Centre for Development of Advanced Computing

A Scientific Society of Ministry of Electronics & IT,
Government of India

Plot No: 6&7, Hardware Park, Sy. No.1/1, Srisailam Highway

Hyderabad – 501510

www.cdac.in /

email: **purchase-hyd@cdac.in**

C-DAC invites bids from System Integrators (S.I)/OEMs through GeM for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution

Prospective Bidders may download the Tender Document from www.cdac.in / https://gem.gov.in. Bidders are advised to go through instructions and submit bids online on the GeM portal as per the schedule given in the Tender Document.

Tender Schedule

Name of the Institute	**Centre for Development of Advanced Computing, Hyderabad - 501510.**
Place of Supply, Installation & Commissioning, Support etc.	**Plot No: 6&7, Hardware Park, Srisailam Highway , Hyderabad – 501510** **&** **Anusandhan Bhawan, C-56/1, Sector-62, Noida – 201307, Uttar Pradesh (India)**
Date of Release of Tender	**19.01.2024**
Last Date (with time) for sending queries – if any on email	**23.01.2024 before 17.00 hrs**
Date and Place of Pre-Bid Meeting	**24.01.2024 @ 11.00 AM through online mode** *** Meeting link will be posted as amendment**
Last date of submission of bids	**01.02.2024 before 17:00 hrs** *** *Due Date for submission of Bids will not be extended under any circumstances***
Date of opening of Bids	**02.02.2024 at 11.00 hrs**
Place of opening of technical bids	**C-DAC, Hyderabad - 501510.**
Name of the Contact Person for any clarification	**The Head (Purchase)** **Centre for Development of Advanced Computing** **Plot No: 6&7, Hardware Park, Sy. No.1/1,** **Srisailam Highway, Hyderabad – 501510** **Email: purchase-hyd@cdac.in**
C-DAC Bank Details	**A/C Name: Centre for Development of Advanced Computing, Hyderabad** **Name of Bank: Bank of India** **Branch: Shamshabad, Hyderabad** **A/C No:566310110004393** **IFSC: BKID0005663**
Websites for downloading Tender Document, Corrigendum, Addendum etc.	https://gem.gov.in **&** www.cdac.in

1. Instructions for On-line Bid Submission

The bidders are required to submit soft copies of their bids through the portal (https://gem.gov.in/).

2. Assistance to Bidders:

Any query relating to the process of online bid submission or queries relating to GeM Portal in general may be directed to the

- Helpdesk on: - 1800-419-3436 / 1800-102-3436,
- e-mail for Technical - helpdesk-gem[at]gov[dot]in.

In case of any doubts and/ or queries pertaining to technical solution, specifications terms and conditions of the tender, prospective bidder may send their queries in writing through e-mail (purchase-hyd@cdac.in). The queries, requests for clarifications etc. must be sent within 7 days from the date of publication of the Tender. The bidders are requested to go through the entire tender document thoroughly, before raising any query. C-DAC, Hyderabad shall address the queries raised by the bidders. The replies to queries would be made available on GeM Portal and C-DAC's web site in due course of time. All the queries, doubts, clarifications etc. must be submitted in xls format only as below.

Name of the bidder:				
Sl.No	Section / Page No	Clause Reference	Query from bidder	C-DAC Response

SECTION I: INSTRUCTIONS TO BIDDERS (ITB)

- ***Introduction*:**

Centre for Development of Advanced Computing (C-DAC) - is a scientific society under the administrative control of Ministry of Electronics & Information Technology, Government of India. As a part of the ISEA project a dedicated Cloud and Common Infrastructure for all ISEA activities has to be established, C-DAC invites bids from eligible System Integrators (S.I)/OEMs for Implementation of Turnkey Solutions for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR Locations along with Replication Solutions, as per Schedule of Requirements **(Section- IV)** and other terms and conditions stipulated in this document.

- ***Contact information:***

The Head (Purchase)
Centre for Development of Advanced Computing,
Plot No: 6&7, Hardware Park, Sy. No.1/1, Srisailam Highway
Hyderabad – 501510
Email: purchase-hyd@cdac.in

- ***Two bid System:***

Two bids - Least Cost System will be followed and bidders shall submit bids Online through https://gem.gov.in. In this system, bidder must submit their offer - online as follows:

1: Technical Bid Shall contain – Pre-Qualification & Technical Scoring Criteria including Technical Presentation as specified in the bid, Technical Specifications and Supporting Documents/Annexures.

2: Financial Bid – Price quoted for the Solution shall be filled in the provision made by Portal, Price Break-up document should be uploaded in the provided format (Annexure – III).

1. **Technical Bid:**

A. Pre-Qualification Criteria:

All the qualification criteria & credentials are to be fulfilled by the bidder only and consortium (arrangement) bid participation is NOT allowed in this tender.

The bidders should be either the Original Equipment Manufacturer of the items covered by the Schedule of Requirements given in this document OR an authorized Data Centre IT infrastructure system integrator in India for all the Original Equipment Manufacturer(s) providing service for the items covered by Schedule of Requirements.

S. No.	Mandatory Criteria	Documentary proof to be submitted in the technical bid section.	Enclosed Yes/No
1	Bidder Must be a registered entity in India. Bidders having office / branch both in Hyderabad & Delhi /National Capital Region are only allowed to participate in this bid.	Copy of the Certificate of Incorporation issued by Registrar of Companies. In case of Partnership firm, duly signed and notarized copy of the partnership deed or a Certificate of Registration issued by the Registrar of Firms; or in case of a sole proprietorship, a GST registration certificate and/or PAN number.	
2	Bidder Should have been in existence for atleast Five (5) years in the market as on the date of issuance of this Tender.		
3	Bidder Should have average annual turnoverof at least Rs. 180 Crores in the last three (3) preceding financial years (FY 20-21, 21-22 & 22-23)	CA Certificate indicating average annual turnover details along with Audited Balance Sheet and Profit and Loss Account of last three years.	
4	Bidder should have executed similar turnkey projects (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/SDN Solution with 100Gbps backbone/Security Solution for a production throughput of minimum 10 Gbps.) with Central/State Governments Ministries/Departments/PSUs/Autonomous Bodies during the last 5 Financial Years and current Financial year i.e FY 2018-19, 2019-20, 2020-21, 2021-22, 2022-23 & 2023-24 as follows; i) Single similar turnkey project work order/contract valuing Rs.36 Cr. (or) ii) Two similar turnkey project work orders/contracts valuing Rs.22.50 Cr. (or) iii) Three similar turnkey project work orders/contracts valuing Rs.18 Cr. **Note: the project should be completed in all respects and ongoing projects shall not be considered.**	Certificate/ Copy of the work Order & completion certificate from the concerned Ministries/Departments/PSUs/Autonomous bodies to that effect needs to be submitted.	

5	EMD (Earnest Money Deposit) or Bid Securing Declaration in lieu of EMD. Note: MSE & Start-Ups also need to provide this Declaration letter invariably.	An EMD (Earnest Money Deposit) of Rs. 1.35 Crores in the form of a Bank Guarantee from a Scheduled Commercial Bank valid for 180 days from date of opening of bid or deposit of amount in online mode into CDAC's Bank account. Transaction details of the transfer/Copy of BG Guarantee should be uploaded along with the Technical Bid. Bidder should ensure that Original BG should reach CDAC, Hyderabad on or before the due date/time. **Alternately**, Bidders should sign a Bid Securing Declaration accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for a period upto two (02) years from the date of disqualification, provided that the Bidders shall be given a cure period of one (1) month before any such action is taken. **Annexure-A**	
6	Minimum 2 OEM Certified resources on the direct job role of the bidder in each of the following areas; (a) Cloud solution (b) SDN Solution (c) Security Solution	Supporting documentary proof.	
7	The bidder should be certified with ISO 9001 (QMS) and ISO 27001 (ISMS) and submit the valid certificates as on date of submission of the bid.	Copy of certificate	

8	Compliance statement indicating the compliance of the items, Equipment, solution offered with the tender specifications and Scope of Work.	**As per Annexure-B**	
9	The undertakings from the Principal Manufacturers (OEMs) of equipment / items offered.	As per **Annexure – C.**	
10	The bidders need to fill the detailed technical solution to be offered	As per **Annexure –D**	
11	Following General Annexures to be uploaded in the technical bid section duly signed & stamped; i. Tender acceptance Letter ii. No Deviation Certificate format iii. Undertaking for non-black listing iv. Authorization Letter v. Litigation Impact Undertaking vi. Make in India Local Content Declaration Letter duly certified by the statutory auditor or cost auditor. vii. Land Border Sharing OM-declaration viii. Details of bidder's organization ix. Draft NDA	As per **Annexure –E to Annexure-M**	

Note:-I) In case of bidders not qualifying in the pre-qualification stage, their bid will not beconsidered for Technical Evaluation process and will be declared as "Disqualified".

B. Technical Scoring Criteria:

i. In this stage, the Technical Proposal will be evaluated on the basis of the bidder's experience, its understanding of the Scope of Work, proposed supply & installation plan and technical presentation of the solution to be offered.
ii. Each technical proposal will be assigned a technical score (TS). The maximum technical score which a bidder can attain is 100 marks.
iii. A minimum of 75 marks should be scored in the technical proposal for the bid to be declared as **"Technically Qualified"**. The Financial Bids of only those bidders who have obtained a Technical Score of 75 or more shall be opened.
iv. The technical evaluation shall be in terms of the following parameters and marking scheme:

S. No.	Parameter	Max. Marks	Criteria for Technical Evaluation
1	Previous experience of bidder for similar (Data Centre IT Infrastructure installations, maintenance and support of complete Cloud Solution of not less than 20 Nodes/ SDN Solution with 100Gbps backbone/ Security Solution for a production throughput of minimum 10 Gbps.) Turnkey projects of valuing more than Rs. 18 Cr executed with Central/State Government Ministries/Departments/PSUs /Autonomous bodies Note: the project should be completed in all respects and ongoing projects shall not be considered.	30	Each similar Turnkey projects valuing Rs.18 Cr to 22.50 Cr will get **4 marks**. Each similar Turnkey projects valuing more than Rs.22.50 Cr and upto 36 Cr will get **6 marks.** Each similar Turnkey projects valuing more than Rs.36 Cr will get **12 marks.**
2	Overall project management; i) Project Schedule with delivery plan. **(max.10 marks)** ii) Proposed plan of installation, integration, testing & commissioning in line with tender requirement. **(max.10 marks)** iii) PMP certified resources on the direct job role of the bidder. **(2 marks for each resources and Max. 10 Marks)**	30	Bidder has to make a detailed presentation before the Tender Evaluation Committee.

3	Technical Solution to be offered covering following; **i)** Understanding of the Scope of Work. **(max.10 marks)** **ii)** Proposed solution. **(max.10 marks)** iii) Detailed deployment architecture. (max.10 marks) **iv)** Integration & Testing Plan. **(max.10 marks)**	40	Bidder has to make a detailed presentation before the Tender Evaluation Committee. Technical Demonstration & Presentation: The Bidders will be required to give a live demonstration of its solution and presentation to the Purchaser at a date, time and venue decided by the Purchaser. The Bidders will need to cover all technical details of Technical Proposal. It is expected that the key members proposed for the Project will be present during the demonstration and Presentation.
Total		**100**	

Note: All the bidders who meets the minimum qualifying criteria i.e 75 Marks as prescribed above, during technical evaluation will be considered for opening of the financial bids. Bidders whose proposals doesn't meet the technical evaluation criteria or were found non- responsive to tender will be notified as rejected.

C. Other documents necessary in support of eligibility criteria, product catalogues, brochures etc.

2. Financial Bid shall contain:

i. In this stage, the financial evaluation of the proposal will be carried out of the bidders who qualify in the technical evaluation after determining whether the Financial Proposals are complete, qualified and unconditional.

ii. While quoting the contract value in the financial bid stage in GeM portal, the bidders need to quote only the Total Lump-sum contract value with GST for the subject scope of work of "**Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution"** and also Bidders need to upload the detailed item wise price break-up in pdf format in this section.

3. Last Date of submission/ uploading:

The on-line bids, complete in all respect should be uploaded through https://gem.gov.in on or before the date given in tender schedule. The bidders are advised to upload the documents at least one day before the last date for uploading of documents, in order to avoid the possibilities of any last minute surprises. C-DAC does not take any

responsibility towards technical snags pertaining to the Portal and/or connectivity issues.

4. Opening of Technical bids:

The online bids will be opened in the GeM portal on Due date of the bid or the next working day, if due date of bid happens to be holiday.

Note: Please do not provide any "Commercial details" in the technical bid.

5. Evaluation of Proposals:

The Proposals shall be evaluated by a Tender Evaluation Committee (TEC). The Purchaser may appoint any external agency/consultants to assist it in evaluation of the Proposals.

In each stage of evaluation, the respective Proposals shall be first checked for responsiveness with the requirements of the bid Document. The Purchaser reserves the right to reject the Proposal of a Bidder if the contents of the Proposal are not substantially responsive with the requirements of this Bid Document.

In Stage-I of Proposal Evaluation, the Proposals submitted by the Bidders shall be checked for meeting the Pre-qualification eligibility criteria specified in the Bid document and Technical Scoring criteria set out in Bid document.

In Stage-II, the Price Bids of the Bidders who have qualified in the Stage I evaluation would be opened and Lowest Bidder will be identified on lump-sum contract /composite value basis for the subject “Turn-Key” project.

6. Opening of Financial bids:

Financial bids of the technically qualified bidders (***Technical Score of [75] or more)*** only will be opened. The decision of C-DAC’s Tender Evaluation Committee in this regard will be final and binding on bidders. C-DAC’s Tender Evaluation Committee will be authorised to take appropriate decision on deviations, if any.

The date of opening of Financial bids will be decided after Technical Evaluation.

(END OF SECTION I)

SECTION II: GENERAL CONDITIONS OF CONTRACT (GCC)

1. *Location for the Supply, Installation & Warranty Services:*

The Supply, Installation, commissioning and warranty of items mentioned Schedule of Requirements will be at 2 locations as specified in Schedule of Requirements:

Centre for Development of Advanced Computing (C-DAC)
Plot No: 6&7, Hardware Park, Sy. No.1/1,
Srisailam Highway,
Hyderabad – 501510

&

Centre for Development of Advanced Computing (C-DAC)
Anusandhan Bhawan, C-56/1, Sector-62,
Noida - 201307
Uttar Pradesh (India) Phone:
+91-120-3063311-14
Fax: +91-120-3063317

2. *Delivery Period:*

The entire supplies of items covered in this bid must be Supplied, Installed and Commissioned along with the final acceptance testing within **8 weeks** from the date of placement of order. The detailed delivery and payment schedule is provided in Annexure - II. Bidders are required to comply with schedule of delivery, installation and commissioning in accordance to the proposed schedule.

3. *Order Placements:*

The Supply Order shall be released by:

Centre for Development of Advanced Computing (C-DAC) Plot No: 6&7, Hardware Park, Sy. No.1/1,
Srisailam Highway, Hyderabad – 501510

The payments shall be released by:

Centre for Development of Advanced Computing (C-DAC) Plot No: 6&7, Hardware Park, Srisailam Highway,

Hyderabad – 501510

4. *Eligibility Criteria:*

The bidder must comply with the minimum eligibility criteria stipulated below.

4.1. The bidder must submit all the documents as prescribed under pre-qualification criteria section without fail.

4.2. The bidders should be either the Original Equipment Manufacturer of the

items covered by the Schedule of Requirements given in this document OR an authorized Data Centre IT infrastructure system integrator in India by the Original Equipment Manufacturer(s) for sale and providing service for the items covered by Schedule of Requirements

4.3. The bidder should be certified with ISO 9001 (QMS) and ISO 27001 (ISMS) and submit the valid certificates as on date of submission of the bid.

4.4. The bidder must not be blacklisted by any Govt. Organizations as on date of submission of the bids. A certificate or undertaking to this effect must be submitted **(Annexure – G).**

4.5. If the bidder is an authorised system integrator, the specific authorisation letter/s from Principal/s, as per **Annexure - C** must be submitted along with the technical bid. In this case, the authorization letter (Annexure – C) issued by the Indian subsidiary of Principal Manufacturer is acceptable.

4.6. As per Rule 144 (xi) of GFR 2017, any bidder from such countries sharing a land border with India will be eligible to bid in any procurement whether of goods, services (including consultancy services and non-consultancy services) or works (including turnkey projects) **only if the bidder is registered with the Competent Authority**. The Competent Authority for registration will be the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT), Government of India. Political and security clearance from the Ministries of External and Home Affairs respectively will be mandatory. A certificate or undertaking to this effect must be submitted as per **(Annexure – K).**

4.7. In line with OM No. P-45021/2/2017-PP (BE-II) dated 16.09.2020 issued by Ministry of Commerce and Industry Government of India regarding Public Procurement (Preference to Make in India), Order 2017, in cases of procurement for a value in excess of Rs. 10 crores, the 'Class-I local supplier'/ 'Class-Il local supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content. The local content calculation need to done as per the guidelines/clarification given in the OM no. P-45014/19/2021-BE-II (E-54692) dated 02.11.2022 issued by Ministry of Commerce and Industry, Government of India. **The local content to be declared by the respective auditor for the overall solution should be as per Annexure-L**

4.8. If the bid is submitted by the Indian subsidiary of Principal Manufacturer (OEM), the letter from Principal Manufacturer (OEM) must be submitted certifying that the bidder is the subsidiary company of the Principal Manufacturer (OEM) in India.

4.9. In case, if the OEM is directly participating in the subject tender, they should not authorize any of their resellers/channel partners/S.I to quote their product & services for this same tender. All such bids of OEM as well as S.I shall be rejected summarily.

4.10. The bidder must quote for all the items given in **Section V** of this document as a lump-sum contract value including GST in the GeM Portal.

4.11. The bidder must submit all the documents as per Document Checklist – **Annexure -O**.

5. *Amendment to Bidding Documents*

5.1. At any time prior to the deadline for submission of bids, C-DAC may, for any reason, whether on its own initiative or in response to the clarification request by a prospective bidder, modify the bid document.

5.2. The amendments to the tender documents, if any, will be notified by release of Corrigendum Notice on https://gem.gov.in/ www.cdac.in/ tender against this tender. The amendments/ modifications will be binding on the bidders.

6.3.C-DAC at its discretion may extend the deadline for the submission of bids if it thinks necessary to do so or if the bid document undergoes changes during the bidding period, in order to give prospective bidders time to take into consideration the amendments while preparing their bids.

6. *Preparation of Bids*

Bidder should avoid, as far as possible, corrections, overwriting, erasures or postscripts in the bid documents. In case however, any corrections, overwriting, erasures or postscripts have to be made in the bids, they should be supported by dated signatures of the same authorized person signing the bid documents. However, bidder shall not be entitled to amend/ add/ delete/ correct the clauses mentioned in the entire tender document.

7. *Earnest Money Deposit:*

7.1. The Earnest Money Deposit (EMD) of Rs.1.35 Crores must be submitted prior to the DUE DATE & TIME of submission of the online technical bid. The EMD is required to be in the form of Bank Guarantee in favour of C- DAC. **Alternately**, the bidder may choose to submit an EMD / bid security declaration, as given in Annexure - A , subject to the conditions stipulated therein.

7.2. The EMD will be returned to the bidder(s) whose offer is not accepted, within 30 days from the date of opening of commercial bid(s). In case of the bidder whose offer is accepted, the EMD will be returned on submission of Security Deposit. However, if the return of EMD is delayed for any reason, no interest/ penalty shall be payable to the bidder.

