.10.4. 1x USB 3.2 Gen 2 Type-C 1.3.3.1.10.5. 2x USB 3.2 Gen 1 Type-A 1.3.3.1.10.6. 2x USB 3.2 Gen 2 Type-A 1.3.3.1.11. Expansion Slot 1.3.3.1.11.1. 1x PCIe 4.0 x 16 1.3.3.1.11.2. 2x PCIe 3.0 x 1 1.3.3.1.11.3. 1x M.2 connector for Wi-Fi 1.3.3.1.11.4. 2x M.2 connector for storage 1.3.3.1.11.5. 4x DDR4 U-DIMM slot 1.3.3.1.12. Power Supply 1.3.3.1.12.1. 500W power supply 1.3.3.1.13. Keyboard & Mouse 1.3.3.1.13.1. Wired Keyboard (USB)		

1.3.3.1.13.2. Wired Optical mouse (USB)

1.3.3.1.14. Monitor 23.8-inch Full HD

1.4. General Purpose E-Laboratory

This facility intends to provide the learners with appropriate digital tools that will further expand the learning capabilities of the students. At a minimum, it must be equipped with the following:

1.4.1. **Fit out works**

1.4.1.1. Led lightings
1.4.1.2. Renovation of walls, ceiling, and floorings
1.4.1.3. Cooling system
1.4.1.4. 2 units of Dome Camera, 4MP or higher MP
1.4.1.5. Supply of Access Point for Wi-Fi access
1.4.1.6. Provision of furnishing

1.4.2. **Computer Hardware supply**

1.4.2.1. **Desktop Computer**

1.4.2.1.1. CPU Intel i7-12700 2.1 Ghz (25MB cache, up to 4.9 GHz, 12 cores)
1.4.2.1.2. Intel B660 Chipset
1.4.2.1.3. 4GB Discrete GPU
1.4.2.1.4. With UHD Graphics
1.4.2.1.5. Memory 16GB DDR4 U-DIMM (4xDIMM Slot, Dual Channel DDR4 3200 MHz up to 128GB)
1.4.2.1.6. Serial ATA (4xSerial ATA 6.0 Gb/s
1.4.2.1.7. Storage 1TB SSD
1.4.2.1.8. Wireless discrete Wi-Fi Card, Antenna Type; External
1.4.2.1.9. Rear I/O Port

1.4.2.1.9.1. 1x RJ45 Gigabit Ethernet
1.4.2.1.9.2. 1x HDMI 1.4
1.4.2.1.9.3. 1x VGA Port
1.4.2.1.9.4. 2x DisplayPort 1.2
1.4.2.1.9.5. 1x 7.1 Channel audio (3 port)
1.4.2.1.9.6. 2x PS2
1.4.2.1.9.7. 3x Audio jacks
1.4.2.1.9.8. 4x USB 2.0 Type-A

1.4.2.1.10. Front I/O Port

		1.4.2.1.10.1. 1x Headphone 1.4.2.1.10.2. 1x 3.5mm combo audio jack 1.4.2.1.10.3. 2x USB 2.0 Type-A 1.4.2.1.10.4. 1x USB 3.2 Gen 2 Type-C 1.4.2.1.10.5. 2x USB 3.2 Gen 1 Type-A 1.4.2.1.10.6. 2x USB 3.2 Gen 2 Type-A 1.4.2.1.11. Expansion Slot 1.4.2.1.11.1. 1x PCIe 4.0 x 16 1.4.2.1.11.2. 2x PCIe 3.0 x 1 1.4.2.1.11.3. 1x M.2 connector for Wi-Fi 1.4.2.1.11.4. 2x M.2 connector for storage 1.4.2.1.11.5. 4x DDR4 U-DIMM slot 1.4.2.1.12. Power Supply 1.4.2.1.12.1. 500W power supply) 1.4.2.1.13. Keyboard & Mouse 1.4.2.1.13.1. Wired Keyboard (USB) 1.4.2.1.13.2. Wired Optical mouse (USB) 1.4.2.1.14. Monitor 23.8-inch Full HD **1.5. Robotics** 1.5.1. Supply and delivery of three (3) robots which can be configured to carry light-weight materials like books, magazines, light-tools, and the like. 1.5.2. The robot should be LIDAR-equipped (or equivalent technology) and programmable. 1.5.3. Supply of custom application that runs on Android at least, or any other smartphone. 1.5.4. Supply of three (3) Android tablets for the custom application. 1.5.5. Provide a development kit (SDK) for students and professors to be used in developing new applications for the robot. **1.6. E-Library** This will serve as the main online research facility for the students for them to access their digital textbooks and other online references. 1.6.1. **Fit out works**		

		1.6.1.1. Led lightings 1.6.1.2. Renovation of walls, ceiling, and floorings 1.6.1.3. Cooling system 1.6.1.4. 2 units of Dome Camera, 4MP or higher MP 1.6.1.5. Supply of Access Point for Wi-Fi access 1.6.1.6. Provision of furnishing 1.6.2. **Desktop Computer** 1.6.2.1. CPU Intel i5-12400 2.6 Ghz (18MB cache, up to 4.4 GHz, 6 cores) 1.6.2.2. Intel B660 Chipset 1.6.2.3. Mini Tower 1.6.2.4. With UHD Graphics 1.6.2.5. Memory 8GB DDR4 U-DIMM (4xDIMM Slot, Dual Channel DDR4 3200 MHz up to 128GB) 1.6.2.6. Serial ATA (4xSerial ATA 6.0 Gb/s 1.6.2.7. Storage 512GB SSD. 1.6.2.8. Wireless discrete Wi-Fi Card, Antenna Type; External 1.6.2.9. Rear I/O Port 1.6.2.9.1. 1x RJ45 Gigabit Ethernet 1.6.2.9.2. 1x HDMI 1.4 1.6.2.9.3. 1x VGA Port 1.6.2.9.4. 2x DisplayPort 1.2 1.6.2.9.5. 1x 7.1 Channel audio (3 port) 1.6.2.9.6. 2x PS2 1.6.2.9.7. 3x Audio jacks 1.6.2.9.8. 4x USB 2.0 Type-A 1.6.2.10. Front I/O Port 1.6.2.10.1. 1x Headphone 1.6.2.10.2. 1x 3.5mm combo audio jack 1.6.2.10.3. 2x USB 2.0 Type-A 1.6.2.10.4. 1x USB 3.2 Gen 2 Type-C 1.6.2.10.5. 2x USB 3.2 Gen 1 Type-A 1.6.2.10.6. 2x USB 3.2 Gen 2 Type-A 1.6.2.11. Expansion Slot 1.6.2.11.1. 1x PCIe 4.0 x 16 1.6.2.11.2. 2x PCIe 3.0 x 1 1.6.2.11.3. 1x M.2 connector for Wi-Fi 1.6.2.11.4. 2x M.2 connector for storage 1.6.2.11.5. 4x DDR4 U-DIMM slot 1.6.2.12. Power Supply 1.6.2.12.1. 500W power supply		

		1.6.2.13. Keyboard & Mouse 1.6.2.13.1. Wired Keyboard (USB) 1.6.2.13.2. Wired Optical mouse (USB) 1.6.2.13.3. Monitor 23.8-inch Full HD **1.7. E-Library System** The proposed system must run in a unified, multi-cloud microservices platform. 1.7.1. Must have the capability to manage and store the database of the members 1.7.2. Books must be issued with bar codes that contain the book's title, author, subject, and publication date. 1.7.3. Catalogue of books, journals and library databases must be accessible online. 1.7.4. Must have self-check-in and self-check-out books, and the members of digital libraries can log in, search for, choose, issue, and return books on their own 1.7.5. Must have Dashboard for the librarians to maintain each member's account and collect membership payments 1.7.6. The system must be capable of assessing and calculating penalties for late returns. 1.7.7. The system must enable the library staff to manage the inventory of library resources, including tracking the location and availability of resources. 1.7.8. The system must provide statistical reports and analysis of library usage and resources. The reports will include information such as the number of resources borrowed, the most popular resources, and the patron demographics. 1.7.9. The system must provide the librarian the information what books are out, due for return and returned. 1.7.10. Must provide a seamless process of any book's whereabouts at any given time. 1.7.11. Must have analytics to show, but not limited to, frequently borrowed or delayed return books, users with good standing/bad standing, frequently not available, popular authors and topics. 1.7.12. Can be accessible through mobile apps for reservation, borrowing, scanning or searching for books. Mobile apps must also provide the capability to complain or make reports. 1.7.13. Must be open source, web-based applications with API to connect to a compatible Campus Management System. 1.7.14. Must support open-source databases such as Postgres 1.7.15. Must include the provision of Four (4) units of barcode printers, Four (4) handheld scanners and consumables		

