DEPARTMENT OF EXTERNL RESOURCES

Ministry of Finance, Planning and Economic Development

BIDDING DOCUMENT (VOLUME 02)

National Competitive Bidding (NCB)

Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite and Data Migration of Existing Data from the Present System for the Department of External Resources.

IFB No: ERD/ADM/04/Server

Director General
Department of External Resources
The Secretariat (3rd Floor)
Colombo 01.

Contents

Invitation for Bids (IFB)
Ministry of Finance, Planning and Economic Development

DEPARTMENT OF EXTERNAL RESOURCES (ERD)

Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite and Data Migration of Existing Data from the Present System for the Department of External Resources.

IFB No: ERD/ADM/04/Server

1. The **Chairman**, **Department Procurement Committee** on behalf of the **Department of External Resources of the Ministry of Finance, Planning and Economic Development** now invites sealed bids from eligible and qualified bidders for the **Procurement of Supply, Installation and Data Migration of Virtualized Server, Firewall Infrastructure & Supply, Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite for Department of External Resources.** as specified in the Procurement Document.

   Delivery & Installation period shall be within **04 months** from the Date of Awarding.

2. Bidders must meet the following minimum qualification criteria:

   - Participation as a Supplier in at least One (1) project of supplying and Installation of Data Centre IT infrastructure with a value of at least LKR 400 million that has been successfully completed within the last Three (3) years

   - Minimum average annual turnover of LKR 600 million calculated as total certified payments received for the contracts in progress or completed, within the last 3 years.

   - Bidder shall have below ISO certifications and copies of the valid certifications should be submitted along with the bid response.

     - ISO 9001 – Quality Management System (QMS)
     - ISO 27001 – Information Security Management System (ISMS)
     - ISO 22301 – Business Continuity Management System (BCMS)

3. Bidding will be conducted through the **National Competitive Bidding (NCB – Single Stage, Tow Envelops)** procedures specified in the **National Procurement Guidelines-2024** and are opened to all eligible bidders as defined in the Guidelines.

4. Interested eligible bidders could obtain further information from **Wasantha Dharmasena, Additional Director General (CUD) of the ERD,** Mob: 0714 899 674, Tel : +94 112 484 653, Electronic mail address: wasantha@erd.gov.lk and inspect the Bidding Documents at the address given below from 09.00 to 16.00hrs in working days, Commencing from **24the November , 2025**.

5. A complete set of Bidding Documents in English can be purchased by interested Bidders on the submission of a written application on a business letterhead, and upon payment of a non-refundable fee of **Sri Lankan Rupees Fifty Thousand (LKR 50,000.00),** the method of payment will be cash**.**

6. Bids must be delivered to the address below at or before **15.00 hrs. on 15th December 2025**. Late bids will be rejected. Bids will be opened soon after the bid closing at the address below (No: 7) in the presence of the bidders' representatives, who choose to attend at **15.00 hrs. on 15th December 2025**. All bids must be accompanied by a Bid Security of not less than **Sri Lankan Rupees Four Million (LKR 4,000,000.00)** valid up to 14th April 2026.

7. A pre bid meeting will be held at 10.30 **hrs.** on **29th November 2025 at** the **Conference Room of External Resources**, Room No 303, 3rd Floor, The Secretariat, Colombo 01.

Director General
Department of External Resources
The Secretariat (3rd Floor)
Colombo 01.

Section II. Bidding Data Sheet (BDS)

The following specific data for the goods to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

ITB Clause Reference	**A. General**
ITB 1.1	The Purchaser is: **Department of External Resources, Sri Lanka**
ITB 1.1	The name and identification number of this procurement are: **Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite and Data Migration of Existing Data from the Present System for the Department of External Resources.** **IFB No: ERD/ADM/04/Server**
ITB 2.1	The source of funding is **Government of Sri Lanka**
ITB 4.4	Foreign bidders / Joint Venture are **not allowed** to participate in this bidding.
	B. Contents of Bidding Documents
ITB 7.1	For **Clarification of bid purposes** only, the Purchaser's address is: Attention: **Wasantha Dharmasena,** **Additional Director General (CUD)** Address: **Department of External Resources** **Room No: 310** **Third Floor,** **The Secretariat,** **Colombo 01.** Telephone: **0112 484 653** Mobile number: **0714 899 674** Electronic mail address: wasantha@erd.gov.lk pre-bid conference will be held on: Date:**29th November 2025** Time: **10.30 hrs.** at the Department of External Resources, Conference Room No 303, 3rd Floor, The Secretariat, Colombo 01.
	C. Preparation of Bids
ITB 11.1 (e)	The Bidder shall submit the following additional documents: (i) written confirmation authorizing the signatory of the Bid to commit the Bidder, in accordance with ITB Clause 21;

	(ii) Documentary evidence in accordance with ITB Clause 16 establishing the Bidder's eligibility to bid. (iii) Documentary evidence in accordance with ITB Clause 17, that the Goods and Related Services to be supplied by the Bidder are of eligible origin. (iv) Minimum average annual turnover of LKR 600 million calculated as total certified payments received for the contracts in progress or completed within the last 3 years. The bidder should furnish documentary evidence on all past supplies of comparable value as the bid, over the last three years, together with evidence of satisfactory performance, such as certificate of acceptance. (v) Copies of original documents defining the constitution or legal status, place of registration and principal place of business of the company, firm or partnership, etc. (vi) Details of service centers and information on service support facilities that would be provided after the warranty period. (vii) Reports on the financial standing of the bidder such as Profit and Loss statements, Bankers certificates, balance sheets, auditor's reports, etc. for the past three years. (viii) Bidder should submit the direct OEM Manufactures Authorizations for the All hardware and Software items including **Firewall, HCI, Virtualized Software & Email Solution with Office Productivity Suite should be included.** (ix) The bidder should furnish a brief write-up explaining available facilities, capacity, resource personnel and experience for the manufacturing/ maintaining and supply of the equipment within the specified time.
ITB 14.1	Add the following to ITB 14.1 The price of the goods quoted Delivered Duty Paid (DDP) at the destination given in the Schedule of Requirements. The term DDP shall be governed by the rules prescribed in the current edition of Incoterms published by the International Chamber of Commerce, Paris
ITB 14.3	The Bidders may quote the following minimum quantities: Bidders are requested to quote 100% of the items indicated in the price schedule
ITB 14.4	All taxes other than VAT shall be included to the bid price
ITB 15.1	The bidder shall quote the total bid price in Sri **Lankan Rupees**.

ITB 17	Add the following to ITB 17: 17.4 Standards for workmanship, process, material, and equipment, as well as references to brand names or catalogue numbers specified by the Purchaser in the Schedule of Requirements, are intended to be descriptive only and not restrictive. The Bidder shall offer other standards of quality, brand names, and/or catalogue numbers, provided that it demonstrates, to the Purchaser's satisfaction, that the substitutions ensure substantial equivalence or are superior to those specified in the Schedule of Requirements.

	17.5 To establish the eligibility of Goods and Related Services in accordance with ITB Clause 5, Bidders shall complete the country-of-origin declarations in the Price Schedule Forms, included in Section IV, Bidding Forms.
ITB 17.3	Period of time the Goods are expected to be functioning **at least five years including warranty period.** Supplier shall carry sufficient inventories to assure ex-stock supply of consumables and spares in Sri Lanka.
ITB 18.1 (a)	The bidder shall submit the direct OEM Manufactures Authorizations for the **HCI Hardware, Software, Firewall, Switches, Wi-Fi access points, Servers, Backup Software, Email Solution with Office Productivity Suite and for combined systems separate MAL for hardware.**
ITB 18.1 (b)	After sales service is **required**
ITB 19.1	The bid shall be valid until 16th **March 2026**
ITB 20.1	The Bid shall include a Bid Security included in Section IV Bidding Forms.

ITB 20.2	The amount for Bid Security shall be **LKR 4,000,000.00** The validity period of the bid security shall be until **14th April 2026** Bids shall include a Bid Security issued by Bank Guarantee using (Central Bank of Sri Lanka approved License Commercial Bank) the form included in Section IV (Bidding Forms). and valid for 28 days beyond the original validity period of the bid.
	D. Submission and Opening of Bids
ITB 22.2 (c)	The **Original** and **one copy** of the bid shall be submitted. A separate Softcopy of the technical bid in searchable format should be included. Also, the Name and number of the Bid: **Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite and Data Migration of Existing Data from the Present System for the Department of External Resources.** **IFB No: ERD/ADM/04/Server** should be stated in the top left-hand corner of the envelopes.
ITB 23.1	For bid submission purposes, the Purchaser's address is: Attention: **Director General** Address: **Department of External Resources** **Room No: 310** **Third Floor, The** **Secretariat,** **Colombo 01.**
	The deadline for the submission of bids is: Date: 15th **December , 2025,** Time: **15.00 hrs.** In the Event of the specified date for the submission of bids, being declared a holiday for the Purchaser, the bids will be received up to the appointed time on the next working day.
ITB 26.1	The bid opening shall take place at: Address: **Department of External Resources** **Conference Room No 303,** **3rd Floor, The Secretariat,** **Colombo 01.** Date: 15th **December , 2025,** Time: **15.00 hrs.** **"Telex, Cable, E-mail or facsimile bids will be rejected"**
	E. Evaluation and Comparison of Bids
ITB 34.1	Domestic preference **shall not** be a bid evaluation factor.

ITB 35.3(d)	The adjustments shall be determined using the following criteria, from amongst those set out in Section III, Evaluation and Qualification Criteria: *(a)* Deviation in Delivery schedule: **No** *(b)* Deviation in payment schedule: **No** *(c)* the cost of major replacement components, mandatory spare parts, and service: **No**
ITB 35.4	The following factors and methodology will be used for evaluation: Bidding will be conducted through the National Competitive Bidding (NCB- Two Envelope System : Single Stage - Two Envelope Bidding Procedure) method specified in the Procurement Guidelines - 2024 on Goods, Works, and Non-Consulting Services
ITB 35.5	**Not Applicable**

F. Intention to Award the Contract

The Department shall notify unsuccessful bidders in writing, either by post and/or email, regarding the DPC's intention to award the contract to the successful bidder.

Standstill Period and Appeals

There shall be a minimum interval of ten (10) working days between the submission date of the Department's notification of the intention to award the contract to the successful bidder and the actual award of the contract. This interval is referred to as the Standstill Period.

Submission of Appeals

Any bidder, whether successful or unsuccessful, who wishes to appeal the contract award decision must submit a written appeal to the Chairman, Department Procurement Appeal Committee (DPAC) before the expiry of the Standstill Period. Each appeal must be accompanied by a non-refundable cash deposit of Sri Lanka Rupees Ten Thousand (LKR 10,000/=), which shall be paid to the Account Division at Department of External Resources. The payment receipt must be submitted along with the appeal. The DPAC shall only consider appeals supported by proof of such deposit. It is the sole responsibility of the appellant to ensure that the appeal includes all relevant supporting documents to substantiate the grievance.

Section III. Evaluation and Qualification Criteria

This Section complements the Instructions to Bidders. It contains the criteria that the Purchaser uses to evaluate a bid and determine whether a Bidder has the required qualifications. No other criteria shall be used.

Contents

1. Evaluation Criteria (ITB 35.3 (d))

The Purchaser's evaluation of a bid shall consider, in addition to the Bid Price quoted in accordance with ITB Clause 14, one or more of the following factors as specified in ITB Sub-Clause 35.3(d) and in BDS refer to ITB 35.3(d), using the following criteria and methodologies.

(a) Delivery schedule
Not Applicable

(b) Deviation in payment schedule.
Not Applicable

(c) Cost of major replacement components, mandatory spare parts, and service.
Not Applicable

2. Evaluation Criteria (ITB 35.4)

Bidding will be conducted through the National Competitive Bidding (NCB- Two Envelope System: Single Stage - Two Envelope Bidding Procedure) method specified in the Procurement Guidelines - 2024 on Goods, Works, and Non-Consulting Services.

a) In order to evaluate the quality aspects of the Technical Bid, Bidder must state comprehensively with sufficient details, how their Bid meets the Technical Requirements specified in Section VI (Schedule of Requirements) Sufficient documentary evidence shall be provided where applicable.

b) Bidder's Technical bid must meet all the requirements stipulated in Section VI (Schedule of Requirements) of this Procurement Document.

During the evaluation process, the evaluation committee will assign to each selected feature a whole number rating from 0 to 100, where 0 means that the feature is absent and 100 for significantly exceeding the requirements. Objective of this tender is to get a state of the art, HCI Server Architecture with Hybrid Model , with easy and secure user access, work from anywhere, and increase Office Productivity. With this objective, evaluation committee will determine the critical/Mandatory compliances and major deviations from them. Depending on the criticality of the item to the complete solution, 0 marks can be allocated to the item, as it is none responsive to the requirements.

Table 2.1 Technical marks allocation for each category

Index	Evaluation Criteria	Marks
1	**Experience of the Bidder**	**28 Marks**
1.1	Experience in Similar Projects (Specific and General experience)	4
1.2	Experience in each technology area, with 5 reference projects as per section 6.2	24
2	**Technical Compliance**	**44 Marks**
2.1	Section 6.3	12
2.2	Section 6.4	4
2.3	Section 6.5	1
2.4	Section 6.6	1
2.5	Section 6.7	1
2.6	Section 6.8	3
2.7	Section 6.9	3
2.8	Section 6.10	1
2.9	Section 6.11	1
2.10	Section 6.12	0.5
2.11	Section 6.13	0.5
2.12	Section 6.14	0.5
2.13	Section 6.15	4
2.14	Section 6.16	2
2.15	Section 6.17	2
2.16	Section 6.18	0.25
2.17	Section 6.19/6.20	6
2.18	Section 6.21/6.22	1
2.19	Section 6.23	0.25
3	**Strengths of Proposed Team**	**22 Marks**
3.1	Key Technical Team as per section 6.1	22
4	**Approach, Methodology, Project Plan & Support and Maintenance**	**6 Marks**
4.1	Technical Approach and Methodology	2
4.2	Project Plan	2
4.4	Support and Maintenance	2
		100 Marks

3. Multiple Contractors (ITB 35.5)

No additional factors and select the substantially responsive lowest evaluated bid

4. Post qualification Requirements (ITB 37.2)

(A) Financial Capability

The Bidder shall furnish documentary evidence that it meets the following financial requirements:

(a) Minimum average annual turnover of LKR **600 million calculated** as total certified payments received for contracts in progress or completed, within the last 3 years. (Bidder shall submit Audited financial statements for last 3 years)

(b) The bidder must demonstrate access to or availability of financial resources such as liquid assets, un-encumbered real assets, line of credit and other financial means, other than any contractual advance payment to meet the cash flow requirement of not less than Sri Lanka Rupees **Two Hundred Million (LKR 200 million)** or equivalent, and net of the bidder's other commitments for this project.

(B) Experience and Technical Capacity

The Bidder shall furnish documentary evidence to demonstrate that it meets the following experience requirements:

- Participation as a Supplier in at least One (1) project of supplying and Installation of Data Centre IT infrastructure with a value of at least **LKR 400 million** that has been successfully completed within the last Three (03) years. (Bidder must submit the detailed list of similar projects/orders that the bidder has completed successfully during the period of last three (03) years ending on the deadline of bid submission)
- Supplier Technical Proficiency (Certificates or Documents should be provided),
- In-house qualified and experienced full-time technical staff of proposed technologies/products.

(C) Business Registration And Public Contract Registration

Authorized agent in Sri Lanka represents the manufacturer/manufacturer authorized export agent abroad, shall register himself with the Registrar of Companies and shall produce a valid copy of the Certificate of Incorporation issued by the Registrar of Companies of Sri Lanka together with the bid.

Any person who act as an agent or sub-agent, representative or nominee for or on behalf of a manufacturer/principal supplier, shall register himself and the contract as per Public Contracts Act, No 23 of 1987 for every public contract exceeding Five million Sri Lanka Rupees (LKR 5,000,000.00). The Certificate of Registration (FORM PCA 03) issues by the Registrar of Public Contracts of Sri Lanka in term of section 11 of the said Act shall be submitted along with the bid, only if the total value exceeding Five million Sri Lanka Rupees (LKR 5,000,000.00).

5. Domestic Preference (ITB 3 4.1)

Not Applicable

Section IV. Bidding Forms

4.1 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:_______________

IFB No: ERD/ADM/04/Server

To: **Director General**
Department of External Resources
Room No: 303
Third Floor,
The Secretariat,
Colombo 01.

We, the undersigned, declare that:

(a) We have examined and have no reservations for 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 for the **Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite and Data Migration of Existing Data from the Present System for the Department of External Resources.**

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

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

(d) Our bid shall be valid for the period of time specified in ITB Sub-Clause 19.1, from the date fixed for the bid submission deadline in accordance with ITB Sub-Clause 23.1, and it shall remain binding upon us and shall be accepted at any time before the expiration of that period.

(e) If our bid is accepted, we commit to obtain performance security in accordance with ITB Clause 43 and CC Clause 17 for the due performance of the Contract;

(f) We have no conflict of interest in accordance with ITB Sub-Clause 4.2.

(g) Our firm, its affiliates or subsidiaries, including any subcontractors or suppliers for any part of the contract, has not been declared blacklisted by the Department of Public Finance.

(k) 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.

(l) 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]*

4.2.(A) PRICE SCHEDULE

1	2	3	4	5	6	7	8	9	10
Line-Item No.	Description of Goods or related services	Country of Origin of the Goods	Unit	Qty	Unit price Excluding VAT	Total Price Excluding VAT (Col 4*6)	Discounted Total price (if any) excluding VAT	VAT	Total Price Including VAT (Col. 8+9)
1	**HCI Cluster active DC**		Nr	1					
2	**HCI Cluster DR DC**		Nr	1					
3	**Virtualization software for Active and DR**		Nr	2					
4	**Data Center Switch for Active and DR**		Nr	3					
5	**Data Backup Software Solution for Active and DR**		Nr	2					
6	**Data Backup Repository Hardware for DR**		Nr	1					
7	**Data Backup Repository Hardware for Active DC**		Nr	1					
8	**Firewalls for Active and DR**		Nr	3					
9	**Microsoft AD for Active and DR**		Nr	2					
10	**TOR Aggregation 10G/25G Fiber switch**		Nr	1					
11	**Firewall At Head Office**		Nr	1					

12	**M-Gig Floor Switch with 25G uplinks+ PoE**		Nr	5					
13	**Wi-Fi access point**		Nr	5					
14	**Datacenter IT Operations Platform**		Nr	1					
15	**Centralized Network Management Platform**		Nr	1					
16	**Identity and Access Control Solution**		Nr	1					
17	**Management switch for DCs**		Nr	2					
18	**1 UPS, 1 x22 U Rack, 1x42 U Rack**		Item	1					
19	**SASE for Remote users**		Nr	100					
20	**Price of Microsoft items from Table 4.2(B).3**		Item	1					
21	**End Point Security (for 100 users and 20 servers)**		Nr	1					
22	**Admin Training**		Nr	1					
23	**Support and Maintenance charges for 24x7 NOC and Helpdesk**		Item	Sum					
24	**Solution Implementation**		Item	Sum					
25	**Provisional Sum for power/network/Accessories**		Item	Sum					
Total Bid Price including three-year Comprehensive Warranty Charges									

Note

All charges with regard to the supply of spare parts, labor, travel, per diem and accommodation to supplier's staff etc. shall be borne by the supplier during the 3-year warranty period. The FMEP shall not pay any additional expenditure on services rendered during the 3-year warranty period.

.

4.2.(B) PRICE SCHEDULE For Microsoft items

Prices should be in Sri Lankan Rupees

- Please indicate the amounts for VAT and other applicable tax types separately in all price tables. (US$ conversion date 28 days prior to closing of bids as published by the Central Bank of Sri Lanka)

1.	2.	4.	5.	6.	7.	8.	9.
Line - Item No.	Description of Goods or related services	Unit	Qty	Unit price Excluding VAT	Total Price Excluding VAT (Col 5*6)	VAT	Total Price Including VAT (Col. 7+8)
1	Commissioning of Email Solution with email security	Nr	100				
2	Cloud base Identity Integration	Nr	100				
3	Setup, Migration, Installation and Commissioning of office Productivity Suite with end device management	Nr	100				
4	Support & Maintenance Charges	Item	Sum				
5	Other Implementing Charges (Please specify)						
	Total Price including one year Subscription				(A)		

****The bidder must provide additional e-mail accounts for the same price as quoted, within the initial contract period when requested by ERD.**
****Licenses and support should be provided for a period of three (03) years, with payments to be made on 3-year basis.**

The lowest bid price among substantially responsive bidders will be determined by taking the lowest price given for ‘D’. That is lowest bid price will be the sum of (A) Supply, installation with 1st year subscription fee + (B) + (C) 2nd and 3rd year subscription with L2, L3, L4 support [D=A+B+C].

Name of Bidder: …………………………………………………………………….

Signature of Bidder: ……………………………………………………………....

1.	2.	4.	5.	6.	7.
Line - Item No.	Description of Goods or related services	Unit	Qty	2nd year subscription charge LKR (without VAT)	3rd year subscription charge LKR (without VAT)
1	Subscription charges	Nr	01		
2	Support & Maintenance Charges	Item	Sum		
	Total Price including yearly Subscription			(B)	(C)

4.2(C) Total Bid cost Table

Table	Price Component	Total (excluding VAT)	VAT	Total with VAT & Other Applicable Taxes
4.2.1	Items Indicated in Table	(A)		
4.2.2	2nd and 3rd year subscription with support	(B) + (C)		
	Total Bid Cost to be carried to 4.1. Bid Submission Form	(D)=(A)+(B)+(C)		

*The lowest bid price among substantially responsive bidders will be determined by taking the lowest price given for 'D'. That is lowest bid price will be the sum of (A) Supply, installation, Migration, Commissioning and Maintenance of Email Solution with office productivity suite Installation with 1st year subscription fee + (B) + (C) 2nd and 3rd year subscription with support [D=A+B+C].

Name of Bidder: ……………………………………………………………………….

Signature of Bidder: ……………………………………………………………………....

4.3 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 General
Department of External Resources
Room No: 303
Third Floor,
The Secretariat,
Colombo 01.

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 **IFB No: ERD/ADM/04/Server** ("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)]

4.4 Manufacturer's Authorization

[The Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. The Bidder shall include it in its bid, if so, indicated in the BDS.]

Date: _____________
IFB No: ERD/ADM/04/Server

To: **Director General**
Department of External Resources
Room No: 303
Third Floor,
The Secretariat,
Colombo 01.

WHEREAS

We *[insert complete name of Manufacturer]*, who are official manufacturers of *[insert type of goods manufactured]*, having factories at [insert full address of Manufacturer's factories], do hereby authorize *[insert complete name of Bidder]* to submit a bid the purpose of which is to provide the following Goods, manufactured by us *[insert name and or brief description of the Goods]*, and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty in accordance with Clause 27 of the Conditions of Contract, with respect to the Goods offered by the above firm.

Signed: *[insert signature(s) of authorized representative(s) of the Manufacturer]*

Name: *[insert complete name(s) of authorized representative(s) of the Manufacturer]*

Title: *[insert title]*

Duly authorized to sign this Authorization on behalf of: *[insert complete name of Bidder]*

Dated on ____________ day of __________________, *[insert date of signing]*

4.5 Bidder Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]

Date: ______________
IFB No: ERD/ADM/04/Server
Page ________ of_ ______ pages

1. Bidder's Legal Name [*insert Bidder's legal name]*
2. Bidder's of Business / Company Registration: *[insert of Registration]*
4. Bidder's Year of Registration: *[insert Bidder's year of registration]*
5. Bidder's Legal Address in Registration: *[insert Bidder's legal address in registration]*
6. Bidder's Authorized Representative Information Name: *[insert Authorized Representative's name]* Address: *[insert Authorized Representative's Address]* Telephone/Fax numbers: *[insert Authorized Representative's telephone/fax numbers]* Email Address: *[insert Authorized Representative's email address]*
7. Below ISO certifications and copies of the valid certifications should be submitted along with the bid response. • ISO 9001 – Quality Management System (QMS) • ISO 27001 – Information Security Management System (ISMS) • ISO 22301 – Business Continuity Management System (BCMS)
8. Public Contract Registration : *[insert of Registration]*

Section V. Schedule of Requirements

5.1. List of Goods and Delivery Schedule

Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning and Data Migration for the Department of External Resources.