7.3. The EMD may be forfeited:

- If the bidder withdraws the bid during the period of bid validity specified in the tender.
- In case a successful bidder, fails to furnish the Security Deposit

8. *Period of validity of bids*

8.1. Bids shall be valid for minimum 180 days from the date of submission. A bid valid for a shorter period shall stand rejected.

8.2. C-DAC may ask for the bidder's consent to extend the period of validity. Such request and the response shall be made in writing only. The bidder is free not to accept such request without forfeiting the EMD/BG. A bidder agreeing to the request for extension will not be permitted to modify his bid.

9. Submission of Bids- Online :

All the required documents shall be uploaded as per the provision made in the GeM Portal. They should not contain any terms and conditions, printed or otherwise, which are not applicable to the Bid. **The conditional bid will be summarily rejected**. Insertions, postscripts, additions and alterations shall not be recognized, unless confirmed by bidder's signature.

10. Bid Opening & Evaluation of Bids

The technical bids will be evaluated in two steps.

10.1. The bids will be examined based on pre-qualification eligibility criteria stipulated at Para 4 of Section – II to shortlist the eligible bidders for Technical scoring criteria.

10.2. The technical bids of only the short-listed eligible bidders in the pre-qualification round shall be called for the technical presentation of their solutions on scheduled date and time. The bidder shall be evaluated based on the technical solution as per the scope of work, specifications of the items stipulated at Section – IV and the presentation of bidders. Marks shall be awarded for the solution document and the presentation of the bidders as per the technical evaluation criteria mentioned in Section - IV. The bidders shall be technically disqualified, if the marks obtained is less than 75 marks out of 100 or any of the product do not meet the technical specifications / requirements mentioned in the tender.

10.3. The bidders whose technical bid is found to meet both the requirements as specified above will qualify for opening of the Financial Bid.

10.4. The duly constituted Tender Evaluation Committee (TEC) shall evaluate the bids. The TEC shall be empowered to take appropriate decisions on deviations, if any.

11. Comparison of Bids

11.1. Only the short-listed bids from the technical evaluation shall be considered for commercial comparison.

11.2. The prices quoted by the bidders (Financial Bid) for the subject turn-key project covering **all** the items as listed in Section – V will only be considered for evaluation on composite/lump-sum contract basis.

12. Award of Contract

12.1. C-DAC shall place the order(s) on the eligible bidder whose technical bid has been accepted and determined as the lowest evaluated commercial bid on composite/Lump-sum contract value basis.

However, C-DAC reserves the right and has sole discretion to reject the lowest bid.

12.2. If more than one bidder happens to quote the same lowest price, the GeM Auto L1 run option shall be binding all the parties.

13. Contract Signing

13.1. C-DAC shall place the order on the successful bidder through GeM portal.

13.2. Apart from GeM contract to be generated by system, a separate contract shall be signed in line with the complete tender document including all annexures within 21 days from the date of GeM order, which will constitute a binding contract between successful bidder and C-DAC.

14. Security Deposit:

14.1 Within 15 days of placing the order through GeM portal, the successful bidder needs to submit 5% of total contract value as "Security deposit" in the form of FD Receipt in favour of CDAC, Hyderabad /Bank Guarantee (including e-BG) from a scheduled Bank/ Online Payment i.e., NEFT, RTGS upon award of contract towards performance (Validity of Security Deposit should be 1 Year Plus Additional 3 Months).

14.2 The security deposit shall be refunded after successfully completing the project and receipt of 10% Performance Bank Guarantee towards warranty period of 5 Years and 60 days post project completion. In case of any breach of contract, the successful vendor shall be blacklisted by C-DAC, Hyderabad under intimation to all C-DAC Centres. Further, the Security Deposit shall be forfeited towards such defaults including claim additional damages, if any.

15. Purchaser's Right to amend / cancel

15.1. C-DAC reserves the right to amend the eligibility criteria, commercial terms & conditions, Scope of Supply, quantities, technical specifications etc.

15.2. C-DAC reserves the right to cancel the tender entirely or partially without assigning any reasons thereof.

15.3. C-DAC reserves the right to reject the bid submitted by the lowest evaluated bidder without assigning any reasons.

16. Corrupt or Fraudulent Practices

16.1. It is expected that the bidders who wish to bid for this project have highest standards of ethics.

16.2. C-DAC will reject bid if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices while competing for this contract;

16.3. C-DAC may declare a vendor ineligible, either indefinitely or for a stated duration, to be awarded a contract if it at any time determines that the vendor has engaged in corrupt and fraudulent practices during the award / execution of contract.

17. Interpretation of the clauses in the Tender Document / Contract Document

In case of any ambiguity/ dispute in the interpretation of any of the clauses in this Tender Document, the interpretation of the clauses by Director General, C-DAC shall be final and binding on all parties.

(END OF SECTION II)

SECTION III: SPECIAL CONDITIONS OF CONTRACT (SCC)

1. *Prices*

1.1. The price quoted shall be considered firm and no price escalation will be permitted (except Govt. Statutory Levies).

1.2. The bidder shall quote in INR.

1.3. Bidder must provide Break-Up of Total Price quoted along with GST separately for each item in Price Break-up document.

1.4. Total Price quoted is inclusive of Supply, Installation, Testing & Commissioning and 5 Years Warranty from the date of handing over of the solution to C-DAC.

1.5. In case due to any error/ oversight, the GST rate quoted by the bidder is different than the actual GST rate as per the tariff, the bidder will not be permitted to rectify the error/oversight. The orders/ contract will be placed with the GST rate quoted by the bidder or actual tariff rate (as on placement of order), whichever is LOWER. The difference amount payable, if any, between the quoted GST rate and actual tariff rate shall be borne by the bidder.

1.6. The prices quoted must be "All inclusive- till destination", (including international and local freight, insurance, customs clearance charges- if any, forwarding, loading/un-loading and all incidental charges till destination) and covering entire scope of work including Supply, Installation, Testing & Commissioning.

1.7. C-DAC reserves the right to increase the ordered quantity by upto 25% during the currency of the contract in the same approved BOQ price by giving reasonable notice even though the contractor supplied the initially ordered quantity in full.

2. *Software Licenses: (if applicable)*

The software licenses, if any, shall be required in the name of C-DAC, Hyderabad / C-DAC, Noida as the case may be. The licenses shall contain paper/electronic licenses (wherever applicable).

3. *Performance Security:*

The Performance Security in the form of a Bank Guarantee in INR equivalent to 10% amount of the total order value, as per the format attached to this document **(Annexure – P)**. This bank guarantee should be submitted along with the invoice after successful installation within 15 days. The Bank Guarantee shall remain valid for 2 Months beyond the warranty period of 5 Years (the period of 62 months) from the date of acceptance. The PBG must be negotiable at a branch of issuing bank in India. In case of no warranty/services claims towards the items under warranty and services during the validity period of bank guarantee, the PBG will be returned on completion of warranty period.

C-DAC reserves the right to invoke the Performance Bank Guarantee(s) submitted by bidder, in case of the following:

a. The Components/solutions of Turnkey Solutions for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security

at DC & DR locations along with Replication Solutions fail to achieve the performance as stipulated in this document or

b. The bidder fails to provide the warranty and other services in scheduled time frame, as stipulated in this document or

c. The bidder delays to provide the warranty services as stipulated in this document.

4. *Completeness Responsibility:*

Notwithstanding the scope of work, engineering, supply and services stated in bid document, any equipment or material, engineering or technical services which might not be even specifically mentioned under the scope of supply of the bidder and which are not expressly excluded there from but which – in view of the bidder - are necessary for the performance of the equipment in accordance with the specifications are treated to be included in the bid and has to be performed by bidder.

5. *Warranty:*

The Supplier warrants that all the Goods are new, unused, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the order. The supplier further warrants that all Goods supplied shall have no defect arising from design, materials or workmanship (except when the design and/or material is required by the Purchaser's specifications) or from any act or omission of the supplier. **The warranty should be comprehensive on site, including all labour, service and parts with repair/replacement basis free of cost.**

The supplier also warrants that the said goods would continue to conform to the description and quality aforesaid for a period of min. 5 years from the date of acceptance by the end user and that notwithstanding the facts that the Purchaser/ end user (Inspector) may have inspected and/or approved the said Goods. If during the aforesaid period of 5 years the Goods be discovered not to conform to the description and quality aforesaid or have deteriorated Purchaser will be entitled to reject the Goods or such portion thereof as may be discovered not to conform to the said description and quality. On such rejection, the Goods will be at the supplier's risk and all the provisions herein contained relating to rejection of Goods, shall apply. The supplier if called upon to do so, shall replace within one month or such further period as may be extended by the Purchaser on his discretion on an application made thereof by the supplier the goods or such portion thereof as is rejected by Purchaser and in such an event the above mentioned warranty period shall apply to the Goods replaced from the date of acceptance of the replacement otherwise , the supplier shall pay to the Purchaser such damages as may arise by reason of breach of the conditions therein contained.

All the Goods supplied must have 5 (Five) years onsite comprehensive warranty with 24x7 support along with 4 hours response time and 48 hours resolution time, covering all parts & labor starting from the date after the successful installation, demonstration of performances and acceptance by C-DAC. During the warranty period, supplier will have to undertake comprehensive maintenance of the entire hardware components, equipment, support and accessories supplied at the place of installation of the equipment.

The defects, if any, during the guarantee/warranty period are to be rectified free of charge

by arranging free replacement wherever necessary. Goods requiring warranty replacements must be replaced on free of cost basis.

Onsite comprehensive warranty and support for complete supplies including Hardware, Software for 5(Five) years from the date of acceptance of the solution.

The warranty support will be backed by supplier by submitting a Performance Bank Guarantee, as per para 3 of Section – III.

6. *Acceptance Criteria*

The acceptance criteria for the solution is to demonstrate Complete functionality as per the Schedule of Requirement provided in Section - IV . The approved acceptance test reports must be submitted along with the invoices for claiming payments, wherever applicable.

7. *Payments:*

SL.No	Payment Terms
1	70% of the value of the delivered material will be released within 4 weeks from date of delivery, and acceptance by CDAC. All the necessary/required documents related to the material and Invoices are to be submitted with the material. Software License shall be generated in the name of CDAC, Hyderabad or CDAC, Noida respectively; as per the details provided in Schedule of Requirements
2	30% of the overall contract value will be released after the following activities; I. The overall solution is accepted, after successful installation & integration at Hyderabad & Noida Centre as per approved Architecture. II. Proper hand over of working solution. The 5 years warranty period will commence from the date of handover. III. Submission of 10% PBG towards 5 years warranty period.

7.1 Though the subject turn-key project is on Lump-sum contract value basis, the payment will be settled on actual measurement/receipt of goods/delivery & installation basis only based on the price break-up details already declared by the successful bidder before placement of order.

8. *Penalty for delayed Delivery /Services*

8.1. In case, the supplier fails to complete any part of scope of the work (i.e. delivery, inspection, installation, commissioning, acceptance and training) or part thereof within the period as stipulated in the order, C-DAC reserves the right to recover from

the supplier, as agreed liquidated damages and not by way of penalty, a sum of 0.5% of the price of total order value for each week or parts thereof, of the delay, subject to a maximum of 10% of basic contract value without taxes.

8.2. The period of delay in delivery and/or installation not attributed to the supplier, delay in site preparation, delay in submission of required documents by C-DAC etc. and the conditions arising out of Force Majeure will be excluded from delay period while calculating the delay period for penalties.

8.3. C-DAC reserves the right to cancel the order in case of delays of more than 10 weeks without any justifiable reasons.

9. *Force Majeure:*

C-DAC may consider relaxing the liquidated damages and delivery requirements, as specified in this document, if and to the extent that, the delay in performance or other failure to perform its obligations under the contract is the result of a Force Majeure. Force Majeure is defined as an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, floods, storms etc.), acts of states / state agencies, the direct and indirect consequences of wars (declared or undeclared), hostilities, national emergencies, civil commotion and strikes at successful Bidder's premises or any other act beyond control of the bidder.

10. *Risk:*

All risks, responsibilities and liabilities thereof in all goods shall remain with selected bidder till successful installation and commissioning of the goods as specified in this document.

11. *Limitation of Liability:*

The liability of the bidder arising out of breach of any terms, conditions of the tender, contract, works order and addendums/amendments thereto, misconduct, and wilful default will be limited to the total order value. However, liability of the bidder in case of death, injury, damage caused to the personnel/property due to/arising out of/incidental to any act/omission/default/deficiency of bidder, will be at actuals.

In no event shall either Party, its officers, directors, or employees be liable for any form of incidental, consequential, indirect, and special or punitive damages of any kind.

12. *Validity of Contract:*

Validity of order/ Contract will remain till fulfilment of all obligations including but not limited to providing comprehensive warranty/support till Completion of Five years from acceptance of the solution by C-DAC.

13. *Termination:*

If the successful bidder fails to discharge the contractual obligations/comply with the requirements during the currency of the contract, C-DAC shall have the right to terminate the contract and / or cancel the order/s. The successful bidder agrees and accepts that he shall be liable to pay damages claimed by C-DAC, in the event of termination of contract / cancellation of order, as detailed in this tender.

C-DAC will release the due amount payable to successful bidder towards the material and / or services provided till the date of termination, those are accepted by C- DAC. However,

the amount towards penalty, if any, will be deducted from the payable amounts and such defaulted vendor shall be blacklisted for a period up to 2 years.

14. *Indemnity:*

On acceptance of order, the successful bidder shall automatically indemnify, protect and save C-DAC and end user from/against all third-party claims, losses, costs, damages, expenses, action suits and other proceeding, resulting from/arising out of:

a. infringement of any law pertaining to intellectual property, patent, trademarks, copyrights etc. by the bidder

or

b. such other statutory infringements in respect of any of the equipment supplied by successful bidder,

or

c. any willful misconduct or gross negligence act/omission/ performance/ under or non or part performance/failure of the bidder.

15. *Assignment:*

Selected bidder/ Party shall not assign, delegate or otherwise deal with any of its rights or obligation under this Contract without prior written permission of C-DAC.

16. *Severability:*

If any provision of this Contract is determined to be invalid or unenforceable, it will be deemed to be modified to the minimum extent necessary to be valid and enforceable. If it cannot be so modified, it will be deleted and the deletion will not affect the validity or enforceability of any other provision.

17. *Jurisdiction:*

The disputes, legal matters, court matters, if any shall be subject to Hyderabad jurisdiction only.

18. Integrity Pact:

The pact essentially envisages an agreement between the prospective vendors/bidders and the buyer, committing the persons/officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract. Only those vendors/bidders, who commit themselves to such a Pact with the buyer, would be considered competent to participate in the bidding process. In other words, entering into this Pact would be a preliminary qualification. The essential ingredients of the Pact include:

- Promise on the part of the principal not to seek or accept any benefit, which is not legally available;
- Principal to treat all bidders with equity and reason;
- Promise on the part of bidders not to offer any benefit to the employees of the Principal not available legally;
- Bidders not to enter into any undisclosed agreement or understanding with other bidders with respect to prices, specifications, certifications, subsidiary contracts, etc.

- Bidders not to pass any information provided by Principal as part of business relationship to others and not to commit any offence under PC/IPC Act,
- Foreign bidders to disclose the name and address of agents and representatives in India and lndian Bidders to disclose their foreign principals or associates;
- Bidders to disclose the payments to be made by them to agents/ brokers or any other intermediary,
- Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.
- Integrity Pact, in respect of a particular contract, would be operative from the stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

As per Government of India (Central Vigilance Commission) guidelines, CDAC and the SUPPLIER have to sign an Integrity Pact for the high value contracts, for ensuring transparency, equity and competitiveness in public procurement. The Bidder has to sign Pre-Contract Integrity Pact as per format enclosed and to submit along with Bid (Mandatory condition).

The bidder is required to enter into an Integrity Pact with CDAC. For this, the bidder shall submit the original signed, stamped on Rs.100 non-judicial stamp paper and notarized Integrity Pact as part of Bid as per dates mentioned, failing which, the Proposal submitted by the concerned bidder will be liable to be forthwith and summarily rejected. The format for the Integrity Pact is provided in (**ANNEXURE J**)

19. Fall Clause

i. The bidder shall ensure that the prices charged for the Services etc. to be provided by the bidder shall in no way exceed the lowest price at which the bidder provides services of identical description to any other person/organization during the currency of the contract. If at any time during the currency of the contract, the bidder reduces the price of such services to any other person/organization at a price lower than the prices chargeable under the contract, they shall forthwith notify such reduction or sale to the buyer and price agreed to under the contract for the services provided after the date of coming into force of such reduction/sale shall stand correspondingly reduced.

ii. To comply with the above condition, the bidder shall furnish the following certificate along with each bill for payment to the paying authority:

iii. The price charged for the services provided under the contract by the bidder shall in no event exceed the lowest price at which the bidder providers the services of identical description to any other person/organization for at least one year from the date of order/contract.

iv. If at any time, during the said period, the bidder reduces the price of such services to any other person/organization at a price lower than the price chargeable under the

order/contract, they shall forthwith notify such reduction or services to the buyer and the price payable under the order/ contract for the items supplied after the date of coming into force of such reduction or sale shall stand correspondingly reduced".

