TENDER REFERENCE NO.: KK/206/2025/HTD

MINISTRY OF HEALTH
NEGARA BRUNEI DARUSSALAM

THE REFRESH OF NETWORK INFRUSTRUCTURE OF RIPAS HOSPIAL (PHASE 2), MINISTRY OF HEALTH, BRUNEI DARUSSALAM

TENDER FEES	**: $505.00**
RECEIPT NO.	**:**
CLOSING DATE	**: ON TUESDAY, 02nd September 2025**
TIME	**: 2.00 PM**
FOA	**:**

THE CHAIRMAN
MINI TENDER BOARD, TENDER BOX
GROUND FLOOR, MINISTRY OF HEALTH
COMMONWEALTH DRIVE
BANDAR SERI BEGAWAN BB3910
NEGARA BRUNEI DARUSSALAM

(CLUSTERING)

SECTION 2: GOVERNMENT REQUIREMENTS

TABLE OF CONTENTS

SECTION 2

GOVERNMENT REQUIREMENTS

1 INTRODUCTION

1.1 Background

1.1.1 The network infrastructure within Ministry of Health (MOH) premises, including MOH Headquarters, Departments, Hospitals, Health Centers, and Clinics, was installed in 2012-2013. The network equipment responsible for providing connectivity to the One Government Network (OGN), enabling users to access various government applications such as Brunei Information and Management System (Bru-HIMS), Picture Archiving Communication Systems (PACS), Government e-mail, intranet portal, Sistem Sumber Manusia (SSM), Treasury Accounting and Financial Information System (TAFIS), among others, has become outdated.

As a result of aging hardware, the network components are prone to malfunction and have impacted the following:

- **Performance Degradation**: Outdated network infrastructure often leads to sluggish performance, resulting in slower data transmission speeds and increased latency. This can impede productivity and hinder efficient communication and collaboration within organizations.

- **Security Vulnerabilities**: Older network systems may lack the robust security features necessary to defend against sophisticated cyber threats. Vulnerabilities in outdated infrastructure can be exploited by malicious actors, leading to data breaches, theft, or unauthorized access to sensitive information.

- **Limited Scalability**: As businesses grow and evolve, their network infrastructure must be able to scale accordingly to accommodate increased data traffic and user demands. Outdated systems may lack the flexibility and scalability needed to support expansion, resulting in bottlenecks and limitations on growth.

- **Maintenance Challenges**: Aging infrastructure often requires more frequent maintenance and repairs, leading to increased downtime and higher operational costs. This can disrupt business operations and strain IT resources, diverting attention and resources away from strategic initiatives.

To ensure uninterrupted and reliable network connectivity, as well as to prevent any disruptions or inaccessibility to e-Government services, it is imperative to promptly refresh the obsolete hardware. The Department of Healthcare Technology, Ministry of Health is currently undertaking a phased approach to refresh the network infrastructure across all MOH sites, prioritizing according to urgency and critical requirements.

1.1.2 Presently, the core network layer infrastructure of all district hospitals has been successfully replaced and is undergoing regular maintenance. Additionally, access layer switches have been replaced at several main Health Centers, all Outpatient Department Blocks and Ward Complex Blocks of Raja Isteri Pengiran Anak Saleha Hospital (*through RIPAS Hospital Network Refresh (Phase 1) project under the Network Central Procument 2 contract*).

This tender outlines the need for network infrastructure refresh and upgrade for the remaining department or buildings of Raja Isteri Pengiran Anak Saleha Hospital (RIPASH); Woman and Child Centre Building, Specialist 1 & Specialist 2 Building, Estate Department Building, Biomedical Engineering Building and Emergency Medical Ambulance Services and surrounding areas.

Key objectives of the project are:

- **Infrastructure Modernization**: Upgrading to modern network hardware and software solutions can address many of the limitations of outdated infrastructure. This may involve replacing legacy equipment with newer, more efficient technologies that offer improved performance, security, and scalability.
- **Security Enhancements**: Implementing robust security measures to help protect against cyber threats and safeguard sensitive data. Regular security audits and updates are essential to identify and mitigate vulnerabilities in the network infrastructure.
- **Continuous Monitoring and Maintenance**: Proactive monitoring and regular maintenance are crucial for ensuring the health and performance of the network infrastructure. Automated monitoring tools can detect issues in real-time, allowing IT teams to address them promptly and minimize downtime.

By giving priority to updating infrastructure and embracing new technologies, the Ministry of Health could tackle the obstacles presented by obsolete network systems and pave the way for future achievements in the digital era.

1.1.3 The project site will be at RIPAS Hospital building including Woman & Child Centre (WCC) located at:

Raja Isteri Pengiran Anak Saleha Hospital
Jalan Putera Al-Muhtadee Billah
Bandar Seri Begawan BA1712
Negara Brunei Darussalam

1.2 **Products and Services Sought**

1.2.1 Tenderes are invited for **“**The Refresh of Network Infrastructure of RIPAS Hospital (Phase 2), Ministry of Health” to meet the Government Requirements.

1.2.2 Tenderers shall propose a proven and cost-effective wired and wireless network solution for Raja Isteri Pengiran anak Saleha Hospital, Ministry of Health.

1.2.3 The offered solution must be fully compatible or equivalent with the existing infrastructure deployed in Phase 1 project based on system and support as implemented in RIPAS Hospital environment.

1.2.4 Tenderers are required to propose all items, and be wholly responsible for all products and services offered. The Government reserves the right to accept all or any part of the proposed items or services from the Tenderers.

2 STATEMENT OF REQUIREMENT

2.1 Scope of Work

The project scope includes the following:

2.1.1 To provide the supply, delivery, installation, configuration, testing, commissioning of the hardware or the product sought to meet the Government Requirements.
2.1.2 To provide 1-year warranty (including support) for all hardware proposed.
2.1.3 To provide 5-year maintenance (Preventive and Curative maintenance) after warranty period ended.
2.1.4 To provide 5-year technical support service after warranty period ended.
2.1.5 To implement secure and easy management and monitoring of the wired and wireless infrastructure/environment.
2.1.6 To implement wireless network solution that shall have centralized configuration, data encryption, policy enforcement and network devices, as well as distributed and centralized traffic forwarding.

2.1.7 To implement wireless solution that shall have multiple wireless networks (SSIDs) for client access according to privileges or level of access (eg. Administrator, Employee, Guest etc).

2.1.8 To supply, deliver and install the necessary cabling and interconnection as well as labelling upon agreement by the Government.

2.1.9 To mitigate any issues/vulnerabilities found during Network Vulnerability Security Assessment by Security agencies appointed by the Government.

2.1.10 The connectivity requirements up to the router inclusive at the agencies' remote sites will be provided by OGN (One Government Network), however MOH still required Tenderers to liaised with OGN provider and Bru-HIMS vendor (if necessary) until the connection is successful.

2.1.11 To provide training & certifications for the IT/ Network Administrator

2.1.12 Removal and uninstallation of outdated hardware in compliance with Government procedures including doing backup of the configurations.

2.1.13 Failover test and reconfiguration (where necessary)

2.1.14 Spare units available for immediate replacement of faulty equipment.

2.1.15 To provide project management services for effective implementation of the network upgrade.

2.2 Hardware

2.2.1 The following specifies the hardware to be supplied:-

a. IP Networking
   - ○ Access switches
   - ○ Distribution switches
   - ○ Hardware for SDN Controller & AI Analyzer

b. Wireless Networking (Wi-Fi)
   - ○ Wireless Controllers
   - ○ Wireless Access Points

c. Existing eSight hardware upgrade with value added features and component below:
   - ○ Software Define Network (SDN) Management Controller
   - ○ Intelligent Network Analysis
   - ○ Disaster Recovery Setup
   - ○ Relocation and Migration
   - ○ Exisiting equipment license upgrade to use new features
   - ○ License for new equipment

2.2.2 Detailed specifications for the hardware items in clause 2.2.1 are listed in **Section 2 Annex 2.1 Hardware Specifications**.

2.2.3 To ensure that the hardware proposed will not reach End of Life (EOL) within 5 years.

2.2.4 The solution must ensure seamless integration with RIPAS Hospital current environment (*core switch, distribution switch, access switch, network management system (NMS)*).

2.2.5 The hardware must be equivalent or have full compatibility with the existing Huawei's core switches, distribution switch, firewall, NMS e-Sight and confirm that all hardware is suitable for intended applications and workloads. Tenderer may be required to demonstrate this compatibility during technical evaluation.

2.2.6 The hardware proposed must be able to work perfectly and seamlessly with all the recently refresh network devices which are under warranty & maintenance such as the Core switch, Distribution switch, Access switches, Firewall, Network Management system (NMS) currently located in the MOH Hospitals (all districts). The hardware propose shall be able to use full features or integrate with the existing Network Management System (Huawei E-Sight/NCE-Campus & CampusInsight).

2.2.7 Tenderers shall propose all hardware required for this project in compliance with E-Government National Centre (EGNC) policy and standard. The design of the network infrastructure shall be cost effective.

2.2.8 The Contractor shall be responsible to deliver the hardware with the hardware specifications and quantity listed out in Section 2 Government Requirements Annex 2.2 Hardware Specifications

2.3 **Software**

2.3.1 The following specifies the software & licenses to be supplied for the following hardware where applicable:-

a. Distribution and access switch supbscriptions support, if any;
b. Wireless Controller Management Software
c. SDN Controller
d. AI Analyzer

2.3.2 Detailed specifications for the hardware items in clause 2.2.1 are listed in **Section 2 Annex 2.1 Hardware Specifications**

2.3.3 The tenderer shall propose suitable server operating systems that is equivalent with the existing equipment.

2.3.4 The tenderer shall ensure compliance with relevant licensing models (e.g., perpetual, subscription).

2.3.5 The proposed solution must include support for the required software and application.

2.3.6 Upgrade existing equipment licenses to support value added features and components.

2.3.7 Propose Software License for all new proposed devices.

2.3.8 To ensure that the software proposed will not reach End of Life (EOL) within 5 years.

2.4 **Network**

2.4.1 The Contractor shall be responsible for the design, supply, and deployment of a new Local Area Network (LAN) infrastructure to support the installation of the proposed network equipment. This includes, but is not limited to, the provision and installation of all necessary network cabling, trunking, patch panels, switches, and related components. The new LAN must be properly integrated with the existing infrastructure and ensure full connectivity to the OGN network. The Contractor shall coordinate with the relevant stakeholders, including the OGN provider, to ensure seamless end-to-end connectivity and functionality.

2.4.2 The Contractor shall seek prior approval from the Government Project Officer before conducting any site installations such as wall hacking, laying of network cables, cutting of raised floor panels and accessing to secure areas etc.

2.4.3 The Contractor shall supply and install fibre optic backbone infrastructure at sites lacking existing network backbone connectivity. The backbone cabling shall comply with relevant industry standards and shall be housed in appropriate protective conduits or ducts. Where applicable, the cabling shall be routed through underground or overhead pathways designed to mitigate environmental exposure and shall incorporate rodent-resistant sheathing or enclosures to prevent physical damage

2.4.4 The Contractor shall provide sufficient electrical power outlets to ensure that sufficient power is provided to all Supplied Equipment to prevent power overloading.

2.4.5 The Contractor shall install the proposed network equipment, configure and connect it to RIPAS Hospital network and ensure that any PC, printers and other hospital devices within that site are connected to its respective network.

2.4.6 The Contractor shall be responsible for the supply, delivery, installation, integration, testing and commissioning of the hardware and services required in relation to **Annex 2.2 Network Topologies**.

2.4.7 The Contractor shall be responsible to configure the hardware and software delivered to the current network infrastructure of the sites.

2.4.8 The Contractor shall be an authorized partner of the proposed hardware and submit documentation of it as proof.

2.4.9 All tasks and activities shall be carried out by certified and experienced workers in association to the proposed solution.

2.4.10 Network Infrastructure:

2.4.10.1 The Tenderer shall provide both the physical and logical network architecture design for the proposed system.
2.4.10.2 The design must include redundancy, failover, and load-balancing components to ensure high system availability.
2.4.10.3 Tenderer shall supply all new equipment, appliances and upgrade of existing eSight specified in Annex 2.1 including all related software and licenses for operations in the appropriate quantities.
2.4.10.4 The Tenderer must propose a detailed plan for network segmentation, outlining how the network will be divided into smaller, manageable segments to improve security and performance.
2.4.10.5 The tenderer shall engage the existing vendor for existing eSight Upgrade, migration and disaster recovery plans, license utilizations, and detailed planning for the new version to ensure minimal service impact.
2.4.10.6 The Tenderer shall provide all necessary network cables for the proposed infrastructure, including cables for network uplinks between the distribution switches, switches, access points and etc.

2.4.11 Distribution and Access Switches:

2.4.11.1 The Tenderer shall propose distribution switch configured with High Availability (HA).
2.4.11.2 The distribution switch shall include dual power supplies to ensure continuous operation and minimize downtime.
2.4.11.3 Access switches must be provided on all floors to ensure complete network coverage and an adequate number of switch ports for all requirements (e.g., End user PC, access points, etc)
2.4.11.4 The Contractor shall handle the installation and configuration of both distribution and access switches to ensure optimal performance and network reliability.
2.4.11.5 The Contractor shall ensure that the switches are properly mounted and secured using rack mount kits.

2.4.12 Wireless Infrastructure:

2.4.12.1 The Tenderer shall propose wireless controller which able to support the access points and connect to existing eSight.
2.4.12.2 The Tenderer shall propose a minimum Wi-Fi 6 Access Point (AP) system with ready IoT expansion slot.
2.4.12.3 The APs shall able to support seamless roaming .
2.4.12.4 The exact location of APs will be determined during a site survey to ensure optimal placement, minimize blind spots, and provide comprehensive coverage throughout the building.
2.4.12.5 Installation and mounting of APs shall be performed by the Contractor, ensuring each AP is positioned for maximum coverage and minimal blind spots.

2.4.12.6 The Contractor shall handle all cabling work required for the AP installations including reusing or relocate if necessary. APs must support Power over Ethernet (PoE) to operate at full capacity with a single cable line.

2.4.13 Upgrade of existing Huawei eSight version and setup for Disaster Recovery:

2.4.13.1 To update existing esight version to support value added features and components without service impact.
2.4.13.2 Disaster Recovery setup with automatic switchover by using 3rd site as arbitration by relocating existing hardwares from other hospitals to Primary Site,Disaster Recovery Site and Arbritation Site.
2.4.13.3 Primary Site will be RIPAS Hospital for centralized management while DR site and Arbitration site will be at EGNC Co-Location Zone and Ministry of Health Headquarter respectively.
2.4.13.4 Upgrade existing license to support for the value added features and components specified Annex 2.1
2.4.13.5 All new proposed equipment such distribution switches, access switches, wireless controller, and wireless access point to be configured via the new version eSight.
2.4.13.6 Value added features and components are specified in Annex 2.1

2.4.14 Structured cabling:

2.4.14.1 The Tenderer shall supply new network cable and necessary components for installation of new access point according to the location best fit for maximum coverage.
2.4.14.2 The Contractor shall provide network cable management kits (if required additional) to ensure that network cables are neatly arranged for ease identification and troubleshooting.
2.4.14.3 The Contractor shall terminate all networks cables within the rack enclosure.
2.4.14.4 The Contractor shall ensure that all network cables run in PVC conduit/casing to protect the cable against pests, including proper cable trays, if necessary.
2.4.14.5 All network cable provisioned and installed must be tested and certified according to industry standard to ensure the quality of service.
2.4.14.6 The Contractor shall ensure that each network cable has a unique identifier and are labelled at logical intervals along the length of the cable and at both ends.
2.4.14.7 The Contractor shall label all Supplied Equipment according to the format for Government IT Equipment that will be provided by Department of Healthcare Technology, Ministry of Health.

2.5 Security Assessment

2.5.1 The Government representative shall engage E-Government National Centre (EGNC) or Cybersecurity Brunei (CSB) to perform security assessments on the network infrastructure.

2.5.2 The Contractor shall help facilitate the assessment to include and not limited to the following:

2.5.2.1 The document design of the network architecture;
2.5.2.2 Physical Design Architecture;
2.5.2.3 Logical Design Architecture

2.5.3 The contractor shall address and resolve any issues/vulnerabilities found during the security assessments.

2.6 **Stabilization**

2.6.1 The Contractor shall provide skilled staff to be responsible for the overall management during the Stabilization Period.

2.6.2 The Stabilization Period shall comprise of ensuring the stability of the propose System and ensure that the performances are optimal and all requirements are fulfilled.

2.6.3 The Stabilization Period shall commence immediately following the successful completion of User Acceptance Testing (UAT) and shall run for a continuous period of [ninety (90) calendar days].

2.6.4 This stabilization period aims to ensure the solution operates with full stability, performance, and functionality in the live environment, verify that any post-implementation issues have been effectively resolved, and support the complete handover of operations and support responsibilities to the Government.

2.6.5 The Government may, at its sole discretion and at no additional cost, extend the Stabilization Period if it reasonably determines that the solution has not yet achieved satisfactory stability, performance, or operational readiness within the original timeframe. Any such extension will be formally communicated in writing, along with a justification.

2.6.6 The Contractor shall deploy qualified personnel responsible for the overall management of activities during the Stabilization Period.

2.6.7 Any defects identified during the Stabilization Period shall be promptly addressed and rectified by the Contractor at no additional cost to the Client.

2.6.8 During the Stabilization period, The Contractor shall provide escalated and prioritized support for all aspects of the live system, encompassing:

i. Rapid Incident Management.
ii. Root Cause Analysis Report.
iii. Performance Monitoring.
iv. Data Integrity Verification.
v. Operational Handoff Refinement.
vi. Communication & Reporting.

2.6.9 The Contractor shall provide, including but not limited to, the following specific deliverables as evidence of system stabilization:

i. Weekly Stabilization Report.
ii. Rapid Incident Management Report.
iii. Production Data Integrity Post-Go-Live Verification Report.
iv. Root Cause Analysis Report.
v. Updated System Documentation.
vi. Updated Standard Operating Procedures (SOPs).
vii. Stabilization Final Report & Consolidated Issue Log.

2.6.10 If the solution is deemed stable and meets the agreed-upon performance criteria, a Final Acceptance Certificate shall be issued at the conclusion of the Stabilization Period.

