MINISTRY OF HEALTH & MASS MEDIA

Teaching Hospital Peradeniya

National Competitive Bidding

Procurement of Comprehensive Maintenance and Support Services for ICT Equipment, Local Area Network, Servers of Teaching Hospital Peradeniya 2026 – 2028

Contract No: THP/AF/01/2026

Teaching Hospital Peradeniya

Peradeniya

Invitation for Bids

Procurement of Comprehensive Maintenance and Support Services for ICT Equipment (Including Computers, Printers, barcoding items and UPS etc.), LAN (Including Switches, APs and network accessories) and Servers of Teaching Hospital Peradeniya.

Contract (Bid) Number

- The Chairman of the procurement committee of the Teaching Hospital Peradeniya now invites sealed bids from eligible and qualified bidders for maintenance service of Network, Server and all ICT equipment of Teaching Hospital Peradeniya.
- The intended service period is 02 years.
- Bidding will be conducted through National Competitive Bidding (NCB)
- Interested eligible bidders may obtain further information from Director of Teaching Hospital Peradeniya, 0812388261 or visiting the official website of the "Teaching Hospital Peradeniya" A complete set of Bidding Documents may be collected (as a PDF file) by interested bidders from the hospital website given below from **27th April 2026 to 17th June 2026** "www.peradeniya-hospital.health.gov.lk"
- **Bids must be delivered to Teaching Hospital Peradeniya on or before 17.06.2026 before 10.30 hours. The non-refundable bid fee is Rs. 1,500.00. Receipt of payment of this fee to Shroff of Peradeniya General Hospital or receipt credited to People's Bank Account No. 057100129025207 in the name of Peradeniya General Hospital should be forwarded along with the bid. Please note that bids that are not submitted with the relevant receipts and late bids will be rejected.** Bids will be opened in the presence of the bidder / representatives who choose to attend in person at the Teaching Hospital Peradeniya 17.06.2026 before 10.30 am.
- Pre-bid meeting will be held on 08.06.2026 at 10.30 am in Conference room of Teaching Hospital – Peradeniya.
- The address referred to above is Name of Procurement Entity.

Chairman.
Procurement committee,
Teaching Hospital Peradeniya.

CONTENTS

Section I - Instructions to Bidders

- **General**

1	**Scope of bid**	• The THP, as defined in the Bidding Data, invites bids for the maintenance services of ICT equipment, Local Area Network and Servers (2026-2028), as described in the ***section V- Requirement and description of service to the Contract.***
		• The successful bidder will be expected to carry out the service for 02 years (2026 - 2028) after awarding the contract.
2	**Qualification and experience of bidder**	2.1. All bidders shall provide in Section III, other relevant documents, Forms of bid and qualification and experience information, a preliminary description of the proposed work method and schedule, including drawings and charts, as necessary.
		2.2. If stated in the bidding data, all bidders should include the following information and documents with their bids in Section III:
		A list of relevant ICT services provided to government hospitals of District General Hospital level or above, including the period of service, number of years and months of experience, scope of services provided, ongoing or completed status, and the names and contact details of clients who may be contacted for further information, supported by relevant documentary evidence.
		• Work plan and methodology / Capacity to carry out the work
		• Qualifications and experience of key staff proposed for the contract
3	**Cost of bidding**	3.1. The Bidder shall bear all costs associated with the preparation and submission of his Bid, and the THP will in no case be responsible or liable for those costs.
4	**Site visit**	4.1. The bidder, at the bidder's own responsibility and risk, is encouraged to visit and examine the site of required services and its surroundings and obtain all information that may be necessary for preparing the bid and entering into a contract for the services. The costs of visiting the site shall be at the bidder's own expense

- **Bidding Documents**

5	**Contents of bidding document**	5.1. The set of bidding documents comprises the documents listed below:

Section I	Instructions to Bidders
Section II	Bidding Data
Section III	Forms of Bid and Qualification Information
Section IV	Conditions of Contract
Section V	Requirement and description of the Services
Section VI	Price schedule
Section VII	Method of payment schedule
Section VIII	Qualification of staff
Section IX, X	List of Equipment
Annex 1	Mandatory Criteria
Annex 2	Specification and Requirements for Maintenance and Servicing of ICT Equipment
Annex 3	Requirements for Maintenance and Servicing of Local Area Network, Servers and Other Network-Related Equipment
Annex 4	Services and Facilities Provided by the Employer
Annex 5	Minimum Specifications for Endpoint Security Solution (to be added by THP before final publication)

6	**Clarification of bidding documents**	6.1. A prospective Bidder requiring any clarification of the bidding documents may notify the Employer in writing at the Employer's address indicated in the invitation to bid.

- **Preparation of Bids**

7	**Language of bids**	The bid prepared by the bidder, as well as all correspondence and documents relating to the bid exchanged by the Bidder and the THP shall be written in English Language.
8	**Document comprising the bid**	All related documents (Originals) shall be submitted in sealed envelope. Envelop shall contain the identification of the contract as defined in the contract data. Duplicate / copy may be submitted in a separate envelope.
9	**Bid price**	The contract shall be for the maintenance service of ICT equipment, Local Area Network and Servers as described in the THP's requirements, Section V, based on the priced Activity Schedule submitted by the Bidder.
		The Bidder shall fill in rates and prices for all items of the Services described in Requirements, Section V. Items for which no rate or price is entered by the Bidder will not be paid for by the THP when executed and shall be deemed covered by the other rates and prices in under the section of proposed cost.
		All duties, taxes, and other levies payable by the service provider under the contract, or for any other cause, as of the date 28 days prior to the deadline for submission of bids, shall be included in the total bid price submitted by the bidder. However, VAT shall be included separately.
10	**Currency of bids and payment**	The lump sum price shall be quoted by the bidder shall be in Sri Lankan Rupees.
11	**Bid validity**	Bids shall be valid for **91 (ninety one)** days from **17.06.2026 to 15.09.2026**
12	**Bid Security**	12.1. Bid Security shall be:
		• For an amount of **Rs. 195,000/=**
		• Valid for **119 (one hundred and nineteen)** days from the deadline for submission of Bids **(17.06.2026 to 13.10.2026)**
		Bid Shall include a Bid Security Issued by a) A Local Commercial bank approved by the Central Bank of Sri Lanka, which is operating in Sri Lanka; b) A foreign commercial bank operating in Sri Lanka, which is approved by the Central Bank of Sri Lanka; c) A foreign bank operating outside of Sri Lanka, Provided that the relevant Bank Guarantee is confirmed by a local or foreign bank operating in Sri Lanka, which is approved by the Central Bank d) Refundable Cash Deposit
		12.2. The Bid Security may be forfeited: • if the Bidder withdraws the Bid after Bid opening during the period of Bid validity; • if the Bidder does not accept the correction of the Bid price • in the case of a successful Bidder, if the Bidder fails within the specified time limit to: Sign the contract or furnish the performance security

- **Submission of Bids**

13	**Sealing and Marking**	Bids shall be marked as: **Comprehensive Maintenance and Support Services for ICT Equipment, Local Area Network, Servers of Teaching Hospital Peradeniya - 2026 to 2028**
14	**Submission of bids**	Bids should either be sent by Registered post or deposited in the tender box kept at the **Accountant Office of THP**, a**t or before 10.30 a.m. on 17.06.2026.** The late bids will be rejected

E. Bid Opening and Evaluation

15	**Bid opening**	Will be done at the teaching hospital Peradeniya on 10.30 hours 17.06.2026 at the Learning Room 2 of THP
		The bidder's representative who are present shall confirm their attendance by signing the attendance sheet
16	**Clarification of bids**	To assist in the examination, evaluation, and comparison of bids, the THP may, at the THP's discretion, request any Bidder for clarification of the Bidder's Bid and other information that the Employer may require.
17	**Evaluation**	• The Procurement Entity reserves the right to accept or reject any variation, deviation or alternative offer. • Variations, deviations, alternative offers, and other factors that are in excess of the requirements of the Bidding document shall not be considered in Bid evaluation. The evaluation of bids will be conducted in two stages: primary evaluation and further evaluation. During the primary evaluation, key submission requirements such as • Bid document charges, • The completed bid submission form, • Bid security • Bid validity will be assessed to ensure compliance. Bids that meet above initial requirements will proceed to the further evaluation stage. In this stage, following factors will be considered • Prices of services and goods offered (Section VI) • The bidder's responses regarding their capability to fulfill requirements related to the maintenance and servicing of ICT equipment, and servicing of local area networks, servers, and other network-related equipment (Annex 2, Annex 3) • Compliance with the mandatory criteria (Annex 1) • Bidder's qualification information, including details of nominated staff and the company's past experience. (Section III),Section VIII)

Award of Contract

18	**Award of contract**	THP will award the Contract to the most Substantially responsive, lowest possible evaluated bidder
19	**Right to accept any bid and to reject any or all bids**	THP reserves the right to accept or reject any bid, and to cancel the bidding process and reject all bids, at any time prior to the award of Contract, without thereby incurring any liability to the affected Bidder or bidders or any obligation to inform the affected Bidder or bidders of the grounds for the THP's action
20	**Performance security**	The value of the performance security shall be ten percent (10%) of the contract value. Performance security shall be submitted within 14 days after receipt of the letter of acceptance, the successful bidder shall deliver to the employer a performance security in the amount and in the form (Bank Guarantee)

Section II - Bidding Data

Instructions to Bidders Clause Reference

	The Employer	Teaching Hospital Peradeniya
		The name and identification number of the Contract is **Procurement of Comprehensive Maintenance and Support Services for ICT Equipment, LAN, Servers of Teaching Hospital Peradeniya** **Contract (Bid) Number - THP/AF/01/2026**
i	Intended duration of the contract	**02** years (2026-2028) from the date of awarding the contract.
ii	Address for submission of Bids	Chairman, Regional procurement committee, Teaching Hospital Peradeniya
iii	Period of bid validity	**91 (ninety one)** days from the deadline for submission of Bids
iv	Amount of bid security	For an amount of **Rs.195,000/=** To **Director, Teaching Hospital Peradeniya**
vii	Deadline for submission	**On or before 10.30 hours on 17.06.2026**
viii	Pre -bid meeting	**08.06.2026 at 10.30 am of conference room of THP**
ix	Bid opening	**10.30 hours , 17.06.2026 at the Teaching Hospital Peradeniya**

Section III. Forms of bid and qualification information

Form of Bid

Chairman, Procurement Committee.
Teaching Hospital,
Peradeniya.