(END OF SECTION III)

SECTION IV: SCHEDULE OF REQUIREMENTS-BILL OF QUANTITY

High-end Servers, Storage Components and Networking Equipment

A. Schedule of Items – BoQ

S.N.	Requirements	Specifications	Quantity Delivery at		Remarks
			Hyderabad	Noida	
1	Servers / HCI	Detailed at (i)	13 Nos. (9 DC + 4 DR)	7 Nos.	
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc	Detailed at (ii)	For 8 Nodes at SN. 1 (4+4) DC-DR config	For 4 Nodes at SN. 1	Compatible solution with solutions of all other items.
3	RHEL (Unlimited Virtualization)	Detailed at (iii)	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	
4	Windows Data Centre	Detailed at (iv)	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	
5	NVMe Storage	Detailed at (v)	1 No.	1 No.	Supported by same OEM
6	SAN Switch	Detailed at (vi)	2 Nos. (in HA)	2 Nos. (in HA)	
7	Network Leaf Switch (Copper) with SDN Solution	Detailed at (vii)	6 Nos.	8 Nos.	Solution from single OEM
8	Network Leaf Switch (Fibre / Copper) with SDN Solution	Detailed at (viii)	12 Nos. (8-DC & 4-DR)	16 Nos.	
9	Network Spine Switch with SDN Solution	Detailed at (ix)	4 Nos. (2-DC & 2-DR)	-	
10	Network OOB Management Switch	Detailed at (x)	29 Nos. (25-DC & 2-DR)	35 Nos.	
11	Routers (2-10Gbps)	Detailed at (xi)	4 Nos.	-	
12	Routers (4-10Gbps)	Detailed at (xii)	-	2 Nos.	
13	EDR Solution (Servers)	Detailed at (xiii)	300 Nos.	1000 Nos.	Solution from single OEM
14	EDR Solution (Desktops)	Detailed at (xiv)	-	800 Nos.	
15	DDoS (Hardware Appliance)	Detailed at (xv)	2 Nos. (in HA) or 1 No. with Bypass	2 Nos. (in HA) or 1 No. with Bypass	Solution from single OEM
16	SSL Offloader (Hardware Appliance)	Detailed at (xvi)	2 Nos. (in HA)	2 Nos. (in HA)	
17	WAF (Virtual Appliance)	Detailed at (xvii)	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	

S.N.	Requirements	Specifications	Quantity Delivery at		Remarks
			Hyderabad	Noida	
18	LB (Virtual Appliance)	Detailed at (xviii)	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	
19	NG-Firewall with ATP & Deep Inspection	Detailed at (xix)	2 Nos.	-	

B. Delivery Schedule & Payment Schedule

S.N.	Requirements	Delivery Period	Quantity Delivery at		Payment Schedule
			Hyderabad	Noida	
1	Servers / HCI	4 weeks	13 Nos. (9 DC + 4 DR)	7 Nos.	70% on Delivery
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc	2 weeks	For 8 Nodes at SN. 1 (4+4) DC-DR config	For 4 Nodes at SN. 1	70% on Delivery
3	RHEL (Unlimited Virtualization)	2 weeks	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	70% on Delivery
4	Windows Data Centre	2 weeks	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	70% on Delivery
5	NVMe Storage	4 weeks	1 No.	1 No.	70% on Delivery
6	SAN Switch	4 weeks	2 Nos. (in HA)	2 Nos. (in HA)	
7	Network Leaf Switch (Copper) with SDN Solution	4 weeks	6 Nos.	8 Nos.	70% on Delivery
8	Network Leaf Switch (Fibre / Copper) with SDN Solution	4 weeks	12 Nos. (8-DC & 4-DR)	16 Nos.	70% on Delivery
9	Network Spine Switch with SDN Solution	4 weeks	4 Nos. (2-DC & 2-DR)	-	70% on Delivery
10	Network OOB Management Switch	4 weeks	29 Nos. (25-DC & 2-DR)	35 Nos.	70% on Delivery
11	Routers (2-10Gbps)	4 weeks	4 Nos.	-	100% on handover
12	Routers (4-10Gbps)	4 weeks	-	2 Nos.	
13	EDR Solution (Servers)	4 weeks	300 Nos.	1000 Nos.	100% on handover
14	EDR Solution (Desktops)	4 weeks	-	800 Nos.	
15	DDoS (Hardware Appliance)	4 weeks	2 Nos. (in HA) or 1	2 Nos. (in HA) or 1	

S.N.	Requirements	Delivery Period	Quantity Delivery at		Payment Schedule
			Hyderabad	Noida	
			No. with Bypass	No. with Bypass	
16	SSL Offloader (Hardware Appliance)	4 weeks	2 Nos. (in HA)	2 Nos. (in HA)	100% on handover
17	WAF (Virtual Appliance)	4 weeks	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	
18	LB (Virtual Appliance)	4 weeks	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	
19	NG-Firewall with ATP & Deep Inspection	4 weeks	2 Nos.	-	100% on handover

A. Schedule of Requirement – Specification Compliance Sheet.

(i) Servers / HCI – 20 Nos. (9 Nos. to be delivered at Hyderabad and 11 Nos. at Noida) Out these 12 Nos. shall be pre-installed / installed at site (4 Nos. at Hyderabad and 8 Nos. at Noida)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Processor	Dual CPU based server must adhere to below points: 1. Latest (4th or higher) generation Intel Scalable Processor based on x86 architecture 2. Each CPU with a minimum of 32 cores 3. Minimum base frequency of CPU 2.6 GHz 4. Processor release should be within last one year (on or after year 2023)		
2.	RAM	Minimum 1.5 TB DDR5 RAM (expandable up to 3 TB without replacing the supplied modules)		
3.	Network	4 x 10 G SFP+, 2 x 1G SFP		
4.	HDD	1. 5 x 3.84 TB SSD Disk minimum endurance of 1 DWPD for 5 years, with Support for Software Defined Storage Solution. 2. RAID 1, 5 supported by RAID Controller with 2 GB Cache 3. M.2 400 GB x 2 in RAID 1 for Hypervisor 4. 1 x 800 GB SSD Cache drive minimum endurance of 3 DWPD for 5 years		
5.	HBA	2 x Single port 32 Gbps HBA Cards		

6.	Remote Management	1. 1 Gbps iLO Management port 2. IPMI 2.0 or equivalent Support with KVM and Media over LAN features with additional licenses if any. Should have support API based and SNMP (MIBs available online) server management.		
7.	OS Certifications	1. Certifications from major Hypervisor OEMs – VMWare and Nutanix and certified for proposed cloud solution and software defined storage solution. 2. Certifications from Redhat and Microsoft for Linux and Windows respectively.		
8.	Power supply	Redundant and Hot Pluggable, 80 Plus Platinum or better certified power supply along with Power cables for standard rack PDUs		
9.	Form Factor	2U rack mountable or smaller form factor.		
10.	Depth	Should not exceed 1200 mm including cable manager		
11.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. The quoted model of servers should have support life of 7 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(ii) Cloud Management Software – for 12 Nodes as mentioned above
Delivery – 8 Nos. in the License Account of C-DAC, Hyderabad & 4 Nos. in the License Account of C-DAC Noida
Installation – 8 Nos at C-DAC Noida and 4 Nos. at C-DAC Hyderabad

Sr. No.	Item	Description	Compliance Yes / No	Cross Ref.
1.	General Requirements	1. The solution should provide unified and centralized software defined datacenter platform that brings together market leading compute, storage, networking and security virtualization into a natively integrated stack to deliver enterprise-ready cloud infrastructure for the private, public cloud and across hybrid clouds. 2. The solution should include automated lifecycle management services that automate from bring up to configuration, resources provisioning, upgrades and patching including host firmware, and simplify day-to-day management and operations. 3. The solution should automate the bring-up process of the entire software platform, including deployment of infrastructure VMs, creation of the management cluster, configuration of VLANs, virtual storage, virtual network, and cluster creation and provisioning. Also, resource allocation to individual workloads by automating cluster creation through policy. 4. The solution should provide a centralized Manager that understands the physical and logical topology of the software defined data center and the underlying components relation to each other, and efficiently monitors the infrastructure to detect potential risks, degradations and failures. 5. The solution should provide alert management on problem detection. Each notification should include a clear description of the problem and provides remediation actions needed to restore service, degradations or failures are aggregated and correlated to workload/ virtual domains to enable a clear view of the impact of any issue. 6. The solution should provide all the installed components interoperability data checks: Auto-		

		checks of installed components interoperability and should support proposed licensing entitlements across multiple instances in the solution. 7. The solution should offer automated life cycle management on a per-workload basis. Available updates for all components should be tested for interoperability and bundled with the necessary logic for proper installation order. The update bundles should be then scheduled for automatic installation on a per-workload domain basis to allows administrators to target specific workloads or environments, for example development vs. production, for updates independent from the rest of the environment. 8. The automated upgrade process should ensure that the running workloads are not affected by the upgrade and must provide protection through automated workload migrations as the upgrades happen 9. The solution should provide common infrastructure & platform, consistent management and operational model, giving freedom to run applications (traditional & containers) anywhere without the complexity of application re-writing, portability of workloads between private and public clouds without any downtime. 10. All the components including Software defined data center manager, Compute virtualization, Network virtualization, storage virtualization, Cloud Orchestration & Automation, Operations Management & Network analytics should be from the same OEM for single point of support. 11. The solution should provide simple, secure and agile cloud infrastructure that can be deployed on premises and consumed as a service from public cloud interchangeably, without the need to repurchase the licenses. 12. OEM should provide direct support 24x7x365 with unlimited incident support for severity 1 with L1, L2, L3 level (Telephonic, Web, Email) and 30 mins or less response time including the unlimited upgrades and updates during the tenure of the project/ tender.		

2.	Compute Virtualization	1. Virtualization layer should sit directly on the bare metal server with features like HA, Proactive HA, Zero Downtime & Zero Data-loss without any additional clustering solution, Encrypted Live Migration of VMs, Hot Add (vCPU, vMemory, vStorage & vNetwork) without disruption or downtime of working VMs for both windows & Linux based VMs, distributed switch, VM level encryption, Network & Storage I/O Control, VM based replication with min. 5mins RPO, predictive dynamic resource scheduling for storage and VMs, secure the VMs with offloaded AV/AM, HIPS/ HIDS and stateful firewall solutions without the need for agents inside the VMs of windows & Linux. 2. The solution should provide proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs. 3. The solution should provide secure boot for protection for both the hypervisor and guest operating system, prevent loading of unauthorized components, support TPM 2.0 hardware modules and adds a virtual TPM device to shield guest OS from Operator or in-guest attacks. 4. The solution should have single reboot to dramatically reduce the upgrade times by skipping a host reset and also help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time-consuming hardware initialization. 5. The solution should provide in-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details 6. Virtualization software should provide Kubernetes in the control plane of hypervisor or integrated for unified control of compute, network and storage resources to run both containers and virtual machines on the same		

		platform. Natively / integrated enterprise supported Kubernetes with unified visibility for VMs, Kubernetes clusters, containers from virtualization console for consistent view between Dev and Ops via Kubernetes constructs in virtualization platform. 7. The solution should enforce security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits. 8. Virtualization manager should be highly available with out-of-the-box HA without any dependency on external shared storage or load balancer.		
3.	HCI (Storage Virtualization)	1. The solution should include storage virtualization / HCI software supporting all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any x86 server manufacturer & should support mixing of different compatible x86 Server brands in same Cluster. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM. 2. Storage virtualization should support VM-Centric controls for managing storage service levels for capacity, IOPS, availability QoS by storage policy-based management and should not be dependent on LUNs. Should also support features like rack awareness, deduplication, compression & RAID 1 and RAID 5, 6 through erasure coding (for all flash). Support scale up by adding disk in the node without any additional licenses, scale out by adding nodes or entire racks. This addition of capacity should NOT result in an increase of the number of management points 3. The solution should provide storage systems for the software defined data center which pools together local flash devices to provide a highly resilient shared storage suitable for a variety of workload domains including business critical applications, remote IT, DR, and DevOps infrastructure 4. The solution shall provide a data caching tier		

		that supports SSD, Ultra DIMM or NVMe and support for storage space efficiency features like de-duplication, compression and RAID 1 and RAID 5, 6 with erasure coding without dependence on any proprietary hardware. 5. The solution should provide distributed RAID and cache mirroring for intelligent placement of across disks, hosts and server racks for enhanced application availability. Should support zero data loss in case of disk, host, network or rack failure. 6. The solution should provide VM-level or Cluster-level encryption to protect unauthorized data access both at-rest and in-transit without any dependency on underlying hardware or dependence on SEDs (Self encryption device) and supports key management. 7. The solution design should have features like zero data loss and near zero downtime in case of disk, host, network, rack and near-site failure and support checksum of data to ensure data integrity & to enable automatic detection and resolution of silent disk errors. 8. The proposed software defined solution should use common storage management framework for HCI and traditional FC SAN, iSCSI & NAS Storage environment. Connect external 3rd party SAN/ NAS storage into the HCI cluster for capacity expansion and ease of migration from existing environment to HCI. 9. The solution should not have any hardware dependency to enable HCI Solution. All the nodes within the cluster should be utilized and none of the nodes should be ideal even in case of N+1 architecture. 10. The solution should allow common management across storage tiers and dynamic SLA automation via policy-driven control plane. Policies can be applied on a per-VM level and adjusted on the fly. No LUNs or RAID configurations should be required. 11. The solution shall provide ready to use templates to validate configuration standards on the platform covering security best practices, vendor hardening guidelines and		

		regulatory mandates such as PCI-DSS, GDPR, FISMA and SOX to track & enforce compliance. 12. Solution should provide an option to perform an automated upload of the support bundle an archive file that contains diagnostic information related to the environment, such as product specific logs, configuration files etc. and it does not allow to review, obfuscate, or otherwise edit the contents of your support data prior to it being sent to the OEM. 13. The solution should provide zero-downtime, zero-data loss continuous availability against physical disk failure. This fault tolerance should be offered without any dependency on the guest operating system. The solution should also store at least 2 redundant copy of the data which is accessible immediately by the application. 14. The solution should be able to accelerates read/write disk I/O traffic with built-in caching on server-side flash devices to optimally minimize the storage latency and also provides automated self-rebalancing capabilities to align with defined Storage service levels 15. HCI solution should provide support for Windows Server Failover Cluster (WSFC) technology through a single HCI solution. 16. The solution should expand to non-virtualized/ physical workloads with iSCSI/ NFS/ FCP/SMB access without the need of any additional license or cost and also provide pass-through mode for devices to be connected at both VMs and Host level.		
4.	SDN (Network Virtualization)	1. The solution should provide simplified, programmable, application of network & security policy to deploy virtualized network functions (like switching, routing, stateful firewall, QoS, VPN, NAT, DHCP, container network & security) and provide native application isolation for providing zero trust security for the application and allow for on-demand creation of security groups and policies without the need for complex VLANs, ACLs, or hardware configuration syntax on physical network.		

		2. The solution should provide distributed in-kernel/ integrated routing (BGP), VXLAN / GENEVE based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN services, L2-L4 distributed stateful firewall at vNIC level and at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups and Security policies which must follow the VM in the event of migration (i.e. live migration). 3. The solution should support common L3 and L2 connectivity topologies to the existing datacenter network and choices on the amount of bandwidth that can be configured on its uplinks to the existing datacenter network. 4. The solution should provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/ IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking & micro segmentation for micro services etc. 5. The solution should automate common networking and security policies across traditional VM-based environments, containers, micro service architectures, and clouds. Make infrastructure-as-code-based development cycles faster, more connected, and more secure. 6. The solution should protect every Virtual Machine with a stateful distributed firewall with Distributed IDPS and enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc. and offer virtualized workload at the vNIC level to be protected with a full stateful firewall/IDPS engine at a very granular level based on constructs such as MAC, IP, Ports, objects and tags, active directory groups, Security Groups , etc. 7. The solution should support for heterogeneous		

		underlying infrastructure based on bare metal, KVM and VMware vSphere and provisioning of complete virtual/ SDN services irrespective of make and topology underlying physical network switches and routers. 8. The security policies must be tied to the application, which means whenever any application is moved from one server to another, even between different subnets, and across multiple sites, the security policies should follow the application and there should be no need to redefine the security policies for the application at the new location. Also, when the application is deleted, all the security policies related to the application should also be removed. 9. The solution should have highly granular (per VM or per VM interface) level security capabilities potentially accessed through the network virtualization layer. 10. The solution should provide an integrated networking solution (CNI implementations) as well as provide advance turnkey container networking services at Layer 2 through 7 such as DNAT/SNAT, DHCP and stateful firewall (L4 to L7) in addition to switching and routing (North-South and East-West). 11. The solution should provide native integration with cloud automation layer on-premise and public cloud and fully supported Ansible modules, Terraform provider and PowerShell integration. RESTful API based on JSON for integration with cloud management platforms, DevOps automation tools and custom automation. 12. The solution should be capable to provide multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc. 13. The solution should have integrated distributed IDPS functionality for East-West traffic. Software distributed approach that moves traffic inspection out to every workload and		

		eliminates the need to hair-pin traffic to discrete appliances, ensuring comprehensive coverage without any blind spots. Security policies which must follow the VM in the event of migration (i.e. live migration). 14. The solution should support Stateful firewalling up to Layer 7 (including app identification and URL whitelisting/Filtering), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management without the need of any third -party agents 15. The solution should deliver end to end security for all applications by delivering network-level micro-segmentation, distributed firewalls, load balancers, virtual routers, virtual switches 16. The solution should provide the network virtualization platform for software defined datacenter, delivering the operational model of a virtual machine for entire networks including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment. 17. Solution provide traffic visibility, end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools. 18. The solution should provide the application discovery (names, tags, RegEx), topology view, health checklist, edge load balance dashboard, DNS mapping (import bind file), and visibility across third-party switches, routers, firewalls and load balancers		
5.	Cloud Platform	1. The solution should provide simple and flexible deployment model with easy installer, automated environment replication and validation process, automated management of configurations, certificates, licenses, passwords, and users. Source control and version content with Bitbucket, GitHub, and GitLab. Automate deployment of cloud content across multiple users and different environments. 2. The solution should deliver a comprehensive,		

		integrated product and lifecycle management solution for entire cloud to speed up deployments and updates, optimize and automate ongoing product and content management, and apply operational best practices across all components of cloud. 3. The solution must provide onboarding capability for existing VMs including visibility and show back for all the VM resources, those are not necessarily deployed through Private Cloud Orchestrator. System also must provide Day-2 actions like resize, snapshot, reboot, power on/off etc for on boarded existing VM's into private & Public Cloud. 4. Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS / SaaS services so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM and movement within and across DC & DR. 5. The solution should support multiple levels of approval with E-mail notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application 6. The solution should support creation of services such as 'Single VM' and a 'Multi- tier application infrastructure (including software-based constructs such as load balancers)' as part of a standard template with constructs like virtual switch, virtual router, firewall, load balancer etc. 7. The solution should have Service Catalogue for the cloud services out of the box and provision to add customized services i.e. addition of new services like IaaS & PaaS, pre-defined catalogues of templates. Capability to extend to Public cloud platforms. 8. The solution should provide horizontal and vertical auto scale. E.g., in case of increase in utilization additional VMs should be		

		automatically be created with all network, security and load balancing assigned. All components needed to achieve this including but not limited to cloud portal, orchestration, virtualization, overlay network, security and load balancer should be provided and integrated to achieve full automation. 9. The solution should have Life Cycle Management Work flows: Provisioning, Day-2 operations like cloning, re-sizing, snapshot, deletion etc. There should be zero manual intervention in this entire process across Private and Public Cloud (AWS, Azure, GCP). The software must allow the designer canvas to drag and drop Private and Public Cloud (AWS, Azure, & GCP) including Kubernetes resources to design the blueprints 10. The solution should have Life Cycle Management Workflows: Extensible Capabilities to allow "Self-Management" workflows (Reboot/ Restart, Migrate/Upgrade, Scale etc.), Provisioning, Decommissioning and allow administrator or cloud operator define IaaS and PaaS in the service catalogue for the cloud. 11. The solution should have inbuilt orchestrator platform with ready workflows and ability to build the custom workflow based on SOAP, REST operations and PowerShell scripts for complex tasks and integrated configuration management capabilities to build the custom states for complex tasks for OS and Applications. Use shell script, powershell script to code the for custom workflow automation. 12. The solution should have the ability to create custom workflows to automate the delivery of anything as a service - XaaS (for example Email, Storage as a Service, Network as a Service, Backup as a Service etc.) 13. The solution should provide for creation of complete application blueprints along with required virtual networking (routing, load balancing) and security services for the application using a user-friendly graphical interface by using drag & drop functionality. Allow mixed deployment in a blueprint. E.g.,		