Line-Item No.	Description of Goods or related services	Qty	Final Project site Destination	Delivery Date/Weeks from Date of signing of the contract
1	**HCI Cluster active DC**	1	DR in Kurunegala and PR in Jawatta	8
2	**HCI Cluster DR DC**	1		8
3	**Virtualization software for Active and DR**	2		8
4	**Data Center Switch for Active and DR**	3		8
5	**Data Backup Software Solution for Active and DR**	2		8
6	**Data Backup Repository Hardware for DR**	1		8
7	**Data Backup Repository Hardware for Active DC**	1		8
8	**Firewalls for Active and DR**	3		8
9	**Microsoft AD for Active and DR**	2		8
10	**TOR Aggregation 10G/25G Fiber switch**	1		8
11	**Firewall At Head Office**	1		8
12	**M-Gig Floor Switch with 25G uplinks+ PoE**	5		8
13	**Wi-Fi access point**	5		8
14	**Datacenter IT Operations Platform**	1		8
15	**Centralized Network Management Platform**	1		8
16	**Identity and Access Control Solution**	1		8
17	**Management switch for DCs**	2		8
18	**1 UPS, 22 U Rack, 42 U Rack**	Lot		
19	**SASE for Remote users**	100		8
20	**Email and collaboration Solution on cloud environment for 100 users**	1		4
21	**End point protection (for 100 users and 20 servers)**	120		8
22	**Admin Training**	1		4
23	**Provisional Sum for power/network/Accessories**	Lot		8

5.2. List of Related Services and Completion Schedule for Hybrid Server system

Service	**Description of Service**	**Quantity**	**Physical Unit**	**Place where Services shall be performed**	**Final Completion Date(s) of Services**

01	**Admin Training**	3 persons	Item		

5.3 List of Goods and Delivery Schedule for Supply, Installation, Commissioning , Maintenance and Data Migration of Email Solution with Office Productivity Suite for ERD

5.3.1 List of Goods and Delivery Schedule

Line - Item N□	Description of Goods	Quantity	Physical Unit	Final (Project Site) Destination as specified in BDS	Delivery Date
					Delivery date
01.	Office Productivity Suite with end point management	100	Lot	Department of External Resources Colombo 01	Within two weeks of the Date of awarding the Contract
02	Email Boxes with Security	100	Lot	Department of External Resources Colombo 01	Within two weeks of the Date of awarding the Contract
03	Cloud based identity Integration	100	Lot	Department of External Resources Colombo 01	Within two weeks of the Date of awarding the Contract

5.3.2 List of Related Services and Completion Schedule

Service	Description of Services	Quantity	Physical Unit	Place where Services shall be performed	Final Completion Date(s) of Services
01.	Setup, migration, installation & commissioning	Item	Sum	Department of External Resources Colombo 01	Within Four months of the Date of awarding the Contract
02	Comprehensive Technical training for daily management operation and troubleshooting.	15	Staff	Department of External Resources Colombo 01	Within Four months of the Date of awarding the Contract

5.4 Technical Specification

Procurement of Supply, Installation of Hybrid Virtualized Server, Firewall Infrastructure & Installation, Commissioning for the Department of External Resources.

5.4.1 Scope of Work: System Usage and Capacity Upgrade

Supply delivery installation commissioning, Operations and Maintenance of infrastructure virtualization for Department of External Resources.

The successful bidder of this procurement will hereafter be identified as the Supplier or as the "Solution Implementation Partner (SIP) "in this document.

No	**Item**	**Description/ Item**
5.4.1.1	Input Parameters (input data types and volumes the system will process)	Documents and related database input (word, excel, power point, pdf, jpg, pst, zip, RAR etc.) Project Proposals with related documents, video clips, photos, Document Management System - Scanned documents, TA System Profile Applications, Digital certificates and signatures.
5.4.1.2	Applications (comprehensive list of applications currently running and planned for installation on the server)	ERD Web Server - Joomla TA web and database management Server Mariane Investment web and database Server Database Server/MS SQL Server 2022- Inventory Management, Attendance Management, Document Management, Postal Management, Mail Server- 120 user's mail management system DNS Server and Active Directory Controller Servers Backup Servers and Public Data Sharing Server
5.4.1.3	Current Capacity Requirements (Detail current resource demands (CPU, RAM, Storage…. etc.)	Usage and availability of resources of current server system is attached as annexure 1- Server Details and Annexure 2 - Storage Details.
5.4.1.4	Future Facilities (Any planned services or functionalities to be implemented on the server within the expected lifetime)	Developing Network architecture to enable all users of ERD for Work from Home Concept. Developing e services and web applications in order to facilitate stakeholders. Application for the Digital Signature
5.4.1.5	Services (services expected from the server (e.g., web, database management, application serving)	Services should cover applications mentioned in row 2 and row 4 in this table.

5.4.1.6	Future requirements (Total required capacity increase for the next five years)	Approximately 2 times increment of current RAM and Capacity.

- ➢ Additionally, there will be more applications planned to be deployed in the proposed Hybrid environment in the future. The size given in this document is based on current requirements and some of the predictable future expansion requirements.

- ➢ 3 Domains of web sites migration to new system.

- ➢ Solution provided by Bidder should be able to facilitate migration of workloads to local cloud environment (in the jurisdiction of Sri Lanka) at any time ERD request and solution architecture should support this hybrid cloud environment. Required migration support should be provided by the Bidder.

- ➢ Integration of the ERD Head Office, Data Centers and Local cloud infrastructures, with the links provided by ERD and should be given the IPVPN or P2P specification by Bider.

- ➢ All Data Center power and connectivity Wirings, brakers and other accessories for the installation should be provided.

5.4.2 Overview of scope of work for Solution Implementation Partner SIP

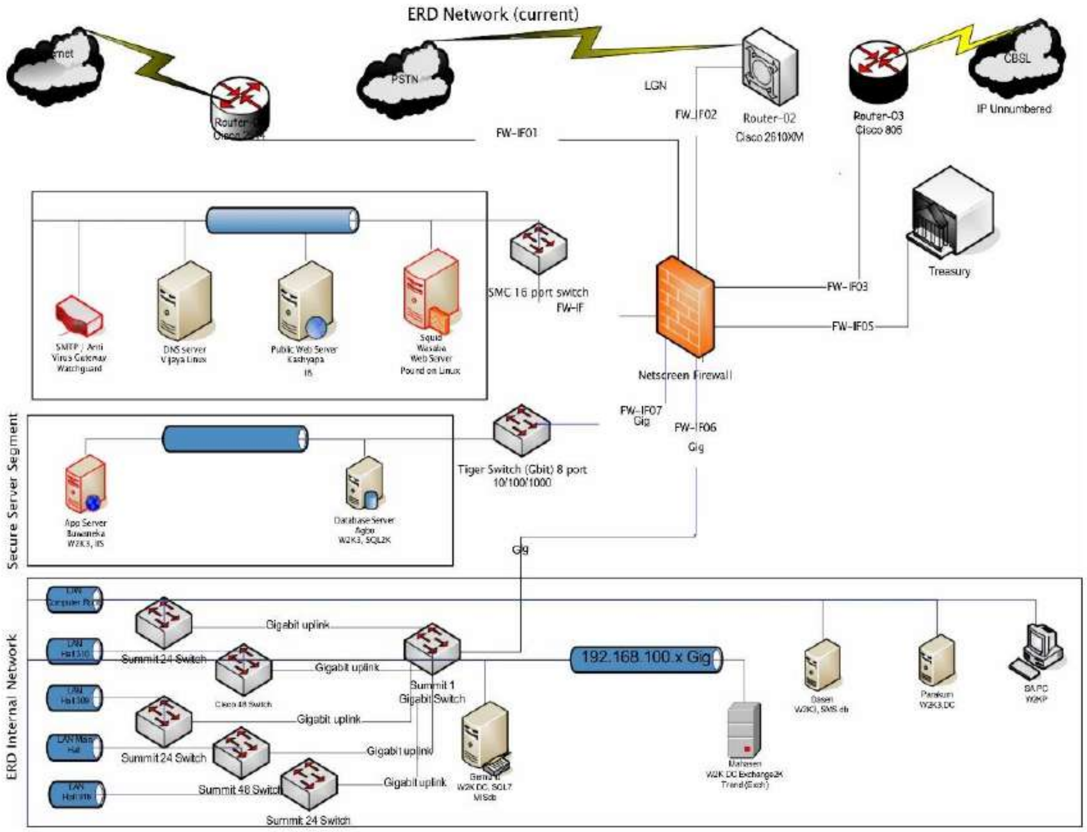
Key areas of scope of work	Summary of Scope of Work
1. Detail Project Plan	SIP need to perform the following key activities: a. SIP needs to study current infrastructure and provide the implementation plan. b. SIP needs to prepare the comprehensive project plan for total implementation. c. SIP needs to mention any application support or any stakeholder support in advance.
2. Design and develop infrastructure virtualization solution and Firewall.	SIP needs to gather detailed requirements on existing server and firewall infrastructure established in the ERD and design the new virtualized server infrastructure, firewall installation and migration requirements from existing infrastructure. The designing and planning documents need to be signed off from ERD before the actual installation begins.
3. Supply, installation and commissioning of the infrastructure virtualization solution and Firewall.	SIP shall deliver and install infrastructure and software included in this bid and perform migration from any existing devices.
4. Training of staff at ERD.	Provide comprehensive training for selected IT staff. The training plan must be signed from ERD for training content, facilities and duration before the commencement of the actual training.
5. User Acceptance Testing	SIP needs to prepare comprehensive test plans and test cases. SIP shall assist ERD in carrying out UAT and produce any documentation required by ERD during testing.

Bidders shall propose all relevant components in line with the minimum specifications published in section 6.1 Technical Specifications.

It is the responsibility of the bidder to propose, cost and provide all necessary accessories required to commission the infrastructure and software included in this procurement. Bidders must also cost, and supply required network cables (copper and fiber) for the proposed solution. Approximate distance between servers and core switches for copper cables is 10m.

Bidders must clearly state the power and cooling requirements and other floor space requirements required for the proposed solution.

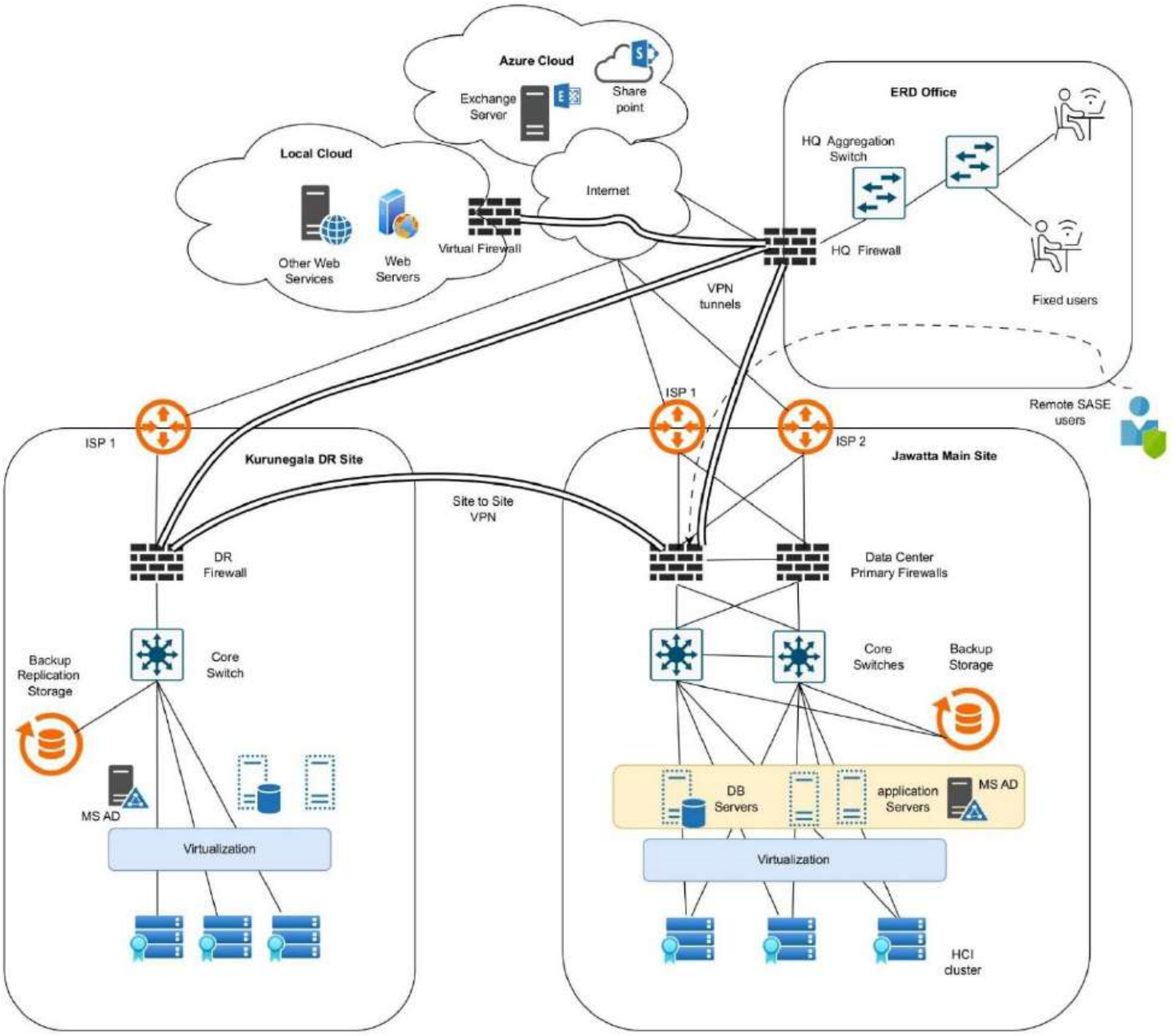
5.4.3 Current Infrastructure in the ERD.



5.4.4 Current Usage and Expected capacity For The ERD.

No	Description	Current Status	Current Usage	Expected capacity
1	Fingerprint Machine System	Running	1.5 GB	2GB
2	Inventory System (MIS)	Running	0.5 GB	2 GB
3	E-Mail (Exchange Server)	Running	1 TB	2 TB
4	ITMIS	Running	Web Based	nil
5	Promise.lk (e-Procurement)	Running	Web Based	nil
6	e-Payroll / Government Payroll System	Running	Web Based	nil
7	Cigas system	Running	Web Based	nil
8	TA Web Application System	Developing	Web Based	2TB
9	Blue Marine Web Application	Developing	Web Based	1 TB
10	Project Monitoring System	Proposal	Web Based	100 GB
11	Document Management System	Proposal	Web Based	2TB
12	User sheard Public Folder	Ongoing	2.5 TB	4 TB
13	ERD WEB Server	Running	60 GB	100 GB
14	DNS Server & AD	Running	100 GB	200 GB
15	SQL Server	Running	200 GB	300 GB
16	VM ware vCenter Server	Running	800 GB	1.5 TB
17	Cisco Fire Power Management	Running	250 GB	400 GB
18	Backup Server	Running	15 TB	30 TB
19	ERD WSUS Server	Running	0.5 TB	1 TB
20	e-payroll	Running	Web Based	nil

5.4.5 ERD Proposed HCI Network Architecture



5.5 Overview of scope of work for Migration

5.5.1 Server Migration Requirements

The successful bidder shall be responsible for the migration of data, applications, and services from the existing server infrastructure to the new server. The migration process must ensure minimal disruption to business operations, maintain data integrity, and adhere to industry best practices.

5.5.2 Server Migration Checklist for Bidders

The following checklist is intended to guide bidders in planning and executing the migration of data, applications, and services from the existing server to the new server. Each item must be addressed and confirmed during the migration process.

Item No.	Requirement	Completed (Yes/No)	Comments
5.5.2.1Pre-Migration Assessment			
5.5.2.1.1	Conduct a comprehensive inventory of applications, databases, services, user accounts, and data on the existing server.		
5.5.2.1.2	Identify dependencies and compatibility requirements with the new server environment.		
5.5.2.1.3	Verifying all required licenses (operating system, applications, and databases) are valid and transferable.		
5.5.2.2 Backup and Recovery			
5.5.2.2.1	Perform a full backup of the existing server (system state and all data).		
5.5.2.2.2	Validate backup		

	integrity and test recovery procedures prior to migration.		
5.5.2.2.3	Maintain secure storage of at least one copy of the backup in an external/offsite location.		
5.5.2.3 Migration Methodology			
5.5.2.3.1	Propose an appropriate data migration approach (e.g., file copy, database migration, virtualization, or phased migration).		
5.5.2.3.2	Define a clear cutover strategy (all-at-once vs. phased migration).		
5.5.2.3.3	Ensure validation of data integrity post-migration using checksums or other verification methods.		
5.5.2.4 Security Requirements			
5.5.2.4 1	Apply the latest security patches and hardening measures to the new server before data migration.		
5.5.2.4 2	Ensure secure transfer of user accounts, access rights, and permissions.		
5.5.2.4.3	Review and update password policies, encryption mechanisms, and digital certificates.		
5.5.2.5 Testing and Validation			
5.5.2.5.1	Conduct thorough functional testing of		

	applications, databases, and services in the new environment.		
5.5.2.5.2	Validate network configurations, DNS settings, firewall rules, and routing.		
5.5.2.5.3	Perform performance benchmarking to compare old and new server environments.		
5.5.2.6 Cutover and Go-Live			
5.5.2.6.1	Schedule migration during low-usage hours to minimize downtime.		
5.5.2.6.2	Provide prior notification to stakeholders regarding downtime and migration windows.		
5.5.2.6.3	Ensure smooth redirection of services (DNS updates, mapped drives, application reconfigurations).		
5.5.2.7 Post-Migration Activities			
5.5.2.7.1	Monitor system performance, resource utilization, and logs after go-live.		
5.5.2.7.2	Confirm that backups, monitoring, and alerting are fully functional on the new server.		
5.5.2.7.3	Retain the old server		

	in standby mode for an agreed period before decommissioning.		
5.5.2.7.4	Provide complete documentation of the migration process, including configurations, credentials, and network details.		
5.5.2.8 Deliverables			
5.5.2.8.1	Migration plan and schedule.		
5.5.2.8.2	Backup and recovery validation report.		
5.5.2.8.3	Post-migration test and validation report.		
5.5.2.8.4	Updated system documentation.		
5.5.2.8.5	Support for the new bidder handing over this Data center upgrade or revamping after the completion of the contract period without any cost for data migration		

5.6 Technical Specification: ERD Proposed HCI Network Architecture

1.Overview

This network architecture is designed to provide a secure, scalable, and highly available IT infrastructure for the ERD (External Resources Department). It features a hybrid setup combining on-premises and Hybrid virtualization, local and remote DR (Disaster Recovery), cloud integration, and modern security approaches.

2. Network Topology

✦ Main Site (Jawatta IRD Datacenter)

✦ Disaster Recovery Site (Kurunegala IRD Data Center)

✦ Local Cloud Infrastructure

✦ Cloud Integration

3. Core Components

A. Virtualization

✦ Type: HCI (Hyper-Converged Infrastructure) Cluster

✦ Function: Hosts virtual machines for web, database, application, MS AD, Exchange, and SharePoint servers.

B. Servers

- Application Servers: Hosts internal ERP or custom business logic applications.
- Database Servers: Host critical databases with secure access controls.
- Web Servers: Host internal/external facing websites.
- Provides user/device communication email services.
- Used for internal document management and collaboration.
- Centralized authentication and policy enforcement.

C. Networking

✦ Primary Firewalls: Frontline defense at the Data Center, configured with VPNs and policy-based routing.

✦ Core Switches: High-throughput L3 switches connecting internal systems.

✦ Aggregation Switch (ERD): Connects all access and server-side traffic at ERD.

✦ Site-to-Site VPNs: Securely connects Jawatta HQ and Kurunegala DR site.

✦ Remote VPN (SASE): Secure remote access for mobile/remote users.

D. Storage and Backup

✦ Primary Storage: High-performance SAN/NAS at the main site.

✦ Backup Storage: Used for daily/weekly backups.

✦ Backup Replication: Replicated to Kurunegala DR site for redundancy.

4. Cloud and Remote Integration

A. Local Cloud

✦ Hosts internal services in a private virtualized environment.

✦ Integrated with internal storage, computer, and network.

B. Cloud Services

✦ Provides hybrid integration for scalability.

✦ Extends cloud user management for identity federation.

✦ Backup storage and possible DR workloads.

C. SASE (Secure Access Service Edge)

✦ Remote users connect securely using cloud-hosted VPN and policy engines.

✦ Ensures Zero Trust Network Access (ZTNA) principles.

5. Internet Connectivity

✦ Dual ISP Connections

✦ ISP 1 & ISP 2 at both ERD(HQ) and DR site.

✦ Load balancing and failover configured via firewalls.

✦ Ensures internet redundancy and continuous access.

6. Disaster Recovery Site (Kurunegala IRD Data Center)

✦ Core Switch & Firewall

✦ Virtualization Platform (for DR VMs)

✦ Backup Replication

✦ Site-to-site VPN with HQ

✦ Can run critical systems in case of primary site failure.

✦ RPO = near zero (depending on link availability) and RTO < 15 min

7. Security Measures

✦ Firewalls: Perimeter and internal segmentation.

✦ VPN tunnels: Site-to-site and remote access.

✦ Zero Trust Model: For remote user access.

✦ Backup Encryption: In-transit

5.6.1 Related Services

Suppliers shall conduct training for Three (3) nominated ERD officials on daily administration/monitoring, immediate troubleshooting of virtualized infrastructure and Firewalls. SIP shall obtain sign-off from ERD for training plan and content before the commencement of the training.

5.6.2. Service Level Agreement (SLA)

“Service Cover Period” shall be assigned to the site and shall dictate the times during which bidder shall act upon incidents and during which incidents shall be considered for assessment against the service level targets as detailed in this Schedule.

The following table defines the key performance indicators for monitoring and measuring the performance of SIP.

The SLA parameters shall be measured on a 24/7 basis, and the SLA reports shall be made available to ERD every week or on demand by ERD. 24x7 NOC and Helpdesk facility Must be provided with the Proposal and number of people allocated for each roster should be clearly stated in the technical proposal. A separate cost breakdown should be included in the price schedule for the Helpdesk and NOC services.

The below SLA parameters are applicable for all software and hardware supplied through this procurement.

The SIP needs to have an internal help desk to log on to issues found in the systems during warranty period. Below are the issue categorization and resolution times of the SLA.

Category	**Some examples of the issues**
Critical	Failure of the main Hardware/Software/Services or Cabling preventing regular operation. o Operating System crashes o Unavailability of systems and services o Critical loss of security configurations (e.g. user group security settings fail)
Major	A very serious error that results in a significant impact on ERD operations and/or a serious loss of productivity or incurrence of significant cost to ERD. o A reasonable work around could be devised but it would be costly or result in some loss of productivity
Minor	Failures or errors that have an impact on regular operations but can be managed with a workaround. o Minor issues o Service alerts

Category	**Resolution time**	
Critical (Severity 1)	Within 2 hrs	Service needs to be provided 24/7
Major (Severity 2)	Within 4 hrs	Service needs to be provided 24/7
Minor (Severity 3)	Within 1 day	Service needs to be provided 24/7

5.6.3 Penalty

The penalty will be 0.1% of the Contract Sum for each SLA violation incident. Accordingly, for each SLA violation, a 0.1% of the contract sum will be deducted and the total accumulated amount will be claimed from the performance bond.