Having examined the bidding documents, we offer to provide the Services ----------
---
----------[name and identification number of Contract] in accordance with the conditions of contract, employer's requirements, drawings and activity schedule accompanying this Bid for the Contract Price of ----------[amount in numbers], ----------
----------[amount in words] or any other sum derived in accordance with the said documents.

This Bid and your written acceptance of it shall constitute a binding Contract between us. We understand that you are not bound to accept the lowest or any Bid you receive.

We hereby confirm that this Bid complies with the Bid validity required by the bidding documents and specified in the Bidding Data.

Authorized Signature	:	
Name and Title of Signatory	:	
Name of Bidder	:	
Address	:	

Bid Submission Form

[The Bidder shall fill in this Form in accordance with the instructions indicated No alterations to its format shall be permitted and no substitutions shall be accepted.]
Date: ----------*[insert date (as day, month and year) of Bid Submission]*
No.: ----------*[insert number of bidding process]*

To: **Director, Teaching Hospital Peradeniya**

We, the undersigned, declare that:

a. We have examined and have no reservations to the Bidding Documents, including Addenda No.: ----------*[insert the number and issuing date of each Addenda];*

We offer to supply in conformity with the Bidding Documents and in accordance with the Delivery Schedules specified in the Schedule of Requirements the following Goods and Related Services related to the procurement of ICT equipment (Computers, Printers, barcoding items and UPS), Local Area Network and Servers maintenance service, of Teaching Hospital Peradeniya (2026-2028)

a. The total price of our Bid without VAT, including any discounts offered is: ----------*[insert the total bid price in words and figures];*

a. The total price of our Bid including VAT, and any discounts offered is: ----------*[insert the total bid price in words and figures];*

a. Our bid shall be valid for the period of time specified in Section II (bidding data), from the date fixed for the bid submission deadline and it shall remain binding upon us and may be accepted at any time before the expiration of that period;

a. If our bid is accepted, we commit to obtain a performance security in accordance with Section IV (Condition of Contract) for the due performance of the Contract;

a. Our firm, its affiliates or subsidiaries—including any subcontractors or suppliers for any part of the contract—has not been declared blacklisted by the National Procurement Agency;

a. We understand that this bid, together with your written acceptance thereof included in your notification of award, shall constitute a binding contract between us, until a formal contract is prepared and executed.

(h) We understand that you are not bound to accept the lowest evaluated bid or any other bid that you may receive.

Signed: ----------*[insert signature of person whose name and capacity are shown]*

In the capacity of ----------*[insert legal capacity of person signing the Bid Submission Form]*

Name: ----------*[insert complete name of person signing the Bid Submission Form]*

Duly authorized to sign the bid for and on behalf of: ----------*[insert complete name of Bidder]*

Dated on _____ day of _____, _____ *[insert date of signing]*

Bid Guarantee

[This Bank Guarantee form shall be filled in accordance with the instructions indicated in brackets]

---------- *[insert issuing agency's name, and address of issuing branch or office]*

Beneficiary: Director, Teaching Hospital Peradeniya

Date: ---------- *[insert (by issuing agency) date]*

BID GUARANTEE No.: ----------*[insert (by issuing agency) number]*

We have been informed that ---------- *[insert (by issuing agency) name of the Bidder; if a joint venture, list complete legal names of partners]* (hereinafter called "the Bidder") has submitted to you its bid dated ---------- *[insert (by issuing agency) date]*(hereinafter called "the Bid") for the supply of *[insert name of Supplier]* under Invitation for Bids No. ---------- *[insert IFB number]* ("the IFB").

Furthermore, we understand that, according to your conditions, Bids must be supported by a Bid Guarantee.

At the request of the Bidder, we ---------- *[insert name of issuing agency]* hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of ---------- *[insert amount in figures]* ---------- *(insert amount in words)*) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) Has withdrawn its Bid during the period of bid validity specified; or

(b) Does not accept the correction of errors in accordance with the Instructions to Bidders (hereinafter "the ITB"); or

(c) having been notified of the acceptance of its Bid by the Purchaser during the period of bid validity, (i) fails or refuses to execute the Contract Form, if required, or (ii) fails or refuses to furnish the Performance Security, in accordance with the ITB.

This Guarantee shall expire: (a) if the Bidder is the successful bidder, upon our receipt of copies of the Contract signed by the Bidder and of the Performance Security issued to you by the Bidder; or (b) if the Bidder is not the successful bidder, upon the earlier of (i) our receipt of a copy of your notification to the Bidder that the Bidder was unsuccessful, otherwise it will remain in force up to ---------- *(insert date)* Consequently, any demand for payment under this Guarantee must be received by us at the office on or before that date._____

[Signature(s) of authorized representative(s)]

Qualification information

Schedule A – Relevant Experience in ICT Assignments in Government Hospitals of District General Hospital Level or Above

Bidders shall state the number of years and months of relevant experience and submit documentary evidence.

- Refer the Mandatory Criteria, Annex – 1
- Attach all supportive documents as proof
- Applicants shall provide details of their experience in reverse chronological (descending) order, with the most recent assignment listed first.

Period	Employer's Name and contact details	Description of Work	Contractor's responsibility	Amount (LKR)

Schedule B – Details of Staff (attach CVs as proof)

Name	Position	Task

Schedule C – Client's Reference

Attach certificates given by clients referring on the services executed by bidder

Schedule D- Annual turnover

Year	Turnover (Rs)	Remarks
		Attach certified income statement and balance sheet

Section IV. Conditions of contract

- **General provisions**

1.1	Applicable Law	The Contract shall be interpreted in accordance with the laws of the Socialist Democratic Republic of Sri Lanka
1.2	Language	This Contract has been executed in English Language
1.3	Notices	Any notice, request, or consent made pursuant to this contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the party to whom the communication is addressed, or when sent by registered mail, to such party at the address specified in the contract data.
1.4	Sub-contracting	Sub-contracting of the contracted services is not allowed without prior written approval of Teaching Hospital Peradeniya. However, escalation to OEM or authorized partner technical support for warranty, license, subscription or product-specific technical support shall be permitted, provided that the service provider remains fully responsible for the service delivery and confidentiality obligations under this contract.

2. Commencement, completion, modification, and termination of contract

2.1	Effectiveness of Contract	This contract shall come into effect on the date the contract is signed by either parties or such other later date as may be stated in the contract data.
2.2	Starting date	The service provider shall start carrying out the services seven (07) days after the date the contract becomes effective, or at such other date as may be specified in the contract data.
2.3	Intended period of the contract	The service provider shall provide services during the contract period as specified in the bidding data. If the service provider fails to provide requested services it shall be liable to pay liquidated damage as indicated.
2.4	Force Majeure	For the purposes of this contract, "Force Majeure" means an event which is beyond the reasonable control of a Party and which makes a Party's

		performance of its obligations under the contract impossible or so Impractical as to be considered impossible under the circumstances
2.5	No breach of contract	The failure of a party to fulfil any of its obligations under the contract shall not be considered to be a breach of, or default under, this contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.
2.6	Payments under the force Majeure	During the period of their inability to perform the services as a result of an event of Force Majeure, the service provider shall be entitled to continue to be paid under the terms of this contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the services and in reactivating the service after the end of such period
2.7	Termination - by the THP	The THP may terminate this contract, by not less than fourteen (14) days' written notice of termination to the service provider, to be given after the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause 2.7 and twenty-eight (28) days' in the case of the event referred to in (f):
		• If the service providers do not remedy a failure in the performance of their obligations under the contract, within fourteen (14) days after being notified or within any further period as the Employer may have subsequently approved in writing;
		• if the service provider become insolvent or bankrupt;
		• if, as the result of Force Majeure, the service provider/s are unable to perform a material portion of the services for a period of not less than thirty (30) days; or
		• if the service provider does not maintain a performance security
		• If the service provider has delayed the completion of the services by the number of days for which the maximum amount of liquidated damages can be paid in accordance with Sub-Clause 3.8 and the contract data.
		• If the Employer, in its sole discretion, decides to terminate this contract.
2.8	Termination - by the service provider	The service provider may terminate this contract, by not less than thirty (30) days ' written notice to the THP, such notice to be given after the occurrence of any of the events specified in paragraphs (a) and (b) of this Clause 2.8

		a) if the Employer fails to pay any monies due to the service provider pursuant to this contract and not subject to dispute pursuant to Clause within forty-two (42) days after receiving written notice from the service provider that such payment is overdue; or
		b) If, as the result of Force Majeure, the service providers are unable to perform a material portion of the services for a period of not less than fifty six (56) days.