1.8. Command and Control Center Equipment Requirements

1.8.1. **Desktop Computer**

1.8.1.1. CPU Intel i5-12400 2.6 Ghz (18MB cache, up to 4.4 GHz, 6 cores)
1.8.1.2. Intel B660 Chipset
1.8.1.3. Mini Tower
1.8.1.4. With UHD Graphics
1.8.1.5. Memory 8GB DDR4 U-DIMM (4xDIMM Slot, Dual Channel DDR4 3200 MHz up to 128GB)
1.8.1.6. Serial ATA (4xSerial ATA 6.0 Gb/s)
1.8.1.7. Storage 512GB SSD
1.8.1.8. Wireless discrete Wi-Fi Card, Antenna Type; External
1.8.1.9. Rear I/O Port

1.8.1.9.1. 1x RJ45 Gigabit Ethernet
1.8.1.9.2. 1x HDMI 1.4
1.8.1.9.3. 1x VGA Port
1.8.1.9.4. 2x DisplayPort 1.2
1.8.1.9.5. 1x 7.1 Channel audio (3 port)
1.8.1.9.6. 2x PS2
1.8.1.9.7. 3x Audio jacks
1.8.1.9.8. 4x USB 2.0 Type-A

1.8.1.10. Front I/O Port

1.8.1.10.1. 1x Headphone
1.8.1.10.2. 1x 3.5mm combo audio jack
1.8.1.10.3. 2x USB 2.0 Type-A
1.8.1.10.4. 1x USB 3.2 Gen 2 Type-C
1.8.1.10.5. 2x USB 3.2 Gen 1 Type-A
1.8.1.10.6. 2x USB 3.2 Gen 2 Type-A

1.8.1.11. Expansion Slot

1.8.1.11.1. 1x PCIe 4.0 x 16
1.8.1.11.2. 2x PCIe 3.0 x 1
1.8.1.11.3. 1x M.2 connector for Wi-Fi
1.8.1.11.4. 2x M.2 connector for storage
1.8.1.11.5. 4x DDR4 U-DIMM slot

1.8.1.12. Power Supply

1.8.1.12.1. 300W power supply (80+ Platinum, peak

		390W) 1.8.1.13. Keyboard & Mouse 1.8.1.13.1. Wired Keyboard (USB) 1.8.1.13.2. Wired Optical mouse (USB) 1.8.1.14. Monitor 23.8-inch Full HD 1.8.2. **Security Surveillance System** 1.8.2.1. TCP/IP Based CCTV Cameras 1.8.2.2. Should support 12-24 VDC or 24 VAC 1.8.2.3. Should support 1920 x 1080 Resolution 1.8.2.4. Should support 25/30/50/60 fps 1.8.2.5. Should support Night Vision/IR for at least 50m 1.8.2.6. Should be at IP67 Ingress protection 1.8.3. **CCTV System must consist of the following:** 1.8.3.1. Dome Camera, 4MP or higher MP 1.8.3.2. Bullet Camera, 4MP or higher MP 1.8.3.3. Network Video Recorder (NVR) with the right-sized storage 1.8.3.4. CCTV software and analytics 1.8.4. Provision of furnishings and other fixtures necessary for a Command Center 1.8.5. Provision of 55" Display Monitor (Video Wall 3 x 2 Setup) **1.9. Retrofitting and Site Development Works** 1.9.1. Must perform Stone Masonry for Slide slope Protection 1.9.2. Able to execute Road Improvement Works 1.9.3. Shall perform Excavation and provide Cemented Concrete Pavement, as well as perform Drainage Concrete Works. 1.9.4. Shall do Painting works. 1.9.5. Shall perform Steel and Glass window works. 1.9.6. Shall provide Sliding Window, Steel bar for Buffer, and Fire Exit Staircase for the safe escape in case of emergency. 1.9.7. Shall perform Power House Works to ensure power is generated safely and relayed from power stations and substations. 1.9.8. Shall perform Structural Concrete, Masonry, Plastering, and provide Door and Window. 1.9.9. Electrical Works for connecting electricity supply wiring to electrical equipment. 1.9.10. Supply and installation of Generator Set, Transformer, Transmission Line, Electrical panel board, and Electrical wirings. 1.9.11. Shall perform Landscaping works		

1.10. Micro Data Center Facility

Must be a modular and portable datacenter solution. Enclosure must be equivalent to a compact data center enclosure to house the data center racking system.

1.10.1. Master Rack (600mm x 1100mm x 200)
1.10.2. Metered PDU half rack (1250mm), 200/240v, 32A, (24)C13, (4)C19
1.10.3. EMS 2000 Gateway
1.10.4. EMS 1000 Sensor Temp & Hum
1.10.5. User interface IP65 10" touch screen IPC with Windows 10 pro
1.10.6. 8PORT POE switch
1.10.7. Row Cooling DXA 21.2KW 380V 60/50HZ with Humidity Control
1.10.8. 20KW(2u) 3 Phase On-Line UPS with 4 EBC 11.8min
1.10.9. Metered PDU 0U Half rack (1250mm,200/240V, 32A, (24)C13, (4)C19
1.10.10. Microdata center Added rack, 600mm x 1100mm x 2000
1.10.11. Microdata center added rack, 800mm x 1100mm x 2000
1.10.12. RT Series Rail Kit
1.10.13. MINI SNMP IPv6 CARD (SWAPPABLE)
1.10.14. RT 5-20 KVA External Battery Pack(3U), 1 string of 12V9Ahx20pcs
1.10.15. CUBE Novec1230 Detection and Extinguishing up to 1.5m3 3U
1.10.16. SNMP Port for PACU
1.10.17. Water Leaking detection Kit for PACU
1.10.18. Water Pump Kit for PACU
1.10.19. Start-up Services for PACU
1.10.20. Start-up Services for UPS
1.10.21. Rack mounted Distribution Board
1.10.22. Start-up Services for DCIM/EMS
1.10.23. High availability

1.10.23.1. Support the highest Class-A availability level. Three national standard GB50174 A, B and C availability levels and provides N, N+1 or 2N configurations.
1.10.23.2. Highly reliable emergency cooling. The cooling system whenever messages such as over-temperature are detected. It should provide a highly reliable power supply system.
1.10.23.3. Distributed control to increase reliability for air-conditioning, UPS, environment and smart rack (temperature and humidity, lighting, PDU, door sensor, and more). The normal display and uploading of other equipment messages should not be affected even if one of the controllers'

malfunctions.

1.11. Infrastructure (Data Center Compute System)

1.11.1. Compute Nodes consisting of Three (3) Rack mounted Servers (Windows Cluster and Linux Cluster), with minimum specifications as follows:

1.11.1.1. Servers

1.11.1.1.1. 2 x Intel Xeon Gold 4310 (28 Core, 2.0 Ghz)
1.11.1.1.2. 512TB Memory
1.11.1.1.3. 1 x Quad Port 10GbE SFP+
1.11.1.1.4. 2 x 480GB SSD
1.11.1.1.5. 4G RAID Controller
1.11.1.1.6. 256GB NVMe 0.3DWPD M.2 SSD
1.11.1.1.7. 1 x 2 Port 32Gbe FC HBA Card
1.11.1.1.8. Redundant Power Supply

1.11.2. Data Center Virtualization Software Licenses for Server Nodes with the following minimum specifications:

1.11.2.1. 1 x VMWare vCenter Perpetual License
1.11.2.2. 6 x VMWare vSphere Perpetual License
1.11.2.3. 3 x Red Hat Enterprise Linux for Virtual Datacenters with Smart Management, Standard-3 Year
1.11.2.4. Microsoft Windows Datacenter Server 2022

1.12. Data Center Block Storage

1.12.1. **Enterprise Block Storage System Specifications:**

1.12.1.1. 12 x 7.8TB NVMe Drives RAID 5 (60TB Useable Capacity NVMe SSD Drives (Physical Capacity)
1.12.1.2. 8 x 32GB FC Ports with Transceivers
1.12.1.3. Must be future-proof and provide data-in-place upgrades within the same generation or next-generation of appliances, or scale out of their existing environment with a second system equal to their current model.
1.12.1.4. Must have proactive monitoring tools for the storage solution.
1.12.1.5. Must include built-in management features to eliminate dozens of time-consuming tasks and decision points.