5.6.4 User Acceptance Testing

1. The Department of External Resources shall perform the infrastructure compliance review to verify the conformity of the infrastructure supplied by SIP against the requirements and specifications provided in the bid and/or as proposed in the proposal submitted by SIP. Compliance review shall not absolve SIP from ensuring that proposed infrastructure meets the SLA requirements.

2. SIP needs to submit the following documents before User Acceptance Testing. SIP needs to conduct its own internal testing before submitting the documents to the ERD.
   - Test cases and Test results.
   - Architecture, network, connectivity and configuration diagrams and documentation

5.6.5 Warranty

The SIP shall provide Three (3) years comprehensive warranty for the entire solution (software & hardware). The SIP shall obtain back-to-back warranty from respective OEMs (manufacturer warranty) for all hardware and software supplied through this procurement and documentary evidence of the same shall be submitted to the ERD before the final payment.

5.6.6 Project Time Lines

SIP is expected to complete the project with minimum timelines to capitalize the infrastructure. Below proposed project timelines are for reference only. SIP should evaluate the components and provide a comprehensive project plan for evaluation.

Phase	**Duration**	**Description**
Goods Delivery	6-8 weeks	Deliver and clearance of goods
Assessment & Design	2–3 weeks	Audit existing VMware ESXi setup, map dependencies, Identify systems and configurations
Passive implementations	1-2 weeks	Complete passive cabling and infrastructure for installation
Build & Commission New Infra	3–4 weeks	Deploy HCI, network, firewalls, backup systems
VM & Data Migration	4–5 weeks	Live/cold migration, replication, cutover
Application & Service Validation	2 weeks	Testing, optimization
Decommissioning Legacy	1 week	Final cleanup and documentation

6. Technical Compliance for Procurement of Supply, Installation, Commissioning and Maintenance of Hybrid Virtualized Infrastructure for the Department of External Resources.

6.0 Compliance for Architectural Objective - Specifications for Hybrid Cloud HCI Architecture

To support the Ministry of Finance digital infrastructure strategy, this RFP seeks solutions that enable a hybrid datacenter architecture spanning on-premises and public cloud environments, built on Hyperconverged Infrastructure (HCI) principles. The objective is to achieve:

- Unified operations across hybrid environments
- Scalable, resilient infrastructure with edge and DR capabilities
- Consistent security, observability, and automation
- Workload mobility and cost optimization without architectural lock-in

The specified features are baseline requirements for ensuring operational consistency, compliance, and future-proof scalability. Each clause reflects a critical capability necessary to support hybrid elasticity, automated lifecycle management, and secure workload governance.

Failure to meet these requirements, either in part or in whole, may result in disqualification from further evaluation. Bidders must demonstrate clear alignment with each clause, supported by validated reference architectures, published interoperability matrices, and documented feature availability.

1	**2**	**3**	**4**	**5**
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
HCI Software Capabilities				
6.0.1	Hybrid-Capable HCI Software	The proposed HCI platform must support native workload mobility, image/VM/container replication, and automated data tiering to public cloud services. Workloads must be able to migrate between on-premises and cloud environments for capacity expansion, cost optimization, or disaster recovery without requiring refactoring or replat forming.		
6.0.2	Data Services	The HCI software must provide native support for inline duplication, compression, thin provisioning, and fast snapshot capabilities. These features must operate without external appliances and must be configurable per workload or storage tier.		

6.0.3	Replication & DR Orchestration	The solution must support synchronous and asynchronous replication between clusters, with automated failover and failback workflows. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be declarable, testable, and enforceable via policy.		
6.0.4	Multi-Workload Support	The platform must support both virtual machines and containerized workloads with consistent storage, network, and security policy enforcement. Native integration with Kubernetes and support for leading hypervisors (e.g., AHV, ESXi) is required.		
6.0.5	Micro segmentation & Policy Enforcement	The solution must support workload-level micro segmentation enforced by the HCI platform or integrated network fabric. Policies must apply consistently across on-premises and cloud environments, with support for dynamic policy updates and audit logging.		
6.0.6	Storage Protocol & Performance Flexibility	The platform must support access via NVMe-oF, SMB, NFS, and S3-compatible protocols. Applications must be able to select appropriate access methods based on latency, throughput, and compatibility requirements.		
6.0.7	Key Management & Encryption Controls	The solution must integrate with external Key Management Systems (KMS) and support Bring Your Own Key (BYOK) models. Encryption must be supported for both data-at-rest and data-in-transit, with centralized key lifecycle management across hybrid environments.		
6.0.8	Licensing & Workload Mobility Portability	The licensing model must permit cloud bursting, workload migration, and hybrid elasticity without re-licensing or incurring punitive costs. Licensing terms must support predictable operational and financial planning.		
6.0.9	Non-Disruptive Lifecycle Management	The platform must support rolling upgrades of firmware and software components, automated rollback in case of failure, and inventory-aware patching. Lifecycle operations must not require workload downtime or manual intervention.		
6.0.10	Validated Enterprise Server Nodes	Proposed server platforms must be validated by the HCI software vendor and support NVMe storage configurations. Each node must include out-of-band remote management capabilities and support automated provisioning and recovery workflows.		

6.0.11	Scale-Out & Edge Capability	The solution must support non-disruptive addition of nodes to existing clusters and deployment of small remote clusters under the same management plane. Edge clusters must be manageable centrally with consistent policy enforcement and lifecycle operations.		
Switching & Network Fabric Requirements				
6.0.12	Leaf-and-Spine Fabric with Overlay Support	The network fabric must support VXLAN/EVPN or equivalent overlay protocols with hardware offload capabilities. The solution must deliver line-rate performance for multi-tenant L2/L3 overlays and support dynamic endpoint mobility.		
6.0.13	Programmable Network APIs	Switches and network controllers must expose northbound REST and/or GRPC APIs. The solution must support integration with orchestration tools such as Terraform and Ansible for automated provisioning, configuration, and change management.		
6.0.14	Cloud Connectivity Options	The architecture must support secure hybrid connectivity via high-throughput VPNs, private cloud interconnects (e.g., ExpressRoute, Direct Connect equivalents), and fast failover paths. Connectivity must be resilient, auditable, and policy enforced.		
6.0.15	Micro segmentation & Policy Enforcement	The network fabric must support enforcement of micro segmentation policies at the switch level using ACLs, overlays, or equivalent mechanisms. Policies must be centrally managed and consistently applied across hybrid environments.		
Consolidated Management, Visibility & Governance				
6.0.16	Unified Management & Control Plane	The solution must provide a unified management interface and API framework capable of orchestrating both on-premises and cloud resources. Policy enforcement, monitoring, and lifecycle operations must be consistent across all environments.		
6.0.17	Infrastructure as Code & Automation	The platform must provide documented REST APIs and SDKs, along with ready-to-use Terraform and Ansible modules. These must enable repeatable deployments, CI/CD integration, and automated configuration management.		
6.0.18	Observability & Telemetry	The solution must provide high-fidelity metrics, logs, and streaming telemetry. These must be integrable with enterprise monitoring and SIEM platforms and support proactive incident detection and root cause analysis.		

6.0.19	Security & Identity Integration	The platform must support Role-Based Access Control (RBAC), LDAP/AD/SAML integration, encrypted management and data planes, and SIEM hooks. Access must be auditable and enforceable across hybrid environments.		
6.0.20	Cost, Usage & Chargeback Visibility	The solution must provide consolidated billing and usage telemetry across on-premises and cloud resources. This must support cost optimization, capacity planning, and departmental chargeback models.		
6.0.21	Third-Party Interoperability & Reference Validation	All proposed components must be listed in published interoperability matrices or validated reference architectures. The solution must be supportable by vendors and proven to operate as an integrated system.		

6.1 Technical Resource Compliance

Bidders are required to provide compliance with each of the resource qualification requirements listed on the staffing table. Failure to provide a compliance response for all or any listed position may result in the bid being treated as non-responsive.

Bidder should attach the copies of the certifications and mention the certifications number, with the bid submission, for verification.

Multiple Roles for one person is not permitted.

If the bidder's response for any qualification requirement is marked **No (N)**, the bidder must specify the proposed alternative qualification or certification in the **Remarks** column. If the bidder's response is marked **Yes (Y)**, the bidder may also provide additional supporting details or equivalent certifications in the **Remarks** column.

Line-Item No	Key Area / Position	Scope of Work	Minimum Positions	Required Qualifications (or Equivalent/Similar Certifications)	Required Experience	Bidder's Confirmation (Yes / No / Alternative Qualification)
6.1.1	**Infrastructure Professionals** (Overall Multi Cloud and HCI Solution design and deployment)	Design and define overall HCI solution and Multi cloud architecture. ensure scalability, performance, and reliability. Ability to lead installation, configure, administer, and operate a multi-cloud infrastructure.	2	Bachelor's/master's in computer science, IT, or related field. Must have one or more of the following types of professional qualifications, related to the solution proposed. VMware Certified Advanced Professional (VCAP) / VMware Certified Professional - Cloud Operations (VCP-CO)/ VMware Certified Professional - Cloud Management and Automation (VCP-CMA)/ Microsoft Certified: Azure Solutions Architect Expert / Red Hat Certified Architect /Nutanix Certified Professional – Mult Cloud Infrastructure (NCP-MCI) or similar proposed vendor-level certification related to multi cloud deployment and architecture.	7+ years in IT infrastructure design, architecture and implementation	

6.1.2	**Systems Engineer** (new HCI Hardware/Software)	Install, configure, and manage HCI hardware/software; perform system administration and troubleshooting.	3	Bachelor's in computer science, IT, or related field; Must have one or more of the following type of qualifications. VMware Certified Professional (VCP), Microsoft Certified: Windows Server Hybrid Administrator, Red Hat Certified Specialist in Cloud Infrastructure , Nutanix Certified Professional (NCP) or similar proposed vendor professional-level certifications	5+ years in systems engineering and administration	
6.1.3	**Systems Engineer** (migration scope)	Manage migration from old system to new one	1	Bachelor's in computer science, IT, or related field; Must have one or more of the following type of qualifications. VMware Certified Professional (VCP)	5+ years in systems engineering and administration	
6.1.4	**Information Security (Firewall) Engineers**	Implement and maintain firewall solutions; manage and monitor security rules, logs, and incident response.	2	Bachelor's/master's in computer science, IT, or related field. Must have one or more of the following type of qualifications. Following certifications or similar level of proposed vendor certifications, FCP, FCSS certifications, Palo Alto Networks Certified Network Security Engineer (PCNSE), Cisco Security CCNP Security, Fortinet NSE Level 7–8.	5+ years in information security	

6.1.5	**Network Engineer** (HCI Network Design & Security)	Design and implement HCI network architecture; manage VLANs, routing, and network security integration.	2	Bachelor's/master's in computer science, IT, or related field. Must have one or more of the following type of qualifications or similar professional level certifications from proposed vendor (e.g., Juniper JNCIP-ENT, CCNP, CISM certifications, Aruba Certified Network Professional, Microsoft Certified: Azure Network Engineer Associate)	5+ years in network engineering	
6.1.6	**Systems Engineer – Backup Platform**	Deploy and manage enterprise backup platforms; configure policies, monitoring, and restore testing.	2	Bachelor's in computer science, IT, or related field; Must have one following or similar professional certifications/ qualifications from proposed Vendor. For e.g: Veritas Certified Specialist, Dell EMC Data Protection Advisor, VMCE, Commvault Certified Professional	5+ years in systems engineering and administration	
6.1.7	**Microsoft Solution Architects**	Deploys and manages Microsoft 365 and performs Microsoft 365 tenant-level implementation and administration of cloud and hybrid environments	2	Bachelor's in computer science, IT, or related field; Must have following professional certification. Microsoft Certified: Azure Solutions Architect Expert or Microsoft 365 Certified: Administrator Expert	4+ years in IT systems and administration	

6.1.8	**Microsoft Security Architects**	Design Microsoft solutions Security architecture and deployment	1	Bachelor’s in computer science, IT, or related field; Must have following professional certification. Microsoft Certified: Cybersecurity Architect Expert	4+ years in IT systems and administration	
6.1.9	**Windows Server Hybrid Administrator**	Administering Windows Server as a workload in both on-premises and hybrid environments	2	Bachelor’s in computer science, IT, or related field; Must have following professional certification. Microsoft Certified: Windows Server Hybrid Administrator Associate	4+ years in IT systems and administration	
6.1.10	**Database Administrator** (SQL Server Migration & Optimization)	Migrate, optimize, and manage SQL databases (2008–2022); ensure performance tuning and backup strategy.	2	Bachelor’s/master’s in computer science, IT, or related field; Microsoft Certified Database Administrator or Azure Database Administrator (SQL Server 2016–2022); or similar certifications (e.g., Oracle Certified Professional, PostgreSQL Professional Certification)	5+ years in database administration	
6.1.11	**Project Manager** (Implementation & Coordination)	Oversee HCI project implementation; manage teams, timelines, deliverables, and reporting.	1	Bachelor’s in business, IT, or related field; Project Management Professional (PMP); similar certifications (e.g., PRINCE2 Practitioner, Certified ScrumMaster, PMI-ACP)	10+ years in project management (preferably IT infrastructure)	

6.1.12	**Service Support Engineers (L1, L2, L3)** (HCI/ Backup, Network/ Firewall, , Microsoft)	Provide operational support (incident management, troubleshooting, escalation) across infrastructure components on 24x7 basis	6	ITIL V4 certification. Bachelor's in computer science, IT, or related field; Must have similar certification or better for each category of service. (2 Nos of - Microsoft Certified: Azure Administrator Associate, 2 Nos of - VMware Certified Technical Associate/ Nutanix Certified Associate (NCA) or similar industry certificates , 2 No of – CCNA or similar industry certificates)	3+ years in infrastructure projects	

6.2 Bidder Experience and Reference Compliance

Each bidder must provide a minimum of **five (5) customer references** for every solution or service listed below. The references must be for **complete and successfully implemented projects**, preferably of similar size and complexity.

- At least one (1) reference must be from the **quoted product/solution** (where specified).
- For each reference, bidders must provide:
    1. **Customer / Organization name & project details**
    2. **Contact person and valid phone number** for verification
    3. **Supporting document** (Purchase Order / Letter of Award / Contract) – marked clearly and attached with the bid.

Failure to provide complete and verifiable references **may lead to disqualification**.

1	2	3	4	5	6
Line-Item No.	**Description of Goods / Services**	**Reference Requirement**	**Reference Site (Organization Name & Project Details)**	**Contact Person & Number**	**Supporting Document (PO/LOA/Contract) Attached (Yes/No)**
6.2.1	**HCI Solution**	Minimum 5 references for HCI implementation projects. At least 1 must be from the **same quoted HCI nodes and HCI software**.	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..
6.2.2	**Data Backup Solution**	Minimum 5 references from the datacenter backup solution implementation. **At least 1 must be from the same quoted Solution**	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..

6.2.3	**Data Center Switches**	Minimum 5 references from the same quoted datacenter switch installation.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....
6.2.4	**Datacenter and LAN Firewalls**	Minimum 5 references from the same quoted datacenter firewall installation.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....
6.2.5	**TOR Aggregation & Floor Access Switches**	Minimum 5 references from the same quoted LAN aggregation and access switch deployment.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....
6.2.6	**Network Management Platform**	Minimum 5 references from the same quoted network management platform deployment.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....
6.2.7	**Identity and Access Control Solution**	Minimum 5 references from the same quoted identity and access control solution implementation.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....
6.2.8	**Microsoft Active Directory (Active + DR)**	Minimum 5 references from the similar quoted Microsoft AD and Disaster Recovery deployment.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5.	1. .... 2. .... 3. .... 4. .... 5. ....

6.2.9	**Microsoft Solution (Cloud Environment)**	Minimum 5 references from the similar quoted cloud-based solution implementation.	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..
6.2.10	**Datacenter IT Operations Platform**	Minimum 5 references for datacenter operations platform implementation.	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..
6.2.11	**Wireless Solution**	Minimum 5 references for wireless implementation projects.	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..
6.2.12	**SASE (Secure Access Service Edge) for Remote Users**	Minimum 5 references for SASE solution implementation for remote users.	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..	1. ……….. 2. ……….. 3. ……….. 4. ……….. 5. ………..

6.3 Specifications for HCI (Production and DR Sites)

It is a must to record compliance against each of the line items in the specifications tables and failure to mark compliance for all or any line item can result in bid been treated as non-responsive. If the bidder’s response for any line item is marked as N or No, then the bidder must specify its offer in column 5 – Remarks. If the bidder’s response is Y or Yes in column 4, then the bidder has the option of providing additional information in Column 5. All complied items should be provided with the reference link in section 5 to correct and updated documentation, for evaluators to validate information. Failure to do so will result in bid been treated as non-responsive.

1	**2**	**3**	**4**	**5**
Line-Item No	**Description of goods/Category**	**Purchaser’s Requirements/ Technical Specifications and Standards**	**Bidder’s Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.3.1	General & Compliance	Make		
6.3.2		Model		
6.3.3		Country of Origin		
6.3.4	Bidder Qualification	Bidder must at least hold top-tier 2 partnership with the HCI OEM and attach proof.		
6.3.5		The vendor and HCI platform must be recognized by industry analysts. As Gartner does not currently publish a dedicated Magic Quadrant for HCI, bidders may demonstrate enterprise-grade adoption through inclusion in Gartner Market Guides, Gartner Peer Insights, equivalent analyst research, or audited enterprise references, to ensure reliability and as proven industry solution		
6.3.6		The solution must include a virtualization platform recognized as leaders in Gartner's Latest report August 2024, for Distributed Hybrid Architecture.		
6.3.7		All compute/storage nodes in the solution must be fully certified for the chosen hypervisor by the hardware vendor or manufacturer		
6.3.8		Should have at least one successful contracted reference for the quoted HCI and virtualization solution with same software and hardware and should provide PO or customer reference letter as proof.		
6.3.9		Provide two certified engineers (≥2 yrs experience) and evidence of ≥3 SD-Datacenter installs in last 5 yrs.		

6.3.10	Architecture	Offered Solution shall be a next generation software defined storage platform which shall offer the functionality of Hyper-converged with independent scaling of both Storage and Compute without any downtime.		
6.3.11		The solution should provide enterprise-class storage services using latest x86 server infrastructures without dependence on a separate Storage Area Network Storage & associated component such as SAN Switches & HBAs. The offered HCI system should be a software-centric system for delivering compute, storage and networking resources in a tightly integrated system.		
6.3.12		The solution should use a unified server architecture with consistent hardware and integrated networking to ensure OEM certification and deployment consistency across all nodes.		
6.3.13		The system shall support a modular and scalable node design with hot-swappable components, supporting consistent cabling and simplified maintenance.		
6.3.14		All HCI compute and storage nodes shall be deployed in a vendor-certified architecture that supports either rackmount or modular-blade servers with integrated or discrete networking modules.		
6.3.15		The solution design must follow industry-standard design guidelines and reference architecture for HCI deployments, including guidelines for with best practices for high availability, scalability, and interoperability, cabling, power, cooling, service profiles, and high availability.		
6.3.16		The architecture must be based on OEM-certified designs. Solution must run on industry-standard, vendor-supported x86 servers and be certified for compatibility by the HCI software vendor. non-certified fabric/network components shall be deemed non-compliant.		

6.3.17		The proposed HCI solution should be a factory shipped engineered & integrated appliance. The HCI solution should support SSD/NvME Drives. The HCI solution should support scalability up to 32 nodes in a single cluster. Each server node should have dedicated redundant hot swap power supply, cooling fans. There should not be any separate disaggregated components in the proposed HCI solution i.e. The 3 Major components of the HCI node i.e. Compute, RAM and Storage should be physically inside the node, no resource should be provisioned from outside the HCI Node.		
6.3.18	Hardware	Each computer node shall be a rackmount or blade design with redundant power, fans, and network interfaces, optimized for hyperconverged workloads.		
6.3.19		Solution should be provided with Total 3 nodes All NVME SSD cluster configuration, each node providing 6th Gen Intel processors or *AMD* and DDR5 6400 MHz Memory with following onfiguration:		
6.3.20		Solution must be proposed with 3 Node HCI cluster providing at least 144, 3.0GHz usable physical cores, 768 GB total usable memory and 50 TB usable storage without considering any deduplication, compression, erasure coding or any saving techniques benefits. A complete solution must be proposed with RF2/FTT1 (2 copies of the data). System configurations should be specified in the remarks column.		
6.3.21		The solution must be configured with 2 x 480 M2 boot drive		
6.3.22		Over and above the configuration mentioned, bidder must ensure 70000 IOPS per node from the HCI cluster, assuming 8kb block size, and 70:30 read: write ratio with 5ms response time.		

6.3.23		The HCI software should pool all HDDs from all the nodes in the cluster to present a single storage resource pool to all server nodes in the cluster. The HCI storage should be a scale-out distributed storage. The platform offered should have flexibility to utilize all offered drives on storage layer for a given virtual machine for both read and write operations. The intelligent software should consolidate the resources from each server node into a shared resource pool, delivering a high degree of flexibility while also simplifying management.		
6.3.24		Nodes must include 4x 25 GbE or faster network adapters with support for link aggregation (LACP), VLAN tagging, QoS and RDMA where applicable.		
6.3.25		A minimum of six full-height PCIe Gen 4/5 slots shall be available per server for additional NICs, HBAs, GPUs or accelerators. Expandability must be non-disruptive and support future technology upgrades.		
6.3.26		HCI solution should support NVMe, SSD disks without compromising any of enterprises storage efficiency provided by stack.		
6.3.27		HCI solution must provide on the fly change of ESE (Enterprise Storage Efficiency)-Deduplication/Compression for workload without any visible impact on storage and their operations.		
6.3.28		The proposed solution should provide 1TB of Unified storage (Object/File) from day 1 without any additional licensing.		
6.3.29		Performance Features – Automated Tiering & Caching: Hardware must support policy-driven data tiering (hot/cold) and inline caching on NVMe devices. – Inline Data Services: Support for deduplication and compression without perceptible latency impact. – Resiliency: N+1 fan and power-supply redundancy, with predictive failure alerts for all components.		
6.3.30	Software & Data Services	Nodes shall be certified and fully supported for latest industry-standard virtualization and hyperconverged infrastructure platforms and include distributed filesystem, snapshots, erasure coding, and integrated backup/DR orchestration.		

6.3.31		The HCI software layer must provide a distributed filesystem (no external SAN required) with built-in data protection features (replication, erasure coding, snapshots, deduplication, compression).		
6.3.32		The Solution should support Instant space optimized point-in-time Snapshots. Should allow for taking snapshots of individual Virtual Machines to be able to revert to an older state, if required.		
6.3.33		The Solution should allow for taking clones of individual Virtual Machines for faster provisioning.		
6.3.34		The HCI storage should have integrated wizard to schedule snapshot for hourly/weekly/monthly snapshot policies.		
6.3.35		The solution should automatically rebalance data to maintain balanced utilization of storage across the HCI nodes. When storage capacity is scaled up or scaled out, the HCI nodes must automatically redistribute data equally across all nodes equally without migrating VMs. Each HCI node in the cluster should have at least 32 DIMM slots and 10 drives slots for future scalability.		
6.3.36		Virtualization software shall provide a Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability and security. Virtualization software should allow for a hot addition of vCPU, memory, and disk without any downtime. Supplied hypervisor must have all the enterprise functionalities like HA, DRS and vMotion etc.		
6.3.37		HCI solution should support more than one hypervisor with cloud native integration (Container)/OpenStack		
6.3.38		HCI solution should support leveraging external physical servers (not part of HCI Cluster) access to HCI storage using native ISCSI with highly available connectivity using HCI native load balanced and distributed data architecture across all nodes in cluster.		
6.3.39		HCI solution should support WAN Bandwidth optimizer along with defined schedule across two sites and only increment data should be replicated post one time data sync.		