3. Obligations of the service provider

3.1	General	The service providers shall perform the services in accordance with the THP's requirements stated in the section V and carry out their obligations with all due diligence, efficiency, and economy, in accordance with generally accepted professional techniques and practices, and shall observe sound management practices, and employ appropriate advanced technology and safe methods. The service providers shall always act, in respect of any matter relating to this contract or to the services, as faithful advisers to the THP, and shall at all times support and safeguard the THP's legitimate interests.
3.2	Confidentiality	The Service Provider shall not disclose any proprietary, confidential, patient-related, administrative, technical or operational information relating to the Project, the Services, this Contract or the Employer's business or operations without the prior written consent of the Employer. Confidentiality obligations relating to patient data, passwords, server access details, network configurations, system credentials and hospital information shall survive the expiry or termination of the contract.
3.3	Service providers' actions requiring THP's prior approval	The service providers shall obtain the THP's prior approval in writing before taking any of the following actions:
		• Appointing members of the personnel not listed by name in section B ("details of staff") and Section VIII
		• Changing the program of activities
		• Any other action that may be specified in the contract data.
3.4	Documents prepared by the service	All plans, drawings, THP's requirements, designs, reports, and other documents and software submitted by the service providers shall become and remain the property of the THP, and the service providers shall, not

	providers to be the property of the employer	later than upon termination or expiration of this contract, deliver all such documents and software to the THP, together with a detailed inventory thereof. The service providers may retain a copy of such documents and software. Restrictions about the future use of these documents, if any, shall be specified in the contract data.
3.5	Liquidated damage	If failure to provide the specified services within the specified period (mentioned under the section V) the provisions of the procurement Guidelines and Manual 5.20 shall apply.
3.6	Payment of liquidated damages	The service provider shall pay liquidated damages to the THP at the rate per day stated in the contract data for each day that the completion date is later than the intended completion date. The total amount of liquidated damages shall not exceed the amount defined in the contract data. The THP may deduct liquidated damages from payments due to the service provider. Payment of liquidated damages shall not affect the service provider's liabilities.
3.7	Correction for over-payment	If the intended completion date is extended after liquidated damages have been paid, the THP shall correct any overpayment of liquidated damages by the service provider by adjusting the next payment certificate. The service provider shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment.
3.8	Performance security	The service provider shall provide the performance security to the THP no later than the date specified in the letter of acceptance. The performance security shall be issued in an amount and form and by a bank or surety acceptable to the THP. The performance security shall be valid until a date 28 days from the completion date of the contract.

4. Service provider's staff

4.1	Description of personnel	The titles, job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the services of the service provider's technical personnel are described in section VIII.
4.2	Removal and/or replacement of personnel	• Except as the THP may otherwise agree, no changes shall be made in the technical personnel. If, for any reason beyond the reasonable control of the service provider, it becomes necessary to replace any of the technical personnel, the service provider shall provide as a replacement a person of equivalent or better qualifications
		• If the THP finds that any of the personnel have (a) committed serious misconduct or have been charged with having committed a criminal action, or (b) have reasonable cause to be dissatisfied with the performance of any of the personnel, then the service provider shall, at the THP's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the THP.
		• The service provider shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of personnel.

5. Obligations of the Teaching Hospital Peradeniya

5.1	General	If, after the date of this contract, there is any change in the applicable law with respect to taxes and duties which increases or decreases the cost of the services rendered by the service provider, then the remuneration and reimbursable expenses otherwise payable to the service provider under this contract shall be increased or decreased accordingly by agreement between the parties
5.2	Services and facilities	Detail of the services and facilities provided by the hospital is listed in the Annex 4

6. Payments to the service provider

6.1	Payment method & condition of payment	Method of payment and details are described in the section VII
6.2	Payment for additional services	This encompasses repair of defective equipment otherwise the cost is not mentioned in this contract. Service provider shall have to abide by the method stated in the Section V - specification and requirement of maintaining and servicing of ICT equipment, Local Area Network and Servers of TH Peradeniya

Section V – Requirement and description of the Services

Comprehensive Maintenance and Support Services for ICT Equipment, Local Area Network, Servers of Teaching Hospital Peradeniya (2026 – 2028)

Introduction

Teaching Hospital Peradeniya uses a Local Area Network, built with a fiber backbone and Cat 6/Cat 6A UTP cabling, together with related network devices and LAN equipment listed under **Section X – List of LAN Equipment**, and ICT equipment listed under **Section IX – List of ICT Equipment**, to support routine patient care services and administrative work. Therefore, any failure of the network, ICT equipment, or related services may seriously affect hospital functions, and network downtime is considered a critical issue.

Under this service agreement, the service provider shall provide comprehensive **preventive maintenance services** and necessary **corrective maintenance services** for the Local Area Network, network equipment, peripheral devices and ICT equipment listed in the relevant sections of this document. Preventive maintenance refers to regular checking, servicing and monitoring to identify and prevent possible faults before they occur. Corrective maintenance refers to troubleshooting, repairing, replacing or restoring equipment and services after a fault or failure has occurred.

In addition, the service provider shall be able to provide **24-hour end-user support** for the Hospital Information Management System when requested by end users or by officers of the Health Information and Research Unit of Teaching Hospital Peradeniya.

A brief description of the Hospital Information Management System is given below.

ICT equipment details and Local Area Network and Server details attached in Section IX and Section X

Description of HIMS

The Hospital Information Management System (HIMS) is a comprehensive hospital software system designed to support the functions of multiple departments and service areas within the hospital. The system consists of several modules. The following modules are currently implemented at Teaching Hospital Peradeniya.

Module	**Description**
Master Patient Index (MPI)	Used to register all inward patients, OPD patients and clinic patients. Annually, this module supports the registration and management of approximately **80,000–90,000 inward patients**, **250,000–300,000 OPD patients**, and **350,000 clinic patients**.
Admission, Discharge and Transfer module of Wards	Used for the admission, transfer and discharge of patients in wards and other relevant units. This module is currently used in **22 wards**, the **ICU**, **SBU**, **Operation Theatre** and **Labour Room**.
Laboratory Information Management System (LIMS)	Automates laboratory investigation ordering, sample processing, result entry and result publishing for all wards and relevant units of the hospital.
PACS (picture archiving and communication system) system integrated with RIS (Radiology Information System)	The Picture Archiving and Communication System (PACS), integrated with the Radiology Information System (RIS), supports radiology investigation ordering, processing, reporting, result publishing, image archiving and image retrieval for radiology services of the hospital.
MRO Module	A computerized module used to generate indoor morbidity and mortality statistics of the hospital. It is integrated with the eIMMR system of the Medical Statistics Unit for data transfer.
OPD system	A computerized system that automates the functions of the Outpatient Department. It supports outpatient treatment, operates in connection with the Pharmacy Module, and is also used for admitting patients for inward care. In addition, it supports referrals to clinics, dressing rooms, physiotherapy and other relevant services.

Pharmacy Module	Supports the complete automation of drug management activities in relevant hospital units. This module is integrated with the Medical Supplies Management Information System (MSMIS) of the Medical Supplies Division, Ministry of Health. Locally, it is integrated with the Clinic Module and OPD Module.
Clinic Module	Supports clinic patient registration, appointment scheduling, clinical documentation, investigation management and drug management for clinic patients.
Theatre Module	The Theatre Module is planned to digitize the existing manual theatre workflow up to a defined operational level, including theatre lists, procedure information, instrument details, and WHO Safety Checklist management.

Once a patient is admitted for inward care, the patient is registered in the Master Patient Index. The relevant ward where the patient receives inpatient care can access the MPI and complete the admission process through the HIMS. When investigations are required, ward staff use the Laboratory Information Management System to order investigations and view results.

The HIMS generates barcodes at the time of patient registration in the MPI and also when investigations are ordered from the point of care. Most ward registers, including admission registers, discharge registers and specimen registers, are generated through the HIMS.

The HIMS was developed by and is owned by the Ministry of Health. It is built using PHP and MySQL technologies. The system operates on a client-server model and is hosted on hospital servers.

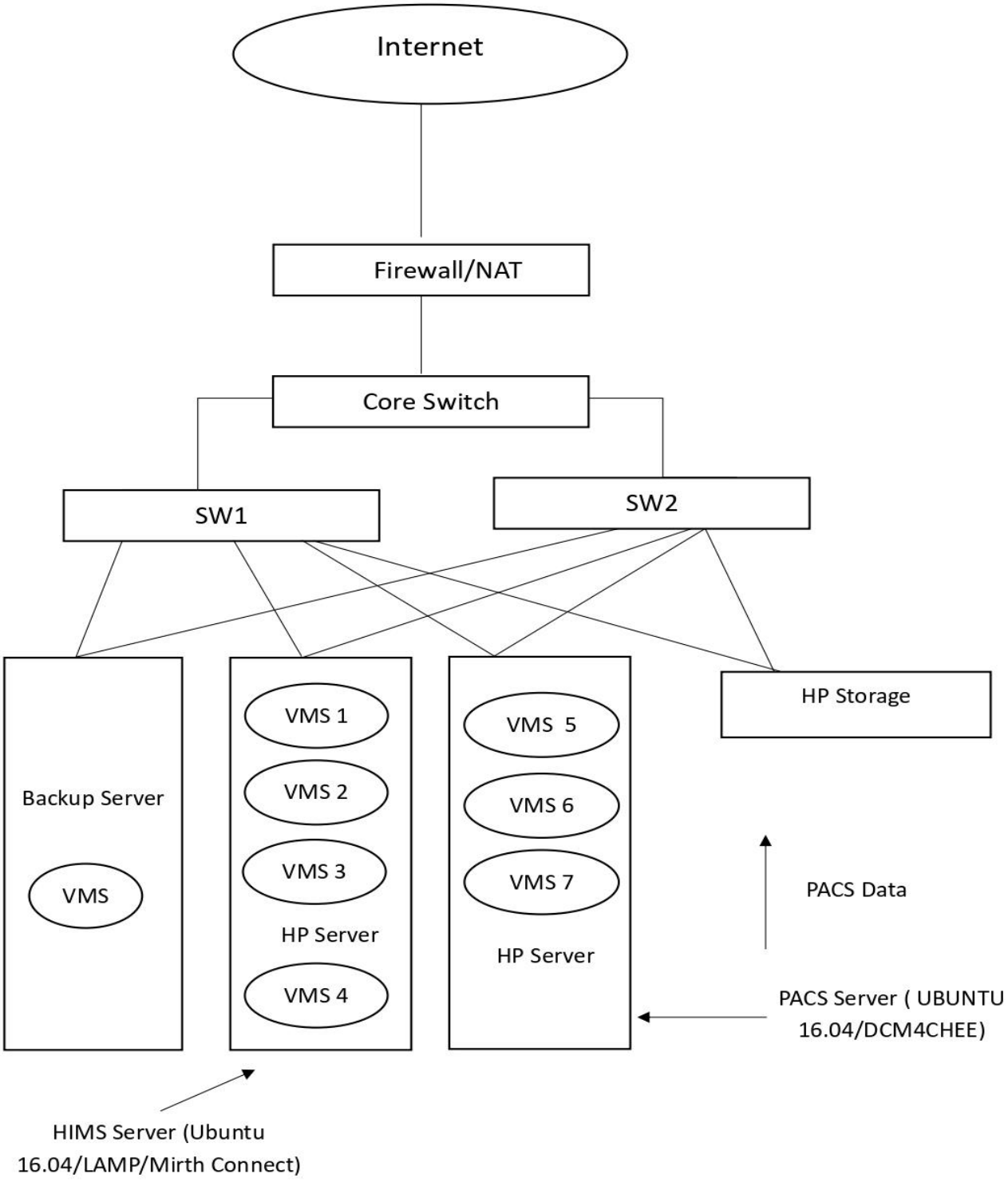
Description of Network and Server System

Teaching Hospital Peradeniya uses HIMS and PACS solutions to support patient care services. The HIMS software has been locally developed, while the PACS software is an open-source solution. The installation of a new licensed RIS system is currently ongoing under the supervision of the Ministry of Health.