3 IMPLEMENTATION AND RELATED SERVICES

3.1 **General Requirements**

3.1.1 Implementation and related services refer to the services provided by the Contractor from the commencement of the implementation of the project, until successful completion of distribution to the end users including training, as below:

a. Implementation Services

b. Labelling
c. Training (and Knowledge Transfer)
d. Warranty, Maintenance and Support Services

3.1.2 The Government shall furnish the Contractor with pertinent information, knowledge and assistance as the Contractor may reasonably and properly require enabling it to perform its obligations hereunder.

3.1.3 All the materials supplied to the Contractor by the Government for the purpose of this Contract shall remain the property of the Government and shall be returned in reasonable order after the completion of the Implementation and Related Services.

3.1.4 The Contractor shall comply with all reasonable instructions of the Government representative in so far as they are applicable to the Implementation and Related Services.

3.2 Implementation Services

3.2.1 Implementation Services consists of the following, with respect to the requirements set out in **Clause 2 Statement of Requirement.**

3.2.1.1 Supply
3.2.1.2 Delivery
3.2.1.3 Installation
3.2.1.4 Configuration
3.2.1.5 Testing
3.2.1.6 Commissioning

3.2.2 During the Implementation, the Contractor shall be responsible for the following:

i. Provide day-to-day planning, control and administration of the project;
ii. Advise the Government, on a timely basis, about any unavoidable deviation from plans and recommend appropriate corrective and preventive actions;
iii. Ensure the successful delivery of all related hardware and software to the listed locations within the specified schedule and budget;
iv. Conduct on-site installation tests on the hardware and software before Government acceptance of delivery;
v. All tasks and activities shall be carried out by certified and experienced workers in association to the proposed solution especially in dealing with crucial hardware or components of the project that needs proper support from the manufacturer.
vi. Ensure that all bundled deliverables for hardware and software are accountable prior to Government acceptance of delivery;
vii. Provide day-to-day liaison between other suppliers/sub-contractors and the project teams;
viii. Attend regular and ad-hoc meetings which are chaired by the Government's representatives;
ix. Keep the Government informed of all matters related to the project within the knowledge of the Contractor and shall answer all reasonable enquiries received from the Government representative;
x. Exercise all reasonable skill, care and diligence in its conduct of the Implementation and Related Services, including the following;
a. All ordinances or regulations enforced in Brunei shall be followed;
b. Appropriate measures shall be taken to protect the installation location and the existing facilities from damage caused by installation works; and
c. All necessary measures shall be taken to prevent interruption to the Government's operations.
xi. Inform the government of any change or replacement of key Contractor staff during the project delivery;
xii. Provision for sufficient resources to carry out the Implementation Services, Support Services and Training requirements, including:
   a. Provide one full-time Project Manager stationed in Brunei for the duration of the Implementation Period;

b. Provide one full-time Accounts Manager stationed in Brunei for the duration of the Support Services Period;

c. Provide qualified trainers for the software as specified in **Clause 2.3 Software**

3.2.3 Multi-Contractor Co-ordination

3.2.3.1 The Contractor shall be responsible for coordinating with their Sub-Contractor(s) for the provision of all services supplied by the Tenderer and their Sub-Contractor(s). Should there be any problems that affect the proper implementation of the project, the Contractor shall act as a single coordinator to work with their Sub-Contractor(s) so as to identify causes of such problems and resolve them.

3.2.3.2 The Contractor is required to oversee itself and their Sub-Contractor(s) to complete their tasks according to schedule.

3.3 Supply

3.3.1 The Contractor are to supply required hardware, software (where needed) and other materials or equipments listed in Clause 2.2 Hardware and Clause 2.3 Software & License

3.3.2 The Contractor are to supply all required hardware and software based on minimum or proposed quantity in Annex 2.1 – Hardware Specifications.

3.3.3 The Contractor are to inform the Government if there are changes on the supplied hardware and software as listed in Annex 2.1- Hardware Specifications due to the unavailability or discontinuity from manufacturer.

3.3.4 In case on product unavailability or discontinuity of production for the required items, the Contractor shall seek for product replacement with the same or higher specification than required. The Contractor shall ensure that the replacement item should work with the existing infractructure and system.

3.3.5 Any price changes due to the product replacement shall be borne by the Contractor.

3.4 Delivery

3.4.1 The Contractor shall deliver the hardware, software and other materials or equipment as stated in Annex 2.1, 2.2 to respective locations required in the project.

3.4.2 The Contractor shall conduct the delivery of the required hardware and software following the dates set out in the Implementation Plan Schedule.

3.4.3 The Contractor shall ensure the hardware, software and other materials or equipment are properly packed and secured in such manner as to enable them to reach their destination in good condition.

3.4.4 The Government reserves the right to inspect and test the hardware, software and other materials or equipment at any time on or after delivery.

3.5 Installation & Configuration

3.5.1 The Contractor are to ensure all delivered hardware are installed with the related and required drivers, software and application.

3.5.2 The Contractor are to install the required hardware and software listed in **Clause 2.1 Hardware Specifications** within the respective locations required in the project.

3.5.3 The Contractor must ensure complete hardware and software installation services, working in good condition and conduct self-test to user satisfaction.

3.5.4 The Contractor are to configure the proposed Hardware to meet the necessary requirement to ensure the system are in working condition.

3.5.5 The Contractor shall observe the following requirements during installation:

3.5.5.1 All ordinances or regulations enforced in Brunei shall be followed;

3.5.5.2 Appropriate measures shall be taken to protect the installation site and the existing facilities from damage caused by installation works; and

3.5.5.3 The Contractor shall take all necessary measures to prevent interruption to the RIPAS Hospital operations.

3.5.6 The Contractor shall inform the Government Project Team for work to be carried out during and after office hours.

3.5.7 The Contractor shall plan, manage, coordinate, design and provide the layout of the wired network infrastructure.

3.5.8 The proposed wired infrastructure must be secured, reliable and scalable for the next 10 years.

3.5.9 The Contractor shall ensure the newly setup infrastructure shall connect all users to use the services or hosted applications of MOH and EGNC shared services or applications including Internet.

3.5.10 The Contractor shall provide the necessary information required by the Government Project Team to implement the requirement in stated in this Section 2.

3.5.11 The Contractor shall perform the installation and setup services as stated below, but not limited to:

3.5.11.1 Distibution and Access Layer Switches

3.5.11.1.1 Setup and rack mounts all hardware and other materials or equipment.

3.5.11.1.2 Install, test, label, configure and commissioning of all the hardware.

3.5.11.1.3 Patch, test and commissioning the required fiber patch cords/ SFP transceivers.

3.5.11.2 Wireless Controller and Wireless Access Points

3.5.11.2.1 Setup and rack mounts the hardware and other materials or equipment.

3.5.11.2.2 Install, test, label, configure and commissioning of all the hardware.

3.5.11.2.3 Patch, test and commissioning all the UTP cables/fiber patch cord.

3.5.11.3 Exisitng E-Sight Hardware with value added features and components below:

3.5.11.3.1 Software Define Network (SDN) Management Controller

3.5.11.3.2 Intelligent Network Analysis

3.5.11.3.3 Disaster Recovery Setup (with Arbitrary Site to ensure automatic failover)

3.5.11.3.4 Relocation and Migration

3.5.11.3.5 Existing Equipment License Upgrade to use new features

3.5.11.3.6 License for new equipment

3.5.12 The Contractor shall leverage on RIPAS Hospital Proper existing racks for the allocation of hardware and other equipment.

3.5.13 The Contractor shall recommend resolution for any issues encounter and provide feedback or information to the Government in ensuring the successful implementation of this project.

3.5.14 The Contractor shall ensure that any cables required to be installed must be uniquely labelled at both ends.

3.5.15 The Contractor shall ensure that all the conduit casings are neatly secured in place and taking into account health safety and environment (HSE) compliance.

3.5.16 The Contractor shall remove all replaced and unused network equipment such as Network Switches, Wireless Controller & Access Points etc.

3.6 Testing

3.6.1 The Contractor shall prepare, plan and perform Installation Test for the hardware delivered as stated in Annex 2.1.

3.6.2 The Contractor shall prepare, plan and perform the Acceptance Testing as stated below, but not limited to:

3.6.2.1 On Site Acceptance Test for Hardware
3.6.2.2 On Site Acceptance Test for Software, if any
3.6.2.3 User Acceptance Test for Network
3.6.2.4 User Acceptance Test for Network Security

3.6.3 The detail Acceptance Testing requirement for this contract to be perform by the Contractor are stated in Clause 5.

3.7 **Commissioning**

3.7.1 The Tenderer with assigned Government representative shall conduct commissioning to ensure that the solution is properly configured, performing and working in meeting the MOH requirement.

3.7.2 The Tenderer shall conduct the commissioning based on the criteria document supplied by the Government but not limited to the requirements mentioned in **Clause 2 – Statement of Requirement**.

3.8 **Labelling**

3.8.1 The Contractor shall label the Hardware according to the formats as in **Annex 2.5 – Labelling Format** provided by Health Informatics, Department of Healthcare Technology, Ministry of Health for the purpose of asset tagging.

3.8.2 The Contractor shall label correctly from one end to another end for all the patch cords of FOC and CAT6/CAT6A.

3.8.3 The Contractor shall label correctly all the Power cords.

3.8.4 All labellings are to be tabulated in a proper manner with all the details required as per the template supplied by Department of Healthcare Technology, MOH.

3.9 **Training**

3.9.1 The Tenderer shall provide a detailed training plan and approved by the Government MOH (*Department of Healthcare Technology*) Officers.

3.9.2 The Contractor shall conduct the training to build the capabilities, abilities and skills of the end-users to appropriate and adequate levels.

3.9.3 The Contractor shall be responsible in proposing and providing end-user training for items in **Clause 2 - Statement of Requirements** above.

3.9.4 The Contractor shall provide all the necessary training equipment's and training facilities where necessary to fulfill the training requirements.

3.9.5 The Government reserves all rights to accept part or all of the training courses and the Contractor shall be required to make the necessary amendments to the training course and materials wherever necessary.

3.9.6 The Contractor shall be responsible for the arrangement and provision of well qualified and knowledgeable professional trainers in each site.

3.9.7 The Contractor shall be responsible to provide all the relevant training materials. The training materials shall be made available in either as printed materials or softcopies or as appropriate for use for the intended training participants.

3.9.8 For every course conducted by the Contractor, a complete set of up-to-date instruction guides (in hard- and soft-copies) shall be made available to the Government.

3.9.9 The Government shall have the right to use these training materials to conduct in-house courses for its personnel.

3.9.10 All training materials developed by the Contractor shall become the property of the Government of Brunei Darussalam. Master copies of training materials shall be provided to allow for reproduction, as deemed appropriate and necessary.

3.9.11 The training shall cover the network administration and end-user operation and not limited to the following:

- Distribution Switch
- Access Switch
- Network Management Controller & Ai Analyzer
- Wireless Controller/Access Point

3.10 **Warranty**

3.10.1 Product Warranty - General Requirements

3.10.1.1 The Contractor shall provide One (1) year Warranty & Five (5) Years maintenance support services for all Hardware items including product support, parts and labour of the propose hardware.

i. Replacement or repair of unserviceable parts during warranty period shall apply where any of the items covered is found to be:

a. Defective in either design, materials or workmanship; or

b. Not in accordance with the specifications; or

c. Having been installed, operated, stored and maintained in accordance with the written instructions of the Contractor, fails to function properly or fails to meet any performance requirements.

3.10.1.2 Product Warranty shall commence after official delivery and acceptance of the hardware to MOH designated premise.

3.10.2 System Warranty - General Requirements

3.10.2.1 The Contractor shall provide One (1) year Warranty & Five (5) Year Maintenance Support Services including spare parts, labour and overall health of the System after the Stabilization Period.

3.10.2.2 System Warranty shall commence after the issuance of the Final Acceptance Certificate.

3.11 **Maintenance**

3.11.1 General Requirements

3.11.1.1 The Contractor shall provide **Five (5) years** Maintenance for all hardware as shown in **Annex 2.4- Progress Schedule**.

3.11.1.2 Maintenance shall commence after the System warranty period has ended.

3.11.1.3 Maintenance shall comprise "Preventive Maintenance" and "Curative Maintenance" (as respectively defined under **Clauses** Error! Reference source not found. **and 3.11.3** below).

3.11.2 Preventive Maintenance

3.11.2.1 Preventive Maintenance shall be done quarterly for Five (5) year and shall be provided by the Contractor during Normal Working Hours which is Monday to Thursday & Saturday, from 7:45 am to 12:15 pm and 1:30 pm to 4:30 pm.

3.11.2.2 The Contractor shall perform routine inspection and testing of each hardware and software shall be in accordance with the Contractor's and manufacturer's reasonable recommendations;

3.11.2.3 The Contractor shall provide installation and testing services for software updates and patches whenever new software releases are made available.

3.11.2.4 The Contractor shall provide software update and patches materials and documentation whenever new software releases are made available;

3.11.2.5 The Contractor shall provide upgrade services of the firmware to the network equipment, where applicable and upon the Government Approval;

3.11.2.6 The Contractor shall carry out repairs, replacement of worn or marginally performing parts, cleaning, and/or adjustment(s) to each item of the Hardware as may be determined by the Contractor to be necessary as a result of the aforesaid inspection(s) and/or test(s).

3.11.3 Curative Maintenance

3.11.3.1 The Contractor shall perform adhoc or upon request Curative Maintenance Services, (by attendance onsite and remotely);

3.11.3.2 The Contractor shall assess, diagnose and repair the cause of faults and defects in all Hardware, equipment, software and configuration within the Contractor's responsibilities.

3.11.3.3 The Contractor shall bear the costs of replacement of unserviceable parts during the warranty periods.

3.11.4 Loan Hardware

3.11.4.1 The Contractor shall, at no costs provide the Government with a functionally equivalent hardware ("Loan Hardware"):

i. if, by the sixth (6th) hour after the service engineer or technician arrives at the Location, it is determined that the faulty hardware cannot be repaired within the prescribed response time; or

ii. if the Contractor determines that it is necessary to move a Hardware or part thereof ("the Removed Hardware") to the Contractor's premises in order to repair or service the Removed Hardware and as a consequence the Removed Hardware cannot be used by the Government.

3.11.4.2 Once the Removed Hardware is repaired and restored to good working order, the Contractor shall forthwith replace the Loan Hardware with the Removed Hardware, upon successful completion of the user acceptance tests.

3.11.4.3 All incidental costs including parts, transportation and labour charges incurred by the Contractor pursuant to **Clauses 3.11.4.1** and **3.11.4.2** shall be borne by the Contractor.

3.12 Support Services

3.12.1 General Requirements

3.12.1.1 The Contractor shall provide ["5 years Support Services for all hardware and software items with the possibility to extend 1 more year" or "3 years Support Services for all hardware and software items"].

3.12.1.2 The Contractor shall offer support service for all IT-related issues, including but not limited to software troubleshooting, hardware malfunctions, network connectivity problems, and user account management.

3.12.1.3 Support Services shall commence after the end of System Warranty period.

3.12.1.4 The Contractor shall provide at least two (2) Certified Support Engineer to be on-call during business operating hours & during activities that requires urgent support.

3.12.1.5 The Certified Support Engineer provided by the Contractor shall be capable to fulfil any request made by the Government relating to administrating, operating and configuring the hardware supplied.

3.12.1.6 The Contractor shall appoint a skilled customer service representative to be responsible for the overall management of the Support Services and the keeping of the hardware in good working order in accordance with the terms of this agreement.

3.12.1.7 The Contractor must provide proper Help Desk procedures to the users. These procedures must be produced in hard copy during delivery and explained to the users.

3.12.1.8 The support service shall provide monthly reports detailing support activities, including the number of tickets handled, resolution times, and any recurring issues.

3.12.2 Standard Coverage Period

3.12.2.1 For Severity Level 1, the Contractor shall provide 24/7 support, and is available through on call, email and remote access.

3.12.2.2 For Severity Level 2 and 3, the Contractor shall provide support hours from Monday to Thursday and Saturday, from 7:45 AM – 12:15 PM and 1.30 PM – 4:30 PM.

3.12.3 Incident Analysis, Resolution and Management

3.12.3.1 The Contractor shall categorise every Incident according to the following severity level:

Severity Level	Impact
1	Affects the System such that the Government is unable to perform its business functions; and/or has major security implication.
2	Affects a particular process or system for which there are acceptable alternatives for bypassing the Incident.
3	Minimal impact on the Government's ability to perform on its functions.

3.12.3.2 The Contractor shall perform a thorough analysis of the Incident and provide deliverables including but not limited to incident report, root cause analysis, incident resolution plan, post incident review and documentation of lesson learned.

3.12.4 Prescribed Response Time(s)

3.12.4.1 The Prescribed Response Time shall start from the time the Incident is communicated tothe Support Services team to the response by the Support Services team to the Incident.

3.12.4.2 The Prescribed Response Time for any reported Incidents shall be as follows:

Severity Level	Response Time
1	Within thirty (30) minutes.
2	Within one (1) hour.
3	Within two (2) hours.

3.12.5 Resolution Time(s)

3.12.5.1 The Resolution Time shall begin upon the response by the Support Services team through remote access or telephone until the Incident is resolved and the system is restored to a satisfactory working condition.

3.12.5.2 The Resolution Time for any reported Incidents shall be as follows:

Severity Level	Support Service Resolution Time
1	Within four (4) hours.
2	Within eight (8) hours.
3	Within twenty-four (24) hours.

3.12.5.3 In the event that the Support Services team cannot resolved the Incident through remote access or telephone, Curative Maintenance shall be activated.

3.12.5.4 In the event that Curative Maintenance is activated:

i. The response time for Support Services is the period commencing after the maximum resolution time has elapsed, until the time the Support Services team calls back the user to inform them on the estimated arrival of the Curative Maintenance team. The maximum response time shall be not more than thirty (30) minutes.

ii. The response time for Curative Maintenance is the time period between the Incident is escalated by Support Services team, until the time of the Curative Maintenance team's arrival to the user's location. The Curative Maintenance team to arrive on-site within one (1) hour.

iii. The Resolution Time for Curative Maintenance is the period between the time of the Curative Maintenance's arrival to the Government's designated location, until the time the Incident has been resolved. The Resolution Time for Curative Maintenance to resolve problem is within 4 hours.

iv. In the event that resolution time is exceeded four (4) hours, and the problem has not been resolved and hardware replacement is not required, the Contractor shall be penalized for every hour it has lapsed.