		Provision database, Provision Application & Web Servers from a single blueprint. 14. The solution should reduce cost and improve efficiency with real-time, ML-based capacity and cost analytics. Deliver optimal consolidation and proactive planning using a real-time, forward-looking capacity analytics engine, predict future demand and provide actionable recommendations that include reclamation, procurement and cloud migration planning options. 15. The solution should have a Unified graphical canvas for designing machines, software components and application stacks with the ability to extend or define external integrations in the canvas through XaaS 16. The solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, capacity planning, performance management etc. 17. Administrator must be able to manage/control the marketplace view for the tenants and enable multi tenancy. Any authorized user must be able to deploy the application using the published blueprint in his application marketplace. Services provided in marketplace should cut across existing and upcoming infrastructure components. 18. The solution shall provide support to export/import the architecture blueprints into standard formats such as YAML for programmatic manipulation through Infrastructure-as-code. Should support bulk Import of underlying hypervisor virtual machines and multi-cloud VMs. 19. The solution should provide cloud agnostic templates to deploy resources on private and public clouds (AWS, Azure, Google Cloud) with Infrastructure as Code and native cloud resources via a plugin-based framework. 20. The solution should allow to create simple, human-readable infrastructure-as-code to provision, configure systems & software, infrastructure pipelining and iterative development, and have Self-Healing ability to		

		automatically enforce desired state of configuration of application, system services of any machine. 21. The solution should provide flexibility in deployment with having cloud-independent VM/application profile coupled with its cloud-specific logic that abstracts the application from the specific cloud, interprets the needs of the application, and translates those logical needs to cloud-specific services and APIs. The tool should eliminate the need of cloud specific scripting/IaaS to prevent cloud lock-in. 22. The solution should provide native integration with cloud automation layer on premise and public cloud and fully supported Ansible modules, fully supported Terraform provider and PowerShell integration. RESTful API based on JSON for integration with cloud management platforms, DevOps automation tools and custom automation. 23. The solution should automate the application and infrastructure delivery process with release pipeline management, including visibility and analytics into active pipelines and their status for troubleshooting and leverage existing tools and processes with out-of-the-box integration such as Ansible, Bitbucket, Github, Gitlab, IPAM, Puppet, Openshift, salt, terrafomr, bamboo, Docker, Docker Registry, GIT, Jenkins, Jira and TFs etc 24. Platform should have capability to support latest Kubernetes versions. Manage & Govern Kubernetes Clusters and Namespaces, Discover & Import Clusters. Request K8s Cluster, Namespace from Catalog, Manage Clusters and Namespaces. Kubernetes resources should be available as resources in Blueprints for creating multi-tier environment templates/blueprints. 25. Should support in built CI/CD tool for devsecops to automate build, release and deploy from continuous and repeatable basis by integrating on prem cloud across VMs and containers. Should be able to track artifacts and automate deployment configurations to ensure correct versions are used across all stages of the		

		development lifecycle. 26. The solution should provide out-of-the-box monitoring and troubleshooting for Packaged applications with Open Source Telegraf Agent and application performance management tool integrations. 27. The solution should allow connecting to data-center ecosystem components e.g., operating systems, applications, servers, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale. 28. The solution should provide intelligent log analytics to be able to bring unstructured and structured data together, for enhanced end-to-end operations management, collect and analyze all types of machine-generated log data, for example, network traces, configuration files, messages, performance data, system state dumps, and more. 29. The solution should provide real-time predictive capacity management, including trending, metering, rightsizing, optimization, super metrics, metric correlation, relationship mapping, business and operational intent-based automated and schedulable workload balancing and optimization. 30. The solution should have log analytics available in one single management window to make troubleshooting easier. Should provide a single location to collect, store, and analyze unstructured data from OS, VMs, apps, storage, network devices, containers, Kubernetes etc. at scale. Should provide intuitive dashboard and should allow IT teams to search for certain event patterns & types for troubleshooting. 31. The solution should be able to add all types of structured and unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand, perform long term Log retention and Log archival for future access and centralize log storage and analytics feature with Dashboards, Reports and Alerts with Webhook integration for Automated Remediation 32. The solution should utilize predictive analytics,		

		machine learning and root cause analysis tools across physical, virtual and multi-cloud environments for faster problem resolution and automatically choose the best visualization for data, saving time, pinpoints and tracks potential issues before they arise via automated alerts 33. The solution should provide predictive analytics, AI drive actions to proactively avoid contention, prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behavior, over-sized, under-sized, idle and powered-off virtual workloads, reclaim resources from idle VMs and allocate to other VMs in automated fashion, upcoming problems, what-if scenarios, root cause analysis, and opportunities for efficiency improvements. 34. The solution shall preemptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times and also provide smart Alerts, guided remediation, self-learning analytics with dynamic thresholds to deliver recommendations, or trigger actions, that optimize performance and capacity and enforce configuration standards. 35. The solution should have the capability to create a dashboard by adding widgets. Shall create and modify dashboards with reporting functions, can generate a report to capture details related to current or predicted resource needs, can download the report in a PDF or CSV file format for future and offline needs.		
6.	DR Solution	1. The solution should allow centralized creation and management of recovery plans directly from Virtualization Manager Console. Automatically discover and display virtual machines protected. 2. The solution should provide the extension of recovery plans with custom scripts and also able to Control access to recovery plans with role-based access control. 3. The solution should receive automatic alerts about possible site failure and allow execution of recovery plan directly from virtualization		

		manager with a single click and also support automated boot of protected virtual machines with pre-specified boot sequence. 4. The solution should manage and monitor execution of recovery plans from virtualization manager and support automated reconfiguration of virtual machine IP addresses at failover site. 5. The solution should automate failback to original production site using original recovery plan and also automatically re-protect virtual machines by reversing replication to the original site without any additional hardware appliance. 6. The solution should use storage snapshot to perform recovery tests without losing replicated data and also provide multiple point-in-time recovery which will allow reversion to earlier known states. 7. The solution should connect virtual machines to an existing isolated network to avoid impacting production applications while doing a testing and automate clean-up of testing environments after completing tests. 8. The solution should store, view and export results of test and failover execution from virtualization manager. 9. The solution should automate planned migrations with graceful shutdown of protected virtual machines at the original site thus ensuring no data loss and application-consistent migrations. 10. The solution should manage replication directly through the common virtualization manager, at a granular virtual-machine level and ensure complete replication of virtual machine data and storage based replication, prior to initiating migration. 11. The solution should be possible for the same site to serve as a protected site and recovery site when replication is occurring in both directions and protecting virtual machines at both sites. 12. "From initial setup to ongoing management, DR solution should deliver simple and policy-based operations: a. Centralized recovery plans to create and		

		manage recovery plans for thousands of VMs directly from the intuitive HTML5 user interface. b. Policy-based management to utilize storage profile protection groups to identify protected storage, automate the process of protecting and unprotecting VMs, and adding and removing storage from protection groups. c. Self-service provisioning to allow application tenants to provision DR protection using blueprints in Automation layer." 13. "The solution should offer: a. Application-agnostic protection eliminates the need for app-specific point solutions b. Automated orchestration of site failover and failback with a single-click reduces recovery times. c. Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives d. Centralized management of recovery plans from the virtualization manager console replacing the manual runbooks e. Planned migration workflow enables disaster avoidance and Data Centre mobility f. Reduce the DR footprint through hyper-converged, software defined storage infra g. VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage any discrete infra h. Support for array-based replication offers choice and options for replication with zero data loss." 14. "The solution should Map virtual machines to appropriate resources on the failover site a. Option to customize the shutdown of low-priority virtual machines at the failover site to get more resources or proper utilization of resources"" b. Option to recover multiple sites into a single shared recovery site c. Automatically stop replication between sites		

		and promotion of replicated storage for recovery. d. The solution should provide technology so that live migration of virtual machine disks would be supported between different storages and provide distributed resource scheduling of storage" 15. The solution should be storage-agnostic replication that supports use of low-end storage, including direct-attached storage and also provides host based replication which will replicate only changed blocks to increase network efficiency. 16. The solution should provide flexibility and choice through native integration with hypervisor/ VM based Replication, Virtual Volumes (vVols), and array-based replication solutions from all major storage partners. 17. The solution should provide automatic generation of history reports after the completion of workflows such as a recovery plan test and clean-up are performed in DR solution. These reports should document items such as the workflow name, execution times, successful operations, failures, and error messages which are useful for internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to HTML, XML, CSV, Microsoft Excel, Word document. 18. The Automated DC-DR replication and management solution should be licensed for minimum of 200 VMs or higher / unlimited number of VMs. 19. The solution should be able to provide minimum of 5 mins RTO & RPO. 20. OEM should provide direct support 24x7x365 with unlimited incident support (Telephonic, Web & Email) and 30mins or less response time including the unlimited upgrades and updates for a period of complete project.		
7.	Installation & Testing	1. Direct installation by OEM Professional as per the Scope of Work mentioned in the document 2. OEM has to provide the test cases as per the defined scope of work and demonstrate the required features during testing for successful		

		commissioning		
8.	Training & Certification	OEM has to provide on-site training on the Cloud & DC-DR replication, Network & Security minimum of 2 weeks for around 20 members along with certification exam coupons.		
9.	Support Subscription period	5 years complete 24x7 production support with 4 Hrs response - Unlimited updation for Patches and Bug fixes within support period, Unlimited upgradation of version within support period		

(iii) RedHat Virtual Data Centre Standard License for 5 years – for 4 Nodes

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	License	RedHat Enterprise Linux – Virtual Data Centre License (Open Source Operating System Software)		
2.	Type of License	Subscription		
3.	Licensing Option	Per Physical Server (2 Sockets each)		
4.	Type of Edition	Standard		
5.	Number of VMs or devices supported	Unlimited		
6.	Support Subscription period	5 years for complete support - Unlimited updation for Patches and Bug fixes within support period, Unlimited upgradation of version within support period		
7.	Generic Features	Support Native APIs, Support Non-Native APIs, Resource Access Control, Support for Multi-Tasking OS, Support for Multi user, Support Containers		

(iv) Microsoft Windows Server 2022 Data Centre Edition License for 5 years – for 4 Nodes

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	License	Microsoft Windows Server 2022 Data Centre License (Proprietary Operating System Software)		
2.	Type of License	Perpetual		
3.	Licensing Option	Per 2 Cores in the Server mention in (i)		
4.	Type of Edition	Data Centre		
5.	Number of VMs or devices	Unlimited		

	supported			
6.	Support Subscription period	5 years for complete support - Unlimited updation for Patches and Bug fixes within support period, Unlimited upgradation of version within support period		
7.	Generic Features	Real-time Operating System, High availability extension, Resilient Storage, Support for Containerization		

(v) NVMe Storage

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Connectivity/Port	1. Should support both FC and iSCSI from Day One. Storage shall have both FC & iSCSI Front end ports 2. Minimum of 8 Nos. of FC Ports of 32 Gbps or higher speed and 4 Nos. of 10/25 Gbps iSCSI ports expandable to 16 Nos. of FC and 8 Nos. of iSCSI 3. Back end ports min 4 Nos. of 12 Gbps SAS or higher 4. Min 2 FC / Ethernet of 10 Gbps or higher for dedicated remote replication ports		
2.	Controllers	1. 2 Nos. Number of Controllers/VSD/ Node available in the storage System on common back plane without using external switch/device OR without common backplane using switches 2. Controllers should be Active-Active HA mode from day one.		
3.	Data Replication	1. Should support both Synchronous and Asynchronous replication methods. Asynchronous replication has to be configured from day one. All replication licenses should be included for full capacity from day one.		
4.	Capacity, Disks & RAID configuration	1. Usable capacity of the Storage is 100 TB in RAID 5 (with not more than 8 disks in a group) without considering any DRR features like Dedup or Compression. The individual NVMe disk drive capacity should not be more than 16TB. 2. Storage should be expandable up to 1 PB. The usable capacity NVMe (with drives less than 16 TB) should be expandable to capacity up to 250		

		TB. 3. The offered drives should be Hot Pluggable. Additional Hot-spare drive should be supplied as per OEM recommendation in their standard deployment document. 4. Should support both SSD (SAS connector) and NVMe Disks 5. License for Snapshot included. 6. Automated Storage Tiering feature across the NVMe and SSD Drives types and all the required license has to be included. 7. The supplied disk (wear & tear) and data should be comprehensively covered under the warranty of Storage		
5.	Features	1. Data at rest Encryption should be hardware based either using self-encrypting drive or through specialized controllers. All required licenses for encryption should be included. 2. Software level or hardware level Deduplication & Compression without affecting more than 10% of the performance of the storage. All the required licenses should be included.		
6.	Form Factor & Power Supply	1. Form Factor 4 U max. The storage enclosures shall be mountable in a standard server Rack 42 U Racks. 2. The depth of storage should not be more than 1200 mm including cable management. 3. Dual Redundant Hot Swappable AC Power Supply		
7.	Performance & Availability	1. Data Availability min. 99.9999%. 2. Cache 384 GB per controller or Higher with Battery backup for Cache 3. The offered storage should be supplied with dual Active-Active controllers with no Single Point of Failure (SPoF) in any of the components. 4. The storage should deliver 200 K IOPS with latency less than 0.7 ms maximum from day one at a bandwidth of 4 GBps. 5. OEM has to demonstrate the IOPS, bandwidth and latency 6. No Single point of Failure with Non-Disruptive replacement of Hardware, The Storage provide Non-disruptive Firmware/Microcode upgrade.		

7.	Scope of supply installation & management	1. Storage should be supplied with 32 Gbps FC cables (i) 40 nos. of 20 metres length (ii) 40 nos of 10 metres length. 2. Installation should be performed directly by OEM as per the Scope of work document. 3. All the licenses have to be provided from day one. 4. Direct Web based management without any Server requirement. 5. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
8.	Training	1. OEM has to provide on-site training on the Storage, SAN Switch & DC-DR replication for minimum of 2 days along with certification.		
9.	Warranty & Support	1. The storage has to be monitored proactively by OEM and trouble tickets has to be raised & resolved automatically. 2. 24x7, 4 hours production support for Storage & Switch with 4hrs response & 24 hrs resolution for critical issues for 5 years including all the licenses. 3. Storage shall be supported for a period of min. 7 years directly by the OEM comprehensively including parts, labor & updates.		

(vi) SAN Switch

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Ports & bandwidth	1. Switch should have 48 FC ports or higher each port with min of 32 Gbps speed with autosensing & backward compatibility with 16 Gbps and 8 Gbps speed. 2. 24 FC ports should be populated, licensed and available from day one. 3. Supported port types U/E/F/M/D 4. 1.5 Tbps Aggregate Switch Bandwidth FC (end to end full duplex)		
2.	Form Factor & Power Supply	1. Form Factor 1 U max and shall be mountable in a standard server Rack 42 U Racks.		

		2. Front to back Airflow. 3. Dual Redundant Hot Swappable AC Power Supply		
3.	Scope of supply installation & management	1. Installation should be performed directly by OEM (Storage / SAN Switch) as per the scope of work document. 2. Direct Web based management without any Server requirement.		
4.	Warranty & Support	1. On Site Comprehensive Warranty of 5 years from the Storage OEM with production support (24x7 - 4 hours response) 2. The quoted model of SAN Switch should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(vii) SDN Solution – Network Leaf Switch - 48px10G-BASE-T, 4px40/100G

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Solution requirement	1. The Switch should support non-blocking Layer 2 switching and Layer 3 routing. 2. Switch should support the complete STACK of IPv4 and IPv6 services. 3. The Switch used have the capability to function in line rate for all ports		
2.	Hardware and Interface Requirement	1. Switch should have the following interfaces: a. Min. 48p x 10 Gbps or higher baseT (All 10G Copper port switches) b. Min. 4p x 40/100 Gbps or higher ports which supports QSFP / QSFP28 transceivers on all ports, populated with 4 Nos. of QSFP28-SRBD compatible Dual Rate 40G / 100G (supporting 100m LC distance on OM4 MMF) c. Switch should have console port for local management & Out of band management interface for remote management 2. Switch should be 1 RU fixed form factor 3. Switch should be rack mountable and support side rails, if required. 4. Switch should be provided with redundant power supply units		
3.	Performance requirement	1. Switch should support dedicated process for each routing protocol 2. Switch should re-converge all dynamic routing		

		protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, BGP. 3. Switch should support minimum 256 VRF instances with route leaking functionality 4. The switch should support min 350k IPv4 LPM routes 5. The switch should have MAC Address table size of 200k 6. The switch should support 8K multicast routes 7. Switch should support 4000 VLANs 8. Switch should support minimum 64 ECMP paths 9. Switch should support minimum 3 Tbps of switching throughput 10. The Switch should support intelligent buffer management with a minimum buffer of 32MB.		
4.	Network Virtualization Features	1. Switch should support VXLAN to achieve Network Virtualization using Virtual Over Lay Network. 2. Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the Data Centre		
5.	Layer 2 Features	1. Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) 2. Switch should support VLAN Trunking (802.1q) 3. Switch should support minimum 200k of MAC addresses 4. Switch should support VLAN tagging (IEEE 802.1q) 5. Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy 6. Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures 7. Switch should support layer 2 extension over VXLAN across all Data Centers to enable VM mobility & availability 8. The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN). 9. The switch should support Minimum 48 number of port channels 10. A port channel should support up to 32 no. of ports		

		11. The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane		
6.	Layer 3 Features	1. Switch should support static and dynamic routing 2. Switch should support VRF route leaking functionality from day 1 3. Switch should support VRF, VRF Edge, Virtual Routing to achieve multi instance routing 4. Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP), IGMP v1, v2 and v3		
7.	Quality of Service	1. Switch should support 802.1P classification and marking of packet using CoS (Class of Service) and DSCP (Differentiated Services Code Point) 2. Switch should support different type of QoS features for real time traffic differential treatment using Weighted Random Early Detection and Strict Priority Queuing. 3. Switch should support Rate Limiting - Policing and/or Shaping 4. Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
8.	Security	1. Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy 2. Switch should support external database for AAA using TACACS+ and RADIUS 3. Switch should support to restrict end hosts in the network in order to secure the port by limiting the number of learned MAC addresses to avoid MAC address flooding. 4. VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware 5. Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined 6. Switch should support DHCP Snooping 7. Switch should support Dynamic ARP Inspection or equivalent feature to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol 8. Switch should support IP Source Guard to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN 9. Switch should support unicast and multicast		

		blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 10. Switch support broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities. 11. The Switch should support LLDP. 12. Switch should support Spanning tree BPDU protection		
9.	Manageability	1. Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail 2. Switch should provide remote login for administration using SSHv2 3. Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures 4. Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN/Remote SPAN on physical, Port channel, VLAN interfaces 5. Switch should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 6. Switch should provide different privileges for login in to the system for monitoring and management 7. Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose. 8. The Switch Should support monitor events and take corrective action like a script when the monitored events occur. 9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end) 10. Should support software telemetry - a. Utilization of MAC table, Route table b. Hardware resources like interface utilization, BW utilization		

		c. Switch environment like CPU, memory, FAN and Power Supply unit d. Interface statistics like CRC errors etc.		
10.	Availability	1. Switch should have provision for connecting to 1:1/N+1 power supply for usage and redundancy 2. Switch should provide gateway level of redundancy IPV4 and IPV6 using HSRP/VRRP 3. Switch should support for BFD For Fast Failure Detection		
11.	General requirements	1. Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. 2. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 3. All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 4. All relevant licenses for all the features and scale should be quoted along with switch 5. Visibility & Automation: All Network switches should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring		
12.	Scope of supply installation & management	1. Installation should be performed directly by OEM as per the Scope of work document. 2. All the licenses have to be provided from day one. 3. Direct Web based management without any Server requirement. 4. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
13.	Training	1. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20 members along with certification exam coupons.		