6.3.40		HCI Solution should support one view for physical and virtual network along with their real time usages and configuration		
6.3.41		HCI solution should support natively Microsoft and Linux based Guest VM's Clustering using block storage.		
6.3.42		HCI solution should support Block, File and Object (S3) natively or using third party solution from Day1. Solution should support file storage supporting NFS v3/v4 and SMB 2.0/3.0 for Linux and Windows Guest with unlimited shares integrated with Active directory/LDAP		
6.3.43		Hypervisor software must provide Data at rest encryption with Native KMS which protects unauthorized data access.		
6.3.44		Compute/storage nodes and network switches shall be certified for interoperability with high-performance data center switches supporting features such as VXLAN, BGP-EVPN, QoS, and FCoE.		
6.3.45		The solution should support Micro segmentation.		
6.3.46		Network compatibility must include support for advanced switching features (e.g., multi-chassis link aggregation, L2/L3 segmentation, control-plane security features) in the target switch environment.		
6.3.47		The solution shall integrate with the existing network fabric (Layer 2/3) to allow configuration of switch ports and virtual networks from the HCI management interface.		
6.3.48		Switches and nodes should support programmability (e.g. OpenConfig, REST APIs) to enable automated deployment and policy enforcement on the fabric.		
6.3.49		HCI management interfaces should be integrated with existing IT management tools via APIs (e.g. for creating tickets on alerts) to ensure visibility in central dashboards.		
6.3.50	Sizing & Scalability	The architecture shall support adding storage drives to a node and immediately using the added capacity without node replacement or service interruption.		
6.3.51		The solution shall allow adding new computer/storage nodes to an existing cluster without downtime, automatically redistributing data and compute workloads as needed.		

6.3.52		The system must allow hardware upgrades on existing nodes (e.g., additional memory or CPU) without requiring cluster redeployment or major reconfiguration.		
6.3.53		Storage performance shall meet enterprise-tier expectations: each node must include both NVMe and SSD, with configurable caching tier to optimize I/O performance for mixed workloads.		
6.3.54		Automated storage tiering must enable moving cold data to lower-tier or cloud storage (with encryption) based on policies, without impacting active workload performance.		
6.3.55		The storage layer must support inline deduplication and compression across all data tiers, reducing capacity needs without significantly impacting performance.		
6.3.56	Networking & Fabric	The HCI solution includes min. 2 Qty of low latency network switches to manage east-west traffic, each with minimum 24 port, upgradable to 48 ports per switch with redundant power supplies and cooling fans (as explained in the datacenter switches requirements). The switches should be provided with sufficient 10/25 Gbps for HCI node connectivity and support minimum 6 * 40/100Gb ports for uplink connectivity to ToR/Leaf Switch. All required License, SFPs fiber cable, power cable to be provided. Bidder must offer network switches with standards-compliant (e.g., Ethernet, VLAN, EVPN, QoS) and interoperable with the proposed HCI solution, with independent certification or proven deployments. Min. 4*10/25Gbps network ports per server node to be proposed		
6.3.57		The network switch should support QoS to streamline HCI network traffic to improve traffic filtering, segmentation, packet prioritization and performance.		
6.3.58		Node integration must support native VLAN, QoS, and EVPN configurations using standard Layer 2/3 protocols.		
6.3.59		Each node or chassis must present a unified fabric interface (Ethernet and/or Fiber Channel) to the cluster through redundant, hot-swappable components or uplinks.		
6.3.60	Scalability & Cloud	The proposed solution must support seamless workload mobility and capacity expansion into public cloud environments (AWS, Azure, Google Cloud, etc.) with unified management.		

6.3.61		The design should enable hybrid cloud operations, allowing management of both on-premises and public cloud resources through a single management platform.		
6.3.62		Workloads shall be portable between on-premises clusters and cloud resources via standard migration tools or APIs, ensuring identical VM images and networking policies.		
6.3.63		A unified console shall manage provisioning, backup, and workload mobility across public cloud and on-premises environments.		
6.3.64	Management	The solution must support centralized management for both on-prem and cloud components via a **single management plane**, allowing full visibility into hybrid cloud resources, performance, and security.		
6.3.65		HCI solution should provide all key operation management and performance management from a single console for Hardware/Storage/Hypervisor and VM 's management using HTML 5 internet browser		
6.3.66		Solution should be integrated (send, receive events, alerts to & from) with existing Network and Security monitoring tools like Network Management System (NMS), SIEM etc.		
6.3.67		Solution should be integrated with SMTP for sending appropriate email related to different types of events/alerts for the cluster environment		
6.3.68		The solution must include native disaster recovery (DR) options allowing replication to a public cloud target directly from the HCI management plane.		
6.3.69		A unified management console must provide visibility and control over computer, storage, virtualization, and networking components in a single pane of glass.		
6.3.70		Unified management must support role-based access control, audit logging of user actions, and strict separation of administrative domains (multi-tenancy).		
6.3.71		The management interface shall be web-based (HTML5) and provide real-time dashboards showing resource utilization and health (CPU, memory, storage I/O, network) for each component.		

6.3.72		Management tools must be cloud-enabled (or have a cloud option) to allow zero-touch provisioning and lifecycle management (provisioning, patching, updates) across all devices from any location.		
6.3.73		The management platform must expose APIs or CLI/Ansible modules for automation and integration with existing orchestration frameworks.		
6.3.74		Management console shall integrate compute, storage, and networking telemetry in a single unified dashboard.		
6.3.75		Server configuration, networking, and storage identity must be centrally managed and templated via the platform’s management system to ensure consistency across nodes.		
6.3.76		Firmware and BIOS versions for all servers and networking components must be orchestrated through a unified management interface, ensuring compliance and version consistency.		
6.3.77		The management interface must provide REST- or API-driven provisioning for server profile creation, assignment, and compliance reporting—no manual per-node edits.		
6.3.78		Power and cooling metrics for all server hardware must be centrally monitored and reported within the same management platform that governs compute, network, and storage.		
6.3.79		Node-level MAC/WWN/I/O identity assignments must be consistently applied via centrally defined profiles or templates at provisioning or boot time.		
6.3.80		Management platform shall be delivered as a globally available SaaS service, with zero on-prem management appliances or proxies required.		
6.3.81		Must include AI/ML–driven health and risk analytics, automatically surfacing configuration drifts, performance bottlenecks, and security vulnerabilities with remediation guidance.		
6.3.82		Single console shall natively correlate and display compute, storage, network, virtualization, and firmware telemetry—and allow one-click remediation across all domains.		

6.3.83		The management UI must support fine-grained RBAC and multi-tenant account folders, with full audit trails, so that different teams or customers can be segregated securely in one pane.		
6.3.84		Capacity planning and cost-analysis dashboards must be provided out-of-the-box, with projected growth forecasts, what-if modeling, and charge-back/show back reports—no separate tools allowed.		
6.3.85		The solution should provide with a centralized management solution which can provide advisory services (PSIRT, Field Notice and EOS information) from Day1.		
6.3.86		The Management solution should provide connected TAC and Proactive RMA functionality from day 1.		
6.3.87		The management solution should have the capabilities to monitor 3rd party servers and storage.		
6.3.88		The Management solution should provide workflow-based automation from day 1 without any additional licensing.		
6.3.89		Platform upgrades, security patches, and feature updates must be applied continuously from the SaaS service side, with one-click rollbacks and no downtime to managed infrastructure.		
6.3.90	Monitoring	The solution shall provide fine-grained telemetry (per-VM/per-container stats on CPU, memory, disk I/O, network throughput and latency) with export to standard monitoring protocols (SNMP, Syslog, RESTful APIs).		
6.3.91		Hardware-level monitoring (power, temperature, fans, PSUs) must be available and integrated into the monitoring dashboard with alerting for any threshold breaches.		
6.3.92		Policy-based monitoring and alerting shall trigger notifications (via email, SNMP trap, or webhook) for hardware faults, capacity thresholds, or unusual activity.		
6.3.93		Alerts and performance data must be exported to third-party monitoring and SIEM systems (e.g. Splunk, Nagios, ServiceNow) through standard interfaces (Syslog, REST API).		
6.3.94		Telemetry must support dynamic workload placement based on predictive insights and contention forecasts.		

6.3.95	Security	All data at rest on the HCI cluster shall be encrypted (AES-256 or better) and keys managed securely (e.g. via KMS or HSM).		
6.3.96		HCI solution should support security compliance for at least three or more industry certifications (CCC-Common Criteria Certified, FIPS-140-2, ISO-27000(ISMS), NIST Guideline for Standard security template (PCI-DSS)/HIPAA etc.		
6.3.97		Data in transit (within cluster, between sites, and to cloud) must be encrypted using secure protocols (TLS1.2+/IPsec) and authenticated endpoints.		
6.3.98		The solution must hold security certifications relevant to government and finance (e.g. ISO/IEC 27001, Common Criteria EAL2+, FIPS 140-2 for crypto modules) and comply with data protection regulations (PCI-DSS, GDPR, etc.).		
6.3.99		Access to the management interfaces requires multi-factor authentication (MFA) and enforces the least privilege access controls.		
6.3.100		Detailed audit logs of all configuration changes, access events, and system operations must be maintained and exportable for compliance reporting.		
6.3.101		FIPS 140-2 validated encryption modules must be used for data at rest and in transit		
6.3.102		RBAC must extend across cloud and on-prem resources with federated identity support.		
6.3.103	Backup & Recovery	Built-in disaster recovery must support policy-driven replication between data center sites (e.g., production to DR) with configurable RPO/RTO settings.		
6.3.104		DR orchestration shall allow non-disruptive failover and failback of workloads, with no data loss beyond the configured RPO, and should not require manual reconfiguration of VMs.		
6.3.105		The system must support bi-directional or one-way syncing of data between clusters at separate sites with automated cutover capability.		
6.3.106		The solution must enable tiered backup and DR orchestration across hybrid clouds using policy-based controls.		
6.3.107		Native backup capabilities must allow snapshots and clones of VMs or volumes, with scheduling policies and retention, without performance degradation.		

6.3.108		Backup/replication policies should be configurable per-VM or per-volume, with the ability to replicate backups to another cluster or to cloud object storage (S3-compatible).		
6.3.109		The solution should be integrated with standard backup solutions via plugin or API to allow offloading data to external backup systems if required.		
6.3.110		DR must support asynchronous replication with tunable RPO and bidirectional		
6.3.111	Support	The solution should have documented deployments in least one reference deployment of similar scale and complexity similar sizes, with references available		
6.3.112		Must have deployments in government agencies with multi-site hybrid cloud infrastructure.		
6.3.113		A single, unified 24×7 global support number must be provided for all hardware, hyperconverged software, management platform, and network fabric components.		
6.3.114		All proposed hardware and software must be 24 x 7 supported and a single OEM should take the responsibility of resolving the issues with support period of 3 years and must be enabled from day one.		
6.3.115		All support calls shall be logged via one support portal or case manager interface; the provider must auto-route internally to the correct product teams without extra cases.		
6.3.116		Break-fix and software bug fixes shall be guaranteed under one SLA, covering compute nodes, storage software, management software, and network switches.		
6.3.117		Patches, updates, and upgrades (firmware, BIOS, hypervisor, HCI software, switch OS) must be sourced and scheduled through the same support channel.		
6.3.118		Escalation management (severity levels, RTO/RPO targets) must be consistent across the hardware, HCI software, and networking layers under one support contract.		
6.3.119		Cooperative support with any third-party software must be transparently provided via the same TAC, at no additional interface or case cost.		
6.3.120		Unified license management and entitlement validation shall be handled by the same support organization for all solution components.		

6.3.121		Single support-engineer assignment for critical incidents, with end-to-end responsibility for resolution across all stack layers.		
6.3.122		Comprehensive support reporting (ticket metrics, SLAs met, root-cause analysis) must cover hardware, HCI software, management platform, and network switches in one report.		
6.3.123		The provider shall hold full ownership of issue resolutions including any third-party software fixes—without directing the customer to separate vendors.		
6.3.124	Warranty & License	HCI must be with a warranty of 3-year 24x7x4, parts replacement and 24×7 TAC support at a quoted price with identical terms.		
6.3.125		Licenses for HCI software should be portable between on-premises and cloud deployments, allowing workloads to migrate without incurring new licensing costs.		
6.3.126		License management must track usage across on-premises clusters and cloud workloads, and should allow subscription or perpetual licensing models appropriate for a government organization.		
6.3.127		Lifecycle management must include automated firmware and driver updates for compute/storage nodes and network devices, with minimal downtime and cluster-wide coordination.		
6.3.128		Cloud portability must include license continuity across cloud and on-prem without per-instance adjustments.		

6.4 Data Center Switches

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.4.1	General & Compliance	Make		
6.4.2		Model		
6.4.3		Country of Origin		
6.4.4		The switch must be listed as a Leader in the Gartner's Magic Quadrant or Forrester Wave report for at least 3 years (2023/ 2024/ 2025) in Datacenter Switching/Networking category		
6.4.5	Bidder Qualification	Bidder must at least hold top-tier 2 partnership with the switch OEM and attach proof.		
6.4.6		Provide two data center networking certified engineers (≥2 yrs experience) and evidence of ≥3 SD-Datacenter installs in last 5 yrs.		
6.4.7	Hardware Specifications	Minimum 24 ports of 1/10/25G SFP+ should be available and able to increase the port capacity Up to 48 Ports in Future without any hardware changes. HCI Nodes should be connected with 25G links and Firewall should be connected with 10G links		
6.4.8		Dual hot-swappable AC power supplies; N+1 redundant fan modules; field-replaceable airflow direction (front-to-back).		
6.4.9	Performance & Capacity	1.6 Tbps or above non-blocking capacity and able to increase up to 3.5 Tbps or above non-blocking capacity in Future without any hardware changes and 1000 Mpps or above and able to increase up to 2000 Mpps or above in Future without any hardware changes.		
6.4.10		Switch must be supported for Buffer memory ≥40 MB		
6.4.11	Architecture & Topology	Should support as leaf switch in a spine-leaf topology with fabric-based EVPN/VXLAN underlay and overlay.		
6.4.12	Layer 3 Features	Full IPv4/IPv6 routing: OSPF, BGP (EVPN/VXLAN), PIM-SM/SSM; support ≥1,500,000 IPv4 routes and ≥750,000 IPv6 routes.		
6.4.13		Switch should support a minimum of 1000 VRF instances with route leaking functionality		

6.4.14	Policy Integration	Support Software defines Application Centric Infrastructure integration, with policy-driven endpoint groups and contract enforcement.		
6.4.15	Security & Encryption	Native inline encryption on all ports (AES-256+) at full line rate; no extra licenses or modules.		
6.4.16		MACsec key management and secure ZTP must be supported across fabric sites; FIPS 140-2 validated modules.		
6.4.17	QoS & Traffic Management	Hierarchical QoS with minimum 8 hardware queues per port; support for traffic policing, shaping, and priority-based scheduling.		
6.4.18	Network Automation	REST, NETCONF, gNMI, Ansible, and model-driven telemetry must be supported for turnkey integration with DevOps pipelines.		
6.4.19	Built-in Telemetry	Streaming in-band telemetry (e.g. ENI/INT) with per-flow, per-hop metrics exported in real time.		
6.4.20	Management & Monitoring	Management plane must integrate into the HCI management console—providing single-pane visibility of compute, storage, virtualization, and network health and topology.		
6.4.21	Automation & Orchestration	Built-in orchestration engine with SOAP/REST-ready workflows and PowerShell/Ansible modules for switch provisioning, firmware upgrades, and configuration compliance.		
6.4.22	Redundancy & High Availability	Switch must support virtual stacking or similar technology to maintain high availability in switching cluster		
6.4.23	Cooling & Power Efficiency	Switch must operate within 400–600 W under typical load		
6.4.24	Multicast & Broadcast Control	PIM-SM/SSM, MSDP, and IGMP/MLD snooping; hardware replication trees for efficient multicast distribution.		
6.4.25	future scalability supporting	The proposed switch must be capable of being deployed in a Software-Defined Data Center (SDDC) environment, supporting spine-leaf architecture in accordance with the respective switch manufacturers' recommended design, without requiring any hardware replacement. In addition, the switch should support future scalability by allowing an additional, minimum 16GB of RAM to be added.		

6.4.26		Switch solutions must be able to integrate policy enforcement across computers, storage, virtualization, and network via single management.		
6.4.27	Warranty & Support	The switch must be with a warranty of 3-year 24x7x4, parts replacement and 24×7 TAC support at a quoted price with identical terms.		
6.4.28		All the switch components, optics should be from same manufacture		

6.5 Network Firewall

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.5.1	General & Compliance	Make		
6.5.2		Model		
6.5.3		Country of Origin		
6.5.4		The Firewall Vendor must be listed as a Leader in the Latest Gartner's Magic Quadrant or Forrester Wave report (2023/2024/2025) for Network Firewalls category		
6.5.5		The proposed enterprise firewall solution must be independently tested and validated within the last 24 months by recognized third-party evaluators specializing in network security, such as SE Labs, Miercom, Gartner, ICSA, Forrester Wave, or equivalent. proof must be attached.		
6.5.6	Bidder Qualification	Bidder must at least hold top-tier 2 partnership with the quoted Firewall OEM and attach proof.		
6.5.7		Provide two certified engineers (≥2 yrs experience) and evidence of ≥3 Firewall installs in the last 5 yrs.		
6.5.8	Form Factor	Must be physical appliance (≥1U) with modular NIC, SSD, dual PSU, rack mountable, front-to-back airflow.		
6.5.9	Deployment Modes	Must support routed, transparent, multi-instance, and cluster-based deployments with unified policy control.		
6.5.10	Global Certifications	Must be certified to FIPS 140-2 Level 2, ICSA Labs NGFW, and Common Criteria EAL4+ or equivalent.		

6.5.11	Availability Timeline	Must be actively shipping model with minimum 5-year roadmap and support lifecycle.		
6.5.12	Interface Density	Must include ≥16 x 10Gbps SFP+ ports and ≥8 x 1Gbps RJ45 ports		
6.5.13	Form Factor Detail	Must be 1U rackmount with dual PSU, modular NICs, SSDs, and front-to-back airflow		
6.5.14				
6.5.15	IPS Throughput	Must deliver ≥17 Gbps sustained NGIPS throughput (real-world traffic mix)		
6.5.16	Threat Inspection Throughput	Must achieve ≥17 Gbps threat protection throughput (IPS, malware, URL filtering)		
6.5.17	Concurrent Sessions	Must support ≥2 million concurrent sessions		
6.5.18	New Connections/sec	Must handle ≥130,000 new sessions/sec with deterministic latency with Application visibility and control enable		
6.5.19	NGFW Core Capabilities	Must provide Layer 3–7 inspection, IPS, malware filtering, TLS decryption, NAT, and app-based policy control.		
6.5.20	Application Intelligence	Must support ≥4,000 applications, traffic patterns, risk scoring, and behavior correlation.		
6.5.21	Threat Prevention Stack	Must support inline IPS, malware sandboxing, dynamic threat feeds, URL filtering, and file inspection.		
6.5.22	VPN & Remote Access	Must support IPSec, SSL, DTLS VPN, and 20K+ simultaneous peers.		
6.5.23	Policy Control	Must support object reuse, rule optimization, rollback, and scheduled activation.		
6.5.24	IPv4/IPv6 Full Support	Must support native dual-stack with full inspection, NAT, and VPN capabilities.		
6.5.25	Protocol Decoding	Must identify and control protocols via ports, payload, and behavior—not just header info.		
6.5.26	Quality of Service (QoS)	Must support QoS marking, shaping, and bandwidth-based policy enforcement.		
6.5.27	SD-WAN Readiness	Must integrate with SD-WAN fabric for traffic steering, telemetry, and policy alignment.		
6.5.28	Security Benchmarks	Must align with CIS, NIST SP 800-41/53, and ISO/IEC 27001 benchmarks.		
6.5.29	Documentation & Audit	Must include full audit reports and change logs, signed configuration snapshots, and compliance dashboards.		
6.5.30	Secure Management Interface	HTTPS/TLS ≥1.2 GUI + SSHv2 CLI with role-sensitive views and command-level authorization		

6.5.31	Role-Based Access Control (RBAC)	≥50 customizable roles, nested permissions, audit-ready logs		
6.5.32	Authentication Integration	LDAP, RADIUS, TACACS+, SAML 2.0, OAuth2 support		
6.5.33				
6.5.34	Audit Logging	Immutable logs with user ID, timestamp, source IP, and action details		
6.5.35	Logging Integration	Syslog (RFC 5424), SNMPv3, SIEM forwarding		
6.5.36	Reporting & Dashboards	Configurable dashboards, scheduled PDF/CSV reports, drill-down analytics		
6.5.37	Threat Intelligence Ingestion	Dynamic threat feeds (IPS, malware, URL) with override and scheduling		
6.5.38	OS Hardening & Integrity Checks	CIS-compliant hardened OS, boot-time and runtime integrity validation		
6.5.39	Security Compliance Validation	FIPS 140-2 Level 2+, GDPR, ISO/IEC, NIST compliance with documentation		
6.5.40	Log Granularity	Full traffic, policy, user, threat, and admin activity logging		
6.5.41	Log Format & Standards	JSON, CEF, Syslog (RFC5424) with customizable fields		
6.5.42	Real-Time Monitoring	Event correlation, anomaly detection, customizable thresholds		
6.5.43	SIEM/SOAR Integration	Native integration with ≥3 platforms (Splunk, QRadar, Elastic, Sentinel)		
6.5.44	Reporting Engine	Custom dashboards, scheduled reports, drill-down analytics		
6.5.45	Alerting Capabilities	Multi-channel alerts (email, SNMP, API), escalation paths, role-sensitive templates		
6.5.46	Log Integrity & Verification	Hashing, digital signatures, tamper detection, audit trail validation		
6.5.47	Application Identification	≥5,000 apps with risk, bandwidth, behavior, threat classification		
6.5.48	Threat Prevention	Inline IPS, malware, URL filtering, file inspection with exception handling		
6.5.49	Encrypted Traffic Analytics (ETA)	Support for Encrypted Traffic Analytics to detect threats in encrypted flows without full decryption.		
6.5.50	Warranty License/ Subscription	Firewalls must be with a warranty of 3-year 24x7x4, parts replacement and 24×7 TAC support at a quoted price with identical terms.		
6.5.51		License and subscription for all above features must be quoted with 3 years		

6.6 TOR (Top-of-Rack) Aggregation Switch

1	2	3	4	5
Line-Item No	Description of goods/Category	Purchaser's Requirements/ Technical Specifications and Standards	Bidder's Offer	
		Details	Compliance Yes(Y) / No(N)	Remarks
6.6.1	General & Compliance	Make		
6.6.2		Model		
6.6.3		Country of Origin		
6.6.4		The switch must be listed as a Leader in the Gartner's Magic Quadrant or Forrester Wave report for at least 3 (2023/2024/2025) years in Datacenter Switching category		
6.6.5	Bidder Qualification	Bidder must demonstrate authorized partnership with the OEM sufficient to provide warranty, support, and certified deployment		
6.6.6		Provide two certified engineers (≥2 yrs experience) and evidence of ≥3 SD-Datacenter installs in last 5 yrs.		
6.6.7	Hardware Specifications	The switch shall provide at least populated 24 10Gbps SFP+ on ports supporting 1/10/25 GbE speeds, the switch also shall with 2x 40/100 GbE uplinks u. All transceivers from the same OEM and fiber patch cables must be vendor-certified to ensure compatibility and optimal performance.		
6.6.8		Dual hot-swappable AC power supplies; N+1 redundant fan modules; rack mountable accessories		
6.6.9	Performance & Capacity	Minimum switching capacity ≥2Tbps and forwarding rate ≥1 Bpps (for full port population).		
6.6.10		must provide a minimum of 36 MB dedicated buffer memory		
6.6.11		Switch should support at least 25K hardware-based ACL		
6.6.12		It should be possible to connect switches in virtual stack to increase performance and active-active performance		
6.6.13		Switch should support up to 64,000 Mac address		
6.6.14		Should support 16 GB of DRAM and 16 GB of Flash Memory		
6.6.15				
6.6.16	Architecture & Topology	The proposed switch shall be configured as an aggregation layer switch, serving as the central point for consolidating traffic from multiple access switches before forwarding to the core network		

6.6.17	Layer 3 Features	Full IPv4/IPv6 routing: OSPF, BGP routing protocols to facilitate resilient and scalable network architecture.		
6.6.18		Should Support VRF		
6.6.19	QoS & Traffic Management	Hierarchical QoS with minimum 8 hardware queues per port; support for traffic policing, shaping, and priority-based scheduling.		
6.6.20	Network Automation	REST, NETCONF, gNMI, Ansible, and model-driven telemetry must be supported for turnkey integration with DevOps pipelines.		
6.6.21	Management & Monitoring	switch must provide comprehensive support for health monitoring features, including Health Dashboards covering Network, Client, and Application status, as well as detailed monitoring of Switch and Wired Client health.		
6.6.22	Compliance Evidence	Bidders must submit a completed Component Worksheet (CPU, FPGA, ASIC, PSUs, fans) with part numbers and vendor datasheets as proof of compliance.		
6.6.23		Use of white-boxes, non-certified optics, or third-party firmware is disallowed and results in non-compliance.		
6.6.24	Warranty & Support	The switch must be with a 3-year 24x7x4, parts replacement and 24×7 TAC support at a quoted price with identical terms.		