The HIMS, RIS and PACS server environment consists of the servers, storage systems and related equipment listed in Section X. The service provider shall maintain the complete server environment, including any additional servers or related equipment introduced during the contract period.

The service provider is expected to maintain this server system and provide technical support for future expansion when required. The service provider should also have the capability to reinstall, configure, restore and manage the entire system when necessary. The hospital Local Area Network consists of **HP/Aruba switches** and **two Sophos firewalls**. The current system deployment is shown in the diagram below.

Current System Deployment (LAN & Server)



VM1 – HIMS Data Replication Server (Ubuntu 16.04)
VM2 – System Monitoring VM (Ubuntu 16.04)
VM3 – Analyzer Server (Windows 2012 R2)
VM4 – AV Update Server (Windows 10)
VM5 – Test Server (Ubuntu 16.04)
VM6 – Internet Server (Ubuntu 16.04)
VM7 – DMS Server (Ubuntu 16)

Scope of the project

No.	Service Requirement	Details
1.	System Installation	The service provider shall be capable of installing and configuring the complete system from scratch whenever required. This includes installation and configuration of operating systems, high availability software, replication software, databases, web services, PACS software and other related system components. The service provider shall carry out these activities without depending on the hospital IT staff and without proposing any solution that requires additional hardware, unless specifically approved by the hospital. The service provider shall also propose a suitable virtualization solution to run virtual machines, together with a monitoring solution to monitor the entire system, including network switches, server hardware, operating systems, databases, Mirth Connect, web services and other relevant services for performance and availability. The service provider shall clearly demonstrate their technical capacity and previous experience by submitting all necessary supporting documents with the bid.
2.	HIMS System Maintenance	The HIMS/RIS/PACS server environment consists of the servers, storage systems and related equipment listed in Section X. The service provider shall maintain the complete server environment and ensure its proper operation. In the event of server failure or replacement of hardware components, the service provider shall reinstall the operating system and all related software, restore required services and return the system to normal operation. The service provider shall regularly monitor the servers and take necessary preventive actions to avoid issues such as disk space limitations, service failures, performance degradation and system downtime.
3.	System Change Management	The service provider shall provide installation, configuration and technical support services for software upgrades, hardware upgrades, new software installations and new hardware installations whenever required. Such services shall be provided without any additional service charge during the agreement period, unless the hospital specifically approves otherwise.
4.	System Monitoring and Reporting	The complete HIMS, RIS and PACS server environment shall be monitored continuously on a **24x7 basis** to ensure proper operation, performance and availability. The service provider shall submit daily reports covering the system status, identified issues, corrective actions taken, preventive actions taken, and all activities carried out by the service provider during each day.

Section VI - Price schedule

Price schedule - ICT equipment maintenance

Item	Unit price	Quantity	Cost
Servicing of desktop computers / all-in-one computers			
Servicing of laptop computers			
Servicing of dot matrix printer			
Servicing of laser printer			
Servicing of ink tank printer			
Servicing of thermal sticker printer			
Servicing of thermal transfer printer			
Any other cost – specify details			
Total cost for servicing all ICT equipment of THP **(Sub Total 1)**			

Additional ICT equipment introduced during the contract period shall be covered without an additional service charge where such additions are within the normal operational scope of the hospital. Major expansions may be handled with prior approval and separate costing where required.

Service	Cost
Set up and update endpoint security solution (Sub Total 2)	

Price schedule - Local Area Network, Servers and other network related equipment

Service	Cost
Complete comprehensive maintenance of servers, firewalls, switches and other network accessories	
a. Hardware maintenance of switches, access points, firewalls, servers and all other network accessories	
b. Software maintenance of switches, access points, firewalls, servers and all other network accessories	
c. Operational maintenance of switches, access points, firewalls, servers and all other network accessories	
Total (Sub Total 3)	

<u>Summary of the Price Schedules</u>

Schedule	Amount
ICT equipment maintenance (Sub Total 1)	
Set up and update endpoint security solution (Sub Total 2)	
Local Area Network, Servers and other network related equipment (Sub Total 3)	
TOTAL (Sub Total 1 + Sub Total 2 + Sub Total 3)	

Cost of ICT equipment parts

Item	Brand/ Model	Unit price
USB Mouse		
USB Keyboard		
UPS battery for 650 VA UPS		
UPS battery for 3 KVA UPS		
Power cable for desktop PCs and printers		
VGA cable for desktop monitors		
RAM DDR3 / DDR4 – 4 GB		
Hard disk – 500 GB		
USB printer cable – 2 m		
Printer data cable		
Cat 6 patch cable – 2 m		
Cat 6 keystone and faceplate		
Cat 6 network cable – 1 m		
ATX power supply unit for desktop computers		
Universal power adapter for laptop computers		
USB extension cable – Type A		
USB extension cable – Type C		
USB Wi-Fi adapter		
HDMI cable – 1 m		
Single sunk box		
Cable tie – 6 inch		
RJ45 Cat 6 connector		

Note:

In addition to the items and materials specified above, if the selected bidder is required to carry out any additional work using other materials, payment for such work shall be made based on an estimate prepared by the Technical Officer of CECB.

Examples include PVC casing, conduit, Rawl plugs and screws, and flexible hose.

Section VII - Method of payment

1	Method of payment	Payment shall be made quarterly. For each contract year, 25% of the annual contract value shall be paid at the end of each quarter, subject to satisfactory service performance, submission of required service reports, monitoring reports and invoices, and acceptance by Teaching Hospital Peradeniya. The same payment method shall apply to both years of the contract period.

Section VIII – Qualification of Staff

The service provider shall deploy an adequate number of suitably qualified and experienced technical staff to provide ICT equipment maintenance, Local Area Network maintenance, server maintenance, HIMS end-user support, PACS/DICOM-related support, endpoint security support, network monitoring and related services at Teaching Hospital Peradeniya.

The proposed staff shall possess the required educational qualifications, professional qualifications, technical skills and relevant experience to perform the services specified in this tender document. Full details of the proposed staff members, including their roles, educational qualifications, professional qualifications, relevant experience and contact details, shall be submitted with the bid.

The hospital reserves the right to verify the qualifications and experience of the proposed staff. The service provider shall not replace the proposed key staff without prior written approval from Teaching Hospital Peradeniya. Any replacement staff shall possess equal or higher qualifications and experience than the originally proposed staff member.

1. Minimum Staff Composition

The service provider shall assign the following minimum technical staff for this contract.

No.	Staff Category	Minimum Number Required
1	Network Engineer / Network Administrator or equivalent	01
2	System Administrator / Server Administrator or equivalent	01
3	Network Technician	01
4	ICT Technician / Hardware Technician	02
5	HIMS / ICT End-User Support Officers	Adequate number to provide the required day and night duty coverage

The service provider shall ensure that staff leave, absence, resignation, shift changes or other internal administrative issues do not interrupt the required support coverage.

2. Network Engineer / Network Administrator or Equivalent

Minimum Qualification and Experience

The Network Engineer / Network Administrator shall have a Bachelor's Degree, Higher Diploma or equivalent qualification in Computer Networking, Information Technology, Computer Science or a related field, with at least five years of relevant experience in enterprise network administration.

Professional certifications in networking, firewall administration, network security or related areas will be considered an added advantage.

Main Responsibilities

The Network Engineer / Network Administrator shall be responsible for maintaining, configuring and troubleshooting the hospital Local Area Network and related network infrastructure, including:

- Switches, routers, access points and firewalls
- VLANs, VPNs, LAN, WAN and wireless networks
- Network security, access control and internet access restrictions
- Network monitoring and performance optimization
- Load balancing and high-availability-related network configurations
- Remote access through secure VPN where required
- Network documentation and change management records
- Troubleshooting and rectification of network failures
- Supporting future network expansion as requested by the hospital

The officer shall be capable of analyzing network issues, recommending suitable technical solutions and ensuring minimum network downtime.

3. System Administrator / Server Administrator or Equivalent

Minimum Qualification and Experience

The System Administrator / Server Administrator shall have a Bachelor's Degree, Higher Diploma or equivalent qualification in Information Technology, Computer Science, Server Administration or a related field, with at least five years of relevant experience in server and system administration.

Experience in Linux, Windows Server, virtualization, database services, backup systems, storage systems, web services, endpoint security and system monitoring is required.

Main Responsibilities

The System Administrator / Server Administrator shall be responsible for maintaining, configuring and troubleshooting hospital servers and related systems, including:

- Linux and Windows server environments
- Virtual machines and virtualization platforms
- Databases, including MySQL or related systems
- Web services required for HIMS, RIS, PACS and related applications
- Backup systems and restoration procedures
- Storage systems and disk space monitoring
- Server performance and availability monitoring
- Endpoint security solution deployment and updating

- Windows Update Server setup and maintenance
- Reinstallation and restoration of server systems when required
- Supporting PACS, DICOM Viewer, RIS and related hospital systems

The officer shall be capable of restoring services after server or system failure and shall support the hospital in maintaining continuous availability of critical ICT services.