3.12.6 Penalty

3.12.6.1 In the event that resolution time is exceeded, and the Incident has not been resolved, the Contractor shall be penalized as follows:

Severity Level	Penalty
1	The amount of one percent (1%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per four (4) hours.
2	The amount of one tenth of a percent (0.1%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per eight (8) hours.
3	The amount of one hundredth of a percent (0.01%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per twenty-four (24) hours.

3.12.6.2 The table below shows the Severity Levelm Response Time, Resolution Time and Penalty.

Severity Level	Response Time	Resolution Time	Penalty
1	Within thirty (30) minutes.	Within four (4) hours.	The amount of one percent (1%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per four (4) hours.
2	Within one (1) hour.	Within eight (8) hours.	The amount of one tenth of a percent (0.1%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per eight (8) hours.
3	Within two (2) hours.	Within twenty-four (24) hours.	The amount of one hundredth of a percent (0.01%) (including part thereof) of the quarterly Support Service Charges or Maintenance and Support Services Charges up to a maximum of ten (10%) percent of the quarterly Maintenance and Support Services Charges, per twenty-four (24) hours.

4 DOCUMENTATION AND DELIVERABLES

4.1 General Requirements

4.1.1 The Contractor shall produce all relevant deliverables for the purpose of ensuring a successful delivery of the proposed hardware, software and related services.

4.1.2 The Contractor shall ensure all deliverables are handed over to the Government. At least two (2) printed copies and one (1) soft copy of the required deliverables in Microsoft Office document compatible format on CD-ROM shall be provided.

4.2 Hardware

4.2.1 The Contractor shall provide the documentation for all the hardware specified in **Clause 2.2 Hardware**.

4.2.2 The Contractor shall provide a documentation that list out the hardware tag of the supplied equipment following the asset tag information provided in Clause 3.3 and also listed it side by side with the info of the current firmware version, SKU information, serial number information and service/asset tag information from principle distributor where applicable.

4.3 Implementation and Related Services

4.3.1 The Contractor is required to specify and agree with the Government the target acceptance date for each documentation in the Detailed Project Workplan.

4.3.2 The Contractor shall be responsible for having the drafted documentation ready in advance of the target acceptance date, allowing sufficient time for review by Government representative and any subsequent revisions required.

4.3.3 The required deliverables under Implementation and Related Services are as follows:

Table 1 - Deliverables for Implementation and Related Service

Implementation and Related Services	**Documentation and Deliverables**
Contract Signing	Contract
Project Management	Detailed Project Workplan Project Progress Reports Project Handover Report Stakeholder Register & Communication Plan Commisioning and Acceptance Report Project Risk Management Plan High- Level Training Strategy
Project Design	System Architecture Design (SAD) Detailed Design Specification (DDS) Interface Control Document (ICD) Test Strategy & Master Test Plan Hardware Specification Document Software License Certificates/Keys Detailed Migration Plan System and Integration Test Plan Project issue log
Supply and Delivery	Proof of Delivery of Hardware and On Site Acceptance Sign-off Proof of Delivery of Software licenses/Subscriptions and On Site Acceptance Sign-off Hardware and Software Inventory Document Hardware Procurement & Delivery Report
Installation and Configuration	Design Document Installation Documentation Installation Verification Results Network Administration and Operation Guide Physical and Logical Design Architecture Network Infrastructure Floor Layout Plan Configuration Document, included with Network Mapping and Allocation Hardware Asset Tag document Hardware Specification Document Software License Certificates/Keys Hardware Maintenance and Support Documentation Hardware Warranty Commencement Notification Technical Design Documentation
Testing	Fixes report (for Security Assessment) Pre-Migration, Process Migration and Post-Migration Testing Document User Acceptance Test (UAT) Documentation including: ▪ UAT Plan and Specifications

Table 1 - Deliverables for Implementation and Related Service

Implementation and Related Services	Documentation and Deliverables
	▪ UAT Test Results (included with issues/problem raised and recommended resolution) ▪ Performance Test Plan and Specification ▪ Performance Test Results ▪ Update Access Credential Lists ▪ User Acceptancce Test Certificates
Training	Training Materials Training Session Delivery & Attendance Records Training Completion Report Operation Procedure Run Book/Service Operating Procedure (SOP) Knowledge Transfer & Material Network and Harware Administration and Operation Guide Troubleshooting Manual
Go-Live & Commisioning	System Commissioning Plan Go-Live Plan and Cutover Procedures Operational Readiness Report System Commission Plan Production Data Migration Execution Report Performance Monitoring Reports Commissioning Completion Report
Stabilization	Weekly Stabilization report Rapid Incident Management Report Production Data Integrity Post-Go-Live Verification Report Root Cause Analysis Report Updated System Documentation Updated Standard Operating Procedures (SOPs) Stabilization Final Report & Consolidated Issue Log Final Acceptance Certificate System Warranty Commencement Notification Final Documentation Project Closure report
Warranty	Warranty Support Contact Information & Escalation Matric Quarter Warranty Period Status Report Manufacturer Hardware Warranty Documentation
Maintenance & Support Service	Service Operation Manual

Table 1 - Deliverables for Implementation and Related Service

Implementation and Related Services	Documentation and Deliverables
	Quarterly Preventive Maintenance Report Monthly Incident and Problem Resolution Reports (Adhoc) Incident/Defect Log System Health Check & Performance Reports Security Patching & Vulnerability Scan Reports Release Notes for Maintenance Releases Annual Service Review Meeting

5 ACCEPTANCE TESTING

5.1 User Acceptance Tests

5.1.1 Prior to conducting acceptance test, the Contractor together with the Government representative shall complete the on-site acceptance of the hardware delivered before the Delivery Order is signed by the Government representative.

5.1.2 The Contractor shall propose "Acceptance Tests" as stated in Clause 3.6 and the testing approaches to test and ensure the following:

- i. Functional testing - to check for basic connectivity, interface configuration , routing and switching function and wireless testing etc
- ii. Security Configuration: user authentication and device hardening etc
- iii. Network service integration - DNS, NTP and monitoring tools etc
- iv. Performance testing - throughput, latency, failover and redundancy
- v. Management and monitoring - test access via management tools etc

5.1.3 The Acceptance Tests shall consist of the following tests.

- i. System Tests
  - a. System Tests shall run in the testing environment and includes (i) Product Test and (ii) Integration Test.
  - b. Product Test - Product Test shall be performed on the proposed System to demonstrate that all functional aspects of the Specifications are met.
  - c. Integration Test - Integration Test shall be performed on the proposed System to verify the functions and performance of the System's integration among different modules, and interfaces with other external systems running on relevant infrastructure.
- ii. Function Tests
  - a. Function Tests shall run in the production environment and includes (i) User Acceptance Test and (ii) Exception Test.
  - b. User Acceptance Tests - User Acceptance Test is the process of verifying the proposed System and the business processes against user requirements. The objective is to determine whether the System and the processes are acceptable to its users.
  - c. Exception Test - Exception Test is to verify that the System shall not behave abnormally under exceptional cases.
- iii. Performance Tests
  - a. Performance Tests shall run in the to be production environment and includes (i) Load Test and (ii) Stress Test.
  - b. Load Test - Load Test is to test the System with high volumes of data. The objective is to determine whether the System can handle the volume of data specified in its objective.
  - c. Stress Test - Stress Test is to test the System with heavy loads or stress (e.g. large numbers of users and jobs). A heavy stress is to test the System with abnormal situations by executing it in a manner that demands resources in extremely large/high quantity, frequency, or volume. The Contractor shall propose the benchmarks for the test for the Government Representative's consideration and agreement, prior to the commencement of the test.
- iv. Reliability Tests
  - a. Reliability Test shall run in the production environment by the Government using its data, in accordance with the requirements and criteria set out in Requirements **Section 3: Tender Schedules, Schedule 14: Acceptance Tests**.
- v. Security Assessment
  - a. Security Assessment shall be carried out by 3rd party vendor. Tenderers shall refer to **Clause 3.2.11: Security Assessment.**
  - b. Vulnerability and Penetration Tests shall run in the production environment by the Government using its data, in accordance with the requirements and criteria set out in Requirements **Section 3: Tender Schedules, Schedule 14: Acceptance Tests**.

vi. Migration Testing

a. Migration Tests shall run in the production environment by the Government using its data, in accordance with the requirements and criteria set out in Requirements **Section 3: Tender Schedules, Schedule 14: Acceptance Tests**.

b. Migration testing activities shall includes best practice pre-migration testing, migration process testing, post-migration testing and other necessary testing for migration (hardware/software/data) that shall be conductd to ensure the upgrade and proposed solution are working effectively and security posture and regulatory compliance is maintained.

c. The Migration Testing activities shall includes but not limited to:

- *Pre-Migration Testing***:** to validate readiness of infrastructure, components, and configurations before live migration.

Test Type	**Description**
Environment Verification Testing	Ensure hardware, OS, and software versions for SDN Controller and Ai Analyzer are properly installed and configured.
License Validation	Confirm that licenses for existing devices are correctly upgraded and will remain valid post-migration.
Connectivity Testing (Southbound)	Verify southbound communication between eSight instances and the SDN Controller.
Prerequisite Check	Validate all dependencies, configuration files, and system compatibility (e.g., NTP, DNS, firewall rules).

- *Migration Process Testing*: to Ensure migration steps (synchronization and transitions) occur without data loss or functional degradation.

Test Type	**Description**
Synchronization Integrity Test	Verify that all devices, configurations, alarms, and performance data are correctly synchronized from eSight to the SDN Controller.
Data Mapping Validation	Ensure all device data (e.g., IP addresses, topology, configurations) is accurately represented in the new system.
Incremental Sync Testing	Test whether real-time or scheduled changes in eSight are captured and reflected during migration.
Performance Benchmarking	Measure and compare key performance metrics (e.g., latency, response time) before and after synchronization.

- *Post-Migration Testing*: Confirm that the new system (SDN Controller and Ai Analyzer) is functioning as expected.

Test Type	**Description**
Device Management Test	Ensure all devices previously managed by eSight are now fully manageable from the SDN Controller.
Northbound & Southbound Interface Test	Confirm proper communication between the SDN Controller, Ai Analyzer, and any connected upstream systems.
Service Functionality Test	Validate all value-added features such as AI-driven insights, analytics, and automation workflows.
Alarms and Monitoring Test	Ensure that alerting, fault detection, and system health monitoring are operational and accurate.
User Access and Roles Test	Verify that user accounts, roles, and permissions are correctly migrated and function properly.

5.1.4 The user acceptance test approach must be approved by the Government Representative, at least one (1) week prior to the carrying out of the acceptance tests. If in the reasonable opinion of the Government representative such specification does not provide sufficient details to test all the functions and facilities, the Contractor shall make the amendments as requested by the Government representative.

5.1.5 The Contractor shall complete successful acceptance tests as specified in Clause 5.1.2. The tests must be conducted in the presence of Government representative. If the acceptance tests are not successfully completed, the Government representative may call for a retest, which shall be at the expense of the Contractor.

5.1.6 The Contractor shall provide all labour, materials, transportation and documentation to complete all acceptance tests.

5.1.7 The Contractor shall prepare the **Acceptance Certificate and two (2) copies of a Test Report** as soon as possible after the completion of each test. Government representative shall countersign the Test Report and Acceptance Certificate to indicate his agreement.

6 PROJECT PAYMENT

6.1 General Requirements

6.1.1 Payment milestones are given in **Annex 2.3 Payment Milestones**.

6.1.2 The implementation progress schedule is given in **Annex 2.4 Progress Schedule**.

6.1.3 Payment to the Contractor will be made locally and in **Brunei Dollars**.

6.2 Payment Claims

6.2.1 Payment claim for Detailed Project Workplan by the Contractor to the Government shall be accompanied by the Contractor's invoice and the Detailed Project Workplan.

6.2.2 All payment claims for delivery of hardware and software by the Contractor to the Government shall be accompanied by the Contractor invoice, Acceptance Certificate and delivery order, describing, as appropriate, the goods delivered and related services performed.

6.2.3 All payment claims for installation and user acceptance tests by the Contractor to the Government should be accompanied by the Contractor invoice, Acceptance Certificate and Test Reports.

6.2.4 All payment claims for the support services shall be made monthly with the attachment of Contractor invoice and service reports.

ANNEX 2.1 – HARDWARE SPECIFICATIONS

Item	Hardware	Quantity (Unit)	Compliance (Y/N)
1	**Distribution Switch**		
1.1	**48 Port Fiber Switches** *Technical Specifications:* *(Please state Y/N at Compliance)* 48*10GE SFP+ ports, 6*40GE QSFP28 ports, optional license for upgrade to 6*100GE QSFP28 -Switching capacity: 2.16Tbps/2.4Tbps -Forwarding performance: 490 Mpps -600W AC Power Module (Back to Front, Power panel side exhaust) -Dual pluggable power modules, 1+1 power backup -Deployed by SDN controller network automation and optimized by AI analyzer. *Features/Requirement (please state Y/N):* 1. Supports Netconf & Telemetery 2. The proposed shall able to be managed by existing Network Management System (eSight) / iMaster NCE-Campus & CampusInsight 3. Supports 4094 Vlans 4. Supports MPLS and VXLAN 5. Supports the following layer 3 functions: Static routes, RIP v1/2 and RIPng, OSPF and OSPFv3, IS-IS and IS-ISv6, BGP and BGP4+, MLDv1/v2 snooping, IGMPv1/v2/v3 snooping, IGMPv1/v2/v3, PIM-SM, and PIM-SSM, MSDP, Multicast VPN 6. Supports the following QoS/ACL functions: Rate limiting for incoming and outgoing packets on an interface, 802.1p and DSCP priority re-marking, Packet redirection, Layer 2 to Layer 4 packet filtering, Queue-based rate limiting and traffic shaping on an interface 7. Supports the following DHCP functions: DHCP client, DHCP relay, DHCP server, DHCP snooping 8. Support Four fan modules 9. The independent blue ID indicator commonly used in the industry is used to quickly locate devices in the equipment room. 10. The device provides one independent PNP button (which can reset the device and restore the factory settings): a. To commission and reset the device, you need to remove and install the power modules. You can press the button to reset the device. b. If you forget the password, you can press the button to restore the factory settings. 11. ≥ 384K MAC address entries 12. ≥ 256K IPv4 routing entries 13. ≥ 80K IPv6 routing entries 14. VXLAN, BGP EVPN, and distributed anycast gateways; VXLAN fabric configuration on the controller web page and delivery to switches. An authoritative third-party test report is provided.	4	

	15. G.8032 (ERPS) standard Ethernet ring protocol. The switchover time upon fault occurrence is less than 50 ms. 16. Segment routing based on the IPv6 forwarding plane 17. Horizontal stacking, number of stacked hosts ≥ 9 18. ETH OAM, 802.1ag, 802.3ah, and Y.1731 19. Hardware-based BFD/OAM is supported to ensure stable transmission of detection packets at an interval of 3.3 ms, improving device reliability. An authoritative third-party test report is provided. 20. Multi chassis Link Aggregation Group (M-LAG) is supported to allow devices to be deployed and upgraded separately. The service interruption time during the upgrade is less than 1s. 21. ≥ 16,000 VXLAN IPv4 tunnels 22. UCL-based user group mode is supported. Users in a user group have the same access rights regardless of whether they are wired or wireless users, where they log in, and which IP address they obtain. An authoritative third-party test report is provided. 23. The Telemetry technology is supported to collect device data in real time and send the data to the network analysis component platform. The intelligent fault identification algorithm is used to analyze network data, accurately display the real-time network status, demarcate faults and fault causes in a timely manner, and accurately ensure user experience. 24. iPCA2.0 is supported to detect network quality based on real flows.		
1.2	**Hi-Care/Co-Care Services-Helpdesk Support, Spare part Management, Maintenance**		
	i. Five (5) years	4	
1.3	**N1-Advanced License (Perpetual Usage + 5 Years SnS)**		
	i. Perpetual (Usage)	4	
	ii. Five (5) years (SnS)		
2	**Access Switch**		
2.1	**48 Port Access Switch (POE)** *Technical Specifications:* *(Please state Y/N at Compliance)* 48*10/100/1000BASE-T ports, 4*10GE SFP+ ports, 2*12GE stack ports, PoE+ -Switching capacity: 224 Gbps/520 Gbps -Forwarding performance: 168 Mpps -1000W AC Power Module (Back to Front, Power panel side exhaust) -3 power supplies, N+1 power supply backup -Deployed by SDN controller network automation and optimized by AI analyzer. *Features/Requirement (please state Y/N):* 1. The proposed shall able to be managed by existing NMS(eSight) / iMaster NCE-Campus & CampusInsight 2. Supports Netconf & Telemetery 3. Supports -5°C to +50°C operating temperature 4. Supports -40°C to +70°C storage temperature 5. Supports a relative humidity of 5% to 95% (non-condensing) 6. Supports 4094 Vlans	65	