6.7 Firewall at Head office (ERD)

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.7.1	General & Compliance	Make		
6.7.2		Model		
6.7.3		Country of Origin		
6.7.4		The Firewall Vendor must be listed as a Leader in the Latest Gartner's Magic Quadrant or Forrester Wave (2024/2025) report Network Firewalls category		
6.7.5		The proposed enterprise firewall solution must be independently tested and validated within the last 24 months by recognized third-party evaluators specializing in network security, such as SE Labs, Miercom, Gartner, Forrester Wave, or equivalent. proof must be attached.		
6.7.6	Bidder Qualification	Bidder must demonstrate authorized partnership with the OEM sufficient to provide warranty, support, and certified deployment		
6.7.7		Provide two certified engineers (≥2 yrs experience) and evidence of ≥3 Firewall installs in the last 5 yrs.		
6.7.8	Form Factor	Must be physical appliance (≥1U) with, rack mountable, front-to-back airflow.		
6.7.9	Deployment Modes	Must support routed, transparent, multi-instance, and cluster-based deployments with unified policy control.		
6.7.10	Global Certifications	Must be certified to FIPS 140-2 Level 2, ICSA Labs NGFW, and Common Criteria EAL4+ or equivalent.		
6.7.11	Availability Timeline	Must be actively shipping model with minimum 5-year roadmap and support lifecycle.		
6.7.12	Interface Density	Must include ≥4 x 10Gbps SFP+ ports, and ≥8 x 1Gbps RJ45 ports		
6.7.13	IPS Throughput	Must deliver ≥11 Gbps sustained NGIPS throughput (real-world traffic mix)		
6.7.14	Threat Inspection Throughput	Must achieve ≥9 Gbps threat protection throughput (IPS, malware, URL filtering)		
6.7.15	Concurrent Sessions	Must support ≥400,000 concurrent sessions		

6.7.16	New Connections/sec	Must handle ≥50,000 new sessions/sec with deterministic latency with Application visibility and control enable		
6.7.17	NGFW Core Capabilities	Must provide Layer 3–7 inspection, IPS, malware filtering, TLS decryption, NAT, and app-based policy control.		
6.7.18	Application Intelligence	Must support ≥4,000 applications, traffic patterns, risk scoring, and behavior correlation.		
6.7.19	Threat Prevention Stack	Must support inline IPS, malware sandboxing, dynamic threat feeds, URL filtering, and file inspection.		
6.7.20	VPN & Remote Access	Must support IPSec, SSL, DTLS VPN, and 800 simultaneous peers.		
6.7.21	Policy Control	Must support object reuse, rule optimization, rollback, and scheduled activation.		
6.7.22	IPv4/IPv6 Full Support	Must support native dual-stack with full inspection, NAT, and VPN capabilities.		
6.7.23	Protocol Decoding	Must identify and control protocols via ports, payload, and behavior—not just header info.		
6.7.24	Quality of Service (QoS)	Must support QoS marking, shaping, and bandwidth-based policy enforcement.		
6.7.25	SD-WAN Readiness	Must integrate with SD-WAN fabric for traffic steering, telemetry, and policy alignment.		
6.7.26	Security Benchmarks	Must align with CIS, NIST SP 800-41/53, and ISO/IEC 27001 benchmarks.		
6.7.27	Documentation & Audit	Must include full audit reports and change logs, signed configuration snapshots, and compliance dashboards.		
6.7.28	Secure Management Interface	HTTPS/TLS ≥1.2 GUI + SSHv2 CLI with role-sensitive views and command-level authorization		
6.7.29	Role-Based Access Control (RBAC)	≥50 customizable roles, nested permissions, audit-ready logs		
6.7.30	Authentication Integration	LDAP, RADIUS, TACACS+, SAML 2.0, OAuth2 support		
6.7.31				
6.7.32	Audit Logging	Immutable logs with user ID, timestamp, source IP, and action details		
6.7.33	Logging Integration	Syslog (RFC 5424), SNMPv3, SIEM forwarding		
6.7.34	Reporting & Dashboards	Configurable dashboards, scheduled PDF/CSV reports, drill-down analytics		
6.7.35	Threat Intelligence Ingestion	Dynamic threat feeds (IPS, malware, URL) with override and scheduling		

6.7.36	OS Hardening & Integrity Checks	CIS-compliant hardened OS, boot-time and runtime integrity validation		
6.7.37	Security Compliance Validation	FIPS 140-2 Level 2+, GDPR, ISO/IEC, NIST compliance with documentation		
6.7.38	Log Granularity	Full traffic, policy, user, threat, and admin activity logging		
6.7.39	Log Format & Standards	JSON, CEF, Syslog (RFC5424) with customizable fields		
6.7.40	Real-Time Monitoring	Event correlation, anomaly detection, customizable thresholds		
6.7.41	SIEM/SOAR Integration	Native integration with ≥3 platforms (Splunk, QRadar, Elastic, Sentinel)		
6.7.42	Reporting Engine	Custom dashboards, scheduled reports, drill-down analytics		
6.7.43	Alerting Capabilities	Multi-channel alerts (email, SNMP, API), escalation paths, role-sensitive templates		
6.7.44	Log Integrity & Verification	Hashing, digital signatures, tamper detection, audit trail validation		
6.7.45	Application Identification	≥5,000 apps with risk, bandwidth, behavior, threat classification		
6.7.46	Threat Prevention	Inline IPS, malware, URL filtering, file inspection with exception handling		
6.7.47	Encrypted Traffic Analytics (ETA)	Support for Encrypted Traffic Analytics to detect threats in encrypted flows without full decryption.		
6.7.48	License/ Subscription Warranty & Support	License and subscription for all above features must be quoted with 3 years		
6.7.49		The Firewall must be with a 3-year 24x7x4, parts replacement and 24×7 TAC support at a quoted price with identical terms.		

6.8 Backup Software

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.8.1	General & Compliance	Make		
6.8.2		Model		
6.8.3		Country of Origin		
6.8.4	License	The license should be a workload base license and there should not be any restriction on capacity. 30 License should include For VMS and Physical servers which are not limited to VMware, Oracle, Widows 2016/2019/2022 Linux and etc.		
6.8.5		Licenses should be for Backup and Replication of workloads as well. as Production and DR failover, failback automation,		
6.8.6		Same License should be valid for physical, Virtual or cloud Workloads and should. be able to use interchangeably as a, when necessary, without requiring purchasing additional. license. All below requirement should be provided by a single vendor		
6.8.7	Analyst Rating	The backup software proposed should be in the Leader position in Latest Gartner Magic Quadrant or Foresster wave report for Data Protection & Backup Software (or equivalent independent analyst validation)		
6.8.8	Management Console	The solution should offer centralized, web-based administration with a single view of all back up activities and should have an alerts generation facility in case of an issue in backup process		
6.8.9	Media Support	Disk, Tape, Cloud		
6.8.10	Backup Type	Backup Software must support multiple levels of backup including, Full, Incremental, Synthetic, Oracle RMAN.		
6.8.11	Backup Support for Hypervisors and Applications	Backup software should be a Hardware Agnostic, and it should support snapshot integration with industry-standard virtualization hypervisors and support de-duplication on any storage target. It should be able to backup data for long term retention.		
6.8.12		The proposed backup software should provide instant recoveries for any backup to any hypervisor or any cloud		

6.8.13		Backup software should support file level recovery from any backup of any VM or physical server. It should support a full recovery system in case of a crash, either on a physical system or virtual machine or as a Cloud Instance.		
6.8.14		Backup software should have integrated data de-duplication engines with multi-vendor storage support to save space by storing de-duplicated copies of data, 'The de-duplication engine should also facilitate IP base replication of de-dupe data. All necessary hardware and software required to support this functionality should be supplied along with other components		
6.8.15	Data Base Support & Recovery	Backup Solution should be capable of scheduling and automating the testing of Backups.		
6.8.16		Backup software should support instant database recoveries of MS SQL, and Oracle.		
6.8.17		Backup software should support instant recovery of multiple VMs in parallel to support quick application recovery. It should also allow instant recovery of selected VM disks, without having to do instant recovery of all VM disks for achieving highest levels of RTO for relevant business data		
6.8.18	Data Migration	The proposed solution should support universal recovery to restore from P2P, P2V, V2V and V2P without having to wait to extract the full backup to production storage without additional Cost		
6.8.19	Data Deduplication	The solution should support data deduplication to reduce the backup data storage and should be able to integrate with purpose build data deduplication hardware and support inline data deduplication.		
6.8.20	RPO/RTO and Recovery Assurance	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered on in a sandbox environment and tested for its recoverability.		
6.8.21		Recovery verification should automatically boot the server from backup and very the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup/recovery audits.		

6.8.22		Backup software should provide Backup and Relocation capabilities in one console only and allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only these VMs to which they have access, without administrator intervention, thereby delivering self-serve capabilities.		
6.8.23		Proposed backup software should be able to provide data immutability as a feature on the primary repository using any commodity storage		
6.8.24		There proposed Backup software must Support Seamless Integration with Point-in-time storage snapshots with Major OEM SAN Storages in the environment to perform faster LAN Free backup without any overhead to Hypervisor Computer Layer, allowing recovery at the application level, the tile level, and the VM level.		
6.8.25		The proposed backup software should be able to integrate with anti-virus software and scan before recovery of VMs and ensure that any infected VM is not restored or restore it with disabled network adapters to prevent any infection to spread through the network.		
6.8.26		Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files/ records which should not be restored from the backup copies. This will help in complying with " right to be forgotten" regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.		
6.8.27		Backup software should support instant file share recovery in NAS storages to allow users to access files fast after disaster.		
6.8.28	Backup and replication performance and SLA	The proposed Backup software must allow us to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.		
6.8.29		Backup software should provide Recovery of Application items, File, Folder and Complete VM recovery capabilities from the image level backup within15Mins RTO.		

6.8.30		The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.		
6.8.31	Disaster Recovery Capabilities	Replication in the software should be a VM level replication, and you must replicate the VM level data with or without backing it up at the source site. It should also include failover and tailback capabilities and should be able to perform automatic acquisition of network addresses at the destination site.		
6.8.32		The Proposed solution should support Continuous replication at VM level, The RPO must be less than 5 Seconds, and it must Deliver application consistency.		
6.8.33		Backup and replication software must deliver maximum investment protection by supporting replication of workloads between (dis-similar systems like hyper converged infrastructure to stand along servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of underline hardware.		
6.8.34		The proposed solution should be able to publish Disaster recovery plans arid update them through automated discovery whenever prompted after changes in Infrastructure.		
6.8.35		Should be able to publish DR drill reports, DR test reports and DR readiness check reports for audit and compliance purposes.		
6.8.36		Backup software should have the ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes. This bare metal recovery should be built in for the physical servers and should even work on the dissimilar hardware.		
6.8.37		Backup software should have the ability to backing up a Cloud VM running in AWS or Azure and restore it as a valid VM workload back onto a Virtual server farm		
6.8.38	Data Protection and	Software should be able to restore VMs		

6.8.39	Recovery in the cloud	Software should be able to extend the backup repository to a public cloud service provider by LGC.		
6.8.40		Backup software should have the capability to archive backup data to Amazon Glacier or Microsoft Azure storage Archive tier. The Software must have the capability to restore the data from archive tier; it should not be dependent on cloud Service Supplier .		
6.8.41		Backup software should support agentless backups of applications residing in VMS like SQL, Exchange, SharePoint, Oracle, SAP, SAP HANA, MySQL etc. with non-staged granular recovery of all these applications and backup software should also support DB2 environments.		
6.8.42		Proposed backup software should be able to leverage Immutable Cloud based storage like S3-Immutable service to prevent backup copies of data from any corruption or ransomware attacks.		
6.8.43	IP Support	Backup Software should support both IPV4 & IPV6		
6.8.44	Ransomware Protection	Ability to detect a combination of high CPU activity along with sustained write I/O on a drive and generate alarms accordingly.		
6.8.45		Ability to report that- an incremental backup is suspiciously large due to the source being encrypted		
6.8.46	Analytics	The solution should provide capacity planning for backup storage space utilization.		
6.8.47		Easily forecast resource usage and utilization trends for Hypervisors and backup environments to accurately determine when resources will run out.		
6.8.48		The solution should provide real-time monitoring of backup infrastructure components, such as a backup server, backup repository etc.		

6.8.49	Reporting Capabilities	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied.		
6.8.50		Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.		
6.8.51		Proposed solutions should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drills down views of health, performance and workload of the virtual hosts.		
6.8.52	Product Support	Should have Access to 24x7 Manufacturer's Customer Service and Support over the phone for trouble shooting assistance of Product. Bidder should have top – tier 2 partnership with the quoted product.		
6.8.53	Hardware and Support	The Vendor should provide the cost of required hardware (Servers, Storage etc.) operating Systems and any other third-party Licenses required for both production data center and disaster Recovery sites to implement the backup solution. 3 years onsite comprehensive warranty (including parts, labor and transportation) is required for the proposed hardware. Backup policy and hardware should support *Daily backups retained for 14 days. *Weekly backups retained for 4 weeks. *Monthly backups retained for 12 months. *Yearly backups retained for 5 years. Backup solution must meet the stated retention policies and provide OEM authorization or equivalent certification to ensure warranty, updates, and support.		

6.9 Backup Storage

1	*2*	*3*	4	*5*
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
Backup Repository in DR				
6.9.1	General & Compliance	Make		
6.9.2		Model		
6.9.3		Country of Origin		
6.9.4	Industry Leadership	The offered scale out storage solution shall be a scale-out software defined storage being with required compute, network, and storage hardware.		
6.9.5		Should be listed in latest magic Quandarnt for Distributed File Systems and Object Storage		
6.9.6	Software Defined	The Scale out Storage solution offered shall be true Scale-out software defined storage with the following features:		
6.9.7		Shall be able to port and configure on standard x86 servers		
6.9.8		Shall have flexible OS support with Linux distributions.		
6.9.9		There shall be no need to maintain or qualify hardware compatibility list needed except for the resource requirement for Compute, Storage and network.		
6.9.10		Solution might be installed on 1 server or 1 VM as a production appliance		
6.9.11		Object storage should be based on micro-services architecture supporting Kubernetes		
6.9.12		Solution must support replication between DCs		
6.9.13		Object storage must support S3 Bucket Lifecycle Expiration & Data Transition		
6.9.14		Object storage must support Prometheus application for event monitoring and alerting		
6.9.15		Object storage must support Object Lock & SOBR offload for backup solution proposed		
6.9.16		Object storage must be validated with API on backup solution proposed		
6.9.17	Core technology - Object	Object storage core technology shall be able to abstract the underlying servers, to create a uniformly scalable storage pool		
6.9.18		There shall be No size limit for object or files which can be stored in the cluster.		

6.9.19		Offered storage shall do automatic Rebalancing when adding a new server in the cluster		
6.9.20		Offered storage shall allow capacity extensions done by adding disks to existing servers (scale-up) or adding additional servers to the system (scale-out).		
6.9.21		Object storage must support erasure coding 2+1 & 9+1 schemas to protect data		
6.9.22		Object storage must support IAM Policy configuration		
6.9.23		Object storage must integration with Authentication Infrastructure (SAMLv2, OIDC and LDAP)		
6.9.24		Object storage must have SSD & HDD to provide the best performance with cost-effective price		
6.9.25	Capacity, Scalability and Metadata	Offered Storage shall be supplied with minimum of 100 TiB Capacity and should provide 3.2TB NVMe SSDs for Metadata on Backup Workload.		
6.9.26		There shall be no separate and dedicated control node or metadata node in the cluster. In case, nodes are separate then vendor shall over Metadata / control nodes in HA using active / active approach.		
6.9.27	Availability, Reliability & Durability	The solution must provide a minimum of eight 9 durability on a Single Site and shall have the capability to provide 11 nines on multiple Site.		
6.9.28		The solution offered shall be completely redundant and there shall be no single point of failure.		
6.9.29	Data Protection	Offered storage shall support both replication & Erasure coding.		
6.9.30		Offered software defined storage shall be able to expand the given cluster across locations using both Replication factor and Erasure coding technique.		
6.9.31		For better performance, Storage solution shall automatically use Replication & Erasure coding operations for all objects less than 60KB in size. This shall be adjustable, if required.		
6.9.32	Connectivity - Object interface	Object interface would be scalable S3. its architecture shall include the following:		
6.9.33		o S3-Server: S3 API Server for Buckets/Objects, MPU and more		
6.9.34		o Scale-Out "any-to-any" access		
6.9.35		Security model S3-Vault: Security service for Accounts		

6.9.36		a. Multi-tenant, Support for S3 IAM – Identity and Access Management.		
6.9.37		b. Authentication with Signature v2 and v4		
6.9.38		c. Microsoft Active Directory over SAML 2.0 (ADFS) Integration		
6.9.39		d. Comprehensive AWS IAM security model for Users & Groups with Roles		
6.9.40		e. Bucket & Object ACLs		
6.9.41		o S3-Metadata: Distributed Metadata Engine		
6.9.42		o S3 Bucket Versioning		
6.9.43		o S3 Object Lock		
6.9.44		o Transparent Bucket-Level At-REST Encryption		
6.9.45		o S3 Console: GUI Web interface to manage accounts, users, policy and monitor usage.		
6.9.46		o S3 Browser: GUI Web interface to create buckets and upload objects.		
6.9.47		o Quota for S3.		
6.9.48	Data Management Features	It shall be possible to tag and search S3 Metadata.		
6.9.49		Lifecycle Management - It shall be possible to automatically transition, and expiration of data based on criteria.		
6.9.50		It shall be possible to asynchronously replicate buckets to several Cloud targets		
6.9.51		Offered storage shall support multi-tenancy and data isolation		
6.9.52	Ease of USE	The storage offered shall have full management and control with Supervisor and CLI		
6.9.53		integration with Nagios, Zabbix & others.		
6.9.54		Auditing capabilities.		
6.9.55		REST APIs for monitoring & management		
6.9.56		Offered storage shall support role Based Access Control (RBAC)		
6.9.57	Simplifying operations and management	The storage offered shall have Simplified Operations & Management and shall provide:		
6.9.58		100% availability		
6.9.59		Software Upgrades, Server replacements, or Capacity Extensions don’t stop the system		
6.9.60		Automated disk failure detection		
6.9.61		Automatically rebuilt for failed drive		
6.9.62		Automated storage rebalancing		
6.9.63		Disk replacement utility		
6.9.64		Easily add servers or hard drives in the server		

6.9.65		The system shall automatically rebuild the missing data in case of hardware component failure.		
6.9.66	Multi-cloud Controller	The storage offered shall have an in-built multi-cloud controller engine and shall provide the following features:		
6.9.67		Shall Support writing data to any Cloud (Amazon S3, Google Cloud Storage, Microsoft Azure, Wasabi) via a single S3 API.		
6.9.68		Shall have an Open-Source interface allows developers to quickly test compatibility.		
6.9.69		Shall Preserves native format of the data on any Cloud for providing the ability to read data directly on the public Clouds.		
6.9.70		Shall support Replicating one to many asynchronously so that a given bucket can be replicated to several private and public Cloud targets.		
6.9.71		Shall support Lifecycle data to any Cloud for automatic transition and expiration of data based on criteria.		
6.9.72		Shall support Out of band updates especially when data is directly updated on the public cloud, related metadata information is synchronized to the multi-cloud controller.		
6.9.73		Shall have GUI Web interface to manage multi-cloud environment.		
6.9.74		In case a vendor doesn't support above features natively then vendor shall provision the complete cloud automation suite in their bid and shall provide the complete documentation in the bid.		
6.9.75	storage	Offered storage shall ensure that Data must be tamper-proof.		
6.9.76		Data cannot be deleted, which means offered storage shall provide object lock capability.		
6.9.77		Data must be kept for a specified period which means offered storage shall provide retention mechanism.		
6.9.78		Offered storage shall have capability to migrate the data to an alternative media		
6.9.79	Hardware Specification	Offered Platform shall be a dense platform supporting at-least 24 x Large Form factor drives so that it can be used for multi-purpose uses like Software defined storage, Scale out databases, data warehousing solution etc.		
6.9.80		Minimum 2 number (s) of latest generation Intel or AMD 16 Cores processors or more		

6.9.81		Intel C621A Series Chipset or AMD equivalent with PCI 4.0 Architecture		
6.9.82		Each Node shall have a minimum of 24 x DIMM slots and shall be scalable up to 3TB memory when using 128GB DDR4 Load Reduced DIMM (LRDIMM) operating at 3200 MT/sec		
6.9.83		The system offered shall be supplied with a minimum of 192 GB DDR4 memory.		
6.9.84		Each offered Server shall support 24 x LFF drives.		
6.9.85		Each server offered shall also support an additional 8 number of additional SAS / SATA / NVMe SSD drives.		
6.9.86		Each server offered shall also be supplied with at least 4 *10Gb SFP+ Ports with two redundant adapters. All transceivers and cables should be included.		
6.9.87		Server should support the networking cards:		
6.9.88		1. 1Gb 4-port network adaptors		
6.9.89		2. 10Gb 2-port Ethernet adaptor		
6.9.90		3. 10/25Gb 4-port Ethernet adaptor		
6.9.91		4. 100Gb 2- port network adaptor		
6.9.92		5. 200Gb single port network adaptor		
6.9.93		should support InfiniBand Options:		
6.9.94		1. 100Gb Single and Dual port Adapter		
6.9.95		2. 200Gb Single and Dual port adapter		
6.9.96	System Security	UEFI Secure Boot and Secure Start support		
6.9.97		Immutable Silicon Root of Trust		
6.9.98		FIPS 140-2 validation		
6.9.99		Common Criteria certification		
6.9.100		Configurable for PCI DSS compliance		
6.9.101		Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser		
6.9.102		Support for Commercial National Security Algorithms (CNSA)		
6.9.103		Smart card (PIV/CAC) and Kerberos based 2-factor Authentication		
6.9.104		Tamper-free updates - components digitally signed and verified		
6.9.105		Secure Recovery - recover critical firmware to known good state on detection of compromised FW		
6.9.106		Ability to rollback firmware		
6.9.107		Secure erase of NAND		
6.9.108		TPM (Trusted Platform Module)		
6.9.109		Bezel Locking Kit		

6.9.110	Secure encryption	System should support Encryption of the data (Data at rest) for internal storage using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.		
6.9.111	Firmware security	For firmware security, system should support remote management chips creating a fingerprint in silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable		
6.9.112		Should maintain a repository for firmware and drivers' recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware		
6.9.113	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resource's user is authorized to view.		
6.9.114		The Dashboard minimum should display a health summary of the following:		
6.9.115		• Server Profiles		
6.9.116		• Server Hardware		
6.9.117		• Appliance alerts		
6.9.118		The Systems Management software should provide Role-based access control		
6.9.119		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
6.9.120		Bidders should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalized dashboard to monitor device health, hardware events, contract and warranty status. should provide a visual status of individual devices and device groups. The Portal should be available on premises (at our location - console based) or off premises (in the cloud).		
6.9.121		should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		