4. Network Technician

Minimum Qualification and Experience

The Network Technician shall have a Technical Diploma, NVQ Level 4 or above, or an equivalent qualification in Networking, ICT or a related field, with at least three years of relevant experience in network support.

Main Responsibilities

The Network Technician shall provide technical support for:

- LAN cabling
- Network points
- Patch panels
- Access points
- Switches and related network accessories
- First-level troubleshooting of connectivity issues
- Support for network expansions
- Assistance to the Network Engineer during maintenance and fault rectification activities

Previous experience in supporting ICT infrastructure in a hospital or large institutional environment will be considered an added advantage**.**

5. ICT Technician / Hardware Technician

Minimum Qualification and Experience

Each ICT Technician / Hardware Technician shall have a Diploma, NVQ Level 4 or above, or an equivalent qualification in ICT, Computer Hardware or a related field, with at least three years of relevant experience in ICT equipment maintenance.

Main Responsibilities

The ICT Technician / Hardware Technician shall maintain and troubleshoot:

- Desktop computers
- All-in-one computers
- Laptop computers
- Printers, including laser, ink tank, dot matrix and thermal printers
- Barcode printers and barcode-related equipment
- Scanners and other peripheral devices
- UPS units and related accessories
- Basic operating system and software issues
- Hardware replacement and minor repairs
- Preventive maintenance of ICT equipment

At least two ICT Technicians / Hardware Technicians shall be assigned to this contract.

6. HIMS / ICT End-User Support Officer

Minimum Qualification and Experience

The HIMS / ICT End-User Support Officer shall have at least NVQ Level 4 in ICT or an equivalent qualification, with relevant experience in end-user support.

Previous experience in a hospital ICT environment or Health Information Management System support will be considered an added advantage.

Main Responsibilities

The HIMS / ICT End-User Support Officer shall provide first-level support for:

- HIMS user support
- Login and access-related issues
- Basic troubleshooting of HIMS modules
- Printer and barcode-related issues related to HIMS workflow
- Support for ward, OPD, clinic, pharmacy, laboratory and other HIMS users
- Escalation of unresolved issues to the relevant technical staff
- Communication with hospital users and the Health Information and Research Unit

The officer shall have strong interpersonal and communication skills and shall be able to support clinical, administrative and technical users in a professional manner.

---

7. On-Site and Duty Coverage Requirement

The service provider shall provide the following minimum duty coverage:

Duty Period	**Minimum Support Requirement**
Day duty: 8.00 am–5.00 pm	**At least 02 HIMS / ICT support officers**
Night duty: 5.00 pm–8.00 am	**At least 01 HIMS / ICT support officer**

At least two on-site support staff members shall be available within the hospital premises during day duty. These officers shall have knowledge and experience in ICT support services, including barcode printers, barcode printing, barcode-related troubleshooting, computer hardware support, printer support and basic HIMS end-user support.

At least one resident HIMS / ICT Support Officer shall be available within the hospital premises as required by the hospital. This officer shall possess relevant experience and recognized certification or qualification in computer hardware maintenance and troubleshooting.

8. Response Time and Service Availability

The service provider shall be capable of providing services on a 24-hour, 7-days-a-week basis during the contract period.

For HIMS and/or ICT equipment-related requests, the service provider shall attend the issue within 15 minutes of receiving the request.

For network and server-related issues notified by the responsible hospital officer, the service provider shall attend the issue within 15 minutes and rectify the issue at the earliest possible time. Critical network and server issues shall be rectified within a maximum of 04 hours, unless the delay is due to reasons beyond the control of the service provider and accepted by the hospital.

9. Security, Confidentiality and Remote Access

The service provider shall acknowledge in writing that the systems may contain confidential hospital, patient, administrative and technical information. The service provider shall ensure the confidentiality, integrity and availability of all data and systems handled under this contract.

The service provider shall sign a Non-Disclosure Agreement with the hospital at the beginning of the contract. This shall include confidentiality of passwords, server access details, network configurations and any other sensitive information.

Any remote access to servers, firewalls, switches or other active devices shall be carried out only through a secure VPN connection approved by the hospital. The service provider shall establish and maintain the required VPN arrangement at the beginning of the contract.

10. Submission of Staff Details

The bidder shall submit the following documents for each proposed staff member:

1. Curriculum Vitae
2. Copies of educational certificates
3. Copies of professional or technical certificates
4. Service letters or experience letters
5. Details of previous similar work experience
6. Contact details
7. Proposed role under this service agreement

Section IX – List of ICT equipment

No	Equipment	Number	Under warranty	Warranty expired
1	Desktop / All In One computers	233	45	188
2	Laptop computers	87	41	46
3	Dot matrix printers – LQ 310	80	04	76
	Dot matrix printers – LQ 2180	3	1	2
4	Ink tank printers – L 110	2	-	2
	Ink tank printers – M 100	26	-	26
	Ink tank printers – M 1170	18	18	-
	Ink tank printers – L6190	1	-	1
	Ink tank printers – L130	1	-	1
5	KIOSK	2	-	2
6	Laser printers	19	-	19
7	Thermal transfer sticker printer	15	-	15
8	Direct thermal sticker printers	37	3	34
9	Barcode Readers	73	10	63
10	UPS 650 VA	163	65	98
	UPS 2 KVA	7	1	6
	UPS 3 KVA	13	-	13

Section X – List of Local Area Network and Server Equipment

Set 1

Device name	**Model**	**Serial**
Server 1	HP ProLiant DL380p Gen 8	SGH450X44V
Server 2	HP ProLiant DL380p Gen 8	SGH450X44W
NAS	HP Store Easy 1640	CN74510CNN
Core switch	HP 5500	CN40B9R117
Access switch Non-PoE	HP1910	CN47BX20VI
Access switch Non-PoE	HP1910	CN47BX22BH
Access switch Non-PoE	HP1910	CN49BX22LF
Access switch Non-PoE	HP1910	CN48BX113K
Access switch Non-PoE	HP1910	CN49BX22J9
Access switch Non-PoE	HP1910	CN48BX1157
Access switch Non-PoE	HP1910	CN40BX200P
Access switch Non-PoE	HP1910	CN49BX21PT
Access switch Non-PoE	HP1910	CN49BX22MC
Access switch Non-PoE	HP1910	CN48BX115T
Access switch Non-PoE	HP1910	CN49BX21RS
Access switch Non-PoE	HP1910	CN40BX20IT
Access switch Non-PoE	HP1910	CN47BX228Q
Wireless access point	HP MSM410	TW36G424NW
Wireless access point	HP MSM410	TW36G424P7
Wireless access point	HP MSM410	TW36G424P5
Wireless access point	HP MSM410	TW36G424P1
Wireless access point	HP MSM410	TW36G424NZ
Wireless access point	HP MSM410	TW36G424NX
Wireless access point	HP MSM410	TW36G424NT
Wireless access point	HP MSM410	TW36G424NQ
Wireless access point	HP MSM410	TW36G424PD
Wireless access point	HP MSM410	TW36G424PF
Wireless access point	HP MSM410	TW36G424PO
Wireless access point	HP MSM410	TW36G424P2
UPS – 6 KVA	Riello SDL 6000 A4	ME27UT151270011

Set 2

Equipment	No.	Make	Model
Core switch (L3)	02	HP Aruba (5406 R)	J9821A
Switch 24 Port PoE (L2)	06	HP Aruba (2530 series)	J9773A
Switch 48 Port PoE (L2)	05	HP Aruba (2530 series)	J9772A
Switch 24 Port Non-PoE (L2)	02	HP Aruba (2530 series)	J 9976 A
Firewall for servers and internet access including PCs	01	Sophos	XG 310
Wireless access point	48	HP Aruba (303)	J2320 A
KVM switch	01	HPE	HPE LCD 8500
UPS – 6 KVA	01	Techfine	CE 6KS
UPS – 1 KVA	11	Techfine	CE 1KS
Power distribution unit	02	AUSTIN HUGHES	V12C13-16A W/F-EN/3B-1

Set 3

Equipment	No.	Make	Model
Server 1	01	Dell PowerEdge	R760XS
24G PoE Switch	01	HPE, Aruba	CX6100
UPS – 3kVA	01	BHP	BP 3KS

Annex 1 – MANDATORY CRITERIA

Documentary evidence need to be submitted with the

(Not being able to fulfill one or more of the mandatory criteria or providing false details for mandatory criteria will reject the bid during the evaluation) tender

	MANDATORY Criteria	Response (Yes/No)	Explanations (If required)
1	The bidder shall be a company registered in Sri Lanka in accordance with the laws of the country. A certified copy of the business registration certificate shall be submitted with the bid.		
2	The bidder shall submit certified financial statements of the company for the last three years.		
3	The bidder shall provide documentary evidence of financial capacity to import, supply, install, commission and carry out corrective and preventive maintenance services during the contract period.		
4	The bidder must have experience, **within the last six years** from the closing date of bid submission, in providing ICT infrastructure services and solutions to government hospital/s where Health Information Management Systems implemented by the Ministry of Health are implemented. The bidder shall clearly state the **number of years and months of such experience**, **the names of hospitals served**, **the period of service**, **the scope of services provided**, and **whether the services are completed**, **ongoing or contractually committed**. Relevant documentary evidence shall be submitted with the bid. **(Annex III - Qualification information)**		
5	The bidder shall submit documentary evidence of experience in providing end-user support for modules of Health Information Management Systems implemented by the Ministry of Health in government hospitals. The bidder shall clearly state the **number of years and months** of such experience, **the names of hospital/s served**, **the period of service**, **the HIMS modules supported**, and the **scope of end-user support provided**.		