1.12.2. **SAN Switch Specifications:**

1.12.2.1. 2 units switch 24 ports 32GB FC
1.12.2.2. 48 pcs 5m LC to LC Cables
1.12.2.3. 48 pcs 32GB FC SFP Transceivers

1.13. Data Center Back-Up System

Requirements for Enterprise On-Premise based Back-Up System:

1.13.1. **1 Unit Server:**

1.13.1.1. 2 x Intel Xeon Silver 4310 (12C, 2.1G, 120W)
1.13.1.2. 128GB Memory
1.13.1.3. 1 x Quad Port 10GbE SFP+
1.13.1.4. 2 x 480GB SSD
1.13.1.5. 1 x 2 Port 32Gbe FC HBA Card
1.13.1.6. Redundant Power Supply

1.13.2. **Software:**

1.13.2.1. 5 x 10 Pack VM Back-up (Back-up for 50 VM's)
1.13.2.2. 1 x red hat Linux Enterprise Standard License for Physical/Virtual

1.13.3. **1 Unit External Storage:**

1.13.3.1. 32 x 14 TB NL SAS Drives RAID 6 12+2 (280TB Useable Capacity)
1.13.3.2. 8 x 32GB FC Port with Transceivers
1.13.3.3. 8 x FC LC-LC Cable

1.14. Data Center Network

1.14.1. **Perimeter NGFW**

1.14.1.1. Performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
1.14.1.2. Scans 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
1.14.1.3. Must be capable of proxy-less and non- buffering inspection technology that provides ultra-low latency performance for DPI of millions of

				simultaneous network streams without introducing the file and stream size limitations and can be applied on common protocols as well as raw TCP streams.		
			1.14.1.4.	Must have a single-pass DPI architecture that simultaneously scans for malware, intrusions, and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.		
			1.14.1.5.	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.		
			1.14.1.6.	Must have a technology that detects and blocks mass-market, zero-day threats and unknown malware that does not exhibit any malicious behavior or that hides its weaponry via encryption. The technology should be able to force malware to reveal its weaponry by unpacking its compressed code in memory (for less than 100 nanoseconds) in a secure sandbox environment.		
			1.14.1.7.	Must have a real-time deep memory inspection technology that can discover packed malware code that has been compressed to avoid detection. It will allow the malware to reveal itself by unpacking its compressed code in memory in a secure threat detection environment.		
			1.14.1.8.	Must have a technology (CPU level instruction detection granularity) that stops new forms of malware trying to exploit the Meltdown vulnerability and identifying new processor- based vulnerabilities.		
			1.14.1.9.	Must be able to analyze documents dynamically using proprietary exploit detection technology along with static forms of . These combined techniques have the capability to detect many malicious document categories, including:		
			1.14.1.10.	Dynamic Data Exchange (DDE) based exploits and malware inside Office files		
			1.14.1.11.	Shellcode-based malicious Office and PDF files		
			1.14.1.12.	Macro-based malicious Office		

		documents 1.14.1.13. Malicious multi-layer PDF and Office Documents 1.14.1.14. JavaScript-based exploits in PDF documents 1.14.1.15. Office and PDF-based malware utilizing dynamic proprietary exploit detection technology 1.14.1.16. “Phishing style” malicious PDF documents leading to both phishing and malware hosting websites 1.14.1.17. PDF documents containing “JavaScript infectors" 1.14.1.18. Must have unlimited Gateway Anti-Virus (AV) file size protection. Gateway AV engine without file size limitations. 1.14.1.19. Must have Cloud Anti-Virus (AV) feature to enhance Anti-Virus protection together with Gateway Anti-Virus. 1.14.1.20. Must be ICSA Labs Advance Threat Defense certified with 100% detection of unknown threats for 6 consecutive quarters from Q1 2021 to Q2 2022 1.14.1.21. Must be certified with ICSA labs Firewall, Anti-Virus, and Advanced Threat Defense certifications. 1.14.1.22. Must be NSS labs Recommended Firewall for 6 times or more. 1.14.1.23. Must be certified with NetSecOpen certification with CVE block rates 99% and above. 1.14.1.24. Must be capable to block suspicious files until a verdict is found or determined. 1.14.1.25. Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points. 1.14.1.26. Scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, key loggers, and other malware in files of unlimited length and size across all ports and TCP streams. 1.14.1.27. Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network. 1.14.1.28. Granularly allocates and regulates available bandwidth for critical applications (or application categories) while inhibiting nonessential application traffic. 1.14.1.29. Enforce acceptable use policies and		

			block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive 1.14.1.30. Blocks content using any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups. 1.14.1.31. URL ratings are cached locally on the firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second. 1.14.1.32. Authentication - The system must support LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, and Common Access Card (CAC). 1.14.1.33. Superior threat prevention and performance - The system must be qualified as a next-generation firewall (NGFW) and Multi-core hardware architecture. 1.14.1.34. Network control and flexibility - The system must have a powerful operating system, Application Control Intelligence, Network Segmentations and VLAN's and Wireless Security 1.14.1.35. Robust Networking Capabilities - The system must have extensive switching and routing capabilities and supports high availability and WAN optimization. 1.14.1.36. WAN Load Balancing - The system must be capable of Loadbalancing 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. 1.14.1.37. Encrypted threat prevention - The system must be capable to decrypt and inspect TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions, and data leakage, and applies application, URL, and content control policies in order to protect against threats hidden in encrypted traffic. 1.14.1.38. Intrusion Prevention - The system must be able to leverage signatures and other countermeasures to scan packet payloads for vulnerabilities and		

			exploits, covering a broad spectrum of attacksb and vulnerabilities. Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.		
			1.14.1.39. DDoS/DoS attack protection - The system must be capable of SYN flood protection to provide 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		
			1.14.1.40. Application Intelligence and Control - The system must be able to control applications, or individual applications against a continuously expanding database with thousands of application signatures, to increase network security and enhance network productivity.		
			1.14.1.41. Virtual Private Network - The system must be capable of both IPsec VPN for site-to site connectivity and SSL VPN or IPsec client remote access. High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of other large sites, branch offices, or home offices. Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites, and applications from a variety of platforms.		
			1.14.1.42. IPv6 - The system must support IPv6		
			1.14.1.43. Real-Time Updates - The system must be supported by a 24x7 Global Operations researching security intelligence.		
			1.14.1.44. The system must have a complete suite of security services for nextgeneration firewalls that features Gateway Security, Content Filtering Service, Anti-Spam, 24x7 Support, multiple sandboxing technology, Real-time Deep Memory Inspection technology, and DNS Security.		
			1.14.1.45. MFA/OTP - The system must have the capability to integrate the Central Firewall Management system that supports 2-Factor Authentication via mail / MS / Google authenticator.		
			1.14.1.46. REST API Support - The system must be capable to integrate the Central		

			Firewall Management system which facilitates interoperability with 3rd-party management consoles to increase the efficiency in Security Management. The Central Firewall Management system must be able to support RESTful APIs that can automate firewall operations for any managed firewalls/devices like typical day-to-day tasks such as device group and tenant management, audit configurations, performing system health checks, and more. 1.14.1.47. Enhanced Support - The system must include email and phone support for customers during local business hours. 1.14.1.48. Firmware Upgrades - The system must include firmware upgrades during its warranty period. 1.14.1.49. Comprehensive Support - The system must haveGlobal Support that is available 8x5 or 24x7. 1.14.1.50. Must be American or European Brand/Standard -The technology or brand must either be American or European for a more Global Standard compliance. 1.14.1.51. Standards - TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 1.14.2. SD-WAN Features and Functionalities (Applies to NGFW in all locations) 1.14.2.1. The system must incorporate multi-WAN transport, load balancing, dynamic path selection, advanced routing, and WAN acceleration 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. 1.14.2.2. Analytics for end-to-end visibility and control 1.14.2.3. Quality of Service (QoS) for the ability to recognize, map, modify, and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators. 1.14.2.4. With centralized security analytics, logging, and reporting.		