14.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(viii) SDN Solution – Network Leaf Switch - 48px10G (Fibre / Copper), 4px40/100G

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Solution requirement	1. The Switch should support non-blocking Layer 2 switching and Layer 3 routing. 2. Switch should support the complete STACK of IPv4 and IPv6 services. 3. The Switch used have the capability to function in line rate for all ports		
2.	Hardware and Interface Requirement	1. Switch should have the following interfaces: a. Min. 48p x 10/25 Gbps or higher SFP ports which should support SFP+, SFP28 transceivers on all ports and SFP+10GBASE-T on at least 12 ports. The switch should be populated with 24 Nos. of SFP+ ports and 10 Nos. of SFP+10GBASE-T ports from day one. (Interoperable 10G – Fibre & Copper port switches). b. Min. 4p x 40/100 Gbps or higher ports which supports QSFP / QSFP28 transceivers on all ports, populated with 4 Nos. of QSFP28-SRBD compatible Dual Rate 40G / 100G (supporting 100m LC distance on OM4 MMF) c. Switch should have console port for local management & Out of band management interface for remote management 2. Switch should be 1 RU fixed form factor 3. Switch should be rack mountable and support side rails, if required. 4. Switch should be provided with redundant power supply units		
3.	Performance requirement	1. Switch should support dedicated process for each routing protocol 2. Switch should re-converge all dynamic routing protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, BGP. 3. Switch should support minimum 256 VRF instances with route leaking functionality		

		4. The switch should support min 350k IPv4 LPM routes 5. The switch should have MAC Address table size of 200k 6. The switch should support 8K multicast routes 7. Switch should support 4000 VLANs 8. Switch should support minimum 64 ECMP paths 9. Switch should support minimum 3 Tbps of switching throughput 10. The Switch should support intelligent buffer management with a minimum buffer of 32MB.		
4.	Network Virtualization Features	1. Switch should support VXLAN to achieve Network Virtualization using Virtual Over Lay Network. 2. Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the Data Centre		
5.	Layer 2 Features	1. Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) 2. Switch should support VLAN Trunking (802.1q) 3. Switch should support minimum 200k of MAC addresses 4. Switch should support VLAN tagging (IEEE 802.1q) 5. Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy 6. Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures 7. Switch should support layer 2 extension over VXLAN across all Data Centers to enable VM mobility & availability 8. The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN). 9. The switch should support Minimum 48 number of port channels 10. A port channel should support up to 32 no. of ports 11. The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane		

6.	Layer 3 Features	1. Switch should support static and dynamic routing 2. Switch should support VRF route leaking functionality from day 1 3. Switch should support VRF, VRF Edge, Virtual Routing to achieve multi instance routing 4. Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP), IGMP v1, v2 and v3		
7.	Quality of Service	1. Switch should support 802.1P classification and marking of packet using CoS (Class of Service) and DSCP (Differentiated Services Code Point) 2. Switch should support different type of QoS features for real time traffic differential treatment using Weighted Random Early Detection and Strict Priority Queuing. 3. Switch should support Rate Limiting - Policing and/or Shaping 4. Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
8.	Security	1. Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy 2. Switch should support external database for AAA using TACACS+ and RADIUS 3. Switch should support to restrict end hosts in the network in order to secure the port by limiting the number of learned MAC addresses to avoid MAC address flooding. 4. VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware 5. Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined 6. Switch should support DHCP Snooping 7. Switch should support Dynamic ARP Inspection or equivalent feature to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol 8. Switch should support IP Source Guard to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN 9. Switch should support unicast and multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port.		

		10. Switch support broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities. 11. The Switch should support LLDP. 12. Switch should support Spanning tree BPDU protection		
9.	Manageability	1. Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail 2. Switch should provide remote login for administration using SSHv2 3. Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures 4. Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN/Remote SPAN on physical, Port channel, VLAN interfaces 5. Switch should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 6. Switch should provide different privileges for login in to the system for monitoring and management 7. Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose. 8. The Switch Should support monitor events and take corrective action like a script when the monitored events occur. 9. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end) 10. Should support software telemetry - a. Utilization of MAC table, Route table b. Hardware resources like interface utilization, BW utilization c. Switch environment like CPU, memory, FAN and Power Supply unit		

		d. Interface statistics like CRC errors etc.		
10.	Availability	1. Switch should have provision for connecting to 1:1/N+1 power supply for usage and redundancy 2. Switch should provide gateway level of redundancy IPV4 and IPV6 using HSRP/VRRP 3. Switch should support for BFD For Fast Failure Detection		
11.	General requirements	1. Console cable and power cable (for standard Rack PDU) as per customer requirement to be provided. All Cables shall be factory-terminated. 2. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 3. All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 4. All relevant licenses for all the features and scale should be quoted along with switch 5. Visibility & Automation: All Network switches should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring		
12.	Scope of supply installation & management	1. Installation should be performed directly by OEM as per the Scope of work document. 2. All the licenses have to be provided from day one. 3. Direct Web based management without any Server requirement. 4. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
13.	Training	1. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20 members along with certification exam coupons.		
14.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(ix) SDN Solution – Network Spine Switch - 48px40/100G

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	General requirement	1. The Switch should support non-blocking architecture, all proposed ports must provide wire speed line rate performance 2. Switch should support the complete STACK of IPV4 and IPV6 services. 3. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 4. Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. 5. All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 6. Visibility & Automation: All Network switches should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 7. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring 8. All relevant licenses for all the features and scale should be quoted along with switch and all these licenses and features should be available from Day 1.		
2.	Hardware and Interface Requirement	1. Switch should have the following interfaces: a. Min. 48p x 40/100 Gbps or higher non-blocking ports which supports QSFP / QSFP28 transceivers on all ports, populated with 48 Nos. of QSFP28-SRBD compatible Dual Rate 40G / 100G (supporting 100m LC distance on OM4 MMF) b. Switch should have console port for local management & Out of band management interface for remote management 2. Switch should be 1 RU fixed form factor 3. Switch should be rack mountable and support side rails, if required. 4. Switch should have adequate power supplies for the complete system usage and providing N+1 power supply redundancy		
3.	Performance	1. Switch should support minimum 256 VRF		

	requirement	instances with route leaking functionality 2. The switch should support min 400k IPv4 LPM routes 3. The switch should support 8K multicast routes 4. Switch should support minimum 12 Tbps of switching throughput 5. The switch proposed should have minimum 60 MB Packet Buffer		
4.	Network Virtualization Features	1. Switch should support VXLAN to achieve Network Virtualization using Virtual Over Lay Network. 2. Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the Data Centre		
5.	Layer 2 Features	1. Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) 2. Switch should support VLAN Trunking (802.1q) 3. Switch should support minimum 90k of MAC addresses 4. Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy 5. Switch should support layer 2 extension over VXLAN across all Data Centers to enable VM mobility & availability 6. The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane		
6.	Layer 3 Features	1. Switch should support static and dynamic routing 2. Switch should support VRF route leaking functionality from day 1 3. Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) 4. Switch should support Multicast routing		
7.	Quality of Service	1. Switch should support 802.1P classification and marking of packet using CoS (Class of Service) and DSCP (Differentiated Services Code Point) 2. Switch should support different type of QoS features for real time traffic differential treatment using Weighted Random Early Detection and Strict Priority Queuing. 3. Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		

8.	Security	1. Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy 2. Switch should support external database for AAA using TACACS+ and RADIUS 3. Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined		
9.	Manageability	1. Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail 2. Switch should provide remote login for administration using SSHv2 3. Switch should support management and monitoring status using different type of Industry standard NMS using SNMP v3 with Encryption. 4. Switch should provide different privileges for login in to the system for monitoring and management 5. Should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop c. Per Flow latency (per switch and end to end) 6. Should support software telemetry - a. Utilization of MAC table, Route table b. Hardware resources like interface utilization, BW utilization c. Switch environment like CPU, memory, FAN and Power Supply unit d. Interface statistics like CRC errors etc.		
10.	Scope of supply installation & management	1. Installation should be performed directly by OEM as per the Scope of work document. 2. All the licenses have to be provided from day one. 3. Direct Web based management without any Server requirement. 4. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
11.	Training	1. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20		

		members along with certification exam coupons.		
12.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(x) SDN Solution – Network Access / Management Switch - 48px1G (BaseT), 4px10G (BaseT)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Solution requirement	1. The Switch should support non-blocking Layer 2 switching and Layer 3 routing. 2. Switch should support the complete STACK of IPv4 and IPv6 services. 3. The Switch used have the capability to function in line rate for all ports		
2.	Hardware and Interface Requirement	1. Switch should have the following interfaces: a. Min. 48p x 1 Gbps or higher baseT (All 1G Copper port switch) b. Min. 4p x 10 Gbps or higher ports which supports SFP / SFP+ transceivers on all ports, populated with 4 Nos. of SFP+10GBASE-T c. Switch should have console port for local management & Out of band management interface for remote management 2. Switch should be 1 RU fixed form factor 3. Switch should be rack mountable and support side rails, if required. 4. Switch should be provided with redundant power supply units and redundant fans		
3.	Performance requirement	1. Switch should support minimum 176 gbps of switching capacity 2. Switch should support stacking / MLAG 3. Switch should have forwarding rate of minimum 130 Mpps. 4. Switch should support 4000 VLANs		
4.	Layer 2 Features	1. Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) 2. Switch should support VLAN Trunking (802.1q) 3. Switch should support minimum 64k of MAC addresses 4. Switch should support VLAN tagging (IEEE 802.1q)		

		5. Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy 6. Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures 7. Switch should support layer 2 extension over VXLAN across all Data Centers to enable VM mobility & availability		
5.	Quality of Service	1. Switch should support 802.1P classification and marking of packet using CoS (Class of Service) and DSCP (Differentiated Services Code Point) 2. Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy		
6.	Security	1. Switch should have all security for Secure Shell (SSH) Protocol, HTTPS and DoS protection 2. Switch should be capable of features like static route, RIP, OSPF, ECMP, PIM-SM, should support policy-based routing 3. Switch should support DHCP Snooping 4. Switch should support Dynamic ARP Inspection or equivalent feature to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol 5. Switch should support external database for AAA using TACACS+ and RADIUS 6. Switch should support to restrict end hosts in the network in order to secure the port by limiting the number of learned MAC addresses to avoid MAC address flooding. 7. VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware 8. Switch should support Role Based access control (RBAC) for restricting host level network access as per policy defined 9. Switch should support IP Source Guard to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN 10. Switch should support unicast and multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 11. Switch support broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network		

		attacks and vulnerabilities. 12. The Switch should support LLDP. 13. Switch should support Spanning tree BPDU protection 14. Switch should support MAC address based filters / access control lists (ACLs) on all switch ports. 15. Switch should support Port as well as VLAN based Filters / ACLs. 16. Switch should Support Ipv6 First hop Security with the following functions: IPv6 snooping, neighbor discovery protocol (NDP) address gleaning, IPv6 data address gleaning, IPv6 dynamic host configuration protocol (DHCP) address gleaning, IPv6 DHCP guard or equivalent feature, IPv6 router advertisement (RA) guard or equivalent feature		
7.	Manageability	1. Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail 2. Switch should provide remote login for administration using SSHv2 3. Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures 4. Switch must have Switched Port Analyzer (SPAN) and ERSPAN/Remote SPAN on physical, Port channel, VLAN interfaces 5. Switch should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 6. Switch should provide different privileges for login in to the system for monitoring and management 7. Support for Unidirectional Link Detection Protocol (UDLD) or equivalent to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces 8. Layer 2 trace route eases troubleshooting by identifying the physical path that a packet takes from source to destination. 9. Switch should support hardware telemetry without impacting performance of the switch and without adding overload on the resources like CPU and Memory. a. Flow path trace (ingress to egress switch) b. Per Flow Hop by Hop packet drop with reason of drop		

		c. Per Flow latency (per switch and end to end) 10. Should support software telemetry - a. Utilization of MAC table, Route table b. Hardware resources like interface utilization, BW utilization c. Switch environment like CPU, memory, FAN and Power Supply unit d. Interface statistics like CRC errors etc.		
8.	General requirements	1. Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. 2. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 3. All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 4. All relevant licenses for all the features and scale should be quoted along with switch 5. Visibility & Automation: All Network switches should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring		
9.	Scope of supply installation & management	1. Installation should be performed directly by OEM as per the Scope of work document. 2. All the licenses have to be provided from day one. 3. Direct Web based management without any Server requirement. 4. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
10.	Training	1. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20 members along with certification exam coupons.		
11.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(xi) Router (2x10G, 4x1G)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Hardware and Interface Requirement	1. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 2p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ / SFP+10GBASE-T transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 2p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management 2. All the ports should be in compliance with 802.3 standards 3. Router should be 1 RU fixed form factor 4. Router should be rack mountable and support side rails, if required. 5. Router should be provided with redundant power supply units and redundant fans		
2.	Performance requirement	1. The Device must support minimum 128 concurrent IPsec tunnel with AES 256 encryption expandable to 256 tunnels in future. 2. Device should include a minimum 2 Gbps IPsec throughput 3. Device should support minimum 10 Gbps IPv4 forwarding throughput. 4. Device should support minimum 5 Gbps IPv4 encrypted throughput. 5. Device should support minimum 4 million IPv4 & 4Million IPv6 routes. 6. Device should be able to handle full internet routing table prefixes over BGP from at least 3 ISPs without any performance issues.		

		7. Device should have min. of 8 GB of DRAM and 8 GB of Flash memory. 8. From day one the Device should support termination of MPLS as well as Internet links (in future if needed) and must be able to use both the links for traffic. Any failure of a link must result in steering traffic on another link without any manual intervention. 9. Hardware should be able to work as traditional router and capable of upgrading to SDWAN router. 10. All required licenses should be provided from Day 1.		
3.	Encapsulation	1. Generic Routing Encapsulation; 802.1q VLAN;		
4.	Security	1. AES-128, or AES-256 Encryption 2. Device should support port ACL with L3 and L4 parameters 3. Switch should have all security for Secure Shell (SSH) Protocol, HTTPS and DoS protection 4. Switch should support external database for AAA using TACACS+ and RADIUS		
5.	Networking and Routing	1. System should be able to support LLDP, BFD, VRRP/HSRP, VRF/Multi-VRF, MPLS-L3VPN, VXLAN+EVPN overlay technology, DHCP. 2. Device Should support Static NAT, Dynamic NAT, NAPT 3. System should be able to support IPv6 and IPv4 routing protocols like, BGP, OSPF and Static routing. 4. should support port based DOS protection (PDP) 5. Should support ACL based QoS Classification, Prioritization, DSCP remarking, shaping, scheduling, rate limiting function like policing and shaping. 6. Proposed router should support SD-WAN functionality as well without changing the hardware in the setup. 7. Device should be able to support PIM SM across SD-WAN, PIM SM with neighbor support on LAN and WAN interfaces, PIM SSM, PIM SM Bootstrap RP, PIM Rendezvous- Point, IGMP v2/v3		
6.	Manageability	1. Device should support for sending logs to multiple centralized syslog server for monitoring and audit trail 2. Device should provide remote login for administration using SSHv2		

		3. Device should support for capturing packets using local and remote port mirroring for packet captures 4. Device should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 5. Device should provide different privileges for login in to the system for monitoring and management 6. Support for Unidirectional Link Detection Protocol (UDLD) or equivalent to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces		
8.	General requirements	1. Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. 2. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 3. All Functionalities of Router shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 4. All relevant licenses for all the features and scale should be quoted along with switch 5. Visibility & Automation: All Network switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 6. All Network switches and routers should be able to be managed from Single Dashboard for ease of Management and Monitoring		
9.	Scope of supply installation & management	1. Installation should be performed directly by OEM as per the Scope of work document. 2. Configuration of existing WAN links with eBGP configurations and iBGP configuration for DC-DR connectivity. 3. Establishing VXLAN / EVPN overlay network between DC & DR. 4. Router should be configured in HA mode with Active-Active configurations. 5. All the licenses have to be provided from day one. 6. Direct Web based management without any Server requirement. 7. Commissioning & integration together with all necessary software to make the system fully		

		functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
10.	Training	1. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20 members along with certification exam coupons.		
11.	Warranty	1. 5 Years, 24 x 7, 4 Hrs Onsite Response 2. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(xii) Router (4x10G, 4x1G)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Hardware and Interface Requirement	4. Router should have the following interfaces: a. Min. 4p x 1 Gbps or higher which supports SFP / SFP-BASET transceivers on all ports, populated with 4 Nos. of SFP. Also supply 2 Nos. of SFP-BASET for interoperability of existing copper links. b. Min. 4p x 10 Gbps or higher ports which supports SFP / SFP-BASET / SFP+ / SFP+10GBASE-T transceivers on all ports, populated with 2 Nos. of SFP+ c. Router should have additional interface modules / slot support for future expansion of Min. 4p x 10 Gbps or higher ports or Min. 4p x 1 Gbps or higher d. All the ports mentioned in S.N. a, b & c should be WAN ports e. Router should have 1x RJ45 console port for management 5. All the ports should be in compliance with 802.3 standards 6. Router should be 1 RU fixed form factor 7. Router should be rack mountable and support side rails, if required. 8. Router should be provided with redundant power supply units and redundant fans		

2.	Performance requirement	5. The Device must support minimum 128 concurrent IPsec tunnel with AES 256 encryption expandable to 256 tunnels in future. 6. Device should include a minimum 2 Gbps IPsec throughput 7. Device should support minimum 10 Gbps IPv4 forwarding throughput. 8. Device should support minimum 5 Gbps IPv4 encrypted throughput. 9. Device should support minimum 4 million IPv4 & 4Million IPv6 routes. 10. Device should be able to handle full internet routing table prefixes over BGP from at least 3 ISPs without any performance issues. 11. Device should have min. of 8 GB of DRAM and 8 GB of Flash memory. 12. From day one the Device should support termination of MPLS as well as Internet links (in future if needed) and must be able to use both the links for traffic. Any failure of a link must result in steering traffic on another link without any manual intervention. 13. Hardware should be able to work as traditional router and capable of upgrading to SDWAN router. 14. All required licenses should be provided from Day 1.		
3.	Encapsulation	5. Generic Routing Encapsulation; 802.1q VLAN;		
4.	Security	8. AES-128, or AES-256 Encryption 9. Device should support port ACL with L3 and L4 parameters 10. Switch should have all security for Secure Shell (SSH) Protocol, HTTPS and DoS protection 11. Switch should support external database for AAA using TACACS+ and RADIUS		
5.	Networking and Routing	3. System should be able to support LLDP, BFD, VRRP/HSRP, VRF/Multi-VRF, MPLS-L3VPN, VXLAN+EVPN overlay technology, DHCP. 4. Device Should support Static NAT, Dynamic NAT, NAPT 5. System should be able to support IPv6 and IPv4 routing protocols like, BGP, OSPF and Static routing. 6. should support port based DOS protection (PDP) 7. Should support ACL based QoS Classification,		

		Prioritization, DSCP remarking, shaping, scheduling, rate limiting function like policing and shaping. 8. Proposed router should support SD-WAN functionality as well without changing the hardware in the setup. 9. Device should be able to support PIM SM across SD-WAN, PIM SM with neighbor support on LAN and WAN interfaces, PIM SSM, PIM SM Bootstrap RP, PIM Rendezvous- Point, IGMP v2/v3		
6.	Manageability	11. Device should support for sending logs to multiple centralized syslog server for monitoring and audit trail 12. Device should provide remote login for administration using SSHv2 13. Device should support for capturing packets using local and remote port mirroring for packet captures 14. Device should support management and monitoring status using different type of Industry standard NMS using SNMP v1 and v2, SNMP v3 with Encryption. 15. Device should provide different privileges for login in to the system for monitoring and management 16. Support for Unidirectional Link Detection Protocol (UDLD) or equivalent to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces		
8.	General requirements	7. Console cable and power cable (As per Indian standards) as per customer requirement to be provided. All Cables shall be factory-terminated. 8. 2 m Fibre / Copper factory terminated Patch Cords for all the respective populated ports to be supplied. 9. All Functionalities of Router shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software. 10. All relevant licenses for all the features and scale should be quoted along with switch 11. Visibility & Automation: All Network switches & routers should be from same OEM and should be provided along with software for unified monitoring, provisioning and telemetry solution. The solution should be compatible and integrated with the proposed cloud solution. 12. All Network switches and routers should be able		

		to be managed from Single Dashboard for ease of Management and Monitoring		
9.	Scope of supply installation & management	5. Installation should be performed directly by OEM as per the Scope of work document. 6. Configuration of existing WAN links with eBGP configurations and iBGP configuration for DC-DR connectivity. 7. Establishing VXLAN / EVPN overlay network between DC & DR. 8. Router should be configured in HA mode with Active-Active configurations. 9. All the licenses have to be provided from day one. 10. Direct Web based management without any Server requirement. 11. Commissioning & integration together with all necessary software to make the system fully functional as intended. All features and performance parameters has to configured and demonstrated by OEM during installation.		
10.	Training	2. OEM has to provide on-site training on the SDN Controller, Visibility / Observability, NMS, Network & Security configurations of Switches & routers, minimum of 2 weeks for around 20 members along with certification exam coupons.		
11.	Warranty	3. 5 Years, 24 x 7, 4 Hrs Onsite Response 4. All Network Switches & Routers quoted Models should have support life of 10 years minimum from the Date of delivery at Site, same need to be confirmed in signed MAF		