6	Full details of the staff members assigned to this project, including educational qualifications, professional qualifications, relevant experience, proposed roles and contact details, shall be submitted with the bid. Minimum staff requirements are specified in Section **VIII – Qualification of Staff**.		
7	The maintenance team shall include, at minimum, one Network Engineer / Network Administrator, one System Administrator / Server Administrator, one Network Technician, two ICT Technicians / Hardware Technicians, and an adequate number of HIMSs / ICT End-User Support Officers to provide the required day and night coverage.		
8	At least one resident HIMS / ICT Support Officer shall have relevant experience and recognized certification or qualification in computer hardware maintenance and troubleshooting.		
9	The service provider shall provide at least two HIMS / ICT support officers during day duty from **8.00 am to 5.00 pm** and at least one HIMS / ICT support officer during night duty from **5.00 pm to 8.00 am**. These officers shall have knowledge and experience in ICT support services, including barcode printers, barcode printing and barcode-related troubleshooting.		
10	The service provider shall attend HIMS and/or ICT equipment-related support requests within **15 minutes** of receiving the request from the hospital.		
11	The service provider must provide 24-hour, 7-days-a-week support during the contract period. Network and server-related issues notified by the hospital officer responsible shall be attended within 15 minutes and rectified at the earliest possible time. Critical network and server issues shall be rectified within a maximum of 04 hours. Failure to restore the system within the stated time may result in a penalty of Rs. 10,000.00 per hour after the first 04 hours, subject to the conditions of the agreement.		
12	The service provider shall be able to cover all existing ICT equipment and any additional ICT equipment added during the contract period, as requested by the hospital without any additional charges		

13	The service provider shall be able to cover Local Area Network expansions requested by the hospital during the contract period without any additional charges		
14	The service provider shall cover new service requirements requested by the Ministry of Health or the Government of Sri Lanka during the contract period, where such requirements are within the scope of this contract. Any additional hardware, software licenses or major capital items shall be quoted separately unless already included in the price schedule.		
15	The selected bidder shall assess all hospital ICT equipment at the start of the contract and maintain a digital inventory management system. Each item shall be tagged using a unique registration number and supported by an individual digital file. The system shall include equipment details, warranty information, service history, support arrangements and a central ticket-based module to manage fault reporting, support calls and maintenance activities, preferably through the hospital intranet.		
16	The service provider shall supply, install, configure and regularly update an endpoint security solution for all necessary computers. The minimum specifications required for the endpoint security solution shall be included in **Annex 5.** The name, license period, endpoint count and price of the endpoint security solution shall be stated separately.		
17	The service provider should establish a **Windows Update Server** solution to reduce unnecessary internet bandwidth usage and support controlled updating of Windows computers.		
18	The bidder shall **submit documentary evidence** of experience in the installation, configuration, troubleshooting and maintenance of PACS systems and DICOM viewers in hospitals. The bidder shall clearly state the **number of years and months of such experience**, the names of hospitals served, the period of service and the scope of services provided.		

19	The bidder shall submit documentary evidence of experience in audio-visual broadcasting and audio-visual device configuration with relevant medical equipment, such as endoscopy machines and X-ray machines. Documentary evidence or video evidence shall be submitted with the bid.		
20	The bidder shall submit documentary evidence of experience in broadcasting, video-audio mixing and providing technical support for teaching workshops, training programs and events.		
21	The bidder shall submit certified financial statements of the company for the last three years.		
22	The bidder shall provide documentary evidence of financial capacity to import, supply, install, commission and carry out corrective and preventive maintenance services during the contract period.		
23	The cost of any relevant required licenses shall be furnished separately, where applicable.		
24	The service provider shall implement internet access restrictions when necessary, as instructed by the hospital, and shall support load balancing to ensure high uptime. Necessary instructions will be provided by the Health Information and Research Unit of Teaching Hospital Peradeniya.		
25	The service provider shall acknowledge in writing that the systems may contain confidential data and information. The service provider shall ensure the confidentiality, integrity and availability of all data and information handled under this contract.		
26	The service provider shall sign a Non-Disclosure Agreement with the hospital at the beginning of the contract. This shall include confidentiality of passwords, server access credentials, system configurations and any other sensitive information.		
27	When the service provider accesses servers or active network devices remotely, such access shall be carried out only through a secure VPN approved by the hospital. The service provider shall establish and maintain the VPN arrangement for this purpose at the beginning of the contract.		

Note: Documentary evidence may include contract agreements, award letters, service completion certificates, client confirmation letters, performance reports, service reports, official letters, videos or other acceptable documents issued by relevant institutions.

Annex 2 – Specification and Requirements for Maintenance and Servicing of ICT Equipment

No	Requirement	Details	Agree (Yes/ No)	If no, response
1	General Requirement	The service provider shall provide comprehensive preventive maintenance, corrective maintenance, repair services and end-user support for ICT equipment used at Teaching Hospital Peradeniya. This includes desktop computers, all-in-one computers, laptop computers, printers, barcode-related equipment, UPS units, peripheral devices and other ICT equipment used for HIMS and routine hospital office functions. The service provider shall ensure that ICT equipment remains functional, secure and available for routine patient care services and administrative work.		
2	Preventive Maintenance of ICT Equipment	The service provider shall carry out scheduled preventive maintenance for all ICT equipment covered under this agreement. Preventive maintenance shall include routine inspection, cleaning, performance optimization, software checking, endpoint security checking and identification of possible faults before equipment failure occurs. Preventive maintenance shall be carried out according to the agreed schedule, including monthly, quarterly and six-monthly maintenance activities. The detailed preventive maintenance activities are included under requirement no. 14 of this specification.		

3	Corrective Maintenance and Repair	The service provider shall provide corrective maintenance services whenever ICT equipment becomes defective or non-functional. Corrective maintenance shall include fault diagnosis, troubleshooting, repair, replacement of approved parts and restoration of the equipment to normal working condition. Any defective equipment or part identified during preventive or corrective maintenance shall be reported to Teaching Hospital Peradeniya in writing. Replacement of parts shall be carried out only after obtaining approval from the hospital. Where the cost of a replacement part has not been included in the bidding document, the service provider shall submit an estimate and obtain approval before carrying out the repair or replacement.		
4	Replacement of Parts	Parts used for replacement or repair shall be of the same brand or a genuine/compatible equivalent approved by Teaching Hospital Peradeniya. Replacement of parts shall normally be carried out only for ICT equipment for which the warranty period has expired. For equipment under warranty, the service provider shall coordinate with the relevant warranty provider or supplier as instructed by Teaching Hospital Peradeniya. Defective equipment or removed parts shall be handed over to Teaching Hospital Peradeniya for disposal according to the hospital's ICT equipment and parts disposal policy. The service provider shall not dispose of hospital property independently.		

5	On-Demand ICT Support Services	• The service provider shall provide on-demand support services when requested by the hospital. These services shall include, but shall not be limited to, the following: • Troubleshooting of computer hardware and software issues • Troubleshooting of internet and Local Area Network connectivity issues • Installation and configuration of computers, printers and barcode-related equipment • Configuration of ICT equipment for HIMS and other hospital systems • Replacement of printer ribbons, toner cartridges, ink cartridges, sticker rolls and Health ID tags, where required • Reformatting of computers where required, after hospital approval and necessary backup/data protection measures The service provider shall provide basic technical assistance for the existing hospital CCTV system when requested by Teaching Hospital Peradeniya. This shall be limited to minor support and coordination, excluding major repairs, replacements or upgrades unless separately approved.		
6	End-User and HIMS Support	The service provider shall provide desktop support and end-user support for HIMS users and office users when requested. This shall include support for daily operation of HIMS, basic computer-related issues, printer-related issues, barcode-related issues, login/access issues and other ICT-related user support requirements. The service provider shall provide support according to the duty coverage specified in Section VIII - Qualification of Staff and the Mandatory Criteria, including day and night support where applicable.		

7	Central Ticket-Based Support System	The service provider shall establish a central ticket-based system for fault reporting, support call management, maintenance tracking and service reporting within one month from the date of award of the tender. The hospital intranet may be used for this purpose where appropriate. All ICT equipment faults, support requests, maintenance activities and corrective actions shall be recorded through this system. Until the central ticket-based system is fully implemented, the service provider shall maintain an interim manual or digital fault reporting register.		
8	ICT Equipment Assessment and Inventory Management	The service provider shall assess all ICT-related equipment at the beginning of the contract. All equipment shall be registered in a digital inventory management system and tagged using a unique registration number. Each item shall have an individual digital file containing the following information: • Equipment type • Brand and model • Serial number • Location / unit / ward • Warranty details • Service history • Repair history • Replacement history • Support arrangements • Current functional status • Any Other important information The service provider shall maintain and update this inventory throughout the contract period using suitable software.		

9	**Execution of Services and Reporting**	The service provider shall carry out preventive maintenance activities according to the agreed maintenance schedule. On-demand activities shall be attended within 15 minutes of receiving the request. After completion of each job, the service provider shall submit a complete service report describing the activities carried out. The report shall be countersigned by the technician and the service-requesting officer of the relevant unit or ward. The service provider shall submit service reports and relevant invoices to Teaching Hospital Peradeniya for payment processing where applicable.		

10	**Use of Backup ICT Equipment**	Where backup ICT equipment is provided by the hospital, the service provider shall use such equipment for prompt restoration of services when equipment becomes defective. Thereafter, the defective equipment shall be repaired and returned to the respective unit. Refer to "***List of ICT equipment provided by the hospital***" ICT Equipment Provided by THP as Backup Equipment, where applicable.		
11	**Coverage of Additional ICT Equipment**	Any additional ICT equipment introduced during the contract period shall be included in the maintenance coverage without an additional service charge, unless otherwise agreed by Teaching Hospital Peradeniya		
12	**Data Security and Confidentiality**	The service provider shall ensure the confidentiality, integrity and security of data stored in ICT equipment handled during maintenance.		
13	**Cost**	The cost for all requested services, replacement parts, software solutions, endpoint security solution and additional services shall be furnished separately in the relevant price schedule.		
14	**Preventive Maintenance Schedule for ICT Equipment**	The service provider shall carry out the following preventive maintenance activities as part of the main ICT equipment maintenance requirement. These activities shall be documented in the service report and linked to the central ticket-based system or inventory management system where applicable.		