	7. Supports the following layer 3 functions: Static routes, RIP v1/2 and RIPng, OSPF and OSPFv3, IS-IS and IS-ISv6, BGP and BGP4+, MLDv1/v2 snooping, IGMPv1/v2/v3 snooping, IGMPv1/v2/v3, PIM-SM, and PIM-SSM, MSDP, Multicast VPN 8. Supports the following QoS/ACL functions: Rate limiting for incoming and outgoing packets on an interface, 802.1p and DSCP priority re-marking, Packet redirection, Layer 2 to Layer 4 packet filtering, Queue-based rate limiting and traffic shaping on an interface 9. Supports the following DHCP functions: DHCP client, DHCP relay, DHCP server, DHCP snooping 10. The independent blue ID indicator commonly used in the industry is used to quickly locate devices in the equipment room. 11. The device provides one independent PNP button (which can reset the device and restore the factory settings): a. To commission and reset the device, you need to remove and install the power modules. You can press the button to reset the device. b. If you forget the password, you can press the button to restore the factory settings. 12. The actual power supply PoE capacity ensures that in the event of any single power supply failure, it can still provide 1440W of PoE power output. 13. The proposed switch must support ≥ 32K MAC address entries 14. The proposed switch must support ≥ 8K IPv4 routing entries 15. The proposed switch must support ≥ 3K IPv6 routing entries 16. The proposed switch must support maximum number of IPv4 ACL entries supported at the device ingress: ≥ 2000 17. The proposed switch must support maximum number of IPv4 ACL entries supported at the device egress: ≥ 2000 18. The proposed switch must support VLAN slicing, providing multiple logical networks (slices) on the same shared network infrastructure. Each slice serves a specific service type or industry user, and can flexibly define its logical topology, SLA requirements, reliability, and security level to meet differentiated requirements of different services, industries, or users. 19. The proposed switch must support ETH OAM, 802.1ag, 802.3ah, Y.1731, and BFD 20. The proposed switch must support dedicated stack ports and plug-and-play stack cables, free of configuration 21. The proposed switch must support 16,512 MAC entries 22. The proposed switch must support 4K VLANs 23. The proposed switch must support STP (IEEE 802.1d), RSTP (IEEE 802.1w), and MSTP (IEEE 802.1s) 24. The proposed switch must support Up to 8,192 FIBv4 entries 25. The proposed switch must support Up to 3,072 FIBv6 entries 26. The proposed switch must support 3,072 ND entries 27. The proposed switch must support Packet filtering at Layer 2 to Layer 4, filtering out invalid frames based on the source MAC address, destination MAC address,		

	source IP address, destination IP address, TCP/UDP port number, protocol type, and VLAN ID 28. The proposed switch must support Network-wide E2E quality detection, in-band flow measurement, and fault demarcation for services		
2.2	**Hi-Care/Co-Care Services-Helpdesk Support, Spare part Management, Maintenance**		
	i. Five (5) years	65	
2.3	**N1-Advanced License (Perpetual Usage + 5 Years SnS)**		
	i. Perpetual (Usage)	65	
	ii. Five (5) years (SnS)		
3	**Software Defined Network (SDN) Controller**		
3.1	**SDN Network Automation** *Technical Specifications:* *(Please state Y/N at Compliance)* *TaiShan 200 (Model 2280) 128G Standard Configuration Outside(2*Kunpeng 920-32Core@2.6GHz CPU,4*32G Memory,4*1920GB SSD,Raid(2G cache)+SuperCap,2*4 GE+3*2 25GE SFP28,2*900W AC,Rail) includes Euler OS + Software* *Features/Requirement (please state Y/N):* 1. Equivalent to iMaster NCE-Campus HW 2. The proposed controller must support remote disaster recovery deployment. When the main system fails, it automatically switches to the remote backup system. 3. The proposed controller must support a single software suite for managing wired and wireless devices within a single campus, as well as multiple branch campuses and wide-area networks, and it also features the capability to configure security policies. 4. The proposed controller must support single-node deployment and features automated initialization, user authentication, user group policy definition, unified virtual network management, and big data intelligent analysis for operation and maintenance. 5. The proposed controller must support graphical, drag-and-drop definition of configuration templates, flexible definition of variables, and batch creation of network services. 6. The proposed controller must support user-defined scenario workflows and batch execution of service deployment tasks. Tasks can be retried or rolled back. 7. The proposed controller must support self-developed or third-party network planning tools. You can import network planning files and view the wireless layout on the platform. 8. The proposed controller must support multiple plug-and-play technologies (such as DHCP Option, scanning, email setup, etc.) for concurrent device registration and online access. ESN collection is automated, eliminating the need for command-line, configuration file, and script operations, improving deployment efficiency. Supports device setup using non-VLAN1. 9. The proposed controller must support provide multiple configuration templates to enable batch configuration capabilities. The templates support hierarchical configuration, where subordinate templates can inherit	1	

	common configurations from superior templates, while also allowing for custom personalized configurations. 10. The proposed controller must support pure Layer 2 VXLAN virtual networks without a gateway. 11. The proposed controller must support the construction of a Fabric network through a wizard, enabling automated network configuration over VxLAN in the Overlay. It also supports automatic re-orchestration of Underlay/Overlay triggered by link changes. 12. The proposed controller must support automated configuration for single virtual network with multiple exit points, and be capable of networking with no fewer than 8 independent exit device groups. It should also support automated configuration for both primary/backup mode and load-sharing mode among exit devices. 13. The proposed controller must support in a scenario where multiple access switches exist under the Edge layer, each edge switch distinguishes the authorization of the downstream port, thereby distinguishing the permission management of each access terminal. 14. SD-WAN supports automated business operations for multi-Hub point (≥16) networking, enabling proximity access and load balancing. 15. The proposed controller must support 5G SIM card slots for compatible devices and enables 5G as a backup link (IPv4/IPv6), meeting the needs for internal enterprise connectivity and internet access. 16. The proposed controller must support link quality sensing technology based on in-band detection without generating additional detection packets. Supports SD-WAN solutions based on IPv6/SRv6. 17. The proposed controller must support QoS that meets multi-department bandwidth allocation requirements, as well as dynamic QoS bandwidth allocation and speed limiting between HUB and multiple SPOKE. 18. The proposed controller must support intelligent multi-link selection. It can use packet loss and latency based on links and applications as indicators for link switching; supports using link load as an indicator for link switching. 19. The proposed controller must support a network-wide traffic recommendation strategy for site traffic allocation, recommending the optimal QoS solution to achieve the best load balancing and communication quality. 20. The proposed controller must support application-based multi-path packet replication technology; capable of simultaneous transmission over wired, wireless, and other links. 21. The proposed controller must support Adaptive Forward Error Correction (A-FEC) functionality, capable of real-time detection of application packet loss. In scenarios where the link packet loss rate reaches 30%, it supports packet loss recovery through redundant packet technology, ensuring a lossless experience for services. 22. The proposed controller must support identification of no fewer than 6,000 applications and enables online upgrades for the application library. Provides support for custom application methods. 23. The proposed controller must support self-registration for visitors, with options for no approval, administrator approval, or approval by the host through a mobile		

	terminal for visitor access authentication. Includes at least 5 default Portal pages. The pages support multiple built-in languages including Chinese, English, German, Spanish, and more. 24. The proposed controller must support remote camera reboot through the switch's POE port management. 25. The proposed controller must support the definition of VIP user priority access to the network through air interface scheduling policies, with dedicated bandwidth allocation. When there are no VIP user traffic, non-VIP users can also utilize the full bandwidth. 26. The proposed controller must support HQOS traffic scheduling based on dual conditions of user + application, ensuring experience guarantees for VIP users' critical applications such as video and voice. 27. The proposed controller must support application traffic visibility based on in-stream detection, utilizing per-packet coloring technology to accurately detect application quality parameters such as latency, packet loss, and jitter. It can also be applied to application path visualization, fault localization, and rapid closed-loop network issue resolution. 28. The proposed controller must support displaying the network dashboard across three layers: network, application, and user/terminal. The dashboard is interactive and configurable. It allows for drilling down from GIS to site topology and individual device details. Additionally, it provides comprehensive path visualization capabilities for network faults, user journeys, and application quality. 29. The proposed controller must support device configuration and table item comparison functions. Enables viewing the connectivity status of IP subnets across the entire network and allows GUI-based verification of network connectivity between any subnets. Facilitates simulation and verification of terminal access connectivity, quickly confirming whether terminal access permissions meet expectations. 30. The proposed controller must support packet capture on device ports through the controller interface, and enables remote retrieval of device logs via the web interface for rapid troubleshooting and issue resolution. 31. The proposed controller management page supports dynamic/static IP address management and can intuitively display the status of IP addresses, such as available, unavailable, and occupied. 32. The proposed controller must support three-tier management model and multi-tenant management, enabling service providers (MSPs) to manage and build tenant networks on their behalf and reallocate software-licensed resource pools, ensuring complete resource isolation between different tenants. 33. The proposed controller must support LAN-WAN end-to-end quality visualization, capable of distinguishing and presenting multi-dimensional information such as network, user/terminal, and application. It achieves precise application quality, user journey, user communication quality display, and fault localization. It supports the retrospective analysis of historical moments. It also supports the automatic generation of key		

	application assurance strategies and the automatic distribution of these strategies across the entire network, enabling rapid optimization of application experience. 34. The proposed controller shall enable administrators to import and automatically generate physical topologies, displaying the status of devices, ports, and links within the topology. 35. The proposed controller shall provide support for underlay network automation across various networking solutions, including Layer 2, Layer 3, Layer 4, or Layer 5 forwarding, and ring networking. 36. The proposed controller shall facilitate scenario-specific network construction through templates. It will have the capability to directly generate network topologies, network and service configurations, and replicate these topologies and configurations across different sites. 37. The proposed controller shall have the capability to automatically stack up to nine switches and showcase the stack members within the physical topology. 38. The proposed controller shall support function configuration through radio profiles. These functions encompass planning and automated configuration of 2.4 GHz and 5 GHz radios, Wi-Fi multimedia (WMM), smart roaming, configuring access terminal threshold, and implementing automated radio calibration policies. Upon a WAP going online, it can directly receive configurations and policies from the controller, enabling immediate provision of Wi-Fi service. 39. The Participating Vendor of the proposed switch shall engage principal subject matter expert (SME) to be present in the requirement gathering sessions, deployment and project commissioning with project team. 40. The proposed controller shall have the capability to identify rogue Wireless Access Points (WAPs) and terminals in either Wireless Intrusion Detection System (WIDS) or Wireless Intrusion Prevention System (WIPS) mode. It will enforce logouts, gather statistics, defend against potential attacks, and suppress wireless storms. 41. The proposed controller shall offer support for air interface-based scheduling to prioritize VIP users' access to the network. 42. The proposed controller shall support both centralized and distributed gateway solutions. 43. The proposed controller shall extend support for overlay network construction using OSPF and enable the on-demand deployment of VXLAN networks through BGP EVPN if applicable. 44. The proposed controller shall offer wizard-based fabric network construction and automated network configuration using VXLAN within the overlay network if applicable. Additionally, it will provide automated re-orchestration of underlay and overlay networks, triggered by link changes. 45. The proposed controller shall be capable of implementing local forwarding and tunnel forwarding for Wireless Access Points (WAPs) using wired and wireless convergence technology provided by switches. 46. The proposed controller shall offer support for the local creation of departments, accounts, and roles. These department accounts will align with the existing ones of		

	the customer. Users will have the flexibility to be bound to multiple roles, allowing for the customization of network admission authentication policies based on department, account, and role. 47. The proposed controller shall have the capability to synchronize with multiple AD or LDAP domain name servers, map account attributes to local roles, and execute network admission authorization based on these assigned roles. 48. The proposed controller shall provide support for various authentication technologies, including 802.1X authentication, MAC address authentication, Portal authentication based on HTTP/2 along with VPN authentication. These authentication protocols encompass PAP, CHAP, EAP-MD5, EAP-PEAP-MSCHAPV2, EAP-TLS, EAP-TTLS-PAP, and EAP-PEAP-GTC. 49. At the first authentication, the proposed controller shall automatically bind multiple network attributes for network admission authentication to restrict users' access behavior. These attributes include the IP or MAC address of a user authentication device, IMSI or ESN of a SIM or USIM card, as well as the IP address, access VLAN ID, and access port number of an access device. 50. The proposed controller shall possess the capability to authorize and manage network access policies based on numerous network attributes, such as the user, user group, role, access location, device group, access time, and access mode. Additionally, the controller can utilize customized standard RADIUS attributes as authorization parameters and manage the priorities of multiple authorization policies. 51. The proposed controller shall utilize various network attributes as results for network admission authorization. These attributes encompass VLAN, ACL (Access Control List), dynamic ACL, security group, VIP user status, redirection URL, uplink and downlink bandwidth, and customized RADIUS attributes. 52. The proposed controller shall provide support for different authentication methods, including one-time Portal authentication, MAC address-prioritized Portal authentication based on Layer 2 links, and Boarding tool-based 802.1X authentication. 53. The proposed controller shall offer support for the authentication escape function. In scenarios where an authentication device fails to detect any response from the authentication server, the device will allow users to access the network initially. 54. The proposed controller shall enable users logging in to a device via Telnet or SSH to undergo forced authentication by the TACACS server. Policies for authentication matching may include the user group, account, role, access device group, terminal IP address range, and time range. Furthermore, the authorization results may involve the command set and command template. 55. Authentication and authorization logs, along with user login and logout activities, will be logged and recorded by the proposed controller.		

	56. The proposed controller shall support two-factor TACACS authentication for enhanced security during the authentication process. 57. The proposed controller will offer support for a variety of identification technologies, including User-Agent, DHCP Option, MAC OUI, mDNS, LLDP, SNMP, and NMAP, enabling precise identification of the operating systems, vendors, and models of access terminals. Additionally, customizable terminal identification rules will be available. 58. The proposed controller shall facilitate the automatic or manual grouping of terminals based on terminal type or operating system. These terminal groups can then be used as conditions for network admission authorization. Upon a terminal's network access, it will be automatically authenticated and associated with a specific device type. 59. The proposed controller shall feature an access anti-spoofing function. If the type of terminal bound to a port changes, the system will generate an automatic alarm and enforce traffic blocking from unauthorized terminals according to pre-defined policies. 60. The proposed controller shall enable free mobility for users, dissociating them from specific IP addresses. Security groups will be authorized based on user login conditions using the "5W1H" (Who, What, When, Where, Why, How) method. The UCL (User Capability List) policy matrix will be utilized to limit users' mutual access rights, ensuring consistent access to network services regardless of the location and time. 61. The proposed controller shall provide support for page customization, push services, self-service guest registration, administrator-approved guest admission authentication, and end-to-end guest account management throughout their lifecycle. 62. The proposed controller will allow administrators to conduct region-based management. Multiple guest administrators can be configured within the system to oversee and approve guest self-registration applications in each respective region. 63. The proposed controller will provide support for various authentication methods, including user name and password authentication, Passcode authentication, SMS authentication, two-factor authentication, anonymous authentication, and social media authentication (e.g., Facebook, Twitter). 64. The proposed controller shall offer a WYSIWYG (What You See Is What You Get) Portal editor for page customization. Administrators will have the ability to customize Portal pages by adding or adjusting various controls, such as title, image, text, carousel, dial-up, video, background, language, and Boarding controls. Authentication controls will include user name and password, SMS, anonymous, social media, Passcode, two-factor, and public QR code authentication controls. Furthermore, customization using HTML scripts will be supported. 65. The proposed controller shall have the capability to push different Portal pages based on specific conditions, such as device type, SSID, time, and the operating system of the terminal.		

	66. The proposed controller will allow for the limitation of online duration or traffic speed for a terminal in various authentication scenarios such as 802.1X authentication, and MAC address authentication. If the online duration or traffic speed of a terminal exceeds the preset threshold, the terminal will be forcibly disconnected. 67. The proposed controller shall support intermittent port disconnection and user reauthentication, providing the capability to periodically disconnect ports and prompt users for reauthentication. 68. The proposed controller will offer agile reporting functionalities for terminal identification, displaying icons categorized by vendor, operating system, and device type. Administrators will receive various types of reports, including scheduled reports, periodic reports, and real-time reports, for monitoring and analysis purposes. 69. The proposed controller shall provide support for HQoS (Hierarchical Quality of Service) scheduling based on users and applications, ensuring a quality experience for mission-critical applications, particularly for VIP users' audio and video applications. 70. The proposed controller shall gather wireless access data of users categorized by tenant sites, allowing identification of the ratio of passers-by, guests, and regular access users. It will also capture user access duration and the repeated access rate of guests. 71. The proposed controller will be capable of displaying information about users who have passed Portal authentication, including details such as user name, user group, authentication mode, access policy, access SSID, terminal MAC address, terminal IP address, login time, and site. Additionally, it will offer the functionality to export online user information. 72. The proposed controller will offer a default scenario-based dashboard for simplifying Operations and Maintenance (O&M) procedures. Customers will have the flexibility to customize dashboards according to their specific O&M requirements. Additionally, the controller will support orchestration of common data sources and perform correlative data analysis. The generated analysis reports can be periodically exported in Word, PDF, or CSV formats. 73. The proposed controller shall monitor the overall health, device status, mesh link status, radio frequency information, and topology of each site. Real-time monitoring based on indoor and outdoor maps will be conducted to track and manage the sites effectively. 74. The proposed controller will monitor the network status and display collected statistics, including network traffic statistics, traffic rates, top N device traffic, top N SSID traffic, and the number of online users, providing comprehensive insights into network performance and usage. 75. The proposed controller will present the list of WAP radios at a site, gather statistics on RF channel utilization, RF interference rate, and RF noise, and exhibit the RF trend over the past 24 hours. This information aids in monitoring and optimizing the radio frequency environment. 76. The proposed controller shall facilitate DPI-based (Deep Packet Inspection) application identification on APs and		

	firewalls. It will collect statistics on the traffic volume and usage of each application categorized by time segment, tenant, device, and site. Additionally, it will support online DPI database upgrades and perform analysis of site traffic based on applications. 77. The proposed controller will support device upgrades, either for a single device or in batches. It allows for the creation of offline upgrade tasks and automatic device upgrades upon going online. Particularly, devices can be upgraded in batches using a time template, and patch upgrades can be executed without requiring a device restart, ensuring smoother upgrade processes. 78. The proposed controller will support cloud-based device Performance Management and Improvement (PMI), enabling network-wide online health monitoring and PMI implementation. It will offer professional rectification suggestions based on the O&M industry's expert library to ensure healthy network operations. Additionally, the controller can generate PMI reports and automatically send them to administrators for review and action. 79. The proposed controller will support Command Line Interface (CLI)-based remote control, allowing administrators to control indicator blinking and device restarts. It will facilitate remote control of ping tests for devices and radios, traceroute tests, and virtual cable tests to locate faults remotely and in real time. 80. The proposed controller shall support unified Operations & Maintenance (O&M) and provide various diagnosis tools to aid administrators in identifying the root causes of network exceptions. Basic network diagnosis tools include ping, traceroute, and remote information collection. Furthermore, application quality diagnosis will involve detecting AQM (Active Queue Management), delay, and packet loss rates of TCP applications.		
3.2	**Hi-Care/Co-Care Services-Helpdesk Support, Spare part Management, Maintenance**		
	i. Five (5) years	1	
4	**Artificial Intelligence (AI) Analyzer**		
4.1	**Network Automation AI Analyzer** *Technical Specifications:* *(Please state Y/N at Compliance)* *TaiShan 200 (Model 2280) Standard Configuration Outside(2*48Core/2.6GHz CPU,8*32GB Mem,8*1920GB SSD,Raid(2G cache)+SuperCap,2*4GE+2*2 25GE,2*900W PS,Guide rail)* *Features/Requirement (please state Y/N):* 1. Equivalent to iMaster NCE-CampusInsight HW 2. Supports real-time monitoring of packet loss and latency in the network based on application/stream configuration using iPCA2.0/iFIT. 3. Supports 80% wireless fault self-healing loops for 25 subcategories across 7 major categories in university scenarios such as dormitories and classrooms (including wireless coverage, interference, high channel utilization, air interface congestion, roaming, etc.). 4. Supports natural language interaction for metric queries	1	

	and troubleshooting, where metric queries include basic device information, network element metrics, user lists, wireless health metrics, energy consumption information, and application metrics. Troubleshooting includes network issue inquiries, user and application troubleshooting, and supports 4 cards with 2 concurrent sessions. 5. Support for CSI personnel presence detection, utilizing CSI to sense whether there are people under the AP. If no one is present, it will display an unoccupied result, serving as a reference for building control and energy saving. Support periodic push of personnel status through the northbound interface, providing API interfaces for customer building management systems to call. 6. Full-channel state monitoring, interference source detection 7. Based on user experience evaluation and proactive VIP issue notifications, it supports displaying user locations separately in both spatial views and device topology views. 8. Support VIP user event bubbling through user experience ratings, with proactive alerts via email/SMS/WeChat. 9. Support viewing the entire journey of wireless user access (access, internet experience, roaming, applications), as well as the entire journey of wired user access (access, traffic, applications). 10. Supports automatic analysis of wireless user experience, intelligently identifies metrics affecting user quality, and provides root cause analysis. 11. Supports the presentation of protocol-level processes across the three stages of association, authentication, and DHCP based on all user accesses, providing detailed analysis of issues in the user access process, as well as root cause analysis and troubleshooting recommendations for user access failures. 12. Based on application network experience event push, application flow path reconstruction, and support for per-flow analysis. 13. Supports integrated analysis of LAN and WAN applications, with DPI and custom rule-based application recognition, covering mainstream applications and enterprise private applications. 14. Application fault localization utilizes the IPCA3.0 in-band technology to present application paths and locate application faults. It supports in-band detection on the egress AR and introduces fault detection for audio and video over the air interface. 15. Full-stack support for IPv6 in business areas such as device management, southbound integration, installation, upgrades, and capacity expansion, as well as in management areas. 16. Supports automatic switchover (third-party site arbitration) and manual switchover for remote disaster recovery deployment. 17. Provide Kafka and RESTful API northbound interfaces. 18. Multi-dimensional network status visualization and user experience awareness throughout the journey. ▪ Displays multi-dimensional data statistics views based on different levels and regions. ▪ Supports user-defined views and displays key network and user statistics in large-screen carousel mode.		