(xiii) EDR Solution (Servers)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Management Console	1. The proposed solution must support on-premises deployment (within CDAC Datacenter) for highly regulated environments for Servers. 2. The proposed solution should provide prevention capability across all major Server Operating Systems – Windows & Linux. 3. The proposed solution shall provide Advanced Malware Protection capability on safeguarding of file-less attacks such as web-borne attacks, malicious adobe		

		and office document, zero days attacks, file-less and non persistent malware, ransomware and Trojans. 4. The proposed solution shall provide Endpoint detection and response capability to detect security incident, contain security incident, investigate security incident and provide remediation (whenever possible). 5. The proposed solution shall be a single unified agent to co-exist with the existing endpoint protection on servers. 6. The proposed solution shall be a signatureless solution and does not rely on daily signature updates. 7. The proposed solution shall provide anti-tampering mechanism on, but not limited to the agent, preventing any unauthorized shutdown, modification, corruption or shutdown. 8. The proposed solution should support multi-site configuration and multi-tenancy without any additional cost. 9. The proposed solution should have Policy inheritance from Top to bottom (like parent/child, group/sub-group, site/group, etc) with the ability to inheritance if needed and should also provide the flexibility to have individual policies for every group. 10. The proposed solution should have Integrated KB/documentation into the management console without requiring logging in to another system / URL. 11. The proposed solution should support role based access control (RBAC) 12. The proposed solution should support two factor or single sign on solutions for the management console and sensitive functions such as remote shell. 13. The proposed solution should have capability of centralized auditing and logging of activity should be maintained in the management console. 14. The proposed solution should have capability logged and audited the		

		management activity ,with the ability to send logs to an external source (like SIEM etc.) 15. The solution must be capable of managing endpoints . The bidder must ensure that hardware/software required at the central console can scale to onboard additional endpoints at any time with proposed Configuration and standard. 16. Solutions features must be fully compatible over IPv4/IPv6 network such as hardware, software and application software etc. 17. The solution should provide API access to all management capabilities and access to data. API should be well documented and available without any additional cost and application and hardware. The solution should have ability to quickly run APIs on the console data set without any limitations. 18. Solution must provide non-repudiable Centralized auditing and logging of activity through the management console. Management activity must be logged and audited with the ability to send logs to an external source without restrictions. 19. Solution must provide multi-factor authentication and single sign on solutions for the management console and sensitive functions such as remote shell.		
2.	Operating System Support	1. The proposed solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life. 2. The Solution should include the Server Security Solution or any other Cloud workload solution for Physical /Virtual Servers 3. The proposed solution should support all the latest versions of windows but not limited to: Windows Server Core 2012, 2016, 2019		

		& 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 4. "The proposed solution should support all the latest Linux platforms but not limited to: CentOS (6,7,8) Debian Fedora Ubuntu (16,18,20,22) Red Hat Enterprise Linux (RHEL-6,7,8,9) Oracle SUSE Linux Enterprise Server 5. The Solution should support all the latest virtual environments. Agent support for the following virtual environments: Citrix XenServer Microsoft Hyper-V VMware Horizon VMware vSphere VMware Workstation" 6. The proposed solution should support all the new OS Updates/Versions within 60 days of release.		
3.	Agent Features	1. EPP and EDR capabilities should be available in a single agent without requiring multiple software packages to be installed. 2. The agent must have strong anti-tamper capabilities, ensuring that an end user even with local admin credentials cannot remove, disable or modify the agent. 3. The proposed Solution should have ability to trigger/schedule on-demand scans (from console and /or endpoint) to look for malware, or ensure a threat has been remediated. 4. The proposed solution must have ability to schedule agent upgrades from the management console.		

		5. The proposed solution must have ability to upgrade agents with no impact to the end user. 6. The proposed solution should not stop functioning if license count is exceeded. 7. The proposed solution should automatically remove old agents from console, if agent haven't communicated to the management console for a configurable period of time. 8. The proposed solution should have lightweight agent with minimal system resource utilization for standard system usage (1-2% CPU, <250Mb of memory). 9. The proposed solution must have capability to uninstall agents remotely from the management console directly or through script. 10. The proposed solution should have capability to temporarily disable agent via the management console for temporary troubleshooting or testing. 11. The proposed solution agents should have ability to communicate with Management Console via a web-proxy. 12. The proposed solution should provide ability to send notification messages to the end user computer.		
4.	Threat Prevention	1. The proposed solution should provide prevention capability across Windows & Linux OS. 2. The proposed solution shall support both preventive Static AI and Behavioral AI engines that protects from (unknown) malicious files and malicious activities in real time whether endpoint is online or offline. 3. The proposed solution must provide protection against known and unknown malware. 4. The proposed solution must ensure that files are checked for any infection on read, write and execute operations. 5. The proposed solution must be effective against Zero-Day Attacks by Analyzing		

		Behaviors on an endpoint, along with signature based approach. 6. The proposed solution should have capacity to detect dormant threats. 7. The proposed solution should leverage Artificial Intelligence (AI) or Machine Learning (ML) to analyze files pre-execution & behaviors while a file is running. 8. The proposed solution should protect from malicious scripts and documents. 9. The proposed solution should monitor and protect from lateral movement & insider threats, exploits and file-less attacks. 10. The proposed solution should identify and block potentially unwanted programs on the systems. 11. The proposed solution should provide the flexibility to safely download malicious or convicted file from the management console 12. The proposed solution must have ability to correlate alerts together automatically if related to the same attack. 13. The proposed solution must be capable of detecting evasive patterns or behaviors. 14. The proposed solution must support detection of zero-day malicious file/file-less attacks, ransomware attacks and adopt behavioral analysis/intelligence in carrying out detection, remediation and or reversal to the known good state of an endpoint in the event of a ransomware infection/attack. 15. The proposed solution shall provide protection against malicious DLL files. 16. The proposed solution shall provide anti-ransomware capability. 17. The proposed solution shall support protection against the execution of malicious executables. 18. The proposed solution shall use signature-less algorithm to prevent malware.		

		19. The proposed solution shall have capability to prevent unknown or zero-day malware when the endpoint is not connected to management center. 20. The proposed solution shall have the capability to prevent unknown file or application through restriction policy. 21. The proposed solution shall have the capability to quarantine unknown and zero-day malware. 22. The proposed solution should be driven by patented behavioral AI technology, ensuring robust security measures. Importantly, the solution operates continuously without the need for an internet connection, ensuring constant protection even in offline. 23. The proposed solution must have the capability to quarantine the malicious application/ program/ file automatically without quarantining the entire Server from the network. 24. The proposed solution shall provide prevention against exploit that attack the operating system kernel through kernel privilege escalation. 25. The proposed solution shall prevent attacks which change the execution order of a process by redirecting an asynchronous procedure call (APC) to point to the attacker's malicious shellcode. 26. The proposed solution shall be able to provide real-time prevention against exploits of application vulnerabilities by blocking through core exploit techniques not limited to Software Logic Flaws, Memory Corruptions, code execution, DLL Hijacking, etc. 27. The proposed solution must be able to protect the systems without knowing the CVE numbers. 28. The proposed solution shall prevent zero-day or undiscovered exploits of any application vulnerabilities by blocking core exploits techniques		

		29. The proposed solution should provide the capability to perform exploit monitoring and prevention based on core exploit techniques without requiring a connection to the Management Server and/or Cloud Service and without relying on signatures. 30. The proposed solution shall utilize core exploit technique to prevent or block. The exploit technique modules can be applied to known and popular applications as well as authorized unknown or in-house developed applications. 31. The proposed solution should by default group all related alerts together 32. The proposed solution should provide a visual process tree browser 33. The proposed solution should provide the flexibility to mark an entire group of events as a threat and take response or remediation actions accordingly 34. The proposed solution should have option to search for MITRE ATT&CK Indicators based on a) Initial Access b) Credential Access c) Discovery d) Lateral Movement e) Collection f) Command & Control g) Exfiltration h) Impact i) Indicators		
5.	Response & Remediation Capabilities	1. The proposed solution should support full remote shell for all OS (Windows, Linux & Mac) and not limited or restricted to set of commands. 2. The proposed solution should track all remote shell commands and logged during a remote shell session. 3. The proposed solution should alert on both suspicious and malicious threat behaviour		

		4. The proposed solution should have ability to kill and quarantine an offending process. 5. The proposed solution should be able to unquarantine a file from the management interface or API. 6. The proposed solution should have the ability to remediate all operating system changes and perform corrective action in machine speed. The solution should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc. 7. The proposed solution should reverse destructive data event but not limited to ransomware. The solution should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state. 8. The proposed solution should provide option to network quarantine a device and provide flexibility to configure the same. 9. The proposed solution should have automated threat response capabilities. 10. The proposed solution should have capability to take the remediation actions on multiple systems or events at once 11. The proposed solution should have ability for an analyst to add notes/comments to an event 12. The proposed solution should have options to set the status of an issue or event (i.e. resolved, in progress, unresolved)		
6.	Policy & Installation	1. The proposed solution should provide ability to support policy inheritance across the endpoints. 2. The proposed solution should have the option to provide dynamic policy assignment based on device attributes 3. The proposed solution should have capabilty to place the installed devices directly into a specific device group at the time of installation		

		4. The proposed solution policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines). 5. The proposed solution policy modifications should be applied in near real time. 6. The proposed solution should have the ability to remediate all operating system changes made on servers and perform corrective action in machine speed. Tool should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc. 7. The proposed solution should have full remote shell capabilities on all major Sever platforms, including Windows, Kubernetes and Linux. These capabilities empower security teams with a fast and efficient method to investigate attacks, gather forensic data, and remediate breaches, regardless of the geographical location of the compromised endpoints. 8. Solution should support a full remote shell for all OS (Windows & Linux) and not limit or restrict to set of commands. 9. The proposed solution should reverse destructive data event including but not limited to ransomware,The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state 10. The proposed solution should provide option to network quarantine a device and provide flexibility to configure the same. 11. The proposed solution should have automated threat response capabilities. 12. The proposed solution should have ability for an analyst to add notes/comments to an event 13. The proposed solution should have options to set the status of an issue or event (i.e. resolved, in progress, unresolved) 14. The proposed solution shall be able to		

		easily identify root cause of security event. The Root cause analysis must simplifies investigations for the team by identifying the sequence of events and root cause of alerts. 15. The proposed solution shall provide Powerful search tools that simplify threat hunting with intuitive queries 16. The proposed solution shall support static (Hash, IP, Domain) and dynamic behavior (Attack Pattern) IOCs 17. The proposed solution shall be able to upload the hash of any suspected malicious packages to an analysis farm like Virus Total. 18. The proposed solution shall has the capability to show the suspicious file was loaded or launched by which parent processes 19. The proposed solution shall not limit to only endpoint but also able to show and correlate network data. 20. The proposed solution shall has capability to blacklist / block suspicious file 21. The proposed solution shall be able to detect the following behavior but not limited to Command and Control, Reconnaissance and Lateral Movement. 22. The proposed solution shall be able to detect file less attack and script base attack without using signatures and automatically kill the process based on policy settings. 23. The proposed solution shall be able to provide the visualization flow of the chain of events. It must include processes in the chain that happen before the malicious process 24. The proposed solution shall have remediation capabilities to repair the end point by removing unwanted artifact (such as temp files, registry keys or folders) manually or automatically.		
7.	Exclusions	1. The proposed solution should have predefined list of known or		

		recommended exclusions 2. The proposed solution must provide Path execution capability with option to selected Exclusion Mode (Suppress Alerts, Interoperability, or Performance Focus) applies to files in the path 3. The proposed solution should include workflows to easily exclude false positives 4. The proposed solution should provide the option for administrators to make policy exclusions of the console at multiple levels (account, group). 5. In the solution, exclusions should be configurable by the administrator to handle performance issues down to specific paths or single executables by disabling monitoring of parent processes and/or parent processes and all of their spawned child processes		
8.	Device Control and Application Visibility	1. The proposed solution must have Device Control capabilities. 2. The proposed solution Device Control should support block, read only and allow read-write on USB /Bluetooth. 3. The proposed solution should have granular device control capability which can be applied to a Class, Serial Number, Product ID or Type of Device. 4. The proposed solution should identify unpatched 3rd party software apps that may have vulnerabilities 5. The proposed solution should provide the CVE vulnerability information of the applications installed on the Servers 6. The proposed solution must provide a software inventory for the environment		
9.	Firewall Control	1. The proposed solution should have Firewall Control for Windows / Linux. 2. The proposed solution should have Firewall rules to be built to apply to a specific group of devices (leveraging tagging or policy groups) 3. The proposed solution should have location-aware firewall rules to apply		

		different policies when on or off network		
10.	Device & Network Discovery	1. The solution should automatically discover devices in a network without the need to deploy sensors. 2. The Solution should be capable of identifying the following devices on the network: Windows, Linux and Apple. 3. The proposed solution must have rogue devices discovery capability to reduce the potential attack surface.		
11.	Dashboards & Reporting	1. The proposed solution must have capability to customize the dashboard. 2. The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option 3. The proposed solution shall provide a very good reporting interface for viewing real-time logs and ability to generate recurring customized reports. 4. The proposed solution shall support exporting of reports in different formats including PDF and CSV and with pre-built report templates customizable to the organization's need. 5. The proposed solution shall provide reports templates on the following but not limited to: a) Executive Report b) Threat Information c) Application Information d) Mitigation and Response Information 6. The proposed solution shall provide the capability to generate one-time reports 7. The proposed solution shall provide the capability to generate scheduled reports (weekly, monthly) or custom date range. 8. The proposed solution shall provide additional 3rd party integration tools (such as excel) to allow the creation of custom reports.		
12.	Integration	1. The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association. The solution management server should not		

		have any dependencies on the AD state. The product should support multiple Active Directory domains and forests. 2. The solution should have native integrations with SIEM solutions such as Splunk & Qradar etc. EDR solution should natively send event logs via Syslog. The solution must support the following syslog formats: CEF/CEF2/RFC-5424. It should support SSL/ X.509 certificates for syslog transport encryption and authentication.		
13	Support	1. The proposed solution should offer an option to have a technical account manager or higher level of support, please outline the offering & SLA's. 2. The proposed solution should offer services to assist with the deployment and configuration of the solution. 3. The proposed solution must provide 24x7x365 Support with India toll free number		
14.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
15.	OEM Installation & Training	1. Installation by direct OEM on site. 2. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xiv) EDR Solution (Desktops)

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1.	Management Console	1. The proposed solution must support on-premises deployment (within CDAC Datacenter). (Solution should have management infrastructure, operational		

		monitoring, upgrades, reporting, notifications & 24x7 support.) " 2. The proposed solution should provide a web-based console and should allow administrators to access the management interface from any machine, without installing additional software Unified Web-based console for all functionalities 3. The proposed solution should support multi-site configuration and multi-tenancy without any additional cost. 4. The proposed solution should have Policy inheritance from Top to bottom (like parent/child, group/sub-group, site/group, etc) with the ability to inheritance if needed and should also provide the flexibility to have individual policies for every group. 5. The proposed solution should have Integrated KB/documentation into the management console without requiring logging in to another system / URL. 6. The proposed solution console should be easy to understand and navigate with simple work flows. The console's focus should be on incident response workflows vs feature configuration and management 7. The proposed solution should support role based access control (RBAC) 8. The proposed solution should support two factor or single sign on solutions for the management console and sensitive functions such as remote shell. 9. The proposed solution should have capability of centralized auditing and logging of activity should be maintained in the management console. 10. The proposed solution should have capability logged and audited the management activity ,with the ability to send logs to an external source (like SIEM etc.) 11. The Endpoint Security Solution setup must have the capability to manage endpoints at Central Console, which may		

		be implemented in phased manner. 12. The solution must be capable of managing endpoints . The bidder must ensure that hardware/software required at the central console can scale to onboard additional endpoints at any time with proposed Configuration and standard. 13. Solutions features must be fully compatible over IPv4/IPv6 network such as hardware, software and application software etc. 14. The solution should provide a unified web-based console for all functionalities and should allow administrators to access the management interface to any authorized user, without installing additional software. 15. The solution should provide API access to all management capabilities and access to data. API should be well documented and available without any additional cost and application and hardware. The solution should have ability to quickly run APIs on the console data set without any limitations. 16. Solution must provide non-repudiable Centralized auditing and logging of activity through the management console. Management activity must be logged and audited with the ability to send logs to an external source without restrictions. 17. Solution must provide multi-factor authentication and single sign on solutions for the management console and sensitive functions such as remote shell.		
2.	Operating System Support	1. The proposed solution must support all supported versions of Operating Systems and should continue support for a minimum period of 12 months after the OS version is end of sale/life. 2. The proposed solution should support all the latest versions of windows but not limited to: Windows 10, 11, Window 8 SP1, SP2		

		Windows 7 SP1 3. The proposed solution should support all the latest versions of macOS but not limited to: macOS Catalina macOS Big Sur macOS Monterey macOS Ventura 4. The proposed solution should support all the latest Linux platforms but not limited to: CentOS (6,7,8) Debian Fedora Ubuntu (16,18,20,22) Red Hat Enterprise Linux (RHEL-6,7,8,9) Oracle SUSE Linux Enterprise Server 5. The proposed solution should support all the new OS Updates/Versions within 60 days of release.		
3.	Agent Features	1. The proposed solution must have EPP and EDR capabilities available in a single agent without requiring multiple software packages to be installed. 2. The proposed solution agent size should be less then 100 MB. 3. The proposed solution must have strong anti-tamper capabilities across the platform windows, Mac , Linux (Ensure that an end user (even with local admin credentials) can not remove, disable or modify the product in any way.) 4. The proposed solution must have ability to kick off On-Demand Scans to look for malware, or ensure a threat has been remediated (from console and/or endpoint) 5. The proposed solution should be signtureless (No need of daily signature updates) to detect all types of Malware without compromising the security posture.		