14.1	**Monthly Preventive Maintenance Activities**	• Carry out disk clean-up and system optimization where applicable. • Carry out disk defragmentation only where technically appropriate. Defragmentation shall not be performed on SSDs unless specifically required. • Remove unauthorized or unnecessary software with the approval of Teaching Hospital Peradeniya or the Health Information and Research Unit. • Clean and dust the main unit, keyboard, mouse and monitor of desktop computers and all-in-one computers. • Scan, detect and remove harmful software, including viruses, malware, spyware and other harmful programs. • Delete temporary files, including internet temporary files, Windows temporary files, cookies and other unnecessary files. • Update the endpoint security solution installed on relevant computers. • Update operating systems through an approved update mechanism, subject to compatibility with hospital systems. • Update approved software required for HIMS and other hospital systems, subject to compatibility and hospital approval.		
14.2	**Quarterly Preventive Maintenance Activities**	• Service, clean and dust printers, including laser printers, ink tank printers, dot matrix printers, thermal sticker printers and thermal transfer printers. • Service, clean and dust UPS units and check their functional status.		
14.3	**Six-Monthly Preventive Maintenance Activities**	Clean and remove dust from inside the system unit of desktop computers and other relevant ICT equipment using industry-accepted methods and suitable cleaning materials.		
14.4	**Cleaning Materials**	Chemicals and materials used for cleaning shall be industry-accepted and suitable for use with ICT equipment. The service provider shall ensure that cleaning activities do not damage ICT equipment or affect hospital operations.		

List of ICT equipment provided by the hospital as backup equipment

No	Equipment	Quantity
1	Desktop computer	01
2	650 VA UPS	01
3	2D Barcode Reader	01
4	Inkjet Printer (B/W)	01
5	Brother QL 800 printer	01

Annex 3 - Requirements for Maintenance and Servicing of Local Area Network, Servers and Other Network-Related Equipment

No	Requirement	Details	Agree (Yes/No)	If no, response
1	**General Scope of Maintenance**	1.1. Provide comprehensive software, hardware and operational maintenance for all physical servers, virtual servers, firewalls, switches, wireless network components, fiber backbone, UPS units related to switches and servers, and other network-related accessories. 1.2. Maintain the required server, network and communication environment to support HIMS, RIS, PACS and other hospital information systems. 1.3. Ensure that maintenance activities are carried out with minimum interruption to patient care services and routine hospital operations. 1.4. This contract includes firewall maintenance, configuration support and operational support only. Supply of a new firewall appliance is not included under this tender unless separately specified by Teaching Hospital Peradeniya.		
2	**Daily Monitoring and Reporting**	2.1. Carry out daily monitoring of servers, virtual servers, firewalls, switches, wireless access points, network connectivity, storage, backup services, operating systems, databases, web services and other critical services required for hospital operations. 2.2. Use a licensed or legally authorized network and system monitoring solution. The name and price of the proposed monitoring solution shall be stated separately in the bid. 2.3. Configure automated monitoring, alerts and reports where technically possible to detect performance, availability, storage, security and service-related issues early. 2.4. Submit a daily electronic monitoring report to the designated officer of the Health Information and Research Unit of Teaching Hospital Peradeniya. 2.5. Failure to carry out monitoring and submit the daily report may result in a penalty of Rs. 1,000.00 per day, subject to the conditions of the agreement.		
3	**Server and Virtual Server Maintenance**	3.1. Provide comprehensive maintenance for server hardware, operating systems, virtualization platforms, virtual machines, storage services, backup services, databases and web services. 3.2. Monitor server performance, disk space, logs, availability, backup status and service status, and take preventive action to avoid failures or downtime.		

		3.3. Reinstall, configure and restore operating systems, server software and required services when necessary due to server failure, hardware replacement or system corruption. 3.4. Support required server-side software and services used for HIMS, RIS, PACS and other hospital information systems, as instructed by the authorized hospital officer.		
4	**Firewall and Network Security Maintenance**	4.1. Provide comprehensive hardware, software and operational maintenance for firewall solutions and related network security services. 4.2. Maintain firewall rules, VPN configurations, NAT rules, internet access restrictions, load balancing and other security-related configurations as instructed by the hospital. 4.3. Support high availability, performance and secure access to hospital information systems and internet services. 4.4. Changes to firewall or security configurations shall be documented and carried out only with approval from the authorized hospital officer.		
5	**Wireless Network Maintenance**	5.1. Maintain the hospital wireless network equipment listed in the relevant equipment section, including access points, controllers and other wireless network accessories. 5.2. Provide hardware, software and operational maintenance for wireless network components. 5.3. Monitor wireless network performance, availability, coverage, authentication and connectivity issues. 5.4. Support configuration changes and expansion of the wireless network when requested by the hospital.		
6	**Network Expansion and New Device Configuration**	6.1. Carry out basic network expansion work requested by the hospital during the contract period. 6.2. Install and configure new network active and passive devices, including switches, access points, patch panels and other network-related equipment, when requested. 6.3. Hardware required for expansion shall be supplied by Teaching Hospital Peradeniya unless otherwise specified in the tender document. 6.4. Additional materials, licenses or major capital items not included in the contract shall be quoted separately and used only after approval by the hospital.		
7	**Preventive Maintenance Activities**	7.1. Preventive maintenance shall include inspection, servicing, cleaning, adjustment, configuration checking, software/firmware update where		

		applicable, performance checking and identification of possible defects before failure occurs. 7.2. The service provider shall carry out not less than four preventive maintenance visits per year for all equipment covered under this agreement. 7.3. The interval between two consecutive preventive maintenance visits shall not be less than two calendar months and shall not exceed four calendar months. 7.4. Replacement of defective components identified during preventive maintenance shall be carried out only after reporting to and obtaining approval from Teaching Hospital Peradeniya. 7.5. All ancillary services provided during preventive maintenance visits shall be included in the contract cost, and the hospital shall not be liable for additional service charges for such activities.		
8	**Corrective Maintenance Activities**	8.1. Corrective maintenance shall include diagnosis, repair and restoration of defective equipment or services to satisfactory working condition. 8.2. Corrective maintenance may be initiated when a fault is reported by the hospital through the central ticketing system, email, telephone call or any other approved communication method. 8.3. The service provider shall attend network and server-related issues within 15 minutes of receiving the request. 8.4. Critical network and server issues shall be rectified at the earliest possible time and within a maximum of 04 hours, subject to the conditions of the agreement. 8.5. The cost of any replacement part shall be pre-agreed with the hospital through the due procedure. The list and cost of common replacement items shall be submitted with the bid where applicable. 8.6. Parts used for replacement or repair shall be of the same brand or a genuine/compatible equivalent approved by Teaching Hospital Peradeniya, especially where the original equipment is end-of-life or no longer supported.		
9	**Standby Equipment for Prompt Restoration**	9.1. The service provider shall ensure the availability of at least one standby active LAN device in the Computer Maintenance Unit for prompt restoration of network services during failures. 9.2. Where the standby device is to be supplied by the bidder, the cost shall be stated separately. Where standby equipment is supplied by Teaching Hospital Peradeniya, the service provider shall configure and use such equipment for prompt service restoration.		

		9.3. The defective equipment shall be repaired and returned to service as soon as possible after temporary restoration.		
10	**Reporting and Documentation**	10.1. After each preventive or corrective maintenance visit, the service provider shall submit a complete report describing the activities carried out. 10.2. The report shall include defects identified, corrective actions taken, pending issues, recommendations and any further action required. 10.3. Reports shall be submitted to the Director of Teaching Hospital Peradeniya or an authorized nominee by email and/or hard copy as required. 10.4. Network diagrams, device inventories, IP address records, configuration change records and service logs shall be maintained and updated throughout the contract period.		
11	**Access to Equipment and Security Procedures**	11.1. The service provider shall access servers, firewalls, switches and other active devices only with authorization from the hospital and according to hospital security procedures. 11.2. Remote access to servers or active network devices shall be carried out only through a secure VPN approved by the hospital. 11.3. Passwords, server access details, firewall configurations, network diagrams and other sensitive information shall be handled confidentially. 11.4. The service provider shall comply with the confidentiality and Non-Disclosure Agreement requirements stated in the Mandatory Criteria.		
12	**Ownership and Disposal of Removed Components**	12.1. All components removed during preventive or corrective maintenance shall remain the property of Teaching Hospital Peradeniya. 12.2. Removed components, defective parts and replaced items shall be handed over to the hospital for disposal according to the relevant hospital procedure. 12.3. The service provider shall not remove, discard, reuse or dispose of any hospital-owned equipment or components without written approval from the hospital.		
13	**On-Demand Configuration and System Support**	13.1. The service provider shall provide required configuration support, operating system installation and server-side software installation necessary to run hospital information systems when requested by the authorized hospital officer. 13.2. On-demand configuration support shall include server configuration, service configuration, network configuration, firewall configuration, virtual machine configuration and related technical support within the scope of the contract.		

		13.3. Any change that may affect system availability, data security, network security or clinical service continuity shall be carried out only after approval from the authorized hospital officer.		
14	**Cost, Licences and Additional Items**	14.1. The cost of monitoring software, required licences, standby devices, replacement parts and additional materials shall be furnished separately where applicable. 14.2. No additional cost shall be incurred by the hospital for routine maintenance services already covered under this agreement. 14.3. Any item or service outside the agreed scope shall be carried out only after submission of an estimate and approval by Teaching Hospital Peradeniya.		

Annex 4 – Services and Facilities Provided by the Employer

The following services and facilities shall be provided by Teaching Hospital Peradeniya to support the service provider in carrying out maintenance and support services during the contract period.