		1.14.2.5. Real-time detection across all logs, Indicators of Compromise (IOC), and detection of advanced threats with deep drill-down capabilities, notification, and reports, predefined or customizable dashboard for single pane visibility 1.14.2.6. Enhanced analytics that display bandwidth consumption, SLA metrics, jitter, packet loss, and latency, with real-time monitoring. 1.14.2.7. Supports cloud-based network management to streamline SDWAN provisioning and management. 1.14.2.8. Centralized configuration, change management, dashboard, application policies, QoS, security policies, application-specific SLA, active probe configuration, RBAC, multi-tenant, firmware management, life cycle management (deployment, monitoring, maintenance, and upgrading) for all SD-WAN devices. 1.14.2.9. Can provide security threat information such as malware signature, malware domain or URL, infected host, threat level, malware category, etc. 1.14.2.10. Must be able to provide and monitor secure SD WAN from one console across the network 1.14.3. **Intrusion Prevention System (IPS)** 1.14.3.1. Intrusion Prevention - The system must be able to leverage signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits. 1.14.4. **Core/Distribution Switches** Minimum specifications: 1.14.4.1. 36 x 40/100-Gbps QSFP28 ports 1.14.4.2. Switch should support minimum 7.2 Tbps of bandwidth and over 2.4 bpps switching capacity 1.14.4.3. 4-core CPU 1.14.4.4. 24 GB System memory 1.14.4.5. 128GB SSD		

		1.14.4.6. 40MB System buffer 1.14.4.7. RoHS Compliance 1.14.4.8. MTBF of 352,590 hours 1.14.4.9. Redundant power supply (N+1) 1.14.4.10. Redundant fan (3 dual fan trays) 1.14.4.11. Comprehensive protocol support for Layer 3 (v4/v6) unicast and multicast routing protocol suites, including BGP, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol Version 2 (RIPv2), Protocol Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP 1.14.5. **Spine Switches Specification** Minimum specifications: 1.14.5.1. 36 x 40/100-Gbps QSFP28 ports 1.14.5.2. Switch should support minimum 7.2 Tbps of bandwidth and over 2.4 bpps switching capacity 1.14.5.3. 4-core CPU 1.14.5.4. 24 GB System memory 1.14.5.5. 128GB SSD 1.14.5.6. 40MB System buffer 1.14.5.7. RoHS Compliance 1.14.5.8. MTBF of 352,590 hours 1.14.5.9. Redundant power supply (N+1) 1.14.5.10. Redundant fan (3 dual fan trays) 1.14.5.11. Comprehensive protocol support for Layer 3 (v4/v6) unicast and multicast routing protocol suites, including BGP, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol Version 2 (RIPv2), Protocol Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP) 1.14.6. **Leaf Switch Specifications** (Border/Service/Compute/IP Storage): 1.14.6.1. 48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP 28 ports 1.14.6.2. 6-core CPU 1.14.6.3. 128 SSD 1.14.6.4. 40MB System buffer 1.14.6.5. RoHS compliance		

		1.14.6.6. MTBF of 288,760 hours 1.14.6.7. Redundant power supply (N+1) 1.14.6.8. Redundant fan (4 fans) 1.14.6.9. Must have support for standards based VXLAN EVPN fabrics, inclusive of hierarchical multi-site support. 1.14.6.10. Comprehensive protocol support for Layer 3 (v4/v6) unicast and multicast routing protocol suites, including BGP, Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol Version 2 (RIPv2), Protocol Independent Multicast Sparse Mode (PIM-SM), Source-Specific Multicast (SSM), and Multicast Source Discovery Protocol (MSDP) **1.15. Campus Network Access Switches** 1.15.1. **24 and 48 port Access Switches** 1.15.1.1. UADP 2.0 Mini with integrated CPU 1.15.1.2. 1GE data or PoE+ ports, with 1/2.5/5/10GE (mGig) 1.15.1.3. Fixed uplink with 4 x 1GE SFP or 4 x 10GE SFP+, or 2 x 25GE SFP28 1.15.1.4. Must have optional uplink modules with 4 x 1GE SFP or 4 x 10GE SFP+ or 2 x 25GE SFP28 or 2 x 40GE QSFP+ 1.15.1.5. Must have optional backplane stacking, supporting stacking bandwidth up to 80 Gbps with StackWise-80 or up to 160 Gbps with Stack wise 160 1.15.1.6. Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access 1.15.1.7. Must have enhanced security with AES-128 MACsec encryption, policy-based segmentation, and trustworthy systems 1.15.1.8. Must have advanced network monitoring using Full Flexible NetFlow 1.15.1.9. 24 port POE SW 1.15.1.10. 48 port POE SW 1.15.2. **Wi-Fi Access Points (APs)** 1.15.2.1. **AP Controller** 1.15.2.1.1. The Controller Series Family shall support deployment flexibility without compromising any features 1.15.2.1.2. The controller shall support up to 2K access points, up		

		to 32K clients, and up 40 Gbps tunneling capacity 1.15.2.1.3. The controller shall support hot WLC software patching and hot AP software patching for fixing bugs 1.15.2.1.4. The Controller shall support rolling AP upgrade without need for clustering 1.15.2.1.5. High Availability heartbeat interval shall not be longer than 100 ms. 1.15.2.1.6. The redundant Controller shall sync Access Point and Client Status, including DHCP IP lease status 1.15.2.1.7. The controller shall support multiple PSK keys 1.15.2.1.8. The system shall support control plane encryption on both IPv4 and IPv6 1.15.2.1.9. The controller shall be able to detect employee device connection to Rogue Access Point and contain it automatically 1.15.2.1.10. The controller shall support new application signatures without upgrading controller software 1.15.2.1.11. During system boots, the system's software signatures should be checked for integrity. System should be capable of understanding that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic. Public documents must be provided. 1.15.2.1.12. Controllers shall conform to UL/CSA 60950-1, IEC/EN 60950-1, AS/NZS 60950.1, and CAN/CSA-C22.2 No. 60950-1 for Safety requirements of Information Technology Equipment. 1.15.2.1.13. Controller shall conform to FCC 47CFR15, AS/NZS CISPR 22, CISPR 22, EN55022/EN55032 (EMI-1), ICVCCES-003, I, KN 32 (EMI-2), CNS-13438, EN61000-3-2, EN61000-3-3,		

			IEC/EN61000-4-2, IEC/EN61000-4-3, IEC/EN61000-4-4, IEC/EN61000-45, IEC/EN61000-4-6, IEC/EN61000-4-8, IEC/EN61000-4-11, K35, EN 300 386, EN55022, EN55024/CISPR 24, EN50082-1/EN61000-6-1 Standards for EMC (Electromagnetic Compatibility) requirements. 1.15.2.1.14. Wireless LAN Controller shall have the same OS as the campus core, distribution, and access switches. 1.15.2.1.15. OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from the last 5 years before releasing this RFP. 1.15.3. **Custom Captive Portal Management System** 1.15.3.1.1. Centralized Wi-Fi management system that controls the access of users. 1.15.3.1.2. Built-in AAA components to handle authentication, authorization, and accounting. 1.15.3.1.3. Custom user journey for each SSID which can deliver video, banners, and surveys. 1.15.3.1.4. Dashboards and reports 1.15.4. **Indoor APs** 1.15.4.1. Access Point shall support Wi-Fi6 1.15.4.2. Access Point shall support 4x4 MIMO with four spatial streams 1.15.4.3. Access Point shall support dual 5-GHz radio mode. 1.15.4.4. Access Point shall have integrated or external antenna SKUs. 1.15.4.5. Access Point shall contain 2GB or higher-sized DRAM for capacity and scalability. 1.15.4.6. Access Point shall support USB 2.0 @ 4.5W.		