6.9.122		The Server Management Software should be of the same brand as the server supplier.		
6.9.123	Warranty	Should have Access to 3 years 24x7 Manufacturer's Customer Service and Support over the phone/remote TAC for troubleshooting assistance of Product. Hardware Warranty includes 3-Year Parts, Labor & Onsite support with 24*7 4 Hours response.		
6.9.124	Deployment References	Should have at least one successful contract reference for the complete backup solution (software and hardware) and should provide PO or customer reference letter as proof.		
Backup Repository in PR				
6.9.125	General & Compliance	Make		
6.9.126		Model		
6.9.127		Country of Origin		
6.9.128	Server type	Shall be 2U Rack Servers, Chassis should support Disks Up to 36 x 2.5" SAS/SATA Drives / 20 x 3.5" SAS/SATA Drives		
6.9.129	Capacity	Total Usable capacity of 90TB should be provided with RAID 6		
6.9.130	CPU	CPU Family (4th Gen Intel Xeon Scalable processors): Dual Latest Intel Xeon Processor 6700P or 6500P or equivalent AMD or higher		
6.9.131	RAM	512 GB RAM, 6400MT/s, Dual Rank, or higher. Shall support scalability up to 8TB.		
6.9.132	Network Interfaces	4 x 10Gb/s SFP+ Optic ports or more with fiber Transceivers. (2 x Dual Ports for Redundant)		
6.9.133	PCIe Slots	Should Support Multiple Gen4 and Gen5 riser configurations. up to 8 x PCIe slots) with interchangeable components that capable to seamlessly integrate		
6.9.134	Rack Rails	Ready Rails Sliding Rails with Cable Management Arm		
6.9.135	Server Management	Should consist of a dedicated network interface for remote management. Include all required software and hardware to provide both in Band and Out of Band remote management of the servers.		
6.9.136	Power Supplies	230V, AC, 50Hz, Dual, Hot-plug, Fault Tolerant Redundant Power Supply (1+1)		

6.9.137	warranty	Manufacturer's comprehensive warranty for 03 Years and 4-hour Mission Critical respond Service for all components of the system		
6.9.138	License Required	Red Hat Enterprise Linux, 1-2 VMs, Premium Subscriptions with 05 Years Production Support (24x7)		

6.10 SASE for remote users - To be added for 100 users

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser’s Requirements/ Technical Specifications and Standards**	**Bidder’s Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.10.1	General & Compliance	Make		
6.10.2		Model		
6.10.3		Country of Origin		
6.10.4		The solution should support secure access for 100 users to private applications and internet resources.		
6.10.5		The Solution license/subscription should include for 3 years period		
6.10.6	Security Framework and Architecture	The solution shall be cloud-native with global PoPs ensuring low latency, high availability, and resiliency.		
6.10.7		Must integrate Secure Web Gateway (SWG) for web traffic filtering and threat prevention.		
6.10.8		Must include Cloud Access Security Broker (CASB) capabilities for monitoring and controlling cloud application usage.		
6.10.9		Provide Zero Trust Network Access (ZTNA) for secure, identity-based access without VPN.		
6.10.10		Include Firewall as a Service (FWaaS) for network-level security inspection and control.		
6.10.11		Provide DNS-layer security to block malicious domain access at DNS resolution stage.		
6.10.12		Support Data Loss Prevention (DLP) to prevent unauthorized data exfiltration.		
6.10.13		Support Remote Browser Isolation (RBI) to protect endpoints from web threats.		
6.10.14	Access and Connectivity	Provide seamless secure access from any device including unmanaged/bring-your-own devices.		
6.10.15		Enable granular user- and application-specific access policies enforcing least privilege.		
6.10.16		Support secure connectivity regardless of network type (corporate LAN, public internet, Wi-Fi).		

6.10.17		Support hybrid deployment with integrations to on-premises and multiple cloud platforms. Clearly defined solution documentation should be provided for the Vendors hybrid cloud solution.		
6.10.18	Threat Protection and Monitoring	Provide advanced threat protection leveraging threat intelligence for malware, ransomware, phishing, etc.		
6.10.19		Support continuous security monitoring and anomaly detection for threat response.		
6.10.20		Provide visibility and analytics for cloud app usage, security events, and user experience metrics.		
6.10.21		Support integration with SOAR and XDR platforms.		
6.10.22	Management and Deployment	Centralized cloud-based console for deployment, policy management, and operations.		
6.10.23		Dynamic policy updates without disrupting active user sessions or endpoint changes.		
6.10.24		Provide unified endpoint agent/client for security modules.		
6.10.25	Compliance and Data Protection	Data encryption in transit and at rest meeting industry standards.		
6.10.26		Adhere to regulatory compliance, data sovereignty, and privacy standards relevant to organization.		
6.10.27	Performance and Scalability	Scalable to support growth in users, apps, and data without performance degradation.		
6.10.28		Provide performance monitoring and real-time user experience metrics.		

6.11 Firewall Manager

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.11.1	General & Compliance	Make		
6.11.2		Model		
6.11.3		Country of Origin		
6.11.4		The centralized firewall management appliance must be declared by make and model.		
6.11.5		Appliance must be independently validated within the last 24 months by recognized third-party security evaluators (e.g., SE Labs, Gartner, ICSA). Proof must be attached.		
6.11.6	Bidder Qualification	Bidder must at least hold top-tier 2 partnership status with the OEM of the proposed appliance and provide proof.		
6.11.7		Bidder must assign at least two certified engineers with a minimum of 2 years' experience on centralized firewall management.		
6.11.8	Form Factor	Appliances must be a physical rack-mountable device of 1RU or less.		
6.11.9		Appliance must have modular RAID Controller and Network Interface		
6.11.10		Appliance must include enterprise-grade RAID 1 storage, configured with two 1.2 TB 10K SAS HDDs minimum.		
6.11.11		Appliance must have dual hot-swappable high-wattage AC power supplies (1050 W minimum) for redundancy.		
6.11.12		Appliance should have front-to-back airflow suitable for 19-inch 4-post industry-standard racks.		
6.11.13		Virtual appliance-only solutions are not acceptable.		
6.11.14	Hardware Specifications	Appliance must include at least two network interfaces supporting 1/10 Gbps speeds, including at least one fiber optic uplink port.		
6.11.15		Appliance must include two USB 3.0 Type A ports.		
6.11.16		Appliance must have a dedicated out-of-band management port.		

6.11.17		Appliance must include RJ-45 RS-232 serial console and DB-15 VGA port for local administration.		
6.11.18	Management Capacity	Appliance must support centralized management of 50 sensors.		
6.11.19		Appliances must process at least 30 million intrusion prevention system events per day.		
6.11.20		Solution must support multi-site policy management with zero-touch provisioning.		
6.11.21	Policy & Threat Management	Support unified management of firewall rules across managed sensors.		
6.11.22		Support centralized management of intrusion prevention system policies and signatures.		
6.11.23		Support URL filtering capabilities for web traffic control and compliance enforcement.		
6.11.24		Provide advanced malware detection and analysis integrated with policy management.		
6.11.25		Support application visibility and granular application-level access control policies.		
6.11.26		Provide reusable policy objects that are usable across multiple policies and sensors.		
6.11.27		Enable dynamic security group creation based on attributes such as IP, user, device, or application context.		
6.11.28		Supporting automated threat-driven rule creation and policy adjustment based on threat intelligence.		
6.11.29	Visibility & Analytics	Provide real-time user- and device-identity based event correlation.		
6.11.30		Provide historical event correlation and customizable dashboards.		
6.11.31		Provide traffic behavior analytics and anomaly detection capabilities.		
6.11.32	Access Control & RBAC	Support granular role-based access control with customizable administrative roles.		
6.11.33		Support delegated administrative domains and per-policy edit permissions without full system access.		
6.11.34	Backup & Recovery	Support scheduled encrypted configuration backups.		
6.11.35		Support USB-based recovery options.		
6.11.36		Support rollback capability for configuration and policy changes.		
6.11.37	Integration & APIs	Provide open RESTful APIs for integration with SIEM and SOAR platforms.		
6.11.38		Support integration with IT service management and ticketing systems.		
6.11.39		Support secure events forwarding to external systems.		

6.11.40	Threat Intelligence	Integrate with external and commercial threat intelligence feeds.		
6.11.41		Automatically correlate internal event data with external intelligence.		
6.11.42		Support automated response playbooks for specific threat categories.		
6.11.43	Performance Optimization	Utilize hardware acceleration for policy evaluation.		
6.11.44		Employ multi-core CPU architecture to support concurrent event processing.		
6.11.45	Compliance Reporting	Provide built-in report templates for ISO 27001, PCI-DSS, NIST, and GDPR compliance.		
6.11.46		Reports must be exportable in PDF, CSV, and HTML formats.		
6.11.47		Reports must be customizable to organizational needs.		
6.11.48	Monitoring & Alerts	Support real-time monitoring with customizable alert thresholds.		
6.11.49		Provide SNMP, syslog, and email notification options.		
6.11.50		Provide event tagging and filtering to streamline rapid incident triage.		
6.11.51	Vendor Experience & Support	OEM must provide firmware and security signature updates for a minimum of five years.		
6.11.52		OEM must provide 24×7 global technical support.		
6.11.53		Bidder must provide references from at least three similar centralized firewall management deployments.		
6.11.54	Security Platform Integration	Appliance must integrate with an enterprise-wide security orchestration, automation, and response platform to enable centralized visibility, automated workflows, and response coordination.		
6.11.55	Warranty & Subscription	Warranty, License and Support for all the above features must be quoted with 3 years		

6.12 Network Floor Switch

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.12.1	General & Compliance	Make		
6.12.2		Model		
6.12.3		Country of Origin		
6.12.4	Manufacture	The proposed switch must be from an OEM that has been consistently recognized in the Gartner Magic Quadrant (or equivalent reputed third-party evaluations such as IDC MarketScape or Forrester Wave) for Enterprise Wired and Wireless LAN Infrastructure, or Campus Switching, within the past three years		
6.12.5	Country of Manufacture / Assembled	The bidder shall list the authorized manufacturing and/or assembly site(s) for the proposed switch. These sites must be certified under the OEM's global quality assurance or manufacturing program		
6.12.6	Form Factor	Rack mountable; should provide rack (19-inch) mounting kits		
6.12.7	Port Requirement	The switch must support 24 × 10/100/1000Base-T ports (RJ-45) with IEEE 802.3at (PoE+). 8 ports of among should support 10Gbps speed. The switch should support a modular uplink slot (supporting 4x 10G SFP modules, field-upgradable to 25G SFP)		
6.12.8		Each switch should be populated with 10G Multimode transceiver module		
6.12.9	Memory, Processor & Hardware Architecture	The switch shall be equipped with a CPU of at least 4 cores running at a minimum of 1.4 GHz, based on a modern embedded ARM (or equivalent) architecture, capable of supporting advanced management, automation, telemetry, and security functions without impacting packet forwarding performance		
6.12.10		minimum of 12 MB packet buffer memory, 4 GB DRAM, and 4 GB flash storage.		
6.12.11		The switch must deliver a backplane switching capacity of at least ≥270 Gbps full-duplex switching capacity and a forwarding performance of at least 210 Mpps tested with 64-byte packets		

6.12.12		The switch must support a stacking bandwidth of at least 160 Gbps.		
6.12.13				
6.12.14		support an IPv4 routing table size of at least 10,000 routes and a minimum of 1,500 Access Control List (ACL) entries, to ensure it meets enterprise-grade performance and scalability requirements.		
6.12.15	Layer 2 and Layer 3 Network standard	Support standard Layer 2 and Layer 3 protocols, including but not limited to OSPF, VRRP, LLDP, and HSRP or equivalent proprietary protocol		
6.12.16		DHCP Auto Config, LACP, DTP or equivalent, UDLD or equivalent, IGMP, Voice VLAN, VTP or Open Standard, Layer 2 trace route, NTP, Storm Control		
6.12.17		The switch must support MACsec encryption per IEEE 802.1AE with AES-128 and AES-256.		
6.12.18		The switch must support to integrate/enable centralized policy enforcement and secure user segmentation		
6.12.19	Unicast MAC Addresses	Minimum 32,000		
6.12.20	IPv6 Unicast Direct Routes	Minimum 2000		
6.12.21	Multicast Routes and IGMP Groups	Minimum 1000		
6.12.22	Maximum Active VLANs	Minimum 1000		
6.12.23	VLAN IDs Available	Minimum 4094		
6.12.24	STP Instances	Up to 64; must support IEEE 802.1D, 802.1s (MSTP), and 802.1w (RSTP)		
6.12.25	SPNN Sessions	Minimum 4		
6.12.26	Jumbo Ethernet Frame	Minimum 9100 bytes		
6.12.27	Other Layer 2 / Layer 3 Protocols Features	The switch must support MACsec encryption per IEEE 802.1AE with AES-128 and AES-256.		
6.12.28	Network Security	802.1X, Multi-domain Auth, RADIUS, TACACS+, ACLs, STRG or equivalent, BPDU Guard, IGMP Filtering		
6.12.29		support port security with configurable MAC-address filtering.		
6.12.30	Redundancy and Resiliency	RSTP, MSTP, PVRST+ or equivalent per-VLAN spanning tree		

6.12.31		The switch must include redundant, field-replaceable power supply units and cooling fans.		
6.12.32		The switch must achieve a cold-boot time of no more than three minutes.		
6.12.33		The switch must support flexible, software-based feature upgrades and enhancements that allow the network to evolve and incorporate advanced capabilities without the need for hardware replacement		
6.12.34	Enhanced QoS	802.1p CoS, DSCP, CIR, SRR or equivalent, WTD or equivalent, Auto-QoS, 8 egress queues per port		
6.12.35	Switch Management	Web UI, CLI, SNMP, USB/RJ-45 console		
6.12.36	Environmental Compliance	ROHS, CE, FCC, EMI/EMC certified		
6.12.37	Environmental & Compliance	switch must operate reliably in ambient temperatures from –5 °C to +45 °C.		
6.12.38		The switch must support smart power management features to optimize energy consumption during low usage periods.		
6.12.39		The switch must comply with CE, UL, and RoHS certifications.		
6.12.40	Warranty & OEM Support	The proposed switch must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present a warranty SKU and warranty confirmation letter from the OEM with Next Calendar Day replacement.		
6.12.41		The OEM shall not declare the supplied product as end of support (EoS) or end of Life (EoL) Suring five (05) years period,		
6.12.42		Documentation providing back-to-back warranty has been obtained from the respective OEM should be provided.		
6.12.43		24X7 access to OEM for level 2 and 3 technical supports should be available.		
6.12.44		The OEM must maintain an authorized country office within Sri Lanka. Additionally, a local spare parts depot must be available and operational within Colombo to support expedited escalations and hardware replacements. Proof document is required.		

6.12.45	Management & Monitoring	Next business day replacement of faulty devices should be provided; The OEM of switches should maintain a spare parts depot in Colombo to support this. Relevant documentation confirming the next business day delivery and availability of spare parts depot obtained from the OEM should be submitted with bid proposal.		
6.12.46		switch must provide both a command-line interface (CLI) and an integrated web-based GUI.		
6.12.47		The switch must support SNMP v1/v2c/v3 and syslog for event logging.		
6.12.48		The switch must support integrated RFID functionality, one similar technology to enable real-time asset tracking / location identification within the network.		
6.12.49		The switch must support integration with Security Information and Event Management (SIEM) systems through standard protocols including Syslog and SNMP traps for real-time event monitoring and alerting.		

6.13 Wi-Fi access point

1	**2**	**3**	**4**	**5**
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.13.1	General & Compliance	Make		
6.13.2		Model		
6.13.3		Country of Origin		
6.13.4	General OEM qualification	The proposed Wireless Solution must be from an OEM that has been consistently recognized as leader or challenger in the Gartner Magic Quadrant (or equivalent reputed third-party evaluations such as IDC MarketScape or Forrester Wave) for Enterprise Wired and Wireless LAN Infrastructure, or Campus Switching, within the past three years		
6.13.5		The bidder shall clearly declare the Country of Origin of proposed Access points certified by the OEM		
6.13.6		The bidder shall list the authorized manufacturing and/or assembly site(s) for the proposed switch. These sites must be certified under the OEM's global quality assurance or manufacturing program		

6.13.7		The proposed AP must include a minimum five (5) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present warranty SKU and warranty confirmation letter from the OEM with Next Calendar Day replacement.		
6.13.8		The OEM must guarantee a minimum six (6) year product lifecycle available ahead and clearly mention, the End-of-Sale (EoS) and End-of-Life (EoL) status, OEM EoS/EoL policies with support document		
6.13.9		The OEM must maintain an authorized country office within Sri Lanka. Additionally, a local spare parts depot must be available and operational within Colombo to support expedited escalations and hardware replacements. Proof document is required.		
6.13.10	Vendor Authorization	Bidder is an authorized partner of OEM with ≥10 years WLAN deployment experience in enterprise/campus environments.		
6.13.11		Vendor MUST submit an Active Heat map report, using a Third-Party heat map tool with a latest dedicated wireless spectrum analyzer (Eg: Eakhau heat map tool with Ekahau Side-Kick-2). Heat maps generated using software tools will NOT be accepted.		
6.13.12		Bidder should have at least 2 Professional level certified engineers in wireless technology for related products, proof must be attached		
6.13.13	Radio & Antenna	The access point must offer tri-band radios operating simultaneously on 2.4 GHz, 5 GHz, and 6 GHz and backward compatible with 802.11a/b/g/n/ac/ax. should allowed in local TRC regulation.		
6.13.14		At the time of ordering if 6-GHz band is not allowed, the 6-GHz radio should be disabled. The radio may be enabled with future software, once the product is certified to operate in 6 GHz complying with Local regulation.		
6.13.15		The access point must support Concurrent dual radios: 2.4 GHz & 5 GHz, each with ≥2×2 MIMO and 4×4 on 5 GHz).and should also support Wi-Fi 7 (802.11be)		
6.13.16		Antenna must be Integrated dual band down tilt omni-directional antennas and gain must not be lower than 4dBi on 2.4Ghz radio and 5dBi on 5Ghz radio and 6dBi on 6Ghz radio		

6.13.17		Must include a dedicated scanning/AUX radio and integrated BLE/IoT radio.		
6.13.18		The access point must support flexible radio mode configuration for optimized performance per deployment.		
6.13.19		The access point must support Multi-Link Operation (MLO) for simultaneous multi-band communication.		
6.13.20	Throughput & Performance	≥9 Gbps combined PHY rate across all radios with OFDMA, MU-MIMO, BSS Coloring, TWT.		
6.13.21		Support ≥250 concurrent client associations per AP; ≥30 active clients per radio without performance degradation.		
6.13.22		Should support for 20/40/80/160 MHz channels on 5 GHz; 320 MHz if 6 GHz is supported.		
6.13.23		The access point must support high client density scenarios typical in enterprise deployments.		
6.13.24	Transmit Power & RF Optimization	At least 23 dBm per radio EIRP adjustable in 1 dB steps and should align with local regulations		
6.13.25		Automatic channel/power adjustment, band steering, airtime fairness, load balancing.		
6.13.26	Interfaces	Requires at least one 2.5 GbE port with PoE+ 802.3at support (for full tri-radio), and		
6.13.27		≥1 1 GbE port; ≥1 USB Type-A port (≥5 W) for full functionality including USB port.		
6.13.28	Deployment Modes & Zero Touch Provisioning	Access point must be a compact design with efficient power consumption (<30 W typical, up to 45 W with USB).		
6.13.29		Controller-based, cloud-managed, and standalone operation modes supported.		
6.13.30		Must allow deployment, switchable between on-prem and cloud management without hardware changes		
6.13.31		Support for ZTP, bulk configuration, and controller failover.		
6.13.32		Support ceiling, and wall mounting; include kits.		
6.13.33	Advanced Enterprise Security Standards & Features	WPA3-Personal/Enterprise, 802.1X, AES, secure boot, signed firmware, rogue AP detection, WIPS/WIDS.		
6.13.34		The access point must offer full-time Wireless Intrusion Detection/Prevention and spectrum analytics.		
6.13.35		Hardware trust anchor with Secure Boot, image signing, integrity validation.		

6.13.36		The access point must include support for WPA3, AES encryption, and enterprise-grade security features.		
6.13.37	Analytics & Telemetry	Support SNMPv3, NetConf/RESTCONF, and Web UI for configuration & monitoring.		
6.13.38		Real-time client, spectrum, and traffic analytics; export via APIs or standard protocols.		
6.13.39		The access point must provide enhanced network visibility and troubleshooting with AIOps		
6.13.40	Operational feature	The access point must support DHCP Option 43 for automatic wireless controller discovery.		
6.13.41		Should support Wireless Roaming, Client Steering Advanced Cellular Coexistence (ACC)		
6.13.42		The access point must support DFS and dynamic band steering features.		
6.13.43		Must support integration with location analytics and identity services platforms for contextual policy enforcement.		
6.13.44		Must support: MU-MIMO (UL/DL), OFDMA, BSS Coloring, Target Wake Time (TWT), Multi-Link Operation (MLO), preamble puncturing, 320 MHz channel width.		
6.13.45	QoS and Application-Aware Traffic Shaping	The access point must support advanced QoS to optimize voice and video application performance.		
6.13.46		The access point must support application-aware traffic shaping and bandwidth management.		
6.13.47	Licensing and Support for Upgradable Features via Software	All listed features must be available in subscription licensing model. base license or perpetual license accepted if bidder/OEM should provide enhanced wireless features if available in the industry with no additional cost		
6.13.48		The access point must support software upgrades that expand functionalities without hardware replacement.		
6.13.49	Warranty & OEM Support	The proposed equipment must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present a warranty SKU and warranty confirmation letter from the OEM with Next Calendar Day replacement.		

6.14 Wi-Fi Controller

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.14.1	General & Compliance	Make		
6.14.2		Model		
6.14.3		Country of Origin		
6.14.4	General OEM qualification	The proposed Wireless Solution must be from an OEM that has been consistently recognized as a leader or challenger in the Gartner Magic Quadrant (or equivalent reputed third-party evaluations such as IDC MarketScape or Forrester Wave) for Enterprise Wired and Wireless LAN Infrastructure, or Campus Switching, within the past three years (2023/2024/2025)		
6.14.5		The bidder shall clearly declare the Country of Origin of proposed Access points certified by the OEM		
6.14.6		The bidder shall list the authorized manufacturing and/or assembly site(s) for the proposed switch. These sites must be certified under the OEM's global quality assurance or manufacturing program		
6.14.7		The proposed wireless controller must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present a warranty SKU and warranty confirmation letter from the OEM with 4-hour replacement.		
6.14.8		The OEM must guarantee a minimum six (6) year product lifecycle available ahead and clearly mention, the End-of-Sale (EoS) and End-of-Life (EoL) status, OEM EoS/EoL policies with support document		
6.14.9		The OEM must maintain an authorized country office within Sri Lanka. Additionally, a local spare parts depot must be available and operational within Colombo to support expedited escalations and hardware replacements. Proof document is required.		
6.14.10	Vendor Authorization	Bidder is an authorized partner of OEM with ≥10 years WLAN deployment experience in enterprise/campus environments.		