	▪ Displays issues about network access, network congestion, device status, and error packets from the perspective of buildings. ▪ Searches users from the perspective of buildings and displays information about buildings that users passed by in a specified period of time. ▪ Allows administrators to import topology views and plan AP locations to view fault location distribution. ▪ Automatically discovers the physical network topology, displays network information in a topology view, and monitors the entire network in real time. ▪ Displays the radio heatmap by AP location. ▪ Allows administrators to import network planning data to be compared with the actual network running data, displaying the differences between them. ▪ Supports device profiles and allows administrators to view the health status of switches, APs, and routers. ▪ Displays spectrum analysis results based on APs, including full-channel status monitoring, Wi-Fi interference sources, and non-Wi-Fi interference sources. ▪ Generates dialling test reports for multi-vendor network comparison in real time and allows administrators to intuitively learn the Wi-Fi network experience through dialling tests on apps. ▪ Allows administrators to view the full-journey experience, including who, when, which AP to connect, experience, and issues. ▪ Traces the network access process of a user, including detailed protocol information at the association, authentication (supporting 802.1X authentication, Portal authentication, MAC address authentication, HACA authentication, and PSK authentication), and DHCP phases. The protocol information includes the interaction result and time consumption. If the interaction fails, the failure causes are also displayed. ▪ Correlatively analyzes poor-experience users. When the experience of a user deteriorates, CampusInsight identifies quantified correlation metrics based on the KPI similarity analysis algorithm, which effectively improves the accuracy of root cause identification. 19. Automatic identification and proactive prediction of network issues. ▪ Supports automatic identification of common network issues based on big data analytics and ML algorithms: connectivity, air interface performance, roaming, device environment, device capacity, network performance, network status, and network protocol issues. The issues include authentication failure, weak-signal coverage, dual band-capable clients prioritizing 2.4G, and network congestion. ▪ Supports anomaly detection based on dynamic baselines so that exceptions can be identified at the early stage of network quality deterioration. ▪ Intelligently analyzes data reported at the second level and establishes a network health evaluation system from multiple dimensions. CampusInsight evaluates and ranks regions based on metric weights, driving continuous improvement from poor experience to good		

	experience and gradually improving the network quality. The dynamic baseline comparison between the local region and other regions for each metric can be viewed. It also provides associated root cause metrics, enabling in-depth root cause analysis. In addition, it supports comparison and analysis based on different time points or regions and sends network health reports to administrators in real time or periodically by emails. 20. Intelligent demarcation and root cause analysis of network issues ▪ Supports the issue distribution view, allowing administrators to view the number of issues on different devices and the number of affected users. This helps administrators quickly focus on the affected devices and the time range. ▪ Supports issue impact analysis views, allowing administrators to filter impact factors from multiple dimensions and drill down layer by layer to quickly locate the issue root cause. ▪ Analyzes the root causes based on the rule engine and provides rectification suggestions to assist quick issue closure. 21. Open northbound APIs for diversified intelligent analysis data ▪ Provides different secondary development capabilities based on data characteristics, and uses three types of open APIs to send original data and analyzed data to third-party systems, including network O&M and IT service systems, providing diversified intelligent analysis data. 1) RESTful NBIs: Open resource data (devices, interfaces, links, and boards), health data (health issues and health evaluation), and terminal session data. 2) SNMP NBIs: Report alarm data to third-party systems through SNMP. 3) Kafka NBIs: Use the Consumer API provided by Kafka to consume Telemetry data collected by CampusInsight from Kafka." The Participating Vendor of the proposed switch shall engage principal subject matter expert (SME) to be present in the requirement gathering sessions, deployment and project commissioning with project team. 22. Application visualization and traffic analysis ▪ Accurately identifies more than 1000 mainstream applications through application identification, including Teams, DingTalk, Webex, and XYLink. ▪ Identifies user-defined applications. ▪ Analyzes the network-wide application traffic and number of users based on applications and displays the application usage of each user on the client journey page. ▪ Collects statistics on application traffic from dimensions of interfaces, devices, and hosts. ▪ Constraints:		

	▪ Non-encrypted RTP and TCP applications are supported in IPv4 scenarios. 23. Application experience awareness and poor-QoE analysis ▪ Uses iPCA 2.0 to implement network quality measurement based on actual service flows and display the E2E service flow paths from Wi-Fi, LAN, to WAN in real time, including the devices at both ends and the devices and ports through which each service flow passes; Performs fault mode analysis over the paths to intelligently locate the faulty devices or ports in a short period of time. 24. Intelligent radio calibration ▪ Real-time simulation feedback: Evaluates wireless network channel conflicts based on the neighbour and radio information about devices on each floor and provides optimization suggestions. (Simulation feedback is not supported for regions for which no floor is planned.) ▪ Big data-powered predictive calibration and calibration benefit display: Identifies high-load APs and edge APs through AI algorithms based on historical big data, drives devices to perform differentiated radio calibration based on the big data analytics results, and intuitively displays all calibration records and calibration benefits. The records include both intelligent ▪ radio calibration and local calibration records." 25. AI roaming ▪ Establishes roaming baselines based on different terminal types to provide differentiated roaming steering and better roaming experience for users." 26. RSSI-based wireless positioning ▪ Displays the user distribution heatmap based on the specified time period. ▪ Allows administrators to view locations of all terminals with Wi-Fi enabled, location of individual users, and available paths within a specified period. ▪ Anonymizes terminal MAC addresses. ▪ Locates Wi-Fi and non-Wi-Fi interference sources, including identifying and displaying the locations of interference sources. ▪ Supports Wi-Fi user location analysis, including new and old user detection statistics, frequency distribution, detection duration distribution, user capture rate, and associated user ratio.		
4.2	**Hi-Care/Co-Care Services-Helpdesk Support, Spare part Management, Maintenance**		
	i. Five (5) years	1	
5	**Wireless Controller**		
5.1	**Wireless Access Controller** *Technical Specifications:* *(Please state Y/N at Compliance)* *10 x GE + 2 x 10 GE SFP+* *-Support 10Gbit/s forwarding capability* *-Support 4K users* *-Supports AC 1+1 HSB, and N+1 backup, ensuring uninterrupted services*	2	

	-Deployed by SDN controller network automation and optimized by AI analyzer. Features/Requirements: 1. Flexible networking - the WLAN AC can be deployed in inline, bypass, bridge, and Mesh network modes, and supports both centralized and local forwarding 2. Support Netconf & Telemetry 3. Supports IoT cards on the AP to converge the WLAN and IoT. 4. Allows users to use MAC addresses as accounts for authentication by the RADIUS server. 5. The proposed shall able to be managed by existing Network Management System (eSight) / iMaster NCE-Campus & CampusInsight 6. Portal authentication: *Authentication through an external Portal server *Built-in Portal authentication and authentication page customization 7. 802.1X authentication: *Authentication through an external 802.1X server. *Built-in 802.1X authentication. 8. PSK+MAC authentication 9. 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA,802.1X 10. Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP), and Extensible Authentication 11. Protocol (EAP) types: EAP-Transport Layer Security (TLS), EAP-Transport Layer Security (TLS), EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake, Authentication Protocol Version 2 (MSCHAPv2) 12. The AC should provide 6Gbps forwarding performance. 13. The AC should have at least eight 1GE Ethernet interface. 14. The AC should support static routes, OSPF, BGP, IS-IS, routing policies, and policy-based routes. 15. The AC should support PPSK and assign different PSK keys to different terminals under the same SSID. 16. The AC should support the establishment of CAPWAP tunnels with APs using IPv4 and IPv6 dual stacks. 17. The AC should support IPv6 dynamic routing protocols, including OSPFv3 and BGP4+ 18. The AC should support the antivirus function. 19. The AC should support intrusion prevention, detection, and termination of intrusion behaviors. (including buffer overflow attacks, Trojan horses, and worms). 20. The AC should support spectrum analysis, including real-time FFT charts, channel metrics, FFT duty cycle, interference strength, and channel quality. No additional license is required. 21. The AC should support the function of enabling and disabling the SSID periodically to automatically disable the transmit signals of the specified SSID within a specified period, facilitating network control and providing device configuration screenshots. 22. The AC and AP should be upgraded independently. In dual-AC redundancy mode, services are not interrupted during the upgrade. 23. The AC should monitor the overall wireless network performance and the performance of the AC, AP, radio,		

	and terminal and can be automatically optimized by AI analyzer.		
5.2	**Hi-Care/Co-Care Services-Helpdesk Support, Spare part Management, Maintenance**		
	i. Five (5) years	2	
5.3	**N1-Advanced License (Perpetual Usage + 5 Years SnS)**		
	i. Perpetual (Usage)	2	
	ii. Five (5) years (SnS)		
6	**Wireless Access Point**		
6.1	Access Point Wifi 6 + IoT Ready *Technical Specifications:* *(Please state Y/N at Compliance)* *AirEngine5761-11* *-1 x 10M/100M/1GE (RJ-45) + 1 x IoT slot* *-Support 802.11ax 2*2 MIMO on 2.4 GHz band and 802.11ax 2*2 MIMO on 5 GHz band* *-Support system maximum rate up to 1.775 Gbit/s(0.575 Gbit/s at 2.4 GHz, 1.2 Gbit/s at 5 GHz)* *-PoE power supply: In compliance with 802.3at/af.* -Deployed by SDN controller network automation and optimized by AI analyzer. 1. The AP should support Netconf & Telemetry 2. The AP should support Bluetooth low energy 5.0 and Bluetooth positioning 3. The AP should support Bluetooth serial remote wireless operation and maintenance The AP should support PoE power supply: in compliance with 802.3at 4. The AP should support 6kV surge protection capability of Ethernet interface 5. The AP should support cloud management mode allows users to switch to the cloud mode 6. The proposed shall able to be managed by existing Network Management System (eSight) / iMaster NCE-Campus & CampusInsight 7. The AP should support Operating temperature: -10°C ~ +50°C 8. The AP should support Radio Features: Minimum 16 SSIDs for each radio, Minimum 1024 users 9. Support built-in smart antennas 10. The AP should support smart application control technology and can implement visualized control on Layer 4 to Layer 7 applications. 11. The AP should support application traffic statistics: globally, by SSID, or by user. 12. The AP should support load balancing during smart roaming. 13. The AP should support smart roaming. 14. The AP should support dual-link backup. 15. Qualification Requirements: The Manufacturer of the Access Point shall be positioned in the Gartner Magic quadrant in any of the last 3 years	495	
6.2	**Support USB port, the port can be used for external IoT expansion**		
	i. Five (5) years	495	

6.3	**N1-Advanced License (Perpetual Usage + 5 Years SnS)**		
	i. Perpetual (Usage)	495	
	ii. Five (5) years (SnS)		
7	**SFP Transceiver (Multimode)**		
	SFP 10G MM Optical Transceiver,SFP+,10G,Multi-mode Module(850nm,0.3km,LC)	134	
8	**SFP Transceiver (Single Mode)**		
	SFP 10G SM Optical Transceiver,SFP+,10G,Single-mode Module(1310nm,10km,LC)	68	
9	**Stack Cables**		
	Stack cables 3M SFP+,10G,High Speed Direct-attach Cables,3m,SFP+20M,CC2P0.254B(S),SFP+20M,Used indoor	32	
10	**Fiber Patch Cord**		
	3m SM Fiber Patch Cord	2	
11	**U/FTP Cable**		
	Supply and Install Data Point Cat6A U/FTP Cable run in PVC Conduit/casing with SCREENED Jack, 1 port faceplate & Box	495	
12	**Professional Services**		
12.1	**Implementation service (Planning, Design, Install, Testing, UAT, dismantling, relocation)** Supply, Delivery, Installation, Configuration, Commissioning, Testing, Warranty, Maintenance, Support, Replacement and Decommissioning Services of Network Switches, including the below scope of works: -Installation of 1) Distribution Switches, 2) Upgrade of eSight (to SDN Controller, Ai Analyzer) must engage with existing vendor to configured as critical equipment including migration and relocation from other hospitals. - All existing Huawei equipment in RIPAS Hospital and other MOH sites must connect to the SDN Controller and AI Analyzers. -Conduct requirement study on existing network requirement, configuration & switches, follow by recommendation report & migration plan, including running version, IP addresses, VLANs, AAA, routing, etc. -Installation of new cables required for access points (AP) -Installation of fiber optic backbone or patch cords connecting to/from the core or distribution switch, where no existing backbone is available or the current one is faulty. - Provision of UTP cables for connectivity of Wireless Controller, SDN Controller and AI Analyzer hardware. -Decommission existing network equipment & relocate them to location MOH IT instructed, work closely with cable & rack vendors, and conduct proper migration. -Configuration, testing & commissioning of the proposed network switches, Wireless infra and firewall according to the recommendation report & plan. -Provide post-implementation configuration documentations, including firmware version, physical & logical diagrams, hostname & IP address, VLAN details, configuration backup files, etc. -Conduct Acceptance Test upon commissioning. -Provide one (1) knowledge transfer session to Ministry of Health HTD/ IT Team	1	

	-Must be implemented and supported by relevant certified engineers located in Brunei. -To provide project management services.		
12.2	**Annual Maintenance and Support for Network Switches with the below scope of works (5 years)**		
	i. Five (5) years	1	
	Scope of work: - Perform curative maintenance, including troubleshoot & resolve any switches or network related issue reported. -Perform curative maintenance, including troubleshoot & resolve any switches or network related issue reported. -Provide 8x5x2 Hours phone, email, remote & on-site support services. -Perform quarterly preventive maintenance services, health check, configuration backup, firmware upgrade & patching. -Perform recommended fine tuning as per advice or published by Manufacturer including critical with immediate patching. -Responsible to liaise with Manufacturer support for any unresolved or warranty issue. -Must be maintained & supported by min. two (2) local certified engineers (of related products) located in Brunei. Eg: Huawei Certification		
13	**License Upgrade**		
	Existing Equipment License Upgrade to support value added features of eSight (SDN Controller and Ai Analyzer) *Specifications/Requirement:* - License Upgrade from eSight with NCE Campus & Campus Insight - x 300 units - N1-Advanced License (Perpetual Usage + 5 Years SnS) - Perpetual (Usage) - Five (5) years (SnS) -All existing Huawei equipment installed from Phase 1 and newly proposed to be optimized by AI analyzer. *Note: Existing hardware shall be upgraded if found EOS else the warranty and support shall cover till EOS.*	1	
14	**Training & Certifications**		
	Training (7 days, 12 Pax, includes exam vouchers) Operations and Maintenance: i. Software Define Network (SDN) Management Controller ii. Intelligent Network Analysis iii. Wireless Controller and Access Point iv. Distribution and Access Switches	1	