			1.15.4.7. Access Point shall have a dedicated hardware chipset to offload performance of advanced RF spectrum analysis and security. 1.15.4.8. Access Point shall support Uplink/downlink OFDMA 1.15.4.9. Access Point shall support management console port (RJ-45) 1.15.4.10. Access Point shall support integrated BLE5 radio 1.15.4.11. Access Point shall be able to offer IoT container hosting 1.15.4.12. Access Point shall be able to leverage partnerships for Apple Analytics 1.15.4.13. OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from the last 5 years before releasing this RFP.		
			1.15.5. **Structured Cabling Works:** 1.15.5.1. The winning bidder shall supply, install and test UTP and Fiber Optic Cables and all necessary materials essential for various network nodes as defined in this Terms of Reference 1.15.5.2. The winning bidder must provide a network node schedule that basically tabulates the various network nodes required 1.15.5.3. The winning bidder shall include all necessary equipment and materials. 1.15.5.4. The winning bidder shall also include the IDFs with UPS power supply. 1.15.5.5. 3ft IDF 1.15.5.6. 4ft IDF		
			1.15.6. **Inter-Building Fiber Optic Connection** 1.15.6.1. The winning bidder shall supply, install and terminate the fiber optic cabling that will link the existing Network Switch Room to the new Data Center. 1.15.6.2. FOC installation shall be underground through either micro trenching or		

		Horizontal Direct Drilling (HDD). 1.15.6.3. Supply and Installation of Fiber Termination Equipment and/or network switches. 1.15.7. **In-Building Structured Cabling works** 1.15.7.1. The winning bidder shall furnish all labor, materials, tools, and equipment, and perform all operations necessary to complete the supply, delivery, installation, termination, testing, and commissioning of Structured Cabling Works. 1.15.7.2. Supply, delivery, and pulling of Category 6 UTP cables and Fiber Optic Cables. The winning bidder shall perform proximity measurements and bandwidth requirements assessment to validate the FOC to be supplied whether Single-Mode, Multi-Mode, or a mix of both. 1.15.7.3. Supply and installation of Inter-Rack cabling at the Data Center Facility 1.15.7.4. Supply, Installation, and termination of data cables necessary for the interfacing of devices. 1.15.7.5. Supply and Installation of Cable Ladders, Cable trays, and fiber guides and perform harnessing with appropriate labeling. **1.16. Security Operations Center (SOC)** 1.16.1. **Firewall with the following minimum specifications:** 1.16.1.1. Performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port. 1.16.1.2. Scans 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 1.16.1.3. Must be capable of proxy-less and non- buffering inspection technology that provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing the file and stream size limitations and can be applied on common protocols as well as raw TCP streams. 1.16.1.4. Must have a single-pass DPI architecture that simultaneously scans for malware, intrusions, and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture. 1.16.1.5. 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. 1.16.1.6. Must have a technology that detects and blocks mass-market, zero-day threats and unknown malware that does not exhibit any malicious behavior or that hides its weaponry via encryption. The technology should be able to force malware to reveal its weaponry by unpacking its compressed code in memory (for less than 100 nanoseconds) in a secure sandbox environment. 1.16.1.7. Must have a real-time deep memory inspection technology that can discover packed malware code that has been compressed to avoid detection. It will allow the malware to reveal itself by unpacking its compressed code in memory in a secure threat detection environment. 1.16.1.8. Must have a technology (CPU level instruction detection granularity) that stops new forms of malware trying to exploit the Meltdown vulnerability and identifying new processor- based vulnerabilities. 1.16.1.9. Must be able to analyze documents dynamically using proprietary exploit detection technology along with static forms of. These combined techniques have the capability to detect many		

			malicious document categories, including: 1.16.1.9.1. Dynamic Data Exchange (DDE) based exploits and malware inside Office files 1.16.1.9.2. Shellcode-based malicious Office and PDF files 1.16.1.9.3. Macro-based malicious Office documents 1.16.1.9.4. Malicious multi-layer PDF and Office Documents 1.16.1.9.5. JavaScript-based exploits in PDF documents 1.16.1.9.6. Office and PDF-based malware utilizing dynamic proprietary exploit detection technology 1.16.1.9.7. "Phishing style" malicious PDF documents leading to both phishing and malware hosting websites 1.16.1.9.8. PDF documents containing "JavaScript infectors"		
			1.16.1.10. Must have unlimited Gateway Anti-Virus (AV) file size protection. Gateway AV engine without file size limitations.		
			1.16.1.11. Must have Cloud Anti-Virus (AV) feature to enhance Anti-Virus protection together with Gateway Anti-Virus.		
			1.16.1.12. Must be ICSA Labs Advance Threat Defense certified with 100% detection of unknown threats for 6 consecutive quarters from Q1 2021 to Q2 2022		
			1.16.1.13. Must be certified with ICSA labs Firewall, Anti-Virus, and Advanced Threat Defense certifications.		
			1.16.1.14. Must be NSS labs Recommended Firewall for 6 times or more.		
			1.16.1.15. Must be certified with NetSecOpen certification with CVE block rates 99% and above.		
			1.16.1.16. Must be capable to block suspicious files until a verdict is found or		

			determined.		
			1.16.1.17. Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.		
			1.16.1.18. Scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, key loggers, and other malware in files of unlimited length and size across all ports and TCP streams.		
			1.16.1.19. Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. This helps gain further control over the network.		
			1.16.1.20. Granularly allocates and regulates available bandwidth for critical applications (or application categories) while inhibiting nonessential application traffic.		
			1.16.1.21. Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive		
			1.16.1.22. Blocks content using any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.		
			1.16.1.23. URL ratings are cached locally on the firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.		
			1.16.1.24. Authentication - The system must support LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, and Common Access Card (CAC).		
			1.16.1.25. Superior threat prevention and performance - The system must be qualified as a next-generation firewall		

			(NGFW) and Multi-core hardware architecture.		
			1.16.1.26. Network control and flexibility - The system must have a powerful operating system, Application Control Intelligence, Network Segmentations and VLAN's and Wireless Security		
			1.16.1.27. Robust Networking Capabilities - The system must have extensive switching and routing capabilities and supports high availability and WAN optimization.		
			1.16.1.28. WAN Load Balancing - The system must be capable of Loadbalancing 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.		
			1.16.1.29. Encrypted threat prevention - The system must be capable to decrypt and inspect TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions, and data leakage, and applies application, URL, and content control policies in order to protect against threats hidden in encrypted traffic.		
			1.16.1.30. Intrusion Prevention - The system must be able to leverage signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacksb and vulnerabilities. Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.		
			1.16.1.31. DDoS/DoS attack protection - The system must be capable of SYN flood protection to provide 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		
			1.16.1.32. Application Intelligence and Control - The system must be able to control applications, or individual applications against a continuously expanding database with thousands of application signatures, to increase network security and enhance network productivity.		
			1.16.1.33. Virtual Private Network - The system must be capable of both IPsec VPN for site-to site connectivity and SSL VPN or IPsec client remote access. High-performance IPSec VPN allows the firewall to act as a VPN concentrator for thousands of other large sites, branch offices, or home offices. Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites, and applications from a variety of platforms.		
			1.16.1.34. IPv6 - The system must support IPv6		
			1.16.1.35. Real-Time Updates - The system must be supported by a 24x7 Global Operations researching security intelligence.		
			1.16.1.36. The system must have a complete suite of security services for nextgeneration firewalls that features Gateway Security, Content Filtering Service, Anti-Spam, 24x7 Support, multiple sandboxing technology, Real-time Deep Memory Inspection technology, and DNS Security.		
			1.16.1.37. MFA/OTP - The system must have the capability to integrate the Central Firewall Management system that supports 2-Factor Authentication via mail / MS / Google authenticator.		
			1.16.1.38. REST API Support - The system must be capable to integrate the Central Firewall Management system which facilitates interoperability with 3rd-party management consoles to increase the efficiency in Security Management. The Central Firewall		