		6. The proposed solution must have ability to schedule agent upgrades from the management console 7. The proposed solution must have ability to limit the amount of agents that can download an update at any given point of time. 8. The proposed solution must have ability to upgrade agents with no impact to the end user 9. The proposed solution should provide ability to send notification messages to the end user computer. 10. The proposed solution should automatically remove old agents from console, if agent haven't communicated to the management console for a configurable period of time 11. The proposed solution should have minimal impact on system performance. 12. The proposed solution should have capability to uninstall agents remotely from the management console directly or through script. 13. The proposed solution should have capability to temporarily disable agent via the management console for temporary troubleshooting or testing. 14. The proposed solution should not required a reboot on upgrade 15. The proposed solution agents should have ability to communicate with Management Console via a proxy 16. The proposed solution must support linux agent running solely in user space to avoid kernel panics and tainted kernels that invalidate support 17. The proposed solution should not require any downtime while installing/upgrading Linux agents.		
4.	Threat Prevention	1. The proposed solution should provide prevention capability across all major Operating Systems – Windows, MacOS & Linux. 2. The proposed solution must provide		

		protection against known and unknown malware 3. The proposed solution must have capability to check the files for any infection for both on write and execute with any dependency on external cloud 4. The proposed solution must be effective against Zero-Day Attacks by Analysing Behaviours on an endpoint, rather than only looking at daily signatures 5. The proposed solution must protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need to have any dependency on Management Server or Cloud or ANY resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less , Memory based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected. 6. The proposed solution should have capacity to detect dormant threats 7. The proposed solution should leverage Artificial Intelligence (AI) or Machine Learning (ML) to analyse files pre-execution & behaviours while a file is running 8. The proposed solution should protect from malicious scripts and documents 9. The proposed solution should monitor and protect from lateral movement 10. The proposed solution should monitor and protect from exploits and fileless attacks 11. The proposed solution should look for potentially unwanted programs 12. The proposed solution should monitor and protect from insider threats 13. The proposed solution should provide the flexibility to safely download of malicious or convicted file from the management console		

		14. The proposed solution must have the ability to store the Incident data for at least 365 days without any additional charge 15. The proposed solution must have ability to correlate together automatically if incident related to the same attack and not create separate alerts. 16. The proposed solution should by default group all related alerts together 17. The proposed solution should provide a visual process tree browser 18. The proposed solution should provide the flexibility to mark an entire group of events as a threat and take response or remediation actions accordingly 19. The proposed solution should have option to search for MITRE ATT&CK Indicators based on j) Initial Access k) Credential Access l) Discovery m) Lateral Movement n) Collection o) Command & Control p) Exfiltration q) Impact r) Indicators		
5.	Response & Remediation Capabilities	1. The proposed solution should support full remote shell for all OS (Windows, Linux & Mac) and not limited or restricted to set of commands. 2. The proposed solution should track all remote shell commands and logged during a remote shell session. 3. The proposed solution should alert on both suspicious and malicious threat behaviour 4. The proposed solution should have ability to kill and quarantine an offending process. 5. The proposed solution should be able to unquarantine a file from the management interface or API.		

		6. The proposed solution should have the ability to remediate all operating system changes and perform corrective action in machine speed. The solution should also be able to undo any system level changes related to the attack such as Registry edits, configuration changes etc. 7. The proposed solution should reverse destructive data event but not limited to ransomware. The solution should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state. 8. The proposed solution should provide option to network quarantine a device and provide flexibility to configure the same. 9. The proposed solution should have automated threat response capabilities. 10. The proposed solution should have capability to take the remediation actions on multiple systems or events at once 11. The proposed solution should have ability for an analyst to add notes/comments to an event 12. The proposed solution should have options to set the status of an issue or event (i.e. resolved, in progress, unresolved)		
6.	Policy & Installation	1. The proposed solution should provide ability to support policy inheritance across the endpoints. 2. The proposed solution should have the option to provide dynamic policy assignment based on device attributes 3. The proposed solution should have capabilty to place the installed devices directly into a specific device group at the time of installation 4. The proposed solution policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines). 5. The proposed solution policy modifications should be applied in near		

		real time.		
7.	Exclusions	1. The proposed solution should have predefined list of known or recommended exclusions 2. The proposed solution must provide Path execution capability with option to selected Exclusion Mode (Suppress Alerts, Interoperability, or Performance Focus) applies to files in the path 3. The proposed solution should include workflows to easily exclude false positives 4. The proposed solution should provide the option for administrators to make policy exclusions of the console at multiple levels (account, group). 5. In the solution, exclusions should be configurable by the administrator to handle performance issues down to specific paths or single executables by disabling monitoring of parent processes and/or parent processes and all of their spawned child processes		
8.	Device Control and Application Visibility	1. The proposed solution must have Device Control capabilities. 2. The proposed solution Device Control should support block, read only and allow read-write on USB /Bluetooth. 3. The proposed solution should have granular device control capability which can be applied to a Class, Serial Number, Product ID or Type of Device. 4. The proposed solution should identify unpatched 3rd party software apps that may have vulnerabilities 5. The proposed solution should provide the CVE vulnerability information of the applications installed on the Servers 6. The proposed solution must provide a software inventory for the environment		
9.	Firewall Control	1. The proposed solution should have Firewall Control for Windows / Linux. 2. The proposed solution should have Firewall rules to be built to apply to a specific group of devices (leveraging		

		tagging or policy groups) 3. The proposed solution should have location-aware firewall rules to apply different policies when on or off network		
10.	Device & Network Discovery	1. The solution should automatically discover devices in a network without the need to deploy sensors. 2. The Solution should be capable of identifying the following devices on the network: Windows, Linux and Apple. 3. The proposed solution must have rogue devices discovery capability to reduce the potential attack surface.		
11.	Dashboards & Reporting	1. The proposed solution must have capability to customize the dashboard. 2. The proposed solution should report all known vulnerabilities in programs installed on an endpoint, along with export option 3. The proposed solution shall provide a very good reporting interface for viewing real-time logs and ability to generate recurring customized reports. 4. The proposed solution shall support exporting of reports in different formats including PDF and CSV and with pre-built report templates customizable to the organization's need.		
12.	Integration	1. The solution must Integrate with Active Directory for automatic Agent to Group Mappings and policy association. The solution management server should not have any dependencies on the AD state. The product should support multiple Active Directory domains and forests. 2. The solution should have native integrations with SIEM solutions such as Splunk & Qradar etc. EDR solution should natively send event logs via Syslog. The solution must support the following syslog formats: CEF/CEF2/RFC-5424. It should support SSL/ X.509 certificates for syslog transport encryption and authentication.		
13	Support	1. The proposed solution should offer an		

		option to have a technical account manager or higher level of support, please outline the offering & SLA's. 2. The proposed solution should offer services to assist with the deployment and configuration of the solution. 3. The proposed solution must provide 24x7x365 Support with India toll free number		
14.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
15.	OEM Installation & Training	2. Installation by direct OEM on site. 2. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xv) DDoS (Hardware Appliance)

Sl no	Items	Description	Compliance Yes / No	Cross Ref.
1.	Type	1. The proposed solution should have dedicated DDoS protection device (NOT be a part of Application Delivery Controller, Router, UTM, Proxy based architecture or any with mitigation throughput of 20Gbps.		
2.	Throughput & H/w	1. "DDoS Flood Attack Prevention Rate: 30MPPS (min) 2. Legitimate throughput handling: 20Gbps (min) 3. Attack Concurrent Sessions : Unlimited 4. Inspection Ports supported : 4 x 10G SFP+ from day-1 with inbuilt hardware and software Bypass. Option for additional 4 x 10G SFP+ for future use with inbuilt hardware and software Bypass 5. Latency should be less than 80 microseconds		

		6. The appliance should have dedicated 1 x 1G RJ45 Management Port and RJ45 Console Port."		
3.	Configuration and deployment mode	1. The proposed solution should have the capability to be configured in detect as well as protect mode. 2. The proposed solution should be deployed in inline mode (L2 & L3) and SPAN/TAP mode (out of path). 3. The Solution must have 50K SSL TPS for RSA 2K key, 35K SSL TPS for ECDSA P25 and L7 RPS should be 7 Million and L4 CPS should be 2.5 Million.		
4.	Attack protection	1. The proposed solution should detect and mitigate both network layer DDoS attacks and advanced application layer attacks. 2. The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL handshake atatck 3. The proposed solution should prevent suspicious traffic for threats and blocking malicious traffic. 4. "The solution should protect ICMP attacks: ICMP floods, ping floods, smurf, IP Spoofing, LAND attack, Teardrop, IP Option Timestamp, IP Option Route Record, IP Option Source Route, Ping of Death, Tracert, ICMP Redirect, ICMP Unreachable, ICMP Large Packet." 5. The solution should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection,TCP Fragments Flood, Defense WinNuke, TCP Error Flag. 6. The solution should protect UDP based attacks: UDP Flood, UDP Fragement Flood, UDP Fingerprint, Fraggle, UDP Large Packet 7. The solution should protect HTTP & HTTPS based attacks: HTTP GET Flood,		

		HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation. 8. "The solution should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense , DNS NxDomain Defense, DNS Query Flood Defense , DNS Reply Flood Defense, DNS TTL Check , DNS Source Authentication." 9. The Solution should protect against Zero Day DDoS Attacks. ZERO DAY ATTACK PROTECTION should be provided within few seconds, without any manual intervention. 10. The solution should support Brute Force attack mitigation. 11. The solution should support the behaviour based DDOS mitigation. 12. The solution should provide the traffic AUTO learning function for DDOS traffic monitoring. The traffic Auto learning threshold can be applied automatically after auto learning is completed. 13. The solution should provide multi-level DDOS mitigation policy and different mitigation actions based on DDOS traffic type.		
5.	Access Control	1. The solution should support Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist. 2. The solution should support Access control list based on inbulit GeoIP with configurable duration. 3. The solution should be able to import third party IP database through File or URL.		
6.	HA Support	1. The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP.		
7.	Management	1. The solution must provide the latest Management Information Base (MIB) file for SNMP operation.		

		2. The solution shall provide the flexibility of performing configuration via GUI and command base remotely. 3. The solution should support IPv4 and IPv6 dual-stack without deteriorating performance. 4. The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4/IPv6 traffic to IPv6/IPv4 traffic on the backend. 5. The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing. 6. The solution shall be able to support user authentication based on Local Password, RADIUS & TACACS+. 7. The solution must provide packet capture for debugging.		
8.	Integration	1. The solution shall be able to export syslog to existing syslog server and SIEM system. 2. The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2.		
9.	Reports	1. The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region. 2. The solution must be able to generate summary attack report of daily/weekly/monthly 3. The solution must support the generation of pdf reports containing the detailed statistics and graphs.		
10.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved		

		within 72 hours.		
11.	OEM Installation & Training	3. Installation by direct OEM on site. 2. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xvi) SSL Offloader (Hardware Appliance)

Sl no	Items	Description	Compliance Yes / No	Cross Ref.
1.	Type	1. The proposed appliance should be a dedicated appliance, it should not be the part of any Firewall or UTM.		
2.	Throughput & H/W	1. Traffic Ports: 4 x 10G SFP+ (SX Fiber incl.), 4 x 1G copper ports 2. L4 Throughput: 20 Gbps (min) 3. SSL Throughput: 10Gbps (min) 4. Concurrent Connections: 40 Million 5. HDD: 4TB HDD (min) and dual power supply. 6. The appliance should have dedicated 2x10/100/1000 Copper Ethernet (RJ45) Management Port and RJ45 Console Port.		
3.	Algorithm supported	1. The solution should support RSA and ECDHE public key algorithms. The solution should have hardware acceleration card for RSA & ECC cryptography. 2. The solution support AES, 3DES, DES, RC4 algorithms and ciphers. 3. The solution should support MDS, SHA-1, and SHA-2 hash algorithms. 4. The solution should support 512 through 4096 bit key lengths.		
4.	RPS & CPS	1. The appliance should support L4 CPS 1.5 Million and L7 RPS 2.5 Million. 2. The solution should support a minimum 40,000 SSL TPS for RSA 2048 bit key and 28,000 SSL TPS for ECC.		
5.	IPv6 support	1. The solution should provide full ipv6 support and configurations.		
6.	Deployment	1. The solution must support L2 and L3		

	mode	mode of deployment.		
7.	By-pass capability	1. The Solution must support Bypass capability in-built or through external hardware.		
8.	Header modification	1. The solution must support modification of headers.		
9.	Traffic interception	1. The solution must have both Inbound & Outbound SSL Interception capability. 2. The solution must support before proxy interception (between Client and Proxy) 3. The solution must support SSL interception bypass based on source and/or destination, IP, SNI values, URL category. 4. The solution must support interception of all types of encrypted traffic. 5. The solution should be factored to cover all the major Networks /segments of perimeter firewalls of each data centers for SSL Interception		
10.	LB feature	1. The solution must support load-balancing of multiple security devices.		
11.	Webagent support	1. The solution should support Webagent to enable explicit forward proxy		
12.	Traffic redirection	1. The solution must support traffic redirection based on any L2-L7 parameters		
13.	SSL/TLS support	1. Solution should support the latest TLS/SSL encryption protocols. 2. The solution must support redundancy. The SSL inspection solution should support TLS 3. The solution should support the latest TLS and SSL standards, .The solution should also support SSL decryption for non -standard ports. 4. The solution should have the ability to manage SSL traffic on multiple network segments on the same device. 5. The solution should have the ability to decrypt and re-encrypt traffic within the same appliance (i.e., transmit decrypted traffic to multiple in-line security devices like NGFW, IPS, DLP, APT solutions and re-encrypt traffic after the security		

		device's inspection). At the same time should be able to send the copy of decrypted traffic via configured passive inline ports to passive security devices like security Analytics, IDS, SIEM etc		
14.	Latency	1. The latency should be less than 40 microseconds		
15.	HA Support	1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Per VIP based Active-active & active standby unit redundancy mode.		
16.	Integration	1. The solution must support integration with security solutions such as DLP ,AV, Web content filters, SIEM, etc. 2. Solution should support TACACS, AD / LDAP / RADIUS integrations.		
17.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
18.	OEM Installation & Training	4. Installation by direct OEM on site. 2. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xvii) WAF (Virtual Appliance)

Sl no	Items	Description	Compliance Yes / No	Cross Ref.
1.	Type	1. The proposed solution should be a Virtual appliance vWAF not as add-on license Feature on ADC and NGFW. 2. The vWAF shall be entirely Software based and shall support virtualization platforms like VMware Esxi, Hyper-v, KVM etc. 3. The vWAF solution has to compatible with the proposed cloud solution. It has to be integrated with the proposed cloud solution and orchestrated for Scale-In		

		Scale-Out functionalities.		
2.	Throughput & Instances	1. The solution should provide elastic based model with 10Gbps aggregated throughput, there should not be any limitation on number of instances deployed. Instances of		
3.	Management	1. The vWAF shall be manageable both GUI and CLI using SSH, Web based management (HTTPS) etc. 2. The vWAF shall have feature to provide role based user's access for management. 3. The vWAF shall support authentication and authorization through Radius / TACACS+. 4. The vWAF shall support NTP for date & time synchronization from NTP Server. 5. The vWAF shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.		
4.	L7 Features	1. The vWAF L7 RPS should be 1.5 Million and support 12 K SSL TPS for RSA 2K key, 8K SSL TPS for ECDSA P25. 2. The vWAF should support http normative inspection; support HTTP protocol decoding and check related fields, including URI, request method, response status code, HTTP header fields and other HTTP elements, etc. 3. The legality of the HTTP protocol should be verified based on the RFC, including the length of the HTTP Request line, URL length, protocol name length, header value length, transmission sequence and application format (such as HTML parameters, Cookie version and format, Multipart/form-data encoding of file upload) etc.		
5.	Modes & security model	1. The vWAF should support in-line modes- Bridge, routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN). 2. The WAF should support negative and positive security model.		
6.	Attack Protection	1. The vWAF should support in-line modes- Bridge, routed, transparent		

		mode, reverse proxy mode and out of path (TAP/SPAN). 2. The WAF should support negative and positive security model. 3. The WAF should detect and block SQL injection attacks, support injection detection based on GET, POST, cookie, etc., and support the detection of code bypassing SQL injection; The WAF should prevent XSS cross-site attacks, including the detection of storage and reflection cross-site methods, and the detection of code bypassing XSS cross-site attacks; 4. The WAF should protect against command injection attacks, such as Linux and Windows system command execution; The WAF should protect against common types of injection attacks, including SSI, LDAP, XPATH, mail header, file injection, etc. 5. The WAF should support the detection of uploading web shell attacks. The detection method should be based on the content of the uploaded file, while protecting against illegal access to the web shell; The WAF should support HTTPS-based attack protection and detection of attack behavior in encrypted data packets. 6. The WAF should protect application layer and Network DOS attacks, support application layer resource consumption type denial of service attack detection and denial of service attack detection caused by malformed data and malformed protocol. 7. The WAF should prevent attacks against session tampering and hijacking, including attacks against cookie, session and user parameters, and can prevent attacks such as directory traversal attacks and CSRF attacks. 8. The WAF should have the ability to detect and filter the attacks of abnormal HTTP requests, such as put and delete		

		methods, HTTP request header parameters, such as user-agent and range fields; whitelist filtering based on URL and parameters; HTTP request referer field. 9. The WAF should support Anti-leech to prevent the attacker from using technical means to bypass other commercial end-user windows (such as advertisement) and providing services belonging to other service providers to end users on their own website. 10. The WAF should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client. It should return the cached original web page to make the anti-defacement effects unnoticeable or returns a 503 error page to the client to end the service. 11. The WAF should have the information suppression function for the application platform to prevent the leakage of related information, such as: Web server version information, operating system information, database information, etc. 12. The WAF should perform deep packet inspection to prevent sensitive or private data from leaking. You can define sensitive data models through regular expressions, such as ID number, mobile phone number, credit card number, etc.		
7.	HA support	1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP Per VIP based Active-active & active standby unit redundancy mode.		
8.	Access Control	1. The access control of black and white lists should be supported, and global and local settings should be supported. 2. The WAF should support access control based on client source IP, server URL and port. 3. The WAF should support Access control based on GeoIP regions: The		

		administrator can generate IP blacklist based on the IP region table to achieve the region-based access control. The WebUI can generate and display region-based statistics graphs/security events.		
9.	IP reputation	1. The WAF should support IP reputation subscription to protect against Botnet, Cybercrime, Phishing, SPAM, TOR, scanners etc.		
10.	Monitoring	1. The WAF should support status monitoring. The monitoring information can be incorporated into the network management system through SNMP. The status information of the system monitoring should include: system running status, system running time, system version, CPU usage, memory usage, remaining disk space , Interface status, etc.;		
11.	Upgrade Rollback	1. The WAF should support rollback after system upgrade or signature database upgrade fails. The WAF should have regular own Signature updates.		
12.	Reports	1. The WAF should have reports which can be generated according to time, and the report graphics can be set to column, bar, and pie charts. Reports can be exported to multiple formats, such as PDF, HTML and Excel; The WAF should have reports which can be automatically generated on a regular basis, such as daily, weekly, and monthly; the reports can be sent to the designated recipient via FTP or email.		
13.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
14.	OEM Installation & Training	1. Installation by direct OEM on site. 2. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xviii) LB (Virtual Appliance)

Sl no	Items	Description	Compliance Yes / No	Cross Ref.
1.	Type	1. The proposed solution should be a Virtual appliance. It should not be an add on license feature on NGFW and WAF. 2. The vSLB shall be entirely Software based and shall support virtualization platforms like VMware Esxi, Hyper-v, KVM etc 3. The vSLB solution has to compatible with the proposed cloud solution. It has to be integrated with the proposed cloud solution and orchestrated for Scale-In Scale-Out functionalities.		
2.	Management	1. The vSLB shall be manageable (both GUI and CLI) using SSH, Web based management (HTTPS) etc. 2. The vSLB shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one. 3. The vSLB shall support NTP for date & time synchronization from NTP Server. 4. The vSLB shall have feature to provide role based user's access for management. 5. The vSLB shall support authentication and authorization through Radius / TACACS+. 6. The solution must support Single Sign-On (SSO) for web based applications and web based file server access. It should also supports SAML secure application access.		
3.	Throughput	1. The solution should provide elastic based model with 10Gbps aggregated throughput, there should not be any limitation on number of instances deployed. Instances for SLB should be unlimited. 2. The Appliance should support L7 RPS 1.5 Million and L4 CPS 2 Million from day 1 and support 12 K SSL TPS for RSA 2K key, 8K SSL TPS for ECDSA P25.		
4.	LB & GSLB	1. The solution should able to load balance		

	feature	both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure. 2. The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, Session ID, hash header etc. 3. The Solution should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types. 4. The solution should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1, HTTP 2.0 to enhance the speed and performance of web servers 5. The solution should support Multi-level virtual service policy routing, Static, default and backup policies for intelligent traffic distribution to backend servers 6. The solution should support for policy nesting at layer7 and layer4. It should be able to combine layer4 and layer7 policies to address the complex application integration. 7. The solution should have script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies to customize new features/rules to re-direct the traffic on specific parameters. 8. The solution should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc. 9. The solution should provide application		

		& server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc. 10. The solution should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. TCP optimization option configuration should be defined on per virtual service basis not globally. 11. The solution should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX". 12. The solution should support advance ACL's to protect against network based flooding attacks. Administrator should be able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value. 13. The solution should also have option to define customized rules for gateway health check. The administrator should be able to define a rule to inspect the status of the link between the unit and a gateway 14. The solution should support QOS for traffic prioritization. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application. 15. The solution should support site selection feature to provide global load balancing features for disaster recovery and site redundancy. 16. The solution should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speed-up the failover. It should		

		support for secondary communication link for backup purpose 17. It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.		
5.	HA support	1. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based standard VRRP RFC 2338 on Per VIP based Active-active & active standby unit redundancy mode for virtual instances. 2. The solution should support for multiple communication links for Realtime configuration synchronizations including HA group, gateway health check, decision rules, sessions etc. and heartbeat information 3. The solution should support floating IP address and group for stateful failover support. the solution must have support 256 floating ip address for a floating group. It should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot.		
6.	Reporting, Logging & Alert	1. The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting. 2. The solution should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics. 3. The appliance must support multiple		

		configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. The system should support led warning and system log alert for failure of any of the power and CPU issues.		
7.	Warranty	1. 5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours' response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
8.	OEM Installation & Training	2. Installation by direct OEM on site. 3. Min. 2 days on site Advanced Level product training along with OEM certification.		