ANNEX 2.2 – NETWORK TOPOLOGIES

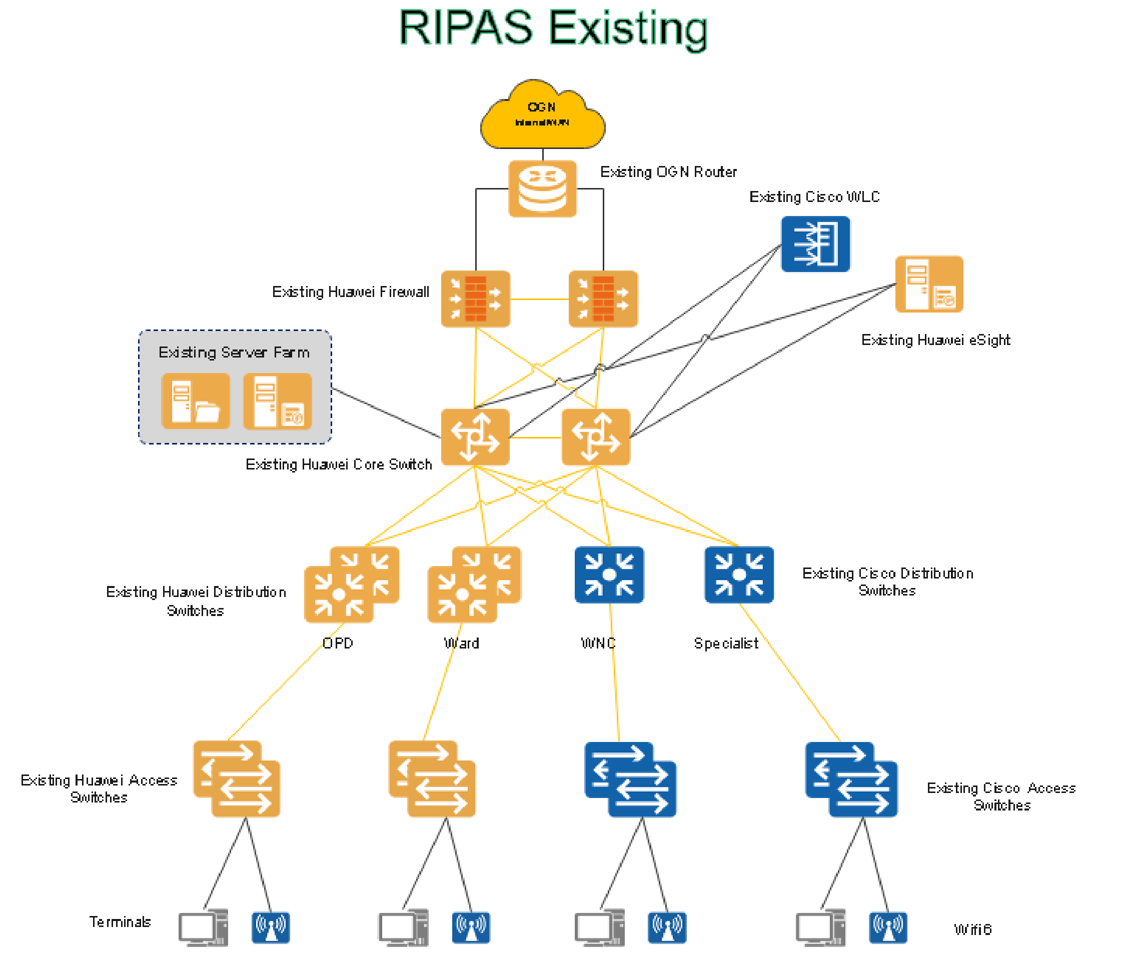


***Figure 1.1** Displays a diagram illustrating both the refreshed hardware and the outdated hardware that requires replacement. The blue icons represent the hardware that needs to be replaced.*

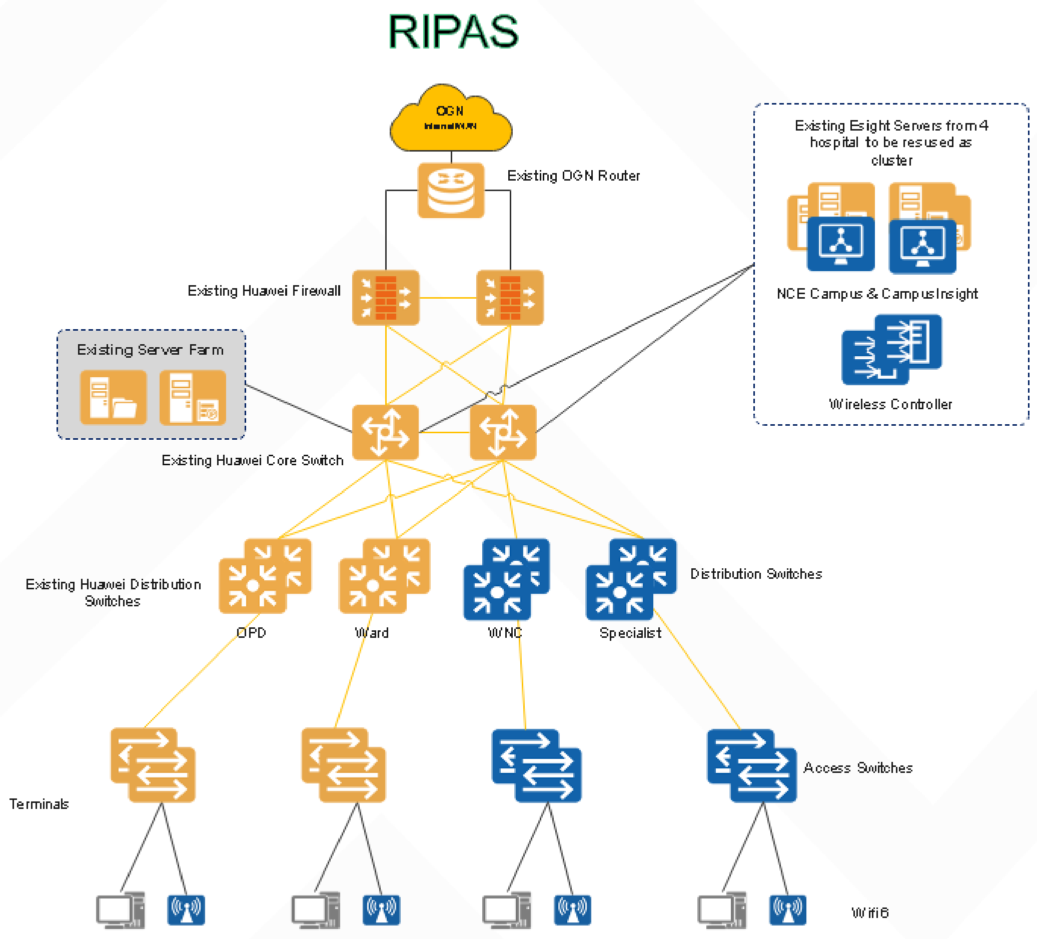


***Figure 1.2** Illustrates the proposed architecture, where the blue icons represent the hardware after replacement along with additional components, including the SDN controller and AI Analyzer.*

Note:

Existing Distribution Switches and Access Switches located in the Woman and Child Centre and Specialist Buildings and the vicinity will be upgraded with the new proposed devices which is equivalent with the previous phase 1 project in Outpatient Department and Ward Complex Blocks. Redundant distribution switches are connected to the core switches via 10G fiber uplink and access switches to the distribution switches also be connected via 10G fiber uplink.

Subsequently the Wireless controllers are connected to the core switches and Access Point will be connected via the access switches. Exact location of APs is to be determined during the detailed survey later on. Access Point must have built in expansion slot for IoT whereby Ministry of Health (MOH) can utilize them during the future Smart Hospital initiative.

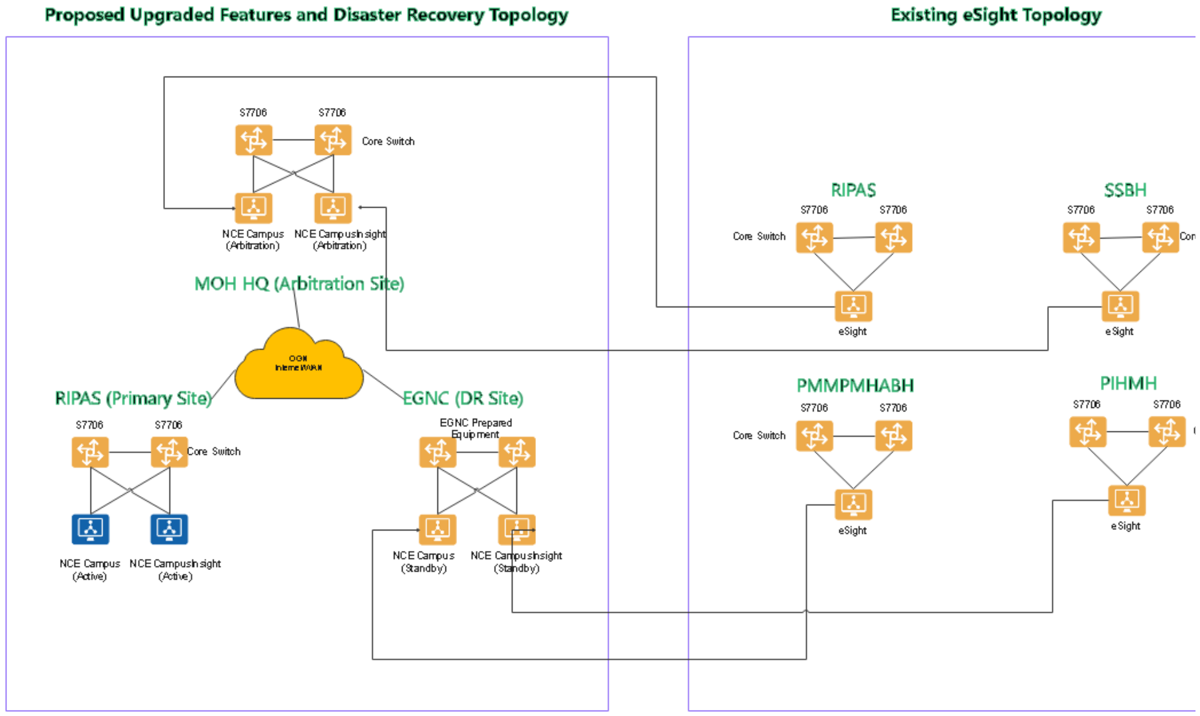


***Figure 1.3** shows the existing e-Sight Topology and Propose Upgarded Features and Disaster Recovery Topology*

Note:
Existing eSight will be upgrade with value added features and components which includes **Software Defined Network (SDN) controller** and **Artificial Intelligence (AI) Analyzer**. These components will benefit MOH immensely in the IT Operations and have total control of their entire network infrastructure across all Hospitals, health centres, and clinics.

ANNEX 2.3 – PAYMENT MILESTONES

No	Project Stage	Deliverables	Percentage Payment	Cumulative Percentage Payment
1	Contract Signing	Contract	0%	0%
2	Project Management	Kick-off Meeting Detailed Project Workplan Project Progress Reports Project Handover Report Stakeholder Register & Communication Plan Commisioning and Acceptance Report Project Risk Management Plan High- Level Training Strategy	5%	5%
3	Project Design	System Architecture Design (SAD) Detailed Design Specification (DDS) Interface Control Document (ICD) Test Strategy & Master Test Plan Hardware Specification Document Software License Certificates/Keys Detailed Migration Plan System and Integration Test Plan Project issue log	10%	15%
4	Supply and Delivery	Proof of Delivery of Hardware and On Site Acceptance Sign-off Proof of Delivery of Software licenses/Subscriptions and On Site Acceptance Sign-off Hardware and Software Inventory Document Hardware Procurement & Delivery Report	30%	45%
5	Installation and Configuration	Design Document Installation Documentation Installation Verification Results Network Administration and Operation Guide Physical and Logical Design Architecture Network Infrastructure Floor Layout Plan Configuration Document, included with Network Mapping and Allocation Hardware Asset Tag document Hardware Specification Document Software License Certificates/Keys Hardware Maintenance and Support Documentation	25%	70%

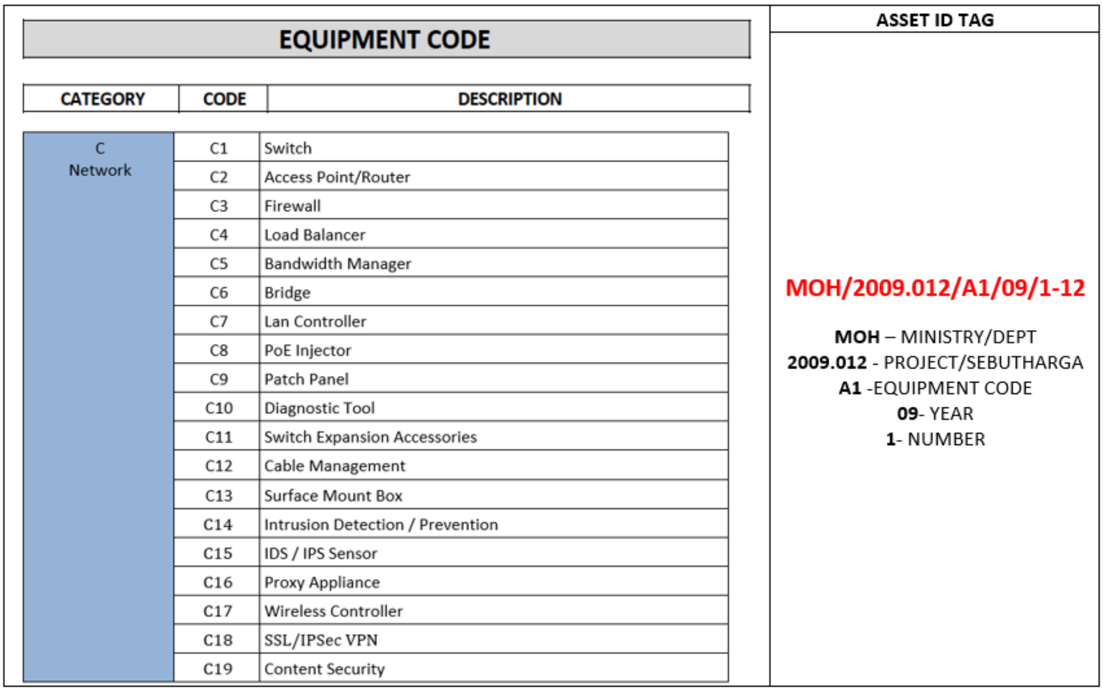
		Hardware Warranty Commencement Notification Technical Design Documentation		
6	Testing	Fixes report (for Security Assessment) Pre-Migration, Process Migration and Post-Migration Testing Document User Acceptance Test (UAT) Documentation including: ▪ UAT Plan and Specifications ▪ UAT Test Results (included with issues/problem raised and recommended resolution) ▪ Performance Test Plan and Specification ▪ Performance Test Results ▪ Update Access Credential Lists ▪ User Acceptancce Test Certificates	5%	75%
7	Training	Training Materials Training Session Delivery & Attendance Records Training Completion Report Operation Procedure Run Book/Service Operating Procedure (SOP) Knowledge Transfer & Material Network and Harware Administration and Operation Guide Troubleshooting Manual	5%	80%
8	Go-Live & Commisioning	System Commissioning Plan Go-Live Plan and Cutover Procedures Operational Readiness Report System Commission Plan Production Data Migration Execution Report Performance Monitoring Reports Commissioning Completion Report	5%	85%
9	Stabilization	Weekly Stabilization report Rapid Incident Management Report	5%	90%

		Production Data Integrity Post-Go-Live Verification Report Root Cause Analysis Report Updated System Documentation Updated Standard Operating Procedures (SOPs) Stabilization Final Report & Consolidated Issue Log Final Acceptance Certificate System Warranty Commencement Notification Final Documentation Project Closure report		
10	Warranty	Warranty Support Contact Information & Escalation Matric Quarter Warranty Period Status Report Manufacturer Hardware Warranty Documentation	10%	100%
11	Maintenance & Support Service	Service Operation Manual Quarterly Preventive Maintenance Report Monthly Incident and Problem Resolution Reports (Adhoc) Incident/Defect Log System Health Check & Performance Reports Security Patching & Vulnerability Scan Reports Release Notes for Maintenance Releases Annual Service Review Meeting	0%	100%

ANNEX 2.4 – PROGRESS SCHEDULE

	Project Phases/Stages	2025					2026				May 2026-Apr 2027	May 2027-Apr 2028	May 2028-Apr 2029	May 2029-Apr 2030	May 2030-Apr 2031	May 2031-Apr 2032
		Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr						
	Contract Signing	🟨														
	Project Management		🟨													
	Project Design		🟨	🟨												
	Supply & Delivery			🟨	🟨											
	Installation & Configurations				🟨	🟨	🟨									
	Testing					🟨	🟨									
	Training						🟨									
	Go-Live & Commisioning							🟨								
	Stabilization							🟨	🟨	🟨						
	Warranty										🟨					
	Maintenance Services & Support (Year 1)											🟨				
	Maintenance Services & Support (Year 2)												🟨			
	Maintenance Services & Support (Year 3)													🟨		
	Maintenance Services & Support (Year 4)														🟨	
	Maintenance Services & Support (Year 5)															🟨

ANNEX 2.5 – LABELLING FORMAT



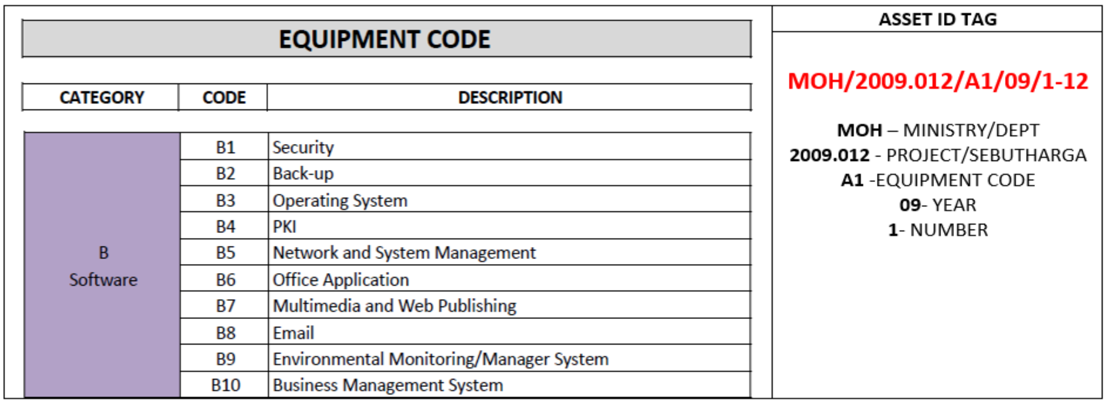
EQUIPMENT CODE

CATEGORY	CODE	DESCRIPTION
C Network	C1	Switch
	C2	Access Point/Router
	C3	Firewall
	C4	Load Balancer
	C5	Bandwidth Manager
	C6	Bridge
	C7	Lan Controller
	C8	PoE Injector
	C9	Patch Panel
	C10	Diagnostic Tool
	C11	Switch Expansion Accessories
	C12	Cable Management
	C13	Surface Mount Box
	C14	Intrusion Detection / Prevention
	C15	IDS / IPS Sensor
	C16	Proxy Appliance
	C17	Wireless Controller
	C18	SSL/IPSec VPN
	C19	Content Security