			Management system must be able to support RESTful APIs that can automate firewall operations for any managed firewalls/devices like typical day-to-day tasks such as device group and tenant management, audit configurations, performing system health checks, and more.		
			1.16.1.39. Enhanced Support - The system must include email and phone support for customers during local business hours.		
			1.16.1.40. Firmware Upgrades - The system must include firmware upgrades during its warranty period.		
			1.16.1.41. Comprehensive Support - The system must haveGlobal Support that is available 8x5 or 24x7.		
			1.16.1.42. Must be American or European Brand/Standard -The technology or brand must either be American or European for a more Global Standard compliance.		
			1.16.1.43. Standards - TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
			1.16.2. SD-WAN Features and Functionalities (Applies to NGFW in all locations)		
			1.16.2.1. The system must incorporate multi-WAN transport, load balancing, dynamic path selection, advanced routing, and WAN acceleration 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.		
			1.16.2.2. Analytics for end-to-end visibility and control		
			1.16.2.3. Quality of Service (QoS) for the ability to recognize, map, modify, and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service		

		(CoS) designators. 1.16.2.4. With centralized security analytics, logging, and reporting. 1.16.2.5. Real-time detection across all logs, Indicators of Compromise (IOC), and detection of advanced threats with deep drill-down capabilities, notification, and reports, predefined or customizable dashboard for single pane visibility 1.16.2.6. Enhanced analytics that display bandwidth consumption, SLA metrics, jitter, packet loss, and latency, with real-time monitoring. 1.16.2.7. Supports cloud-based network management to streamline SDWAN provisioning and management. 1.16.2.8. Centralized configuration, change management, dashboard, application policies, QoS, security policies, application-specific SLA, active probe configuration, RBAC, multi-tenant, firmware management, life cycle management (deployment, monitoring, maintenance, and upgrading) for all SD-WAN devices. 1.16.2.9. Can provide security threat information such as malware signature, malware domain or URL, infected host, threat level, malware category, etc. 1.16.2.10. Must be able to provide and monitor secure SD WAN from one console across the network 1.16.3. **Intrusion Prevention System (IPS)** 1.16.3.1. Intrusion Prevention - The system must be able to leverage signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.		

		1.16.4. **Endpoint Detection and Response (EDR)** The EDR shall secure the entry points of system servers and end-user devices. It shall act as the first line of defense in the university's multi-layered network security. The EDR to be supplied and installed must be able to perform the following, at a minimum: 1.16.4.1. Detect and block malware through deep learning artificial intelligence 1.16.4.2. Detect and block malicious encryption processes 1.16.4.3. Detect and block ransomware 1.16.4.4. Able to stop exploit techniques 1.16.4.5. Able to control and reduce attack surface, block malicious websites and block potentially unwanted applications 1.16.4.6. Detect malicious traffic 1.16.4.7. Able to provide safe browsing environment 1.16.4.8. Able to perform root cause analysis 1.16.4.9. Automatically removes malware 1.16.5. **Security Information and Event Management (SIEM)** The solution must be a next-generation SIEM platform that reduces enterprise risks by identifying and remediating all attack activities early and precisely, as well as increasing security analyst productivity by leveraging an intelligent and automated SOC platform to deliver maximum cybersecurity protection, efficient incident detection and risk mitigation. Minimum specifications as follows: 1.16.5.1. The solution must be able to collect amounts of data without limiting the number of devices to collect from. 1.16.5.2. The software solution must be scalable and capable to accommodate minimum of 150GB data 1.16.5.3. The solution design and data must be		

			designed to allow quick access to terabytes of historical data. It should be able to support distributed searching.		
			1.16.5.4. The solution must be able to put different data types into different logically separated data stores for optimal search performance or data segregation/RBAC purposes.		
			1.16.5.5. The solution must provide a view for raw data stored.		
			1.16.5.6. The solution must support NO license limit in the number of users in the system, searches, alerts, correlations, reports, and dashboards.		
			1.16.5.7. The solution should allow automatic compression of the ingested data.		
			1.16.5.8. The solution must be able to:		
			1.16.5.9. Collect all types of logs and data from various sources i.e., syslog's, custom/in house-built applications, and database logs		
			1.16.5.10. Consolidate all collected logs into a central repository.		
			1.16.5.11. Perform logs aggregation and normalization.		
			1.16.5.12. Perform log analysis based on searching and reporting.		
			1.16.5.13. Analyze and correlate security events.		
			1.16.5.14. Send alert to respective personnel regarding security issue based on correlated event		
			1.16.5.15. The solution must have integrated threats, incident and compliance management.		
			1.16.5.16. The solution must be able to support virtualized environments.		
			1.16.5.17. The solution must include a data collector that is able to send data (log/event) in real-time and batch mode.		
			1.16.5.18. Proposed solution shall be able to support both agent and agentless		

		based log collection. 1.16.5.19. The solution must show a threat score of an event based on confidence, importance, reputation, and duration of an observed event. 1.16.5.20. The proposed solution must be able to do high availability without any additional license cost. Please provide evidence and explanation. 1.16.5.21. The solution must be able for replication to maintain multiple, identical copies of ingested data for data availability, data fidelity, disaster tolerance, and improved search performance. 1.16.5.22. The solution must be capable of performing Server and Network Infrastructure Monitoring out of the box. 1.16.5.23. The solution must be capable of performing Application Monitoring out of the box. 1.16.5.24. The solution must provide functionalities to perform data masking during search time level 1.16.5.25. The solution must support Geolocation Public IP lookup 1.16.5.26. The solution must automatically monitor for known bad events, and use sophisticated correlation via search, to find known risk patterns such brute force attacks, data leakage and even application-level fraud. 1.16.5.27. The solution must be able to detect compromised hosts associated with advanced threats and malware infections 1.16.5.28. The solution must be able to find activities and events associated with successful attacks and malware infections 1.16.5.29. The solution must be able to help security analysts conduct compromise and breach assessments. 1.16.5.30. Ability to monitor security events outside machine data (e.g., monitor		

		security events/threats that have been posted in Internet) 1.16.5.31. Support customization and in-house security logs and deliver on-the-fly correlation for the logs 1.16.5.32. Proposed solution shall provide advance correlation capabilities to detect security incidents such as: 1.16.5.33. DDOS attacks 1.16.5.34. Worm outbreak 1.16.5.35. Port Scan 1.16.5.36. SQL injection 1.16.5.37. Brute Force attack 1.16.5.38. The solution must be capable of monitoring container network interface (CNI) communication such as East-West traffic and North-South traffic. 1.16.5.39. The solution must be able to correlate asset info with threat and vulnerability data 1.16.5.40. The solution must passively collect asset information and network flow information 1.16.5.41. The solution must issue alert upon detection of blacklisted external IP 1.16.5.42. The solution must consolidate threats by normalization, reputation, knowledge and payload of the triggering event 1.16.5.43. The solution must include built in alert manager for bad events generated 1.16.5.44. The solution must have file integrity monitoring 1.16.5.45. The solution must be fully customizable when creating warning or alarms for high risks events 1.16.5.46. The solution provides network visibility from wire data that contains critical insights about payloads,		