No.	Service / Facility	Details
1	**Equipment Room**	Teaching Hospital Peradeniya shall provide a dedicated room or suitable space to store backup ICT equipment, subject to availability and hospital administrative arrangements. The use of such space shall be coordinated through the Health Information and Research Unit.
2	**Equipment Details and Existing Records**	Teaching Hospital Peradeniya shall provide available records of ICT equipment, network equipment, servers and other related equipment, including identification numbers, serial numbers, locations and other available details. The selected service provider shall verify, update and maintain the final detailed inventory in consultation with the nominated officers of the Health Information and Research Unit.
3	**Inspection of Equipment Before Bid Submission**	Bidders may inspect the ICT equipment, Local Area Network, server infrastructure and other relevant equipment before finalizing their bids, with prior approval from Teaching Hospital Peradeniya. Such inspections shall be coordinated through the Health Information and Research Unit or any other officer nominated by the hospital.
4	**Coordination by Technical Personnel**	The Health Information and Research Unit of Teaching Hospital Peradeniya shall coordinate equipment inspection, maintenance arrangements, service requests and communication between the hospital and the service provider during the contract period.
5	**Backup ICT Equipment**	Teaching Hospital Peradeniya shall provide available backup ICT equipment to support prompt restoration of services where possible. The service provider shall use such backup equipment only with the approval of the hospital and shall maintain proper records of issue, use and return. Refer to "***List of ICT Equipment Provided by the Hospital"*** as Backup Equipment.
6	**Consumables**	Printer ribbons, toner cartridges, ink cartridges, sticker rolls, Health ID tags and similar consumables shall be provided by Teaching Hospital Peradeniya or by the officer-in-charge of the relevant unit/ward, unless otherwise specified in the contract.
7	**Access to Equipment**	The service provider shall be given authorized access to the equipment listed in Section IX and Section X for the purpose of preventive maintenance, corrective maintenance and related support services. Access shall be provided in accordance with hospital security procedures, working arrangements and instructions issued by the authorized officers of Teaching Hospital Peradeniya. Access outside normal working hours shall be subject to prior approval or emergency authorization by the hospital.

No.	Service / Facility	Details
8	**Security and Confidentiality**	The service provider shall ensure that access to hospital ICT equipment, servers, network devices and related systems is used only for authorized maintenance and support activities. No data, documents, system credentials or configuration details shall be copied, removed, disclosed or misused. The service provider shall comply with the confidentiality and Non-Disclosure Agreement requirements of the tender.

Annex 5 - Minimum Specifications for Endpoint Security Solution

Antivirus Software (320 Licenses for 2026 – 2028 Years Period)			
Component	***Minimum Requirement***	***Confirm (Yes/No)***	***Remarks***
Product Name	Specify		
Version	Specify		
Country of Origin	Please specify		
General Specification			
Industry certifications	The product must have security certifications such as VB100, ICSA, SE Labs AAA, SC Ratings, etc.		
Recognized vendor	The product should be listed in Gartner reviews and actively participate in evaluations in last tree year continuously. (Evidence should be provided)		
Integrates with other security systems	The antivirus must work smoothly with existing and future security tools to strengthen overall protection.		
Prevents cyber breaches	It should block both known and unknown threats like ransomware, malware, exploits, and new (zero-day) attacks.		
Protects users without slowing them down	Users should be able to use web apps and do their daily work safely without interruptions or performance issues.		
Provides strong detection and protection	The system must detect and stop threats effectively without slowing down or harming the organization's systems.		
Fits into existing systems easily	It should integrate smoothly with the current IT setup without requiring major changes.		
Supports cloud and on-premises	The solution should work either in the cloud or on the organization's own servers.		
Includes next-gen endpoint protection	It must have advanced protection for devices like PCs, laptops, and servers.		
Allows upgrade to EDR without changes	It should be possible to add advanced monitoring (EDR) later without replacing the whole system.		
Supports encryption	It should allow secure data encryption using different algorithms without changing the setup.		

Provides tamper protection	The system must stop unauthorized people from disabling or altering it.		
Easy client upgrades	The antivirus software on user devices must update automatically and smoothly.		
Efficient updates across network	Updates should be shared between devices to reduce internet use, and fall back to vendor servers if needed.		
Functional requirements			
Protection from new (zero-day) attacks	The system must stop completely new cyber threats without depending only on traditional virus signature databases.		
Proven			
ransomware defense	Must have a proven record of blocking ransomware and other advanced threats.		
Allow/block list (whitelist/blacklist)	IT staff must be able to create rules to allow or block apps/files for a single device, groups, or all systems.		
Multi-site support	Should work across multiple offices with centralized IT management, even if staff have different skill levels.		
Protection for all device types	Must protect desktops, laptops, servers (Windows, macOS, Linux).		
Hardware visibility	Must provide reports on device details (hardware, vendor info, accessories).		
Network load info	Should show network usage reports in MB.		
Easy-to-use web dashboard	Must provide a simple, centralized web interface for administration.		
Simplifies routine tasks	Should make regular IT security work easier to manage		
Automated prevention using AI	The solution should automatically adapt based on threat intelligence, machine learning, and behavior analysis.		
Light on resources	Must not slow down computers or use resource-heavy methods.		
OS update alerts	Should notify IT when operating system updates are available.		
Flexible email alerts	Must send email notifications to IT staff about suspicious activities.		
Single lightweight agent	All features should run through one small program that uses less than 15% of system resources.		

Minimal performance impact	Protection should not noticeably slow down users during scanning or normal use.		
24/7 vendor support	Vendor must provide around-the-clock support via remote tools, email, or phone.		
Deployment & problem support	Vendor must help with planning, setup, and problem-solving during implementation.		
Knowledge transfer	Vendor must train IT staff so they can effectively run and maintain the solution long term.		
Technical Requirements			
Device protection	Must protect Windows 8.1, 10, 11 (32 & 64 bit), Windows Server 2012 R2 and above, macOS, and Linux devices.		
	Proposed solution should support cross platform including Mac, Windows, Linux and Android		
Minimum system requirements	Vendor must provide the minimum hardware/software needs and supported browsers for running the security dashboard.		
Single license key	One license key should cover all versions of the solution.		
License management	IT should be able to assign licenses to specific sites and restrict admins so they can only manage licenses for their assigned sites.		
Low false positives	The system should wrongly detect threats less than **0.1%** of the time.		
No performance slowdown	The protection software must not slow down computers or servers.		
Easy deployment	The software must be simple to install, reinstall, or update using tools like GPO, SCCM, or remote deployment.		
Real-time & historical reports	Must provide both live and past data in easy-to-read reports.		
Role-based access	Users should only see information relevant to their role; administrators must have full system access.		
Real-time threat alerts	Any detected threat should instantly notify IT staff.		
Visual dashboards	Threat stats should be shown in both charts and numbers.		
Open reporting system	Reports must be shareable/exportable to other systems.		
Scheduled reports	Should generate automatic reports for monitored devices on a set schedule.		

Email reports	Reports should be sent by email.		
Holistic reporting	Must provide complete, long-term reporting (real-time, on-demand, or for specific time periods).		
Centralized updates	Threat definition updates should be deployed centrally with minimal network usage.		
Remote console access	The admin dashboard should be available anytime, from any device, for authorized IT staff.		
Custom reports	IT should be able to create custom scheduled reports in addition to standard ones.		
Event filtering	Dashboard must filter events to show only important security data.		
Remote workstation control	The management console should allow detailed control and installation of agents on remote devices.		
Operational Protection Features			
Active Directory integration	The solution must connect with Active Directory (ADFS) so users can log in using their organization accounts.		
Device control	IT must be able to centrally manage and schedule device permissions (e.g., USB, external drives).		
Web control	Must include a web filter (by URL or category) with centralized management and scheduling of web access.		
Automated workflows	Should reduce manual IT tasks with automated processes.		
Easy replacement of old system	Must replace the current antivirus solution without losing features or causing issues.		
Fileless malware protection	Should detect malware that runs only in memory (without files).		
Behavioral detection (HIPS)	Must monitor system activities for suspicious behavior and defend itself against attacks.		
Exploit & botnet protection	Should block system exploits and stop connections to botnets (hacker-controlled networks).		
DNA detection	Must detect and block malicious behavior patterns.		
UEFI scanner	Should monitor firmware integrity and alert users if it's tampered with.		
Global search	Must allow IT to easily search and drill down into suspicious activity reports.		
Ransomware protection	Must detect and block ransomware-like behavior.		
	Solution should have capability of Ransomware remediation for selected file types such as restore affected file.		

Prevent unauthorized uninstall	Users, even with admin rights, should not be able to uninstall the antivirus from organization devices.		
Remote uninstall option	IT should be able to uninstall the software remotely via the management console if needed.		
Remote investigation & cleanup	IT must be able to investigate and fix infected devices remotely.		
Detailed reporting	Must provide interactive, drill-down reports on incidents.		
Full audit trail	Should keep complete logs of all activities and workflows.		
Block malicious IPs	Must detect and block malicious IP addresses for a set period, keeping them on a blacklist.		
AMSI script scanning	Must scan PowerShell and Windows Script Host scripts for malicious activity.		
Deep scanning	Must scan memory, boot sectors, emails, archives, runtime packers, etc.		
Office document protection	Solution Should scan Office files and downloads (e.g., ActiveX) before they open.		
Multiple remediation levels	Must offer different levels of response/remediation for threats.		
Host isolation	Should be able to isolate a compromised device to prevent malware spread.		
Brute force protection	Must detect and block brute-force login attempts without needing extra tools.		
	Solution should be able to block IP and Devices temporarily if malicious activities or suspicious activities detected		
Network access protection	Solution should be able to manage network Connection profile and management and control Connection		
	Solution should be providing reputational information of running processes and executable.		
	Provide Realtime network connection statics for further audit and trouble shoot		
Incident management	Solution should identify and alert security incident of the organization.		
	Proposed solution must support incident respond to computers affected by incident		
	Detail root cause overview and incident timeline should be altered		

Additional Licenses	The quoted price should remain applicable for any future license purchases made within a period of three (3) years from the date of this activation.		
Training			
Certified training for staff	Vendor must provide official training from the product manufacturer so IT staff learn how to set up, use, and maintain the system.		
	Certification level should be provided.		
Classroom-style training	Training must cover all important features and be tailored to the chosen solution.		
Support during acceptance period	Vendor must explain how they will provide support and what the guaranteed response time will be.		
On-site emergency support	Vendor must confirm if they can send staff on-site in case of a serious emergency.		