(xix) NG-Firewall with ATP & Deep Inspection

Sl no.	Items	Description	Compliance Yes / No	Cross Ref.
1	Type	NGFW		
2	Form factor	3U or lesser		
3	Features	Layer 3 - Layer 4, NAT, VPN, Application Visibility and Control (AVC), User Identity, Next Generation Intrusion Prevention System (IPS), Zero Day Protection, Advance Malware protection, Web Security Essentials, URL Filtering, Threat Intelligence		
4	Hardware Configuration	Memory - 128 GB or more Type of Processor - X86 Storage Disk - 2X 400 GB or higher for inherent log storage Dual Hot Swappable Power Supplies Redundant Fans Device should supplied with rack mount kit, standard C13 power cord, Fibre cables and required Patch cables all accessories.		
5	Traffic handled	TCP, UDP, HTTP/TCP, TCP/UDP		

6	Throughput & Performance	20 Gbps Real World/Prod Performance Throughput with all features enabled including ATP, Deep Packet Inspection, SSL encryption & decryption, Web/URL Filtering, DNS Security, Sandboxing, Concurrent Session/Concurrent Connection - 30M or higher New session/Connection per second - 600K		
7	Physical Interface	Type of Interface Supported Multi select - GE Copper , 10G SFP+, QSFP+ 40 G and GE SFF Number of 10G SFP+ interface - 12 (populated from day 1) Number of QSFP+ 40 G interface - 2 (populated from day 1) Should have Remote Lights Out Management (Separate mgmt. port) of 1 Gbps or higher RJ45 port.		
8	VPN	Number of IPSec VPN Peers supported (Site to Site) - 10K Number of IPSec VPN Peers supported (Client to Site) – 10K SSL VPN Peers supported (Client to Site) – 2K		
9	High Availability	Device should be supplied and configured in Active-Active HA mode from day 1		
10	Licenses from Day 1	Web Security Essentials / URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection, C& C attacks, Geo IP Protection, Zero Day Threat Protection), DNS Security, Gateway Antivirus. Licenses for virtual logging device for daily logs of 100 GB per day, centralized management, event / incident management should be supplied from day 1.		
11	Security Intelligence & Signatures	IP, URL, Domain, IOC Intelligence NGIPS Signature - 12000 or more		
12	IPv6 Ready from day 1	Yes		
13	On Site OEM Warranty	5 Years - All licenses, updates, upgrades& support has to be provided for at least 5 years with 24x7 production support (4 hours'		

		response and 24 hours' resolution for all critical issues). For all noncritical issues affecting the services in any manner the issue has to be responded within 24 hours and resolved within 72 hours.		
14	Certification	The firewall/ firewall's certified under Indian Common Criteria Certification Scheme (IC3S) by STQC, DEIT, Govt. of India.		
15	Solution Inclusions	Solution must include with centralized mgmt. device/software along with log management and event / incident management. Separate virtual appliance are preferred and in case log management device in physical form is supplied it has to size for Analysis of 100 GB / day for 6 months and it should be with NVMe (preferred) or SSD disks.		
16.	Training & Certification	Min. 2 days on site Advanced Level product training for 10 members along with OEM certification.		

(END OF SECTION IV)

SECTION -V

ANNEXURE-I-TECHNICAL BID SUMMARY

Name of Bidder:
Detail Address:
Contact Person:
Mobile No:

S.N.	Requirements	Specifications	QTY in Nos	Make/ Model No	Declaration as per 6/18/2019-PPD & No.P-45021/112/2020-PP(BE-II)(E-43780) (Of OEM + Bidder)		
					Country of Origin of OEM	Country of Manufacture	Country of Shipment
1	Servers / HCI	Detailed at (i)					
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc	Detailed at (ii)					
3	RHEL (Unlimited Virtualization)	Detailed at (iii)					
4	Windows Data Centre	Detailed at (iv)					
5	NVMe Storage	Detailed at (v)					
6	SAN Switch	Detailed at (vi)					
7	Network Leaf Switch (Copper) with SDN Solution	Detailed at (vii)					
8	Network Leaf Switch (Fibre / Copper) with SDN Solution	Detailed at (viii)					
9	Network Spine Switch with SDN Solution	Detailed at (ix)					
10	Network OOB Management Switch	Detailed at (x)					
11	Routers (2-10Gbps)	Detailed at (xi)					
12	Routers (4-10Gbps)	Detailed at (xii)					
13	EDR Solution (Servers)	Detailed at (xiii)					

14	EDR Solution (Desktops)	Detailed at (xiv)					
15	DDoS (Hardware Appliance)	Detailed at (xv)					
16	SSL Offloader (Hardware Appliance)	Detailed at (xvi)					
17	WAF (Virtual Appliance)	Detailed at (xvii)					
18	LB (Virtual Appliance)	Detailed at (xviii)					
19	NG-Firewall with ATP & Deep Inspection	Detailed at (xix)					

ANNEXURE-II- Delivery and Payment Schedule

S.N.	Requirements	Delivery Period	Quantity Delivery at		Payment Schedule
			Hyderabad	Noida	
1	Servers / HCI	4 weeks	13 Nos. (9 DC + 4 DR)	7 Nos.	70% on Delivery
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc	2 weeks	For 8 Nodes at SN. 1 (4+4) DC-DR config	For 4 Nodes at SN. 1	70% on Delivery
3	RHEL (Unlimited Virtualization)	2 weeks	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	70% on Delivery
4	Windows Data Centre	2 weeks	For 4 Nodes at SN. 1 (2 DC + 2 DR)	-	70% on Delivery
5	NVMe Storage	4 weeks	1 No.	1 No.	70% on Delivery
6	SAN Switch	4 weeks	2 Nos. (in HA)	2 Nos. (in HA)	
7	Network Leaf Switch (Copper) with SDN Solution	4 weeks	6 Nos.	8 Nos.	70% on Delivery
8	Network Leaf Switch (Fibre / Copper) with SDN Solution	4 weeks	12 Nos. (8-DC & 4-DR)	16 Nos.	70% on Delivery
9	Network Spine Switch with SDN Solution	4 weeks	4 Nos. (2-DC & 2-DR)	-	70% on Delivery
10	Network OOB Management Switch	4 weeks	29 Nos. (25-DC & 2-DR)	35 Nos.	70% on Delivery
11	Routers (2-10Gbps)	4 weeks	4 Nos.	-	100% on handover
12	Routers (4-10Gbps)	4 weeks	-	2 Nos.	
13	XDR Solution (Servers)	4 weeks	300 Nos.	1000 Nos.	100% on handover
14	XDR Solution (Desktops)	4 weeks	-	800 Nos.	
15	DDoS (Hardware Appliance)	4 weeks	2 Nos. (in HA) or 1 No. with Bypass	2 Nos. (in HA) or 1 No. with Bypass	
16	SSL Offloader (Hardware Appliance)	4 weeks	2 Nos. (in HA)	2 Nos. (in HA)	100% on handover

S.N.	Requirements	Delivery Period	Quantity Delivery at		Payment Schedule
			Hyderabad	Noida	
17	WAF (Virtual Appliance)	4 weeks	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	
18	LB (Virtual Appliance)	4 weeks	10 Gbps Aggregated throughput	10 Gbps Aggregated throughput	
19	NG-Firewall with ATP & Deep Inspection	4 weeks	2 Nos.	-	100% on handover

ANNEXURE-III- PRICE BREAK-UP FORMAT

Note: This annexure to be uploaded in the price bid section of GeM portal only and not to be enclosed along with Technical Bid documents.

S.N.	Requirements	Specifications	Quantity	Units	Rate	GST	Amount without GST	Amount with GST
1	Servers / HCI	Detailed at (i)						
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc	Detailed at (ii)						
3	RHEL (Unlimited Virtualization)	Detailed at (iii)						
4	Windows Data Centre	Detailed at (iv)						
5	NVMe Storage	Detailed at (v)						
6	SAN Switch	Detailed at (vi)						
7	Network Leaf Switch (Copper) with SDN Solution	Detailed at (vii)						
8	Network Leaf Switch (Fibre / Copper) with SDN Solution	Detailed at (viii)						
9	Network Spine Switch with SDN Solution	Detailed at (ix)						
10	Network OOB Management Switch	Detailed at (x)						
11	Routers (2-10Gbps)	Detailed at (xi)						
12	Routers (4-10Gbps)	Detailed at (xii)						
13	EDR Solution (Servers)	Detailed at (xiii)						
14	EDR Solution (Desktops)	Detailed at (xiv)						
15	DDoS (Hardware Appliance)	Detailed at (xv)						

16	SSL Offloader (Hardware Appliance)	Detailed at (xvi)						
17	WAF (Virtual Appliance)	Detailed at (xvii)						
18	LB (Virtual Appliance)	Detailed at (xviii)						
19	NG-Firewall with ATP & Deep Inspection	Detailed at (xix)						
Total Cost which is inclusive of Supply, Installation, Testing & Commissioning and 5 Years Warranty from the date of handing over of the solution to C-DAC.								

(END OF SECTION V)

SECTION – VI

ANNEXURE - A

BID SECURING DECLARATION LETTER

Date:

To:
The Director,

Dear Sir,

Subject: Bid Securing undertaking as per GFR – 2017, Rule 170(iii)-GeM Bid for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution-Reg

Tender No----------

I/We*, the undersigned, declare that:

I/We* understand that, according to your conditions, bids must be supported by a Bid-Securing Declaration.

I/We* accept that I/we* may be disqualified from bidding for any contract with any Public Body for the period of time that may be determined by the Procurement Policy Office under section 35 of the Public Procurement Act, if I am/we* are* in breach of any obligation underthe bid conditions, because I/we*:
(C.1.a) have withdrawn my/our* Bid during the period of bid validity specified in the Form of Bid; or

(C.1.b) having been notified of the acceptance of our Bid by the *C-DAC* during the period of bid validity, (i) fail or refuse to execute the Contract, if required, or , in accordance with the Instruction to Bidders.

Provided that I/we shall be given a curing period of one (1) month before any such action is taken by C-DAC.

I/We* understand this Bid Securing Declaration shall cease to be valid if I am/we are* not the successful Bidder, upon the earlier of (i) the receipt of your notification of the name of the successful Bidder; or (ii) thirty days after the expiration of the validity of my/our* Bid.

Signed: *[insert signature of person whose name and capacity are shown]* In the capacity of *[insert legal capacity of person signing the Bid Securing Declaration]*

Name: *[insert complete name of person signing the Bid Securing Declaration]*

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

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

Corporate Seal (where appropriate)

[Note: The Bid Securing Declaration must be signed by the authorized signatory or in the name of the Managing Partner of the firm]

Please delete as appropriate

ANNEXURE - B

COMPLIANCE LETTER

Compliance of the offered solution is to be provided on bidder's letter head, in the format provided below:

Schedule of Items – BoQ

S.N.	Requirements	Compliance Yes/No	Deviations (to be clearly specified in detail)
1	Servers / HCI as per specifications detailed at (i)		
2	Cloud Management Software License with Containers, SDN, SDS, SDDC, Orchestration, DC-DR Replication, etc as per specifications detailed at (ii)		
3	RHEL (Unlimited Virtualization) as per specifications detailed at (iii)		
4	Windows Data Centre as per specifications detailed at (iv)		
5	NVMe Storage as per specifications detailed at (v)		
6	SAN Switch as per specifications detailed at (vi)		
7	Network Leaf Switch (Copper) with SDN Solution as per specifications detailed at (vii)		
8	Network Leaf Switch (Fibre / Copper) with SDN Solution as per specifications detailed at (viii)		
9	Network Spine Switch with SDN Solution as per specifications detailed at (ix)		
10	Network OOB Management Switch as per specifications detailed at (x)		
11	Routers (2-10Gbps) as per specifications detailed at (xi)		
12	Routers (4-10Gbps) as per specifications detailed at (xii)		

13	XDR Solution (Servers) as per specifications detailed at (xiii)		
14	XDR Solution (Desktops) as per specifications detailed at (xiv)		
15	DDoS (Hardware Appliance) as per specifications detailed at (xv)		
16	SSL Offloader (Hardware Appliance) as per specifications detailed at (xvi)		
17	WAF (Virtual Appliance) as per specifications detailed at (xvii)		
18	LB (Virtual Appliance) as per specifications detailed at (xviii)		
19	NG-Firewall with ATP & Deep Inspection as per specifications detailed at (xix)		

**** Note: Bidders shall provide details of the deviation in complying with the bid specification for any of the items listed in the above BOQ,***

ANNEXURE - C

UNDERTAKING(S) BY PRINCIPAL MANUFACTURER/OEM

(To be submitted in Original on Letterhead-For all the components from respective OEM)

Date:

The Director,
Centre for Development of Advanced Computing (C-DAC) Plot No: 6&7, Hardware Park,
Sy. No.1/1, Srisailam Highway,
Hyderabad – 501510.

Subject: Undertaking by Principal Manufacturer against tender no. ……. for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution in the Data Centre **at C- DAC.**

Dear Sir,

We, M/s _____ *(Name of the manufacturer)* having registered office at _____ *(address of the manufacturer)* by virtue of being manufacturer for _____*(Name of the product/s)*, hereby certify that M/s _____*(Name of the bidder)* having their office at _____ *(Address of bidder)* are our Authorised System Integrator for our range of products quoted by them.

Within the scope of requirement as per the tender mentioned above, we undertake to provide technical & other support towards fulfilling the requirements of installation, commissioning, benchmarking, acceptance criteria and product warranty services of the components to be supplied and installed at C-DAC, site by M/s. (Name of bidder) against said tender.

We also certify that the products offered are not nearing end-of-life / end-of-support five years down the line from the date of bidding.

The undersigned is authorised to issue this certificate on behalf of M/s _____*(Name of the manufacturer).*

For M/s _____*(Name of the manufacturer)*

Signature & company seal

Name

Designation

ANNEXURE - D

TECHNICAL SOLUTION OFFERED

ANNEXURE - E

TENDER ACCCEPTANCE LETTER

Date:

To:

The Director,
Centre for Development of Advanced Computing (C-DAC) Plot No: 6&7, Hardware Park, Sy. No.1/1, Srisailam Highway, Hyderabad – 501510

Subject:.

Dear Sir,

We, the undersigned, offer to supply the solution to C-DAC, in response to your **Tender No:** . We are hereby submitting our proposal for same, which includes Technical bid and the Financial Bid on https://gem.gov.in/

We hereby declare that all the information and statements made in this bid are true and we accept that any misinterpretation contained in it, may lead to our disqualification.

We undertake, if our proposal is accepted, to submit a Security Deposit of 5 % of the contract / order value and 10% PBG towards 5 years warranty period, as per terms stipulated in the tender.

We confirm that the deliveries, installation, commissioning will be done within 8 weeks, if the order is placed.

We hereby certify that my/ our firm has not been disqualified and / or blacklisted by any Office/ Department/ Undertaking of the State Government / Central Govt. of India, PSU/ Autonomous Body of Government of India, at the time of submission of this bid.

We agree to abide by all the terms and conditions of the tender document, including corrigenda. We would hold the terms of our bid valid for 180 days as stipulated in the tender document.

We understand you are not bound to accept any Proposal you receive.

The undersigned is authorized to sign this bid document. The authority letter to this effect is enclosed.

Yours sincerely, Authorized

Signatory:
Name and Title of Signatory:
e-mail:
Mobile No:

ANNEXURE - F

UNDERTAKING FOR NO DEVIATION

No Deviation Certificate

(To be submitted in the Bidder's letter head)

<Date>

To: *(Tender Inviting Authority)*

Subject: Selection of agency for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations

Reference: No:

Dear Sir,

With reference to above, this is to confirm that as per tender conditions, we have understood the requirements before submission of our offer. We also confirm that we have not changed / modified the tender documents as appeared in the website/ issued by you and in case of such observance at any stage, it shall be treated as null and void.

We hereby confirm that we have not taken any deviation from tender Clauses together with other references as enumerated in the above referred Tender. We hereby confirm our unqualified acceptance to all terms & conditions, unqualified compliance to all the terms and conditions in the above referred tender.

Yours Sincerely

Name:
Designation:

(Company Seal)

ANNEXURE - G

NON BLACKLISTING

(To be submitted on the Letterhead of the bidder)

<Date>

To: *(Tender Inviting Authority)*

Subject: Selection of agency for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations

Reference: No:

Dear Sir,

We confirm that our company is not blacklisted in any manner whatsoever by MeitY, any State Government, Central Government or any other Public sector undertaking or a Corporation or any other Autonomous organization of Central or State Government as on Bid submission date.

Further we confirm that, our company is not convicted of an offence (a) under the Prevention of Corruption Act, 1988; or (b) the Indian Penal Code or any other law for the time being in force, during last 3 years from date of submission of this bid.

It is hereby confirmed that I/We are entitled to act on behalf of the bidder and empowered to sign this document as well as such other documents, which may be required in this connection.

Sincerely,

<Signature>

<Seal>

Name:
Designation:
Name and Address of bidder:

ANNEXURE-H- AUTHORITY LETTER

Date:

To:

The Director,
Centre for Development of Advanced Computing (C-DAC) Plot No: 6&7, Hardware Park,
Sy. No.1/1, Srisailam Highway,
Hyderabad – 501510

To: *(Tender Inviting Authority)*

Subject:

Dear Sir,

I am Shri…… working as a..... (Designation) duly authorized to sign the Tender Response for and on behalf of M/s …(name of the bidding firm):

Signature:……

(Name and Address of Bidder)

(Seal/Stamp of bidder)

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am ……<designation>…… of the ……<Company Name> ....., and that ……<Name of the Respondent>…… who signed the aboveresponse is authorized to bind the corporation by authority of its governing body.

Date:

Name:

Designation:

Signature:

(Seal)

***Note**: Authorized signatory should be an employee of the bidder and should have been authorized, authorizing him/her to sign/execute the proposal as a binding document and also to execute all relevant agreements forming part of RFP. Copy of proof of authorization (Board Resolution copy