6.14.11		Bidder should have at least 2 Professional level certified engineers in wireless technology for related products, proof must be attached		
6.14.12	Maximum Access Point Support	The WLC must provide a minimum of 250 access points, scalable to 500, with performance licensing.		
6.14.13	Maximum Client Support	The WLC must support at least 5,000 clients concurrently, expanding to 10,000 with advanced licensing.		
6.14.14	Throughput	The WLC must offer a minimum throughput of 5 Gbps, scalable to 10 Gbps with licensing.		
6.14.15	Form Factor	The WLC must be a 1RU half-width chassis compatible with standard 19-inch racks.		
6.14.16	Data Ports	The WLC must have at least 2x 10G multigigabit ports (copper or fiber) and 4x 2.5G/1G copper Ethernet ports.		
6.14.17	Console and USB Ports	The WLC must provide dual console ports (RJ45 and micro-USB), an out-of-band management port and one USB 3.0 port for management and expansion.		
6.14.18	Operating Temperature Range	The WLC must reliably operate within an ambient temperature range of 0°C to 40°C.		
6.14.19	Wireless Controller Software	The WLC must run for enhanced programmability, modularity, and security.		
6.14.20	Deployment Modes	The WLC must support deployment in centralized, localized, geographical redundancy, and software define networking modes.		
6.14.21	Security Features	The WLC must provide secure boot, runtime defenses, and hardware-based security features.		
6.14.22	High Availability	The WLC must support high availability features including Stateful Switchover for minimal downtime.		
6.14.23	VLAN and WLAN Scalability	The WLC must support management of at least 4,096 VLANs and WLANs for large-scale network segmentation.		
6.14.24	Interoperability	The WLC must interoperate with proposed access points and future access points from same vendor for seamless migration and mixed environments.		
6.14.25	Uplink Port Versatility	The WLC must support auto-negotiation of uplink ports including 1G, 2.5G, 5G, and 10G speeds to suit diverse backhaul.		
6.14.26	Regulatory Compliance	The WLC must comply with applicable international safety and EMC regulations.		

6.14.27	Cloud and On-Premises Management	The WLC must provide options for cloud-managed and on-premises controller management.		
6.14.28	Energy Efficiency	The WLC design must emphasize energy efficiency and low power consumption.		
6.14.29	USB Port for Expansion	The WLC must include a USB 3.0 port to support hardware expansion modules or storage devices.		
6.14.30	Console Access	The WLC must provide both RJ-45 and micro-USB console ports for versatile management connectivity.		
6.14.31	Multigigabit Ethernet Support	The WLC must support multigigabit speeds (2.5G/5G/10G) on Ethernet ports for high-performance backhaul.		
6.14.32	Software Updates	The WLC must facilitate seamless and modular software upgrades with minimal network disruption.		
6.14.33	Warranty & OEM Support	The proposed equipment must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present a warranty SKU and warranty confirmation letter from the OEM with Next Calendar Day replacement.		

6.15 Data center IT Operations Platform

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.15.1	General & Compliance	Make		
6.15.2		Model		
6.15.3		Country of Origin		
6.15.4	Unified Cross-Domain Infrastructure Management	The platform must provide a centralized interface to discover, monitor, configure, and manage compute servers, network switches, storage arrays (including backup systems), and virtualization/container platforms regardless of vendor.		
6.15.5	Workflow Orchestration	Must include a no/low-code drag-and-drop workflow engine to create and execute complex automation tasks spanning deployment, configuration, updates, and maintenance, with support for custom scripting and conditional logic.		
6.15.6	Comprehensive RESTful API and SDKs	The solution must provide fully programmable REST APIs with SDKs in common languages (e.g., Python, PowerShell) for deep integration with existing IT operations and DevOps toolsets.		
6.15.7	Real-Time and Historical Telemetry and Analytics	Capability to collect, visualize, and alert on real-time and historical performance, health, fault, and capacity metrics from all infrastructure components to enable proactive management and capacity planning.		
6.15.8	Multi-Site and Global Scale Management	The ability to manage and monitor infrastructure deployed across multiple geographically distributed locations, including data centers, edge sites, and remote offices, from a centralized platform.		
6.15.9	Proactive Issue Detection and Support Integration	Automated hardware, firmware, and configuration issue detection with integration to support case/incident management systems for streamlined troubleshooting and faster resolution.		
6.15.10	Flexible Deployment Models	Support SaaS/cloud-based delivery, on-premises virtual appliance, and hybrid deployment options to meet diverse organizational security, compliance, and data sovereignty requirements.		

6.15.11	Power Consumption and Energy Efficiency Management	Monitor power usage at the server and chassis levels, provide power policies, and enable optimization of energy consumption across compute nodes in the infrastructure.		
6.15.12	Networking Infrastructure Integration	Include management, monitoring, and automation capabilities for network switches and fabric components as part of the unified infrastructure management platform.		
6.15.13	Storage and Backup Infrastructure Visibility and Automation	Inventory, health monitoring, and ability to automate storage provisioning, snapshots, replication, and lifecycle management across storage and backup systems from multiple vendors.		
6.15.14	Multi-Vendor Environment Support	Platform must seamlessly support infrastructure components from multiple vendors across compute, storage, networking, and virtualization layers without limiting functionality.		
6.15.15	Role-Based Access Control with Multi-Factor Authentication	Enforce access restrictions based on user roles with support for multifactor authentication methods to secure the management platform.		
6.15.16	Secure Communication	Ensure all data communications are encrypted both in transit and at rest using industry-standard protocols to maintain confidentiality and compliance.		
6.15.17	Audit Logging and Compliance Reporting	Provide comprehensive audit logs of all actions taken on the infrastructure along with reporting capabilities to support security audits and regulatory compliance efforts.		
6.15.18	Mobile Access to Operational Dashboards and Alerts	The platform should include mobile applications or mobile-optimized interfaces allowing users to monitor infrastructure status and receive alerts on-the-go.		
6.15.19	Export on Telemetry and Operational Data for External Reporting and Analysis	Ability to export detailed telemetry, inventory, and operational data in standard formats (e.g., CSV, JSON) to support external reporting, business intelligence, or integration with other analytics platforms.		
6.15.20	Warranty & OEM Support	The proposed system must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support.		

6.16 Centralized Network Management Platform

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.16.1	General & Compliance	Make		
6.16.2		Model		
6.16.3		Country of Origin		
6.16.4	Core Platform	Solution must be an on-premises appliance-based management platform		
6.16.5		If required, the solution must provide intermediate management switches as per the vendor recommendation		
6.16.6		Must support managing both wired and wireless environments centrally from a single dashboard.		
6.16.7		Must provide native support for proposed LAN switches and wireless access points for full lifecycle management.		
6.16.8		Must provide backward compatibility / interoperability to manage all existing network switches in the ERD to protect prior investments.		
6.16.9		Must be appliance-based with hardware acceleration to support enterprise networks.		
6.16.10	Architecture & Scalability	Must support multi-site management with site hierarchy and location-based topology views.		
6.16.11		Must scale to accommodate any number of devices and users in the ERD without performance degradation.		
6.16.12	Automation	Must support zero-touch provisioning (ZTP) for LAN and WLAN devices.		
6.16.13		Must enable software image management (SWIM) for automated firmware upgrades across network devices.		
6.16.14		Must provide config drift detection and automatic rollback/redeployment of golden configs.		
6.16.15		Must provide policy-based automation where intent can be defined and pushed network-wide.		
6.16.16		Must support day-0, day-1, and day-2 automation workflows for deployment and lifecycle.		

6.16.17	Assurance & Analytics	Must include AI/ML-driven assurance for both wired and wireless performance monitoring.		
6.16.18		Must provide 360° user and device visibility with path trace analysis across the network.		
6.16.19		Must provide real-time client health and application experience scores.		
6.16.20		Must provide root cause analysis with suggested remediation actions for faster troubleshooting.		
6.16.21		Must support predictive analytics to forecast failures and proactively alert administrators.		
6.16.22	Security Integration	Must integrate tightly with the proposed identity and policy management solution to enforce access and segmentation policies.		
6.16.23		The solution must support an identity-based access control mechanism that allows assigning security attributes or group-based tags to user sessions or endpoints, and must enforce policies consistently across the network, regardless of IP addressing or VLAN segmentation		
6.16.24		Must support software-defined access (SDA) for automated segmentation and identity-based policy.		
6.16.25		Must integrate with the proposed firewall for threat-triggered policy automation.		
6.16.26	Wireless Management	Must provide AI-driven RF optimization, interference detection, and auto-tuning of WLAN.		
6.16.27		Must provide heatmaps, spectrum analysis, and client journey tracking for WLAN assurance.		
6.16.28		Must enable policy-driven SSID and WLAN configuration across multiple sites in one action.		
6.16.29	Wired Management	Must provide real-time topology maps of all switches, links, and connected devices.		
6.16.30		Must support per-port visibility and control including VLANs, ACLs, PoE, and access policies.		
6.16.31		Must provide path trace tool to map end-to-end packet flow across switches and routers.		
6.16.32	APIs & Extensibility	Must provide open REST APIs, SDKs, and webhooks for third-party system integration.		
6.16.33		Must support northbound integration with ITSM platforms (ServiceNow, BMC, etc.) for workflows.		

6.16.34		Must support integration with SIEM/SOC systems (Splunk, QRadar, ArcSight) for monitoring.		
6.16.35	Compliance & Reporting	Must provide built-in compliance reports (config compliance, image compliance, policy compliance).		
6.16.36		Must allow audit logs with role-based access for change tracking and accountability.		
6.16.37		Must provide intent-based networking with closed-loop automation (policy → enforcement → assurance → remediation).		
6.16.38	Interoperability and future requirements	Must provide single unified platform covering LAN, WLAN, WAN edge, automation, assurance, and security – not separate tools.		
6.16.39		Must provide AI/ML-driven proactive insights that reduce mean time to resolution (MTTR).		
6.16.40		Must support fabric-based segmentation (SDA) natively, which cannot be matched by legacy management tools.		
6.16.41	Deployment References	Bidder must provide at least 5 successful local deployment references in Sri Lanka for this class of appliance, including customer name, year, and contact details for verification.		
6.16.42	Warranty & OEM Support	The proposed system must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support.		

6.17 Identity and Access Control Solution

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.17.1	General & Compliance	Make		
6.17.2		Model		
6.17.3		Country of Origin		
6.17.4	Core Architecture	The proposed solution must be an industry-recognized, proven, and reliable Network Access Control (NAC) platform and proven interoperability with leading security and networking vendors		
6.17.5		Must be a hardware applaince with dual power supplies and rack mounting accessories		
6.17.6		Must support scalable clustering with redundancy for high availability and disaster recovery.		
6.17.7		Must allow hot patches and upgrades without requiring service downtime.		
6.17.8	Authentication	Must support 802.1X, MAB, and WebAuth authentication for wired, wireless, and VPN access.		
6.17.9		Must support context-aware policies based on user, device, posture, and location.		
6.17.10		Must provide centralized policy management with distributed enforcement across sites.		
6.17.11		Must support automated network control actions such as quarantine, VLAN change, or ACL updates.		
6.17.12	Device Visibility	Must provide agentless endpoint profiling using DHCP, RADIUS, SNMP, NetFlow, and passive methods.		
6.17.13		Must classify IoT, BYOD, and corporate endpoints dynamically without manual intervention.		
6.17.14		Must provide real-time dashboards with device type grouping (printers, mobiles, IP phones, etc.).		
6.17.15		Must integrate with proposed endpoint compliance agent for posture assessment and remediation.		
6.17.16	Integration	Must have tight integration with proposed switching and wireless LAN infrastructure for unified control.		

6.17.17		Must have tight integration with existing switching and wireless LAN infrastructure of Ministry of Finance for unified control.		
6.17.18		Must tightly integrate with proposed firewall for automated threat containment.		
6.17.19		Must integrate with proposed network management/automation platform for software-defined access.		
6.17.20		Must integrate with third-party MDM/UEM solutions (Intune, Workspace ONE, JAMF, etc.).		
6.17.21		Must integrate with SIEM/SOC tools (Splunk, QRadar, ArcSight, ELK) via syslog/REST APIs.		
6.17.22	Guest/BYOD	Must offer customizable guest portal with branding, sponsorship, and SMS/email credential delivery.		
6.17.23		Must allow self-service BYOD onboarding with automatic certificate provisioning.		
6.17.24		Must provide differentiated guest access policies (Internet-only, time-limited, sponsored).		
6.17.25	Security & Compliance	Must perform endpoint posture compliance checks (OS version, antivirus, firewall, patches).		
6.17.26		Must support Zero Trust principles: validate identity, device, and context for every access.		
6.17.27		Must dynamically enforce segmentation using security group tags or equivalent.		
6.17.28		Must enforce role-based access with dynamic VLANs, ACLs, or tags.		
6.17.29		Must comply with FIPS 140-2 or equivalent security certifications.		
6.17.30	Reporting	Must provide prebuilt compliance and audit reports (PCI, HIPAA, GDPR, ISO).		
6.17.31		Must provide real-time visibility of active sessions, including devices, location, and policy.		
6.17.32		Must offer historical trend analysis of authentication attempts, failures, and policy hits.		
6.17.33	Inter Operatability	Must provide native integration with proposed firewall, switching, and wireless for end-to-end visibility.		
6.17.34		Must combine NAC, posture, guest, profiling, and device compliance into a single unified platform.		
6.17.35		Must support automation with proposed management platform for policy-driven operations.		

6.17.36		Must support automated security response (quarantine/block) based on threat intelligence.		
6.17.37		Must be continuously updated to support new IoT/OT device categories and Zero Trust initiatives.		
6.17.38	Licensing & Capacity	The solution must support up to 600 endpoints with appropriate license alignment.		
6.17.39		Must provide 150 IT users licenses to support advanced features including:		
6.17.40		• Posture assessment & compliance checks for managed IT users		
6.17.41		• Dynamic policy enforcement based on user compliance status		
6.17.42		• Integration with endpoint security agents (antivirus, EDR)		
6.17.43		• Role-based access control for IT users with full visibility of authentication & authorization events		
6.17.44		Must provide 450 IT device licenses to support:		
6.17.45		• Device visibility and profiling for wired, wireless, and VPN endpoints		
6.17.46		• Basic authentication and network access control policies		
6.17.47		• Guest access and self-registration portals for devices		
6.17.48		• Integration with switches, wireless controllers, and firewalls for enforcement		
6.17.49	Feature Alignment	Must support scalable license growth beyond 600 endpoints and must support 25,000 concurrent active sessions without requiring appliance replacement.		
6.17.50	Deployment References	Bidder must provide at least 5 successful local deployment references in Sri Lanka, including customer name, deployment year, and contact person for verification.		
6.17.51	Warranty & OEM Support	The proposed system must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support.		

6.18 Management switch for DC

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.18.1	General & Compliance	Make		
6.18.2		Model		
6.18.3		Country of Origin		
6.18.4	Manufacture	The proposed switch must be from an OEM that has been consistently recognized in the Gartner Magic Quadrant (or equivalent reputed third-party evaluations such as IDC MarketScape or Forrester Wave) for Enterprise Wired and Wireless LAN Infrastructure, or Campus Switching, within the past three years		
6.18.5	Country of Manufacture / Assembled	The bidder shall list the authorized manufacturing and/or assembly site(s) for the proposed switch. These sites must be certified under the OEM's global quality assurance or manufacturing program		
6.18.6	Form Factor	Rack mountable; should provide rack (19-inch) mounting kits		
6.18.7	Port Requirement	The switch must support 24 × 10/100/1000Base-T ports (RJ-45) and 4 x 10/100/1000 SFP ports		
6.18.8		Each switch should be populated with 2x 1G Multimode transceiver module		
6.18.9	Memory, Processor & Hardware Architecture	The switch shall be equipped with an embedded multi-core CPU running on modern ASIC architecture, capable of supporting advanced management, automation, telemetry, and security functions without impacting packet forwarding performance.		
6.18.10		The switch shall be equipped with minimum of 4 GB DRAM, and 4 GB flash storage.		
6.18.11		The switch must deliver a backplane switching capacity of 56 Gbps and a forwarding performance of 40 Mbps tested with 64-byte packets.		
6.18.12		The switch must support a stacking bandwidth of at least 80 Gbps.		
6.18.13				
6.18.14		The switch must support an IPv4 routing table size of at least 4,000 routes, and a minimum of 1,000 Access Control List (ACL) entries, to ensure enterprise-grade performance and scalability.		

6.18.15	Layer 2 and Layer 3 Network standard	Support standard Layer 2 and Layer 3 protocols, including but not limited to OSPF, VRRP, LLDP or equivalent protocol		
6.18.16		DHCP Auto Config, LACP, DTP or equivalent, UDLD or equivalent, IGMP, Voice VLAN, VTP or Open Standard, Layer 2 trace route, NTP, Storm Control		
6.18.17		The switch must support MACsec encryption per IEEE 802.1AE with AES-128		
6.18.18		The switch must support to integrate/enable centralized policy enforcement and secure user segmentation		
6.18.19	Unicast MAC Addresses	Minimum 16,000		
6.18.20	IPv6 Unicast Direct Routes	Minimum 1000		
6.18.21	Multicast Routes and IGMP Groups	Minimum 1000		
6.18.22	Maximum Active VLANs	Minimum 1000		
6.18.23	VLAN IDs Available	Minimum 4094		
6.18.24	STP Instances	Up to 64; must support IEEE 802.1D, 802.1s (MSTP), and 802.1w (RSTP)		
6.18.25	SPNN Sessions	Minimum 4		
6.18.26	Jumbo Ethernet Frame	Minimum 9100 bytes		
6.18.27	Other Layer 2 / Layer 3 Protocols Features	The switch must support MACsec encryption per IEEE 802.1AE with AES-128		
6.18.28	Network Security	802.1X, Multi-domain Auth, RADIUS, TACACS+, ACLs, STRG or equivalent, BPDU Guard, IGMP Filtering		
6.18.29		support port security with configurable MAC-address filtering.		
6.18.30	Redundancy and Resiliency	RSTP, MSTP, PVRST+ or equivalent per-VLAN spanning tree		
6.18.31		The switch must include redundant, field-replaceable power supply units		
6.18.32		The switch must achieve a cold-boot time of no more than three minutes.		

6.18.33		The switch must support flexible, software-based feature upgrades and enhancements that allow the network to evolve and incorporate advanced capabilities without the need for hardware replacement		
6.18.34	Enhanced QoS	802.1p CoS, DSCP, CIR, SRR or equivalent, WTD or equivalent, Auto-QoS, 8 egress queues per port		
6.18.35	Switch Management	Web UI, CLI, SNMP, USB/RJ-45 console		
6.18.36	Environmental Compliance	ROHS, CE, FCC, EMI/EMC certified		
6.18.37	Environmental & Compliance	switch must operate reliably in ambient temperatures from –5 °C to +45 °C.		
6.18.38		The switch must support smart power management features to optimize energy consumption during low usage periods.		
6.18.39		The switch must comply with CE, UL, and RoHS certifications.		
6.18.40	Warranty & OEM Support	The proposed switch must include a minimum three (3) year advanced hardware replacement warranty, with 24x7 access to technical support. (Limited Lifetime Warranty is not Considered). Bidders must present a warranty SKU and warranty confirmation letter from the OEM with Next Calendar Day replacement.		
6.18.41		The OEM shall not declare the supplied product as end of support (EoS) or end of Life (EoL) during five (05) years period,		
6.18.42		Documentation providing back-to-back warranty has been obtained from the respective OEM should be provided.		
6.18.43		24X7 access to OEM for level 2 and 3 technical supports should be available.		
6.18.44		The OEM must maintain an authorized country office within Sri Lanka. Additionally, a local spare parts depot must be available and operational within Colombo to support expedited escalations and hardware replacements. Proof document is required.		
6.18.45	Management & Monitoring	Next business day replacement of faulty devices should be provided; The OEM of switches should maintain a spare parts depot in Colombo to support this. Relevant documentation confirming the next business day delivery and availability of spare parts depot obtained from the OEM should be submitted with bid proposal.		
6.18.46		switch must provide both a command-line interface (CLI) and an integrated web-based GUI.		

6.18.47		The switch must support SNMP v1/v2c/v3 and syslog for event logging.		
6.18.48		The switch must support integrated RFID functionality, one similar technology to enable real-time asset tracking / location identification within the network.		
6.18.49		The switch must support integration with Security Information and Event Management (SIEM) systems through standard protocols including Syslog and SNMP traps for real-time event monitoring and alerting.		

6.19 Network Rack and UPS Requirement

Primary Site

The proposed solution should be configured with the required devices, patch panels, and power wiring in a 42U floor-standing rack (existing ITMIS rack) to host the network and supporting infrastructure devices in an organized and secure manner at the IRD Data Center, Jawatte, Colombo 05. A 3U rack-mounted 3 kVA UPS should also be supplied for power backup

DR Site

A separate 42U floor-standing rack should be configured with the required devices, patch panels, and power wiring, similar to the existing DR ITMIS rack, for the Kurunegala IRD Data Center. A 3U rack-mounted 3 kVA UPS should also be supplied for power backup.

Planned Rack Layout at head office:

The proposed HQ solution should be configured in a 42U floor-standing rack (Existing ERD Rack) to host network and supporting infrastructure devices in an organised manner, and configured to meet the requirements below at the MOF NOC, 3U rack-mounted 3kVA UPS for power backup.

- ISP patch panel and ISP router for internet connectivity.
- LAN firewall for network security.
- Aggregation switch for core LAN connectivity.
- Patch panel for terminating uplinks from floor switches.
- Patch panel for distributing data points on the same floor.
- Network access control device.
- Network management device.
- Dedicated cable management and ventilation units.
- Reserved U-space for future expansion.

This arrangement ensures:

- Logical connectivity (ISP → Firewall → Aggregation Switch → Access Network).
- Structural cabling discipline with patch panels placed close to relevant devices.

Bidders are requested to quote for a complete rack solution meeting the technical specifications, along with necessary accessories (cable managers, cooling/ventilation, mounting hardware, front/rear doors, and security locking).

1	**2**	**3**	**4**	**5**
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
UPS Specifications				
6.19.1	General & Compliance	Make		
6.19.2		Model		
6.19.3		Country of Origin		
6.19.4	Type	Online		
6.19.5	Output power	3kVA or higher as required		
6.19.6	Input / Output Voltage	230V		
6.19.7	Nominal frequency	50-60Hz		
6.19.8	Battery backup time (Full Load)	Minimum 10 minutes		
6.19.9	Protection	Power failures, Battery discharge, Poor battery and abnormal UPS behaviors must be alarmed through Audible Alarms and Lighting (LEDs)		
6.19.10		Power generator compatible		
6.19.11	Warranty and support	3 year comprehensive warranty		

6.20 General Email Management & Offline desktop, web, and mobile versions of Word processing, spread sheet and presentation.

6.20.A Technical Specifications for Supply, Installation, Commissioning, Maintenance and Data Migration of Email Solution with Office Productivity Suite for Department of External Resources.

6.20.1.1 General Scope of work

The general scope of work includes the supply of Productivity Suites and an Email Solution with cloud-based identity integration, as well as Installation, Commissioning & Maintenance of Email Solution with Office Productivity Suite for Department of External Resources Colombo 01.

The Department of External Resources (ERD) is currently operating an on-premises Microsoft Exchange Server 2016 for e-mail services and Microsoft Office 2013/2016 for productivity applications, along with a separate, internally managed file sharing solution. The infrastructure supports approximately 120 users. However, these systems are approaching end-of-life status, rendering them increasingly obsolete, insecure, and unsustainable for the ERD's operational and strategic requirements. In line with the ERD's digital transformation agenda and to ensure operational continuity, security, scalability, and efficiency, it is imperative to migrate from the existing infrastructure to a modern, cloud-based solution. The proposed solution must align with international standards and best practices in enterprise communication, productivity, and collaboration technologies.

The solution must support differentiated service tiers:

- Privileged Users must be provided with higher storage capacity, e-mail and access to advanced applications, including but not limited to meeting tools and workflow automation.
- Standard Users should have access to essential tools such as e-mail and basic office productivity applications.

The vendor must ensure a complete and error-free migration of all current e-mails, files and user data to the new solution. The integrity, structure, and accessibility of the data must be preserved throughout the migration process, with zero data loss or impact to ongoing ERD operations.

The supplier must disclose the cloud-based network locations to ensure data sovereignty and protection for the purchaser. The proposed solution must offer comprehensive protection against modern threats, including data security, privacy safeguards, and resilience in the event of natural disasters. Security protocols should include features such as double encryption and data replication.

Response time for Level 2 (L2), Level 3 (L3) and Level 4 (L4) support from the principal company must be within 1–2 hours. The proposed product should also be compatible with future AI-driven requirements.