		session information, errors, DNS, etc. 1.16.5.47. The solution must provide ready-to-use apps, utilities and add-ons in providing capabilities ranging from monitoring security and advanced threat management and more. 1.16.5.48. The proposed solution shall be able to capture new events from source devices without reading through the entire data from the beginning. 1.16.5.49. The proposed solution shall be able to provide search function that support Boolean-style patterns search 1.16.5.50. Proposed solution shall be able to allow analysts to build queries using combined search methods. A single query may contain keywords and field-based conditions. 1.16.5.51. The proposed solution must be able to perform sub search in regard to the security on top the current search 1.16.5.52. The solution must be able to monitor Unknown Threats 1.16.5.53. The solution must be capable of correlating and identifying application performance issues due to security incidents (e.g., DDOS attacks, unauthorized access to the system that causes application performance issues.). 1.16.5.54. The solution must support Authentication Authorization Accounting (AAA). 1.16.5.55. The proposed solution must be able to correlate system metrics and events data with data from other technology tiers 1.16.5.56. The proposed solution must be able to find causal links between application performance issues and the underlying OS, hypervisor, storage, network and server infrastructure 1.16.5.57. The solution must be able to discover capacity-constrained or idle systems 1.16.5.58. The solution should have the ability		

		to report when DATA THEFT occurs. 1.16.5.59. The proposed solution must be able to ingest all data (users, applications) and make them available for user monitoring, alerting, investigation, ad hoc searching 1.16.5.60. The solution must have a customizable widget on the dashboard 1.16.5.61. The solution must be a Web Based GUI with HTTPS protocol only 1.16.5.62. The solution must have an option to add additional hosts or subnet 1.16.5.63. The solution must provide flexibility to integrate with third-party reporting tools and portals 1.16.5.64. The solution must support Email notification with content in JSON format 1.16.5.65. The solution must use machine learning based algorithms. Please provide some use cases and evidence that the app is using machine learning based algorithms 1.16.5.66. The solution must provide integration with advanced security advisory modules. 1.16.5.67. The solution must provide support data integration for Risk Analytic 1.16.5.68. The solution must provide support for Risk and Cyber Threat Advisory Alert 1.16.5.69. The solution must provide Management Services for the Security tools such as (UEBA with on-going unlimited dashboard and correlation query update) 1.16.5.70. The solution must provide pre-packaged the Intelligence Module for database system, like, MYSQL, MySQL, DB2, Oracle 1.16.5.71. The solution must provide pre-packaged the Intelligence Module, Dashboard and Report for Windows 1.16.5.72. The solution should provide on		

		premise Signatureless Detection Capability. 1.16.5.73. The solution must come with the integration with at least five open-source threat intelligence. 1.16.5.74. The solution must have a primary management console consist of indexer and dashboard 1.16.5.75. The solution must have Intelligent business analysis module 1.16.5.76. The solution must have risk and compliance advisory module 1.16.5.77. The solution should provide a host-centric view of alert activity for specific hosts. 1.16.6. **Security Orchestration, Automation and Response (SOAR)** The SOAR solution must be able to effectively and quickly allow Security teams to respond to cyber threats using pre-defined playbooks and pre-built integrations to security, IT, and productivity products ensuring identified cyberthreats are mitigated appropriately and consistently. The SOAR solution must comply with the following minimum specifications: 1.16.6.1. The Solution should integrate to various technologies including SIEM, email security, case management, Firewall, Threat Intelligence Feeds, and Active Directory. 1.16.6.2. The solution must automatically trigger playbooks with predefined workflows that perform a variety of instructions that could include executing scripts or integrating with other tools in the environment. 1.16.6.3. The solution must have the ability to threat hunt and automate the threat hunt and apply to SOAR 1.16.6.4. The Solution must have a built-in case management or can integrate to 3rd party case management 1.16.6.5. The solution must have the option to create user-defined playbooks with customized workflows		

		1.16.6.6. The Solution must have already pre built templates for general reporting and compliance reports 1.16.7. **Sandboxing** The Sandbox solution is designed to assist the security team in detecting malicious files, such as polymorphic and disguised threats designed for undetectable targeted attacks, and to provide continuous maximum protection performance against rapidly evolving advanced threats. It should meet the following minimum requirements: 1.16.7.1. The solution must provide detection of APT attacks via network, web. 1.16.7.2. The solution must be capable of detecting malware as it travels through the network and reaches specific hosts. 1.16.7.3. The solution must have the ability to upload files to an external tool. 1.16.7.4. The solution must be capable of tracking the total number of bytes sent to the Sandbox for analysis. 1.16.7.5. The solution should support the ability to link to Threat Intelligence in Alert. 1.16.7.6. The solution should be able to detect threats targeting various Operating Systems. 1.16.7.7. The solution should be able to identify threats in any file type. The bidder must list down file type supported. 1.16.7.8. The solution must be based on full system emulation and be capable of detecting and visualizing the exploit's multi-stage attacks that split into multiple objects. 1.16.7.9. The solution must employ full-system emulation to analyze objects in order to prevent evasion techniques through the use of Environment Fingerprinting, Network Fingerprinting algorithms, and time-based action identification. 1.16.7.10. The analysis engine of the solution		

			must be capable of revealing malware evasion techniques such as stalling loops and environmental checks. 1.16.7.11. In order to ensure a granular analysis of the samples, identifying unknown/0-Day attacks, the analysis engine must be able to reproduce the malware execution on a machine emulator. 1.16.7.12. The solution must provide a description of the malware family. 1.16.7.13. The proposed solution must integrate with the SIEM security solution via the security intelligence adapter and application. 1.16.8. **Threat Intelligence** Threat intelligence feeds are an important component of security infrastructure because they provide information on attacks such as zero-day attacks, malware, botnets, and other security threats, which helps identify and prevent security breaches. This solution integrates with SIEM to provide a better understanding of emerging cybersecurity threats such as zero-day threats, advanced persistent threats, and exploits. It must meet the following minimum requirements: 1.16.8.1. The solution must come with the integration with at least five open-source threat intelligence. 1.16.8.2. The solution should support the ability to link to Threat Intelligence in Alert. 1.16.8.3. The solution must provide threat intel updates from bidder platforms 1.16.8.4. The solution must continuously collect, aggregates, prioritizes, and distribute feeds in near real time to SIEM and UEBA for data enrichment and enhance threat detection 1.16.9. **Network Detection and Response (NDR)** The NDR solution is designed to provide full visibility of all network behaviors (network devices, endpoints, applications, and users) with advanced auto-correlation capabilities to detect threats and provide a more efficient and		

		accurate view of alerts. The NDR solution can also respond to identified threats automatically, such as sending commands to FW or EDR, or manually, such as threat hunting or incident investigation. It must meet the following minimum specifications: 1.16.9.1. The solution's architecture has to be very extensive in network traffic analysis using both Supervised and Unsupervised learning 1.16.9.2. The solution must be capable of capturing raw network packets and storing them for forensic analysis and/or attack replays. 1.16.9.3. The solution must be capable of capturing raw network packets and reducing the data to produce valid security events without the size of a full packet capture. 1.16.9.4. The solution must be capable of collecting and correlating firewall traffic logs, IDS events, NetFlow and cloud flow logs. 1.16.9.5. Provides tracking of the interaction between devices, services, applications that are running on your network in real time and historically. 1.16.9.6. The solution must be able to support SNMP. 1.16.9.7. The solution must be able to connect EDR and IdP data and provide AI based anomalies detection and correlation. 1.16.9.8. The solution shall be able to address all Alert Types Tied to phases of Infection Life Cycle. 1.16.9.9. The solution must be able to categorize Incident Severity attached to Alerts. 1.16.9.10. The solution must support Authentication Authorization Accounting (AAA). 1.16.9.11. The solution should support integration to the firewall to do Inline blocking mode (not TCP Reset). 1.16.9.12. The solution must provide threat intel		

		updates.			
		1.16.9.13. The solution must support community-based intel sharing.			
		1.16.9.14. The solution must have the ability to perform vulnerability and kill chain / weakest link Analysis.			
		1.16.9.15. The solution must provide attribution of alerts to MITRE Framework			
		1.16.9.16. The solution should support integration with Forensic Tools.			
		1.16.9.17. The solution must be capable to do comprehensive network traffic analysis which includes:			
		1.16.9.17.1. Network performance statistics			
		1.16.9.17.2. Server performance			
		1.16.9.18. Application detection and performance monitoring:			
		1.16.9.18.1. Top sources & Top destinations			
		1.16.9.18.2. Asset application performance			
		1.16.9.18.3. Application processing time			
		1.16.9.18.4. Network interactions with asset			
		1.16.9.18.5. HTTP statistics			
		1.16.9.18.6. DNS statistics			
		1.16.9.18.7. Asset Discovery and Statistics			
		1.16.9.18.8. IP address			
		1.16.9.18.9. Device Manufacturer			
		1.16.9.18.10. Application Services			
		1.16.9.18.11. Time discovered and last seen			
		1.16.9.18.12. Asset			