ASSET ID TAG

MOH/2009.012/A1/09/1-12

MOH – MINISTRY/DEPT
2009.012 - PROJECT/SEBUTHARGA
A1 -EQUIPMENT CODE
09- YEAR
1- NUMBER



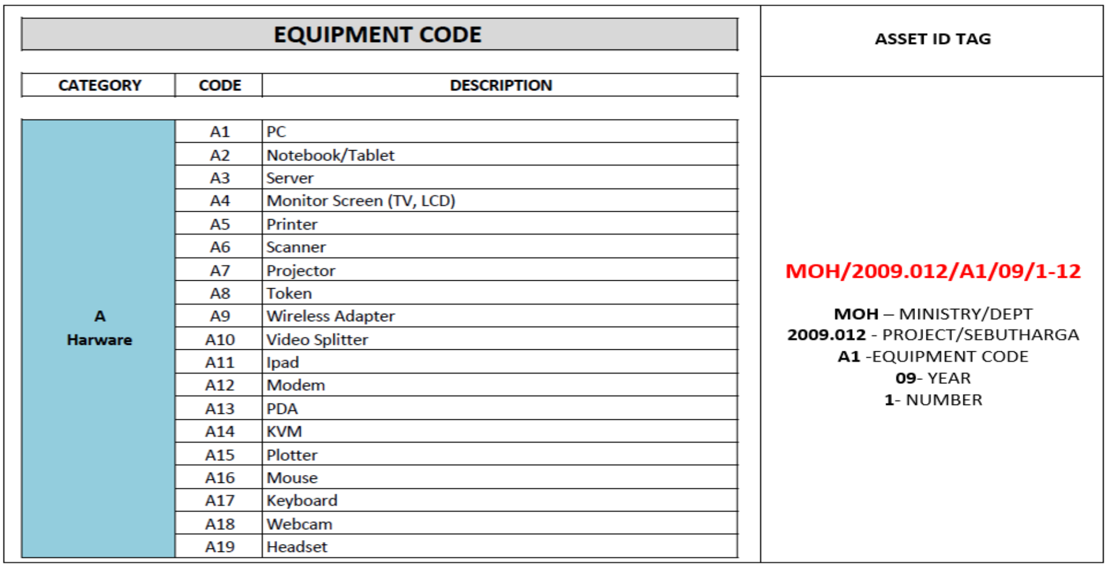
EQUIPMENT CODE

CATEGORY	CODE	DESCRIPTION
B Software	B1	Security
	B2	Back-up
	B3	Operating System
	B4	PKI
	B5	Network and System Management
	B6	Office Application
	B7	Multimedia and Web Publishing
	B8	Email
	B9	Environmental Monitoring/Manager System
	B10	Business Management System

ASSET ID TAG

MOH/2009.012/A1/09/1-12

MOH – MINISTRY/DEPT
2009.012 - PROJECT/SEBUTHARGA
A1 -EQUIPMENT CODE
09- YEAR
1- NUMBER



EQUIPMENT CODE

CATEGORY	CODE	DESCRIPTION
A **Harware**	A1	PC
	A2	Notebook/Tablet
	A3	Server
	A4	Monitor Screen (TV, LCD)
	A5	Printer
	A6	Scanner
	A7	Projector
	A8	Token
	A9	Wireless Adapter
	A10	Video Splitter
	A11	Ipad
	A12	Modem
	A13	PDA
	A14	KVM
	A15	Plotter
	A16	Mouse
	A17	Keyboard
	A18	Webcam
	A19	Headset

ASSET ID TAG

MOH/2009.012/A1/09/1-12

MOH – MINISTRY/DEPT
2009.012 - PROJECT/SEBUTHARGA
A1 -EQUIPMENT CODE
09- YEAR
1- NUMBER

SECTION 3: TENDER SCHEDULES

TABLE OF CONTENTS

COMPOSITION OF TENDER

The composition of the Technical Proposal and Pricing Proposal shall be as follows:

Tender Schedules	Technical Proposal	Pricing Proposal
Schedule 1	All except Table 1.1, 1.2, 1.3, 1.4	
Schedule 2	All	
Schedule 3	All	
Schedule 4	All	
Schedule 5	All	
Schedule 6	All except Table 6.1(a)	Table 6.1(a)
Schedule 7	All except Table 7.1(a)	Table 7.1(a)
Schedule 8	All	
Schedule 9	All	
Schedule 10	All	
Schedule 11	All	
Schedule 12	All except Table 12.2	Table 12.2
Schedule 13	All	
Schedule 14	All	
Schedule 15	All	
Schedule 16	All	
Schedule 17	All	
Schedule 18		All
Schedule 19		All
Schedule 20	All	
Tender Form	Annex 3.1	Annex 3.2

SECTION 3

TENDER SCHEDULES

SCHEDULE 1 – INFORMATION SUMMARY

1.1 Tenderers shall provide in this Schedule the following information:

a. Management summary.

b. List of all the companies (including Contractor and Sub- Contractor (s), if any) involved in the provision of the services and items specified in this tender, and the responsibility of each company.

c. Company profile – Name, Address, Phone Number, Facsimile Number, e-Mail Address, Website (if any), etc.

d. Copies of Company's Certificate of Incorporation or Firm's Certificate of Registration (as registered in One Common Portal – Corporate Registry System), as applicable, and a receipt of the document fee.

e. Copies of Company's Certificate of *Pematuhan Akta Cukai* - Ministry of Finance and Economy (MOFE).

f. Copies of Compliance of *Akta Amanah Pekerja dan Perintah Pencen Caruman Tambahan 2009*, - Tabung Amanah Pekerja (TAP), stating the details of Employer account number and the list of employees registered with TAP.

g. Years of experience (as of the Tender Closing Date) and skills of the Contractor and Sub- Contractor(s) in:

i. Implementing IT projects;
ii. Providing Maintenance and Support Services.

h. Description of the salient features and flexibility of the Hardware Facilities and Software proposed, including wireless connectivity.

i. Status and support policy of each major product.

j. Other information which is considered relevant.

SCHEDULE 2 – SUB-CONTRACTS

2.1 Tenderers shall complete Table 2.1 with information about all the companies involved in the provision of the services and items specified in this tender. This shall include details about the Contractor and each Sub-Contractor involved, as well as their respective responsibilities.

2.2 Tenderers shall also indicate in Table 2.1 any alliance relationship established with each Sub- Contractor. An alliance is defined as a formal and binding business relationship between the allied parties.

Table 2.1 Responsibility Table

Company Name	**Responsibility Description**	**Alliance Relationship between Contractor and Sub- Contractor(s)**		
		Alliance Exists? (Y/N)	**Date Established**	**Alliance Description**
Contractor				
Sub-Contractor(s)				

SCHEDULE 3 – COMPANY'S BACKGROUND

3.1 Each of the companies involved in this tender, including Contractor and Sub- Contractor(s) (if any), shall provide its company profile including company strengths, organisation structure and management background.

SCHEDULE 4 – COMPANY'S TRACK RECORD

4.1 Company Contribution

4.1.1 Tenderers shall complete Table 4.1, with information about the contribution percentages of different companies (which can be the Contractor, Sub-Contractor(s), or other manufacturer(s)) in the provision of the following project services or items:

a. Implementation and Related Services
Tenderers shall list the company(ies) responsible for the provision of Implementation and Related Services. Contribution percentage of each company shall be provided based on the relevant number of man days, service price or cost, over total man days, service price or cost for Implementation and Related Services.

b. Hardware
Tenderers shall list the manufacturer (s) of all the proposed/required hardware item(s). Contribution percentage of each manufacturer/developer shall be provided based on the relevant hardware price/cost over total hardware price/cost.

c. Software
Tenderers shall list the manufacturer (s) of all the proposed/required software item(s). Contribution percentage of each manufacturer/developer shall be provided based on the relevant software price/cost over total software price/cost.

d. Maintenance and Support Services
Tenderers shall list the company(ies) responsible for the provision of Maintenance and Support Services. Contribution percentage of each company shall be provided based on the relevant number of man days, service price or cost, over total man days, service price or cost for Maintenance and Support Services.

4.1.2 The sum of contribution percentages across different companies on a particular project service or item must give a total of 100%.

Table 4.1 Contribution of Companies (in %)

No.	Company Name	Relevant Project Services or Items			
		Hardware	Software	Implementation and Related Services	Please add relevant services as required
	Contractor				
	Sub- Contractors				
	Other Companies/ Manufacturers (if not Contractor and Sub- Contractors)				
	Total:	100%	100%	100%	100%

4.2 Project Management Experiences

4.2.1 Tenderers shall complete Table 4.2, with details of all the IT projects and related services that the Contractor was responsible for.

Table 4.2 Project Management Experiences

Name and Address of Customer	Name and Version of Main Application, Brief Description	Location where & when system was implemented

4.3 Project Partnership Experiences

4.3.1 Tenderers shall complete Table 4.3, with details of all the IT projects in the past years, or indicate with "No partnership" under column "Name & Address of Customer" if this is not applicable:-

a. The Contractor has partnered with any of the proposed Sub- Contractor(s) in this tender, in providing any of the following project services or items for the listed projects:

i. Implementation and Related Services
ii. Hardware
iii. Software
iv. Maintenance and Support Services
v. Other Services (if any please specify) :-
The types of partnership shall include:

- Partnership between the Contractor and Sub-Contractor within the same project in providing **different** services or items as listed above.

- Partnership between the Contractor and Sub- Contractor within the same project in providing the **same** services or item as listed above.

b. The Contractor itself was responsible for any two or more project services or items mentioned above for the listed projects, although without partnership with the proposed Sub- Contractor(s) in this tender.

4.3.2 Tenderers shall indicate the roles of the Contractor and Sub- Contractor(s) for the listed projects in Table 4.3, by providing the companies' reference numbers as specified in Table 4.1.

4.3.3 Tenderers shall enter 'N/A' (not applicable) for the project service(s) or item(s) in the listed project(s), that were responsible by parties other than the Contractor or Sub- Contractor(s) in this tender.

Table 4.3 Project Partnership Experiences

Name & Address of Customer	Project Description	Project Completion Date	Names of Companies Responsible for				
			Hardware	Software	Implementation and Related Services	Maintenance and Support Services	Please add relevant experiences here

4.4 Company Track Records

4.4.1 Tenderers shall provide a list of relevant track records in the tables as listed below, for the companies that are named in Table 4.1.
Table 4.4 Implementation and Related Services
Table 4.5 Hardware
Table 4.6 Software
Table 4.7 Maintenance & Support Services

4.4.2 Tenderers shall complete Tables 4.4 to 4.7 with track records as follows:

a. The track records must be for with similar functions to the system being tendered.
b. The company must have performed a similar role as in this tender for the listed projects.
c. The company shall provide three (3) reference sites for each company under a particular project service or item.

4.4.3 Tenderers shall assign a project reference number to the track records provided. The same project reference number must be used if the same project is referred to by different companies, or under different project services or items.

4.4.4 General guidelines for completing Tables 4.4 to 4.7:

Column Heading	Descriptions
Customer Type	Tenderers shall indicate whether the customer is a Government or Quasi Government organisation. Please put a ‘Y’ under the appropriate category and leave blank if the customer is neither a Government nor a Quasi Government. A Quasi Government is defined as an organisation which (1) is managed and controlled by Government; or (2) has at least 50% shares being held by Government.
Project Scale	Tenderers shall indicate the scale of the project: Table 4.4 – in terms of total contract value (the contract value of the overall project), and total number of man days. Table 4.5 – in terms of contract value of the implementation project, and the total implementation man days. Table 4.7 – in terms of total/ annual contract value of the service, and the number of users supported.

Column Heading	Descriptions
Reference Site	Please mark a 'Y' for the projects/ track records that can be used as reference sites. Tenderers shall provide at least three (3) reference sites for each company under a particular project service or item.
Project Reference Number	Please assign a project reference number for each project/ track record. Tenderers shall note that the same project reference number must be used if the same project is referred to by different companies, or under different project services or items.
Reference Sites Contact Details	Tenderers shall provide contact details for every project/track record that is indicated as a reference site.

Table 4.4 Company Track Records (Implementation & Related Services)

Company Name	

Name of Customer	Customer Type		Name and Version of Main Application, Brief Description	Location Where System was implemented	Project Scale	Project Timeframe		Reference Site	Reference Site Contact Details			
	Govt.	Quasi Govt.				Start Date	Completion Date		Project Reference Number	Contact Person	Title	Contract No, Fax No & Email Address

Table 4.5 Company Track Records (Hardware)

Company Name	

Name of Customer	Customer Type		Name and Version of Main Application, Brief Description	Location Where System was implemented	Project Scale	Project Timeframe		Reference Site	Reference Site Contact Details			
	Govt.	Quasi Govt.				Start Date	Completion Date		Project Reference Number	Contact Person	Title	Contract No, Fax No & Email Address

Table 4.6 Company Track Records (Software)

Company Name	

Name of Customer	Customer Type		Name and Version of Main Application, Brief Description	Location Where System was implemented	Project Scale	Project Timeframe		Reference Site	Reference Site Contact Details			
	Govt.	Quasi Govt.				Start Date	Completion Date		Project Reference Number	Contact Person	Title	Contract No, Fax No & Email Address

Table 4.7 Company Track Records (Maintenance & Support Services)

Company Name													
Name of Customer	Customer Type		Name and Version of Main Application, Brief Description	Location Where System was implemented	Project Scale	Project Timeframe		Reference Site	Reference Site Contact Details				
	Govt.	Quasi Govt.				Start Date	Completion Date		Project Reference Number	Contact Person	Title	Contract No, Fax No & Email Address	

4.5 Reference Site Contact Details (Table 4.4 to Table 4.7)

4.5.1 Tenderers shall provide contact details for every project/track record that is indicated as a reference site.

4.5.2 The Government shall treat all the information submitted under this schedule in strict confidence.

4.5.3 The Government reserves the right to contact the reference sites for tender assessment purposes.

4.5.4 Tenderers may also be requested to make arrangements for the Government’s representative to visit the reference sites. If such site visits are required to be conducted overseas, Tenderers shall render all assistance in arranging the site visits but the Government shall bear the costs of transportation, subsistence and accommodation for the Government’s representative for such visits.

SCHEDULE 5 – CONTRACTOR’S EMPLOYEES AND THEIR DUTIES

5.1 Project Team Structure

5.1.1 Tenderers shall provide a clear organisation chart to show the Project Implementation Team structure including the escalation procedures. Descriptions shall be provided to show how the Implementation Team address the functional and technical requirements and how to discharge the Implementation and Related Services stated in **Section 2: Government Requirements**.

5.2 Project Role and Staffing Arrangement

5.2.1 Tenderers shall provide, in **Table 5.1**, the following information in respect of each of their **key** project staff designated:

a. Name;
b. Company to which the project staff belongs and Job Title;
c. Proposed role in this project including wages;
d. Terms of Service;
e. Language (Spoken); and
f. Deployment of staff for this project, including information about estimated effort and estimated schedule of work.

Table 5.1 Project Role and Staffing Arrangement

Name	Company	Job Title	Language (Spoken)	IC / Passport No.	Proposed Project Role			Terms of Service		Schedule of Work	
					Team / Sub-Team	Staff Category	Wages	Full-time/ Part-time	On-site / Local off-site / Overseas	Start Date	End Date

5.2.2 Tenderers shall state the total and percentage of local and foreign employees.

5.2.3 Tenderers shall propose and present arrangements on the provision of staff and/ or Sub- Contractor establishment.

5.3 Previous Experience of Project Staff

5.3.1 Tenderers shall provide in **Table 5.2** the following information in respect of the previous experience of each of their key project staff designated for the project:

a. Name;
b. Academic qualification;
c. Years of post-qualification IT experience;
d. Number of relevant project experience; and
e. Years of experience in relevant subject areas.

5.3.2 Tenderers shall attach with this Schedule the Curriculum Vitae of each proposed staff for the Project Team. Tenderers are required to cross-reference to the Curriculum Vitae when completing Tables 5.2 to 5.5.

Table 5.2 Project Staff Profile

Name	Academic Qualification	Number of Relevant Project Experience in recent 10 Years			Years of Experience in		
		No. of Years of Post-Qualification IT Experience [1]	No.	Xref [2]	Project Management	Implementation and Related Services	Maintenance and Support Services

Note:

1) For Technology Specialist, this should be "Number of Years of Post-Qualification Functional Experience with Given Technology" (for HW/SW Procurement, not applicable unless it involves high end or complex Hardware)

2) Xref – Cross-reference to the experience provided in Curriculum Vitae

5.3.3 Tenderers shall submit a list of IT procurement projects in Table 5.3 that the proposed Project Manager(s) of this tender has engaged in with a similar role (as of the Tender Closing Date). Tenderers shall provide cross-references to the experiences in Curriculum Vitae.

Please indicate whether the proposed Overall Implementation Methodology, as specified in **Schedule 10 – "Proposed Approach And Methodology"**, was adopted in the projects by putting a 'Y' under column "Used Proposed Overall Impl. Methodology" where appropriate.

Table 5.3 List of projects that the proposed Project Manager(s) has engaged in

Name(s) of Proposed Project Manager(s)	Name and Address of Client	Brief Project Description (e.g. name and nature of application)	Scale of Project			Period of Time Engaged in the Project	Used Proposed Overall Impl. Methodology	Xref
			No. of Users	Total Project Man days	No. of Team Members at Peak			

5.3.4 Tenderers shall submit a list of IT projects in **Table 5.4** that the proposed Technical Supervisor(s) of this tender has engaged in with a similar role (as of the Tender Closing Date). Tenderers shall provide cross-references to the experiences in Curriculum Vitae.

Please indicate whether the proposed Overall Implementation Methodology, as specified in **Schedule 10 – "Proposed Approach and Methodology"**, was adopted in the projects by putting a 'Y' under column "Used Proposed Overall Implementation Methodology" where appropriate.

Table 5.4 List of projects that the proposed Technical Supervisor(s) has engaged in

Name(s) of Proposed Technical Supervisor (s)	Name and Address of Client	Brief Project Description (e.g. name and nature of application)	Scale of Project			Period of Time Engaged in the Project	Used Proposed Overall Impl. Methodology	Xref
			No. of Users	Total Project Man days	No. of Team Members at Peak			

5.3.5 Tenderers shall submit a list of system implementation projects in **Table 5.5** that the proposed Team Leader(s) of this tender has engaged in with a similar role (as of the Tender Closing Date). Tenderers shall provide cross-references to the experiences in Curriculum Vitae.

Please indicate whether the proposed Overall Implementation Methodology, as specified in **Schedule 10 – "Proposed Approach And Methodology"**, was adopted in the projects by putting a 'Y' under column "Used Proposed Overall Implementation Methodology" where appropriate.