A shorter user learning curve will be considered as an added advantage in the evaluation process

6.20. Directory Service, Email, Collaboration and End Point Management

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.20.1	General & Compliance	Make		
6.20.2		Model		
6.20.3		Country of Origin		
6.20.4	Directory & Identity Management	On-premises and cloud directory integration with secure synchronization between sites		
6.20.5		Redundant directory and DNS servers at primary and disaster recovery sites		
6.20.6		Staging/failover sync server in DR site		
6.20.7		Cloud-hosted directory server for resilience		
6.20.8		Secure site-to-site VPN between PR, DR, and cloud for replication		
6.20.9	Email Services	Cloud-hosted business-class email with 50 GB mailbox per user for 120 users		
6.20.10		Ability to send/receive attachments up to at least 150 MB		
6.20.11		Shared mailboxes provided free of charge with no license requirement		
6.20.12		Administrator accounts provided free of charge and excluded from licensing		

6.20.13		Distribution groups, resource mailboxes (rooms/equipment) with calendar booking		
6.20.14		Email access via web, desktop, and mobile clients with offline capability		
6.20.15		Server-side rules, focused inbox, and clutter reduction		
6.20.16		Integrated email archive with configurable retention policies		
6.20.17		eDiscovery for content search		
6.20.18		Integration with collaboration platform for scheduling, chat, and file sharing		
6.20.19		Custom email domain support with DKIM, SPF, and DMARC for sender authentication		
6.20.20	Email & Collaboration Security (Advanced Threat Protection)	Anti-phishing, anti-spam, and anti-malware scanning across email and collaboration services		
6.20.21		Safe Links (real-time URL scanning) through email, chat, and cloud storage		
6.20.22		Safe Attachments (sandbox detonation for attachments before delivery)		
6.20.23		Automated investigation and response workflows for detected threats		
6.20.24		Threat Explorer and trackers for analyzing attack patterns		
6.20.25		Campaign analysis to detect coordinated phishing/malware campaigns		
6.20.26		Attack simulation training for user security awareness		
6.20.27		Zero-Hour Auto Purge to remove malicious content post-delivery		
6.20.28		Advanced hunting and incident correlation across services		
6.20.29	Cloud Collaboration & Storage	Team-based collaboration spaces with threaded chat, document collaboration, and shared calendars		
6.20.30		Real-time co-authoring of documents, spreadsheets, and presentations		
6.20.31		Automatic version history and rollback for shared files		
6.20.32		Secure internal and external sharing with granular permission controls		
6.20.33		Integrated video conferencing with screen sharing, recording, and meeting scheduling		
6.20.34		Presence indicators, mentions, and threaded replies		
6.20.35		Cross-platform access via web, desktop, and mobile (including offline capabilities)		
6.20.36		Integrated task and project management tools		

6.20.37		Minimum 1 TB personal cloud storage per user for 120 users		
6.20.38		2.5 TB shared cloud storage for organizational use		
6.20.39		Data encryption in transit and at rest		
6.20.40	Endpoint Management	Unified device management for Windows, macOS, iOS, and Android from a single cloud console		
6.20.41		Mobile Application Management without requiring full device enrollment		
6.20.42		Device compliance policies (passwords, encryption, OS versions)		
6.20.43		Endpoint analytics with device performance and health monitoring		
6.20.44		Application deployment, patching, and update control		
6.20.45		Remote actions (wipe, lock, restart, rename, passcode reset)		
6.20.46		Management of shared, kiosk, and frontline devices		
6.20.47		Enrollment automation based on identity policies		
6.20.48	Migration Requirements	Migration of all mailboxes from on-premises Exchange 2016 to new cloud email platform with zero data loss		
6.20.49		Migration of file server contents to cloud storage, preserving structure and permissions		
6.20.50		Cutover or staged migration approach to minimize downtime		
6.20.51		Validation and user acceptance testing post-migration		
6.20.52	Bidder qualification	Bidder should have at least 3 certified employees for the proposed solution implementation		
6.20.53		Bidder should demonstrate 5 years of experience in deploying same solution with references		

6.21 End point protection for end points

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**
6.21.1	General & Compliance	Make		
6.21.2		Model		
6.21.3		Country of Origin		
6.21.4		Vendor/solution must be a reputed and present in cybersecurity industry for at least 10 years.		
6.21.5		The proposed solution must be a Commercial off the Shelf Available Software (COTS).		
6.21.6		The proposed solution should be in Leader or challenger in 2022/2023/2024 Gartner Magic Quadrant for Endpoint Protection Platforms.		
6.21.7		The proposed solution should be in Leader or challenger in 2022/2023/2024 Forrester Wave report for Endpoint Detection and Response Providers.		
6.21.8		The proposed solution should be in 2022/2023/2024 Forrester Wave report for External Threat Intelligence Service Providers.		
6.21.9		Proposed OEM should adhere compliance to SOC II. PCI DSS. HIPAA/HITECH, SOX and/or other regulatory frameworks.		
6.21.10		Solution should be able to deploy in workstation and server assets. Should be same agent deployment.		
6.21.11		Solution should be able to deploy in multiple operating systems such as Windows, Mac OS,Linux.		
6.21.12		Solution should offer NGAV using one single agent with single service and single console and should not require multiple agent deployment.		
6.21.13		Solution should be able to monitor and manage the endpoint licenses through one single solution and one single console.		

6.21.14	General & Compliance	Solution deployment and updates (agent, policies. settings. etc ..) should be available globally during and outside maintenance windows, and without introducing business downtime to users or workloads. Should not require reboot during installation and upgrade.		
6.21.15		Solution should be a lightweight agent that includes machine learning, exploit blocking, custom whitelisting and blacklisting, behavioral. attack attribution, and adware blocking.		
6.21.16		Solution should provide this level of protection whether the endpoint is online or offline and must not interfere with business-critical applications and have a low level of resource consumption on the endpoint.		
6.21.17		Solution agent should maintain low CPU utilization. (less than 1%)		
6.21.18		Solution agent should maintain low memory utilization. (less than 50MB)		
6.21.19		Solution agent's bandwidth utilization should be less than 10 MB per endpoint within 24 hours.		
6.21.20		Solution agent installation footprint should below 200 MB.		
6.21.21		Solution should be tampered resistant, protecting against attempts to modify the endpoint sensor.		
6.21.22		Solution should have low frequency system management updates.		
6.21.23		Solution should have conviction engine based on machine learning and the ability to detect and block malicious files without relying on daily/weekly anti-virus or anti-malware definition updates.		
6.21.24		Solution should have the ability to detect and block bad behaviors exhibited from known- good files as outlined in the MITRE ATT&CK framework.		
6.21.25		Solution should be able to track at least 200 adversary groups. The details of adversary and TTP should be available in the management portal along with their other well- known names in the community.		

6.21.26		Solution should have a dashboard with information of global hackers with details such as names, exploiting vulnerabilities, targeting countries, targeting industries etc.		
6.21.27	General & Compliance	Solution should provide detailed TTPs on adversary actions in an easy-to-read notification. Reported details must include hostname, processes, user account, and analysis statement.		
6.21.28		Solution should block ransomware using ML and Behavioral techniques before it could create any damage to the system. i.e. backup deletion or file encryption.		
6.21.29		Solution should offer memory protection (e.g.ASLR., structured exception, handling overwrite protection, null page protection, beap spray pre allocation, etc.)		
6.21.30		Solution should show alter/detections centrally in the UI		
6.21.31		Solution should show alert's associated activity in the UI		
6.21.32		Should be able to view interactive process trees for alerts detections/root cause analysis		
6.21.33		Should be able to view process tree events coming into UI in a near real time for the detected events/root cause analysis		
6.21.34		Should be able to view associated Forensics artefacts such as File I/O, Network connections DNS Requests within the alert summary page.		
6.21.35		Solution should automatically updates known behaviors to adversary groups.		
6.21.36		Should be able to view DNS Lookups that are captured for cache process not per client.		
6.21.37		Should be a tested solution by MITRE against its ATT@CK Framework.		
6.21.38		Solution should be associating detected events with a MITRE ATT@CK Framework Tactic & Technique		
6.21.39		Should be able to manage workflows including sorting, filtering, tracking status, assigning ownership, and creating commentary or annotations of alerts.		

6.21.40		Solution should detect advanced tradecraft and activity across the kill-chain including Exploitation. Execution, Privilege Escalation, Social Engineering, Credential theft, Persistence. Exfiltration, actions on objectives.		
6.21.41		Solution should detect when using file-less and malware-less tools such as PowerShell.		
6.21.42	General & Compliance	Solution should provide OOTB (Out-of-the box) Reports and Dashboards for Different Levels ex: Leaders, Analyst, Security Manager Dashboards.		
6.21.43		Solution should be able to automate remediation task on detected threats at a granular level		
6.21.44		Solution should be able to define roles and permissions according to user responsibilities		
6.21.45		Solution should be able to mitigate risks associated with USB devices		
6.21.46		Solution should be able to control device usage with precision		
6.21.47		Solution should be able to implement and manage policies without hassle		
6.21.48		Solution should be able to automatically get device information for quick and easy policy creation and management workflows		
6.21.49		Solution should be able to define granular policies for drives.		
6.21.50		Solution should be able to exclude devices temporary based (with given time period)		
6.21.51		Should have the capability to upgrade with Sandbox feature for further investigating of malware in future		
6.21.52		Should have the capability to monitor the internal attack landscape as an external party.(External Attack Surface Management) in future.		

6.22 Endpoint Detection and Response (EDR) Solution for Servers

1	**2**	**3**	**4**	**5**
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	

		Details	Compliance Yes(Y) / No(N)	Remarks
6.22.1	General & Compliance	Make		
6.22.2		Model		
6.22.3		Country of Origin		
6.22.4		The proposed solution should be a Leader in 2022/2023/2024 Gartner Magic Quadrant for Endpoint Protection Platforms.		
6.22.5	General & Compliance	The proposed solution should be a Leader in 2022/2023/2024 Forrester Wave report for Endpoint Detection and Response Providers.		
6.22.6		Solution should offer NGAV using one single agent with single service and single console and should not require multiple agent deployment		
6.22.7		Solution deployment and updates (agent, policies, settings, etc ..) should be available globally during and outside maintenance windows, and without introducing business downtime to users or workloads. Should not require reboot during installation and upgrade.		
6.22.8		Solution should be a lightweight agent that includes machine learning, exploit blocking, custom whitelisting and blacklisting, behavioral. attack attribution, and adware blocking.		
6.22.9		Solution should provide this level of protection whether the endpoint is online or offline and must not interfere with business-critical applications and have a low level of resource consumption on the endpoint.		
6.22.10		Solution agent should maintain low CPU utilization. (less than 1%)		
6.22.11		Solution agent should maintain low memory utilization. (less than 50MB)		
6.22.12		Solution agent's bandwidth utilization should be less than 10 MB per endpoint within 24 hrs.		
6.22.13		Solution agent installation foot print should below 200 MB.		
6.22.14		Solution should be tampered resistant, protecting against attempts to modify the endpoint sensor.		

6.22.15		Solution should have low frequency system management updates.		
6.22.16		Solution should have conviction engine based on machine learning and the ability to detect and block malicious files without relying on daily/weekly anti-virus or anti-malware definition updates.		
6.22.17		Solution should have the ability to detect and block bad behaviors exhibited from known- good files as outlined in the MITRE ATT&CK framework.		
6.22.18	General & Compliance	Solution should show Overall Risk Score of endpoint network.		
6.22.19		View interactive process trees for alerts detections/Root Cause Analysis		
6.22.20		Solution should Consolidate Multiple threats into single Incidents		
6.22.21		Generate intelligence driven detection in the UI. Enrich a detected event with the Vendors own threat intelligence and not any 3rd Party intelligence.		
6.22.22		Solution automatically updates known behaviors to global hacker groups		
6.22.23		Solution should have a hacker profiling of 200+ threat actors with information such as Which Nation State, which industries they attack, which countries they attack etc.		
6.22.24		Solution should offer a comprehensive threat actor profile database, tracking over 200+ publicly named nation state, e-crime, and hacktivist threat actors while mapping tactics, techniques, and procedures to the cyber kill chain while enumerating the threat actors origin, last known activity. target nations. and target industries		
6.22.25		The detections in the NGAV/EDR need to be mapped against with hacker profile in the dashboard.		
6.22.26		Detect when using file-less and malware-less tools such as PowerShell.		
6.22.27		Solution should allow scheduling of Reports and automated workflows to send the reports/notifications to the intended recipients over email.		
6.22.28		Solution should allow creation of workflows for Notifications, response and IOC		

		enrichment using no-code logic to support complex sequencing and branching.		
6.22.29		The Workflow capability should support multiple channels for sending out notifications such as email, slack, webhook, Microsoft Teams and PagerDuty		
6.22.30		Solution should provide OOTB (Out-of-the box) Reports and Dashboards for Different Levels ex: Leaders, Analyst, Security Manager Dashboards.		
6.22.31	General & Compliance	Solution should allow easy and scalable querying options to query the telemetry data for threat hunting, investigation and reporting purposes		
6.22.32		Solution should allow saving and scheduling the custom queries written by analysts and hunters		
6.22.33		Solution should provide reporting on incidents that involve activity across multiple hosts. These incidents could feature the Lateral Movement tactic itself. or show suspicious lateral movement accomplished via remote process execution techniques like Windows Management Instrumentation.		

6.22.34		Proposed solution should capture telemetric data to provide threat hunting capabilities for forensic artefacts in real-time and for historical search in less than a minute, even for endpoints offline or out of corporate network without crawling endpoints. * Local IP and Public IP of endpoint had communicated. * User logon activities (login and logoff time with user, name * All Process & Service execution including Admin tools and CMD commands with process id, user details All PowerShell Activities on endpoint. * Suspicious File Activities (Zip, RAR & Scripts written) * Files Written to Removeable Media. *Manual, Registry, Addition *Scheduled Tasks Registered and Firewall, Rules set on endpoint. *DNS request & Network connection with Port number made from endpoint with detailed command line & file name. *Details of Network Listening ports on endpoint with file name and command line. *Should be able to see network connections by Country or External IPs connected to. *List of Usernames or Systems where remote logins have taken place. This can quickly identify suspicious behavior by user account or systems.		
6.22.35		Should be able to network contains a host directly from a detection window		
6.22.36		Should be able to how all endpoints that are currently in a network contained state		
6.22.37	General & Compliance	Solution should be able to automate contain and lift containment process through the management console itself		
6.22.38		Should be able to manage whitelisted IP addresses for network containment		
6.22.39		Should be able to blacklist file hashes and monitor IP Addresses and Domains through the UI		
6.22.40		The proposed solution should be able to replay the attack/incident in step by step with the relevant timelines.		
6.22.41		Should be able to validate that containment and blacklists are preserved across reboots		

6.22.42		Should be able to observe containment action audit logs		
6.22.43		Should be able confirm user role has Real Time Response attribute.		
6.22.44		Should be able to establish Real Time Response Connection to Endpoint.		
6.22.45		Should be able to use the ipconfig and netstat command to get network config data about that system.		
6.22.46		Should be able to use the PS command to list processes and the kill command to terminate a process by its PID.		
6.22.47		Information collectors such as list running processes, query windows registry, extract windows event logs, extract process memory etc. backed with remediation actions such as delete file or delete or modify windows process or kill a process.		
6.22.48		Should be able to download a file directly with the get command or by mounting a share drive and copying it there.		
6.22.49		Solution should provide real-time security posture score for endpoints to view the overall health of endpoints to improve security posture.		
6.22.50		Solution should be able to share the Security posture score with ecosystem partners such as Proxy, CASB, NAC, Cloud and Email security for real-time conditional access enforcement - where the security health of the endpoint can be used as a factor to grant access.		

6.23 User Training

1	2	3	4	5
Line-Item No	**Description of goods/Category**	**Purchaser's Requirements/ Technical Specifications and Standards**	**Bidder's Offer**	
		Details	**Compliance Yes(Y) / No(N)**	**Remarks**

6.23.1		Bidder shall provide comprehensive local & foreign training on 'Maintenance & administration' of the system covering all hardware, software, and any other area relevant to the installation to the IT Team of the Employer. Training shall be carried out by a manufacturing-certified training institute. This training shall be at a level where the trained IT team will be able to maintain the system after the warranty period even without a support agreement. The minimum training period shall not be less than 05 Days & Training content shall be submitted with the proposal. Compliance with this requirement will be considered in the issuance of the training completion certificate.		
6.23.2		The guide should provide on-site technical training covering all software, and any other area relevant to the installation, and the customized training for this installation. Onsite user training should be provided to ERD staff.		
6.23.3		For all the above trainings, Schedules shall be submitted at least four weeks prior to the commencement of the training for approval of the Employer.		
6.23.4		Minimum no. of trainees for the OEM training at their center shall be 03 (Three). Conditions as applicable to government circular No M.F.01/2015/01.		
6.23.5		Bidder should provide a complete unpriced BoQ of the training including quantities of all price items used as an annexure to the technical proposal		
6.23.6		Once all the above are completed, the Employer will issue a Training Completion Certificate.		

6.24 Compliance & Standards

Hardware, Software, and Solutions manufacturers should comply with following standards and must provide documented proof for each item below. Failure to comply with requirement will result in disqualification.

1	2	3	4	5

Line-Item No	Description of goods/Category	Purchaser’s Requirements/ Technical Specifications and Standards	Bidder’s Offer	
		Details	Compliance Yes(Y) / No(N)	Remarks
6.24.1		Ensure IPv6 readiness (mandatory for future government ICT compliance).		
6.24.2		IEEE 802.1X port-based authentication must enable authentication, authorization, and accounting (AAA) and specify the authentication method list. A method list describes the sequence and authentication method to be queried to authenticate a user.		
6.24.3		The Proposed Solution must align with the IT Policy of the ERD. The following features should be included: Disallow Palindromes, disallow password reuse from last 10 passwords, set password expiry in number of days, must have option to warn user 7 days before password expiry, block access for 20 Mins after 3 failed login attempts.		
6.24.4		Energy Star - EPA program for energy-efficient equipment Power and Efficiency Standards		
6.24.5		Manufacturer’s legally binding undertaking guaranteeing 10 years of updates, parts, and security patches		
6.24.6		Compliance with ISO/IEC 27001 security practices & Sri Lanka Personal Data Protection Act.		
6.24.7		Compliance with ISO/IEC 27701 (privacy management)		
6.24.8		Valid FCC, CE/EN, IEC, EMC/RED certification reports from accepted labs		
6.24.9		IEC 62368-1 – International safety standard for IT equipment Environmental and Reliability Standards		
6.24.10		Valid FIPS 140-3 / ISO/IEC 19790 cryptographic module validation certificate		
6.24.11		Common Criteria EAL2+ or higher certification for proposed products		
6.24.12		Alignment with NIST Cybersecurity Framework and Zero Trust (SP 800-207)		
6.24.13		Products must not originate from or involve entities subject to trade restrictions, export controls, or national security measures imposed by applicable authorities		

6.24.14		Independent third-party supply chain audit report confirming no restricted sources and Evidence of transparent sourcing and component provenance.		
6.24.15		Manufacturer must not be subject to trade restrictions or sanctions under EU, UK, U.S., Japan, Australia		
6.24.16		IEEE 802.3 - Ethernet standards		
6.24.17		Support for NETCONF, RESTCONF, YANG models. Support for EVPN-VXLAN or equivalent SDN		
6.24.18		The solution must allow the administrator to choose to read-only or read write mode.		
6.24.19		Solutions must support multiple role-based administration, 1). Routing Administrator must have read write access to all routing protocols, interface configuration, DNS configurations.		

6.25 Inspection, Testing and Acceptance

No.	Requirement	Duration
Advance Payment – 10 % of the Contract Price		
6.25.1	Submission of Advance payment guarantee	Within 14 days from Date of Signing the Contract
Delivery and Installation of Devices and Software 70%		
6.25.2	i. Signed-off solution blue print. ii. Signed Good Receive Notes iii. Completion of initial setup of equipment and software	7 weeks from the date of signing the contract.
User Acceptance Testing (UAT) 20% of the Contract Value		
6.25.3	i. Submission of test cases and test results. ii. ERD sign-off of the solution implemented	8 weeks from the Date of Signing Contract.

Section VIII. Contract Data

The following Contract Data shall supplement and / or amend the Conditions of Contract (CC). Whenever there is a conflict, the provisions herein shall prevail over those in the CC.

CC 1.1(h)	The Purchaser is: **Department of External Resources in Sri Lanka**
CC 1.1 (l)	The Project Site/Destination is **Department of External Resources, The Secretariat, 3rd Floor, Colombo 01.**
CC 8.1	For **notices**, the Purchaser's address shall be: Attention: **Director General** Address: **Department of External Resources** **Room No: 303** **Third Floor,** **The Secretariat,** **Colombo 01.** Telephone: **0112 484 653** Facsimile number: **011 2395551** Electronic mail address: wasantha@erd.gov.lk The Supplier's address is: ....
CC 12.1	Details of Shipping and other Documents to be furnished by the Suppliers are. I. Manufacturer's/ Supplier's warranty certificate with 02 copies II. Supplier's factory inspection report with 02 copies. III. Certificate of origin with 02 copies
CC 15.1	The method and conditions of payment to be made to the Supplier under this Contract shall be as follows: Payment shall be made in Sri Lanka Rupees within thirty (30) days of presentation of claim supported by a certificate from the Purchaser declaring that the Goods have been delivered and that all other contracted Services have been performed. I. **Advance Payment:** Ten (10) percent of the Contract Price shall be paid within thirty (30) day s of signing of the Contract, and up on submission of an advance payment guarantee for equivalent amount valid until the Goods are delivered and, in the form, provided in the bidding document II. Delivery and Installation of Devices and Software: Seventy (70) percent of the Contract Price shall be paid after the supply and installation of items specified in the Price Schedule. III. **User Acceptance Testing (UAT):** The remaining Twenty (20) percent of the Contract Price shall be paid to the Supplier within thirty (30) days after the date of the

	acceptance certificate for the respective delivery issued by the Purchaser. Note: Payments will be made after the fulfillment of the criteria stipulated in 5.3.7. Inspection, Testing and Acceptance of Section V. Schedule of Requirements
CC 17.1	A Performance Security shall be required. After delivery and acceptance of the Goods, the performance security shall be reduced to five (5) percent of the Contract Price and valid up to 30 days beyond the Supplier's warranty obligations.
CC 25.1	The inspections and tests shall be as follows: (i) The supplier shall get all the equipment's inspected and submit a guarantee/warranty certificate that the equipment conforms to lay down specifications. (ii) The acceptance test will be conducted by the Purchaser, their consultant or any other person nominated by the Purchaser at its option at the point of delivery as indicated in the Schedule of Requirements. (iii)If the Equipment fails to meet the laid down specifications, the supplier shall take immediate steps to remedy the deficiency or replace all defective equipment to the satisfaction of the Purchaser (iv) Criteria stipulated in the 5.3.7. Inspection, Testing and Acceptance of Section V. Schedule of Requirements
CC 25.2	The Inspections and tests shall be conducted at: Department of External Resources, Colombo 01. Sri Lanka
CC 26.1	The liquidated damage shall be 0.5% per week
CC 26.1	The maximum number of liquidated damages shall be 10%

CC 27	**27.3** 3 years Comprehensive OEM Warranty (Limited lifetime warranty is not considered) Proposed products should be supported by the respective OEM for a minimum of 4 years from date of delivery to ERD. Documentation confirming the OEM Warranty should be provided. 24x7 access to OEM for Level 2 and Level 3 technical support should be available. Next Business Day replacement of faulty servers, firewalls or parts during the warranty period. **Note:** All charges regarding the supply of spare parts, labour, travel, per diem and accommodation to supplier's staff etc; shall be borne by the supplier during the period of warranty. ERD will not pay any additional expenditure for services rendered during the above period. **Penalty** Penalty will be 0.1% of the Contract Sum for each SLA violation incident. Accordingly, for each SLA violation, a 0.1% of the contract sum will be deducted and the total accumulated amount will be claimed from the performance bond.