		tag(s) and description 1.16.9.18.13. Server certificate visibility 1.16.9.19. The solution must integrate to various technologies including SIEM, SOAR, Firewall, Sandbox, and Active Directory for response 1.16.9.20. User and Endpoint Behavior and Analytics (UEBA) The UEBA solution is designed for discovering new assets automatically and constantly, profiling users, and identifying their behavior and risk. It must meet the following minimum specifications: 1.16.9.20.1. The solution must come with user behavior analytics that collect user information from Active Directory 1.16.9.20.2. The solution must come with entity behavior analytics that collect IP information from network traffic 1.16.9.20.3. The solution must track changes and secure your environment by monitoring for suspicious activity, user role changes, unauthorized access and more. 1.16.9.20.4. The solution, based on observed security events and asset risk profile, assigns a risk score. 1.16.9.20.5. The solution must discover assets dynamically across networks, endpoints, and cloud environments. 1.16.9.20.6. The solution must use either host names, MAC addresses, or IP addresses to uniquely identify assets. 1.16.9.20.7. The solution must collect		

		and fuse user-relevant data from multiple data sources across the security infrastructure automatically. 1.16.9.20.8. The solution's Machine learning must be used to enable sophisticated behavioral analytics in the solution. 1.16.9.20.9. The solution without any rules or signatures, must detect bad behavior. 1.16.9.20.10. The solution for each detected and identified asset, must provide a kill chain view of security events. 1.16.9.20.11. The solution must track threats based on the user rather than the threat type. 1.16.9.20.12. The solution must assign a risk score to each user in order to easily identify risky users **2. Unified Database Platform** The Unified Database Platform must meet the following specifications, at a minimum: **2.1.** Must be cloud agnostic and cloud-native and can support deployments in bare metal, VMs, or Kubernetes both in on-premises infrastructure as well as cloud for at least the following options: 2.1.1. Baremetal 2.1.2. VMware vSphere 2.1.3. AWS 2.1.4. Google Cloud Platform 2.1.5. Microsoft Azure **2.2.** It must support both the SQL and NoSQL APIs under a common storage substrate to address current and future use cases. **2.3.** Capable of enabling client applications to		

		auto-discover cluster nodes and cluster topology using an application-friendly library. **2.4.** Able to support a single synchronous cluster stretched across multiple AZ's/regions/clouds and support multiple advanced replication architectures for the resiliency of the system. **2.5.** Able to horizontally scale out/in/up/down with minimal to no business disruptions **2.6.** Must offer a single user interface across various clouds with simplified database management and monitoring like DB upgrades, backups, security & on-demand scaling of nodes to simplify operation and management **2.7.** The proposed solution shall support distributed ACID and transactions with strong data consistency. **2.8.** The proposed solution must include at least 96 cores of database license subscription for production and 96 cores of database license for non-production **2.9.** Must include 1 year Enterprise Support for production and non-production **2.10.** Able to provide the ability to increase computing capacity linearly by adding new nodes to the existing database system with no downtime. **2.11.** The proposed solution must support data replication between two isolated instances to support application-level active-active deployments. **2.12.** Able to enhance the primary cluster capability with additional read-replica nodes to facilitate reads closer to the customer base. **2.13.** Able to support data affinity to comply with country/region-specific regulatory/compliance requirements. **2.14.** Must support encryption in transit and rest to have a strong security posture. **2.15.** The proposed solution shall be able to provision and manage in a fully air-gapped environment.		

		2.16. Shall support region/zone/cloud affinity to define different data serving topologies to keep the data serving nodes closer to the user base **2.17.** Capable of horizontally scaling with no downtime to support adhoc peak workloads or increase in sizing without interruption **2.18.** The proposed solution must offer a single user interface across various clouds with simplified database management and monitoring like DB upgrades, backups, security & on-demand scaling of nodes to simplify operation and management **2.19.** The proposed solution must have CDC capability to generate events on data change. **2.20.** Must have API for management automation **2.21.** The proposed solution must support advanced SQL features like stored procedure, foreign keys, triggers, json support (filtering, constraints and projections) to support current and future use cases.		
		3. Professional Services **3.1. Project Management** Commitment is to ensure that information and communication technology projects are completed successfully. This involves overseeing the project team, creating project plans, tracking progress, identifying and managing risks, and communicating with stakeholders. 3.1.1. Develop a clear understanding of the project goals and objectives, and ensure that all project team members have a shared understanding of these goals. 3.1.2. Create a detailed project plan that includes		

		timelines, milestones, and deliverables. 3.1.3. Assign roles and responsibilities to the project team members and ensure that everyone understands their roles. 3.1.4. Monitor project progress regularly and adjust the project plan as necessary. 3.1.5. Identify potential risks and develop contingency plans to mitigate these risks. 3.1.6. Communicate regularly with stakeholders, including sponsors, customers, and team members, to ensure that everyone is aware of project progress and any issues that arise. 3.1.7. Ensure that project documentation is accurate and up-to-date, including project plans, progress reports, and risk assessments. 3.1.8. Foster a positive team environment by encouraging collaboration, providing support, and recognizing team members' contributions. 3.1.9. Continuously evaluate project performance and identify opportunities for improvement. **3.2. System and Hardware Installation** 3.2.1. Provision of essential services for installation of devices, software and systems supplied for this project. **3.3. Operating System (OS) Hardening** The OS hardening service shall include the patching and application of advanced system security procedures to secure the server's OS. The OS hardening procedures must include the following, at a minimum: 3.3.1. If available, install service packs, firmware and/or patches to keep the OS up to date 3.3.2. Perform secure configuration by deleting unnecessary programs and/or drivers, apply restrictions to the network, files and applications, assign groups and set the policies and use templates to manage and enforce security configurations 3.3.3. Install End-Point Protection **3.4. Support Services**		

		3.4.1. The winning bidder must ensure that appropriate support services are in place within the active warranty period of all supplied devices and software. **3.5. Knowledge Transfers** 3.5.1. Provide training for all users and IT Support for RSU Agpudlos. 3.5.2. Document handover: 3.5.2.1. Network Diagram 3.5.2.2. System Diagram 3.5.2.3. System Credentials 3.5.2.4. Network Topology and IP VLan 3.5.2.5. Application and system documentation 3.5.3. Prior to the project handover, the winning bidder must conduct a walk-through with university nominated personnel but limited to engineering and IT technical personnel. The intent primarily is to orient on the supplied equipment/devices, completed installations, equipment type, functionalities, basic operations & maintenance, and how these are integrated holistically.		
		3.6. Testing and Commissioning Services 3.6.1. The winning bidder shall be required to perform testing and commissioning. Minimum Scope of Services are as follows: 3.6.1.1. The winning bidder shall submit the testing Methods of Procedures (MoP) to RSU PMT prior to actual testing. 3.6.1.2. Perform actual testing as per Manufacturer prescribed testing methodologies. 3.6.1.3. Testing results must be documented and submitted to RSU PMT not later than 48 hours from completion of the testing activities. Should there be failed testing, the winning bidder is given a maximum of 12 hours to troubleshoot or rectify the problem. Re-testing shall then be performed. After completion of the 2nd testing and such has failed anew, the winning bidder shall		

		furnish RSU PMT with full report not more than 24 hours from the time failed testing has been declared, and must replace the defective hardware and/or software not more than fourteen (14) days from the date of completion of the failed testing. In case of longer replacement period, the winning bidder must inform RSU PMT in writing, stating the reasons thereof and arrival date.		
TOTAL			**1 Lot**	

_____
Name and Signature of the Bidder/
Authorized Representative

_____
Name of the Company