Table 5.5 List of projects that the proposed Team Leader(s) has engaged in

Name(s) of Proposed Team Leader(s)	Name and Address of Client	Brief Project Description (e.g. name and nature of application)	Scale of Project			Period of Time Engaged in the Project	Used Proposed Overall Impl. Methodology	Xref
			No. of Users	Total Project Man days	No. of Team Members at Peak			

5.4 Qualifications of Trainers Responsible for the Training Courses

5.4.1 Tenderers shall submit in **Table 5.6** the qualifications of the proposed trainers (with attached curriculum vitae) in conducting the training as specified in **Section 2: Government Requirement, Clause 3.3: Training**.

Table 5.6 Qualification of the Trainers

Name	Company	Course Title	Academic Qualification	Number of Years of			Others (Please specify)
				Post-qualification experience	Experience in training	Experience in system training	

SCHEDULE 6 – SOFTWARE

6.1 Software

6.1.1 Tenderers shall propose in this part all software items as specified in **Section 2: Government Requirements, Clause 2.3: Software:**

a. Licensed to the Ministry of Health (MOH)
b. Supplied and installed by the Contractor
c. Details of the proposed software items, including product description, version number shall be provided.
d. Tenderers shall attach to Table 6.1(a) a sample of each license agreement available for the software items specified in Section 2.

6.1.2 Tenderers shall propose in this part all relevant software items that will be utilised by the Contractor at Contractor's own cost in performing the functions and services, in accordance with the requirements specified in the **Section 2: Government Requirements.**

6.1.3 Tenderers shall complete **Table 6.1(a)** and **Table 6.1 (b)** with all the software items, that will be supplied by the Contractor and licensed to the Government, in performing the functions specified in **Section 2**: **Government Requirements** (including all the essential functions and desirable functions that the Contractor is committed to offer)

6.1.4 Tenderers shall complete **Table 6.1 (b)** with the same contents (other than cost-related information) **as Table 6.1(a),** ensuring the two tables correspond with each other.

6.1.5 Where applicable, Tenderers shall:

a. Enter 'N/C' (i.e no charge)
b. Charge annual license/subscription fees (where applicable) and annual support/maintenance charges.

Table 6.1 (a) Software

Item No	Product/ Version No	Description	Manufacturer	Qty	One-time cost (e.g. Purchase License)	Year 1		Year 2		Year 3		Year 4		Year 5		Total
						License Fee	Support Charge	License Fee	Support Charge	License Fee	Support Charge	License Fee	Support Charge	License Fee	Support Charge	
Sub-total:																
Total:																

Table 6.1 (b) Software

Item No	Product/ Version No	Description	Manufacturer	Quantity	Description of Made-in-Brunei Component

SCHEDULE 7 – HARDWARE

7.1 Hardware

7.1.1 The tenderer shall list in **Table 7.1 (a)** and **Table 7.1 (b)** all hardware items required in **Section 2: Government Requirements**.

7.1.2 Tenderers shall complete **Table 7.1 (b)** with same contents (other than cost-related information) as **Table 7.1 (a)**, ensuring the two tables correspond with each other.

Table 7.1 (a) Hardware

Item No	Manufacturer	Model / Part No	Software[1] Reference to Table 6.2	Description[2]	Location	Qty	Year 1			Year *2*		Year 3		Year 4		Year 5		Total
							Purchase	Maintenance Charge	Support Charge	Maintenance Charge	Support	Maintenan	Support	Maintenan	Support	Maintenan	Support	
					Sub-total:													
					Total:													

Table 7.1 (b) Hardware

Item No	Manufacturer	Model / Part No	Software[1] Reference to Table 6.1 (b)	Description[2]	Location	Qty	Description of Made-in-Brunei Component

Note:

1. Tenderers shall list all relevant software items to be installed on the proposed hardware items in **Schedule 6 – "Software"**
2. Tenderers shall indicate which Contractor's locations (e.g. primary data centre, disaster recovery data centre etc) the hardware items to be placed if applicable

SCHEDULE 8 – PERFORMANCE CRITERIA

8.1 Tenderers shall include all recommended configurations for each resource for the delivery of Government requirement. The resource should include both Contractor provided and Government provided resources.

SCHEDULE 9 – TECHNICAL SOLUTION

9.1 Tenderers shall provide a technical solution describing the proposed specifications of the hardware and software as listed in **Section 2: Government Requirements**.

SCHEDULE 10 – PROPOSED APPROACH AND METHODOLOGY

10.1 Tenderers shall give a description on the proposed approach, methodology or any associated tools adopted for implementation and control of this project including the following services:

a. Overall implementation (Paragraph 10.2)
b. Project management (Paragraph 10.3)
c. Maintenance and Support Services (Paragraph 10.4)

10.2 **Overall Implementation**

Tenderers shall provide detailed information on the overall methodology and approach to be adopted in implementation and related services as specified in this tender. This should include:

a. where appropriate, the name of the methodology shall be indicated. Tenderers shall also provide background descriptions of the methodology, including the source of the methodology (e.g. is the methodology defined by an international organisation and is well adopted in the industry, or is it a knowledge asset of the Contractor or any Sub-Contractor), year of first introduction and adoption, etc;
b. the approach, steps and procedures to ensure the integration of different services; and
c. an explanation on the linkage between this proposed methodology and the Implementation Plan.

10.3 **Project Management**

Tenderers shall describe the detailed methodology and approach to be adopted in this project for project management. This should include:

a. where appropriate, the name of the methodology shall be indicated. Tenderers shall also provide background descriptions of the methodology, including the source of the methodology (e.g. is the methodology defined by an international organisation and is well adopted in the industry, or is it a knowledge asset of the Contractor or any Sub-Contractor), year of first introduction and adoption, extent of use of the methodology on management system projects in other government or quasi government, etc;
b. the approach in controlling the project implementation processes;
c. the approach in project planning, resource estimation and management;
d. the reporting and escalation procedures, including the responsibilities involved;
e. the methodology in delivering project products in good quality and performance; and
f. all associated procedures for the proper management of project issues, project risks, etc.

10.4 **Maintenance and Support Services**

Tenderers shall describe the detailed methodology and approach for performing maintenance and support services, including:

a. the steps, procedures and deliverables associated to maintenance and support services;
b. the approach for support services planning, resource estimation and management;
c. the reporting and escalation procedures, including the responsibilities involved;
d. the approach and methodology in ensuring quality of the maintenance and support services; and
e. all associated procedures for the proper maintenance and support services of software/hardware related issues, risks etc.

SCHEDULE 11 – IMPLEMENTATION PLAN

11.1 Tenderers shall show the proposed the implementation plan in **Table 11.1**. Tenderers shall propose the appropriate activities and deliverables with reference to **Section 2: Government Requirements** and shall include any other recommended activities and deliverables in the table. Tenderers shall provide detailed breakdown on each implementation service and activity.

Table 11.1 Implementation Plan

Major Activities /Tasks	Tentative Timeframe (Date)		Estimated Effort (Man days)			Measurement Metrics	Deliverables
	Start	End	Contractor	Govt.	Others (Pls. Specify)		
	Total:						

Note:

(i) 1 Manday = 8 hours; 1 Man-month = 22.5 Mandays.

SCHEDULE 12 – IMPLEMENTATION AND RELATED SERVICES

12.1 Implementation and Related Services to be provided by the Contractor

The Contractor shall provide the following Implementation and Related Services, with details stipulated in **Section 2: Government Requirements, Clause 3 Implementation and Related Services**.

12.2 Implementation and Related Services Charges

12.1.1 Tenderers shall fill in **Table 12.1** for the above-said Implementation and Related Services of this with information about detailed implementation tasks and Man days breakdown by Staff Categories.

12.2.2 Tenderers shall include, in **Table 12.1** the effort in the testing and implementation.

12.2.3 Tenderers shall ensure that the Implementation and Related Services, as well as the effort specified in this Schedule correspond with the tasks and effort provided in **Schedule 11 Implementation Plan**.

12.2.4 Tenderers shall enter 'N/C' (i.e. no charge) where applicable.

Table 12.1 Implementation and Related Services to be provided by the Contractor during Implementation

Item No.	Description of Implementation and Related Services	Estimated Effort (Man days)			Total Man days
		Project Manager	Technical Supervisor	Others (Pls. Specify)	
	Total:				

For example: PM – Project Manager; TS – Technical Supervisor

12.2.5 Tenderers shall fill in **Table 12.2** to provide the daily rates for any additional services required for Implementation and Related Services as identified in **Schedule 11 Implementation Plan**.

Table 12.2 Staff Daily Rate

Staff Category	Daily Rate
Project Manager	
Technical Supervisor	
Technical Support	
Trainer	

SCHEDULE 13 – INSTALLATION TESTS

13.1 Tenderers shall state in this Schedule the Installation Tests (as specified in **Section 2: Government Requirements**).

13.2 Tenderers shall propose the test approach and the test tools (if any) for conducting the Installation Tests.

SCHEDULE 14 – ACCEPTANCE TESTS

14.1 Tenderers shall state in this Schedule the Acceptance Tests (as specified in **Section 2: Government Requirements, Clause 5 Acceptance Testing**) to be performed.

14.2 Tenderers shall propose the test approach and the test tools (if any) for conducting the Acceptance Tests.

SCHEDULE 15 – DOCUMENTATION AND DELIVERABLES

15.1 General

Tenderers shall propose a complete list of documentation that will be provided, including all the documents specified in **Section 2: Government Requirements, Clause 4 – Documentation and Deliverables**.

15.2 Software

The Contractor shall produce all necessary documentation for all Software as proposed in **Schedule 6 Software**.

Table 15.1 Software Documentation

Ref. No.	Description (include the version/release no.)	Deliverable (D)/ Ref Material (R)	No. of Copies	
			Softcopy (Pls specify medium)	Hardcopy

15.3 Hardware

The Contractor shall produce all necessary documentation for all Hardware as specified in **Schedule 7 Hardware** during implementation.

Table 15.2 Hardware Documentation

Ref. No.	Description	Deliverable (D)/ Ref Material (R)	No. of Copies	
			Softcopy (Pls specify medium)	Hardcopy

15.4 Implementation and Related Services

The Contractor shall deliver all relevant materials and documentation for the provision of Implementation and Related Services (as specified in **Section 2: Government Requirements, Clause 3 Implementation and Related Services** as Project Deliverables. These must include, the key deliverables specified in **Section 2: Government Requirements, Clause 4 Documentation and Deliverables**.

Table 15.3 Implementation and Related Services Documentation

Ref. No.	Description	No. of Copies	
		Softcopy (Pls specify medium)	Hardcopy

15.5 Maintenance & Support Services

The Contractor shall deliver all relevant materials and documentation for the provision of Services (as specified in **Section 2: Government Requirements, Clause 3.10: Warranty, Clause 3.11: Maintenance and Clause 3.12: Support Services**) as Project Deliverables. These must include, the key deliverables specified in **Section 2: Government Requirements, Clause 4 Documentation and Deliverables**.

Table 15.4 Maintenance & Support Services Documentation

Ref. No.	Description	No. of Copies	
		Softcopy (Pls specify medium)	Hardcopy

SCHEDULE 16 – TRAINING PLAN

16.1 Training Plan and Approach

Tenderers shall describe the training plan and approach, as specified in **Section 2: Government Requirements, Clause 3.9: Training**. These shall include the following:

a. Overall training methodology and approach, for example, training recommendations so that end-user training can be effectively rolled out within the planned timeframe.
b. Detailed approach of the course, for example:
   i. Types of learning modes (e.g. classroom, hands-on assisted training)
   ii. Types of delivery aids (e.g. presentation slides)
   iii. Types of course materials
   iv. Course Contents
   v. Size per class

16.2 Training Resources

Tenderers shall describe in this Schedule their training resources and facilities.

16.3 Training Courses to be provided by Contractor

16.3.1 Tenderers shall propose in this Schedule the course to be provided and conducted by the Tenderer, as specified in **Section 2: Government Requirements, Clause 3.9: Training**.

16.3.2 The proposed training schedule shall be in line with the detailed implementation plan provided in **Schedule 11 Implementation Plan**.

16.3.3 Tenderers shall complete Table 16.1 using the following guidelines:

Column Heading	Descriptions
Course Title	The title of the course, which shall be clear and self-explanatory for the Department of Healthcare Technology, Ministry of Health understanding. Where necessary, brief descriptions shall be included.
Course Contents	The topics/sub-topic to be covered during the course
Format	Classroom and hands on (please specify).
Number of Sessions per Course	The number of sessions that trainees need to attend in order to complete the course.
Total Duration (Hours) per Course	Total number of hours that trainees need to attend in order to complete the course.
Proposed Number of Classes	More than one class shall be proposed for a particular course if the number of trainees is large and considered not manageable in one class.
Category of Trainee	Project team member, end user, others (please specify).
Size per Class	Number of trainees per class.
Scheduled Date(s) for each Class	The proposed date(s) for trainees to attend the sessions.
Venue	Venue to be provided by the Contractor, or third-party training centre, unless otherwise required by Government. Please provide details if the venue is to be provided by Contractor or by third-party training centre.

Table 16.1 Training Plan and Details

Course Title	Course Contents	Format	Number of Sessions per Course	Total Duration (Hours) per Course	Proposed Number of Classes	Category of Trainee	Size per Class	Scheduled Date(s) for each Class	Venue

SCHEDULE 17 – STATEMENT OF COMPLIANCE

17.1 Tenderers shall indicate their compliance by providing a compliance table in Table 17.1, with clause-by-clause including sub-clause by sub-clause statement of compliance corresponding to all Sections of :

i. Section 2 – Government Requirements including the Annexes except Clause 1.1 Background; and
ii. Section 4 – General Terms of Agreement.

17.2 Proposal without the compliance table specified in **Table 17.1** will be considered incomplete and shall be disqualified.

Table 17.1 Statement of Compliance

Section	Sub-section No.	Compliance [1] Yes or No	Tenderer Proposal Reference [2]	Remarks [3]

Note:

1. Please put “Yes” if complied, “No” if not complied.
2. Tenderers shall indicate the reference in their proposal where Tenderers stated “Yes” that comply with the Government requirement.
3. Where appropriate, Tenderers shall specify how the requirement will be met in the remarks column.

SCHEDULE 18 – PRICE SUMMARY

18.1 Tenderers shall provide a summary of the aggregate price for the non-recurrent cost, annual recurrent cost and other price information in **Table 18.1**. Tenderers shall ensure the accuracy and consistency with the items proposed in this tender. This Schedule must be completed in full and the price shall be consistent with the prices listed in the following Schedules and Annex 3.2. In case of discrepancy, this written Schedule document shall prevail.

The charges in **Table 18.1** are for the purpose of total price assessment for this project.

18.2 Items listed in **Table 18.1** are guidelines to Tenderers and may not be exhaustive. Tenderers shall ensure the completeness and accuracy of the information provided for a total price assessment. Tenderers shall also include in this schedule the non-recurrent and quarterly recurrent cost of other items.

18.3 Tenderers shall:

a. Enter ‘N/C’ (i.e. no charge) where applicable.

Table 18.1 Total Charges for Implementation Phase

Descriptions	Year 1	Year 2	Year 3	Total	Schedule Reference
Software					Schedule 6
Hardware					Schedule 7
Implementation and Related Services					Schedule 12
Total					

SCHEDULE 19 – PAYMENT SCHEDULE

19.1 Payments shall be made in accordance with the milestones specified in **Section 2: Government Requirements, Annex 2.3: Payment Milestones.**

19.2 Tenderers shall propose a detailed payment breakdown in accordance with the milestones specified in **Section 2: Government Requirements, Annex 2.3: Payment Milestones** such that it is consistent with the implementation plan proposed in **Schedule 11, Table 11.1**.

SCHEDULE 20 – DECLARATION FORM

20.1 Tenderers are required to make a declaration in the form of the Tenderer’s Declaration (attached overleaf). The purpose of the declaration is to prevent incidences of collusion among potential tenderers to this Invitation To Tender.

Schedule 20 – PENGAKUAN PENENDER / TENDERER'S DECLARATION

PENGAKUAN INTEGRITI PENENDER
TENDERER'S INTEGRITY DECLARATION

ANNEX 3.1: TENDER FORM (TECHNICAL PROPOSAL)

(FOR SUBMISSION IN TECHNICAL PROPOSAL ENVELOPE)

Date : ____________________

TO: THE CHAIRMAN
MINI TENDER BOARD
MINISTRY OF HEALTH
COMMONWEALTH DRIVE
JLN MENTERI BESAR
BANDAR SERI BEGAWAN BB 3910
BRUNEI DARUSSALAM

Sir,

Having examined the documents comprised in the Invitation To Tender, the receipt of which is hereby duly acknowledged, we, the undersigned, offer for **The Refresh of Network Infrastructure of RIPAS Hospital (Phase 2), Ministry of Health** in conformity with the said Requirements and Schedules in the sum stated and sealed in a separate envelope marked "**Pricing Proposal**".

We agree to abide by this Tender for a period of **TWELVE (12) months** from the deadline for submission of tender and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We shall execute a formal agreement in the appropriate form set out in the Tender Document together with such further terms and conditions, if any, agreed upon between the Government and us.

We understand that you are not bound to accept the lowest or any Tender you may receive.

Dated this ______________ days of ____________________ 20 ______________

____
Signature

____
(In the Capacity of)

Duly Authorised to sign Tender for and on behalf of

____

____

Witness ____________________________________

Address ____________________________________

____

____

____
Signature

ANNEX 3.2: TENDER FORM (PRICING PROPOSAL)

(FOR SUBMISSION IN PRICING PROPOSAL ENVELOPE)

Date : ____________________

TO: THE CHAIRMAN
MINI TENDER BOARD
MINISTRY OF HEALTH
COMMONWEALTH DRIVE
JLN MENTERI BESAR
BANDAR SERI BEGAWAN BB 3910
BRUNEI DARUSSALAM

Sir,

Having examined the documents comprised in the Invitation To Tender, the receipt of which is hereby duly acknowledged, we, the undersigned, offer for **The Refresh of Network Infrastructure of RIPAS Hospital (Phase 2), Ministry of Health** in conformity with the said Requirements and Schedules for the sum of

(Total amount in words and figures)

We agree to abide by this Tender for a period of **TWELVE (12) months** from the deadline for submission of tender and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

We shall execute a formal agreement in the appropriate form set out in the Tender Document together with such further terms and conditions, if any, agreed upon between the Government and us.

We understand that you are not bound to accept the lowest or any Tender you may receive.

Dated this ______________ days of ____________________ 20 ______________

____
Signature

____
(In the Capacity of)

Duly Authorised to sign Tender for and on behalf of

____

____

Witness ________________________________

Address ________________________________
____
____

____
Signature

Section 3 – Annex 3.2 Tender Form – Pricing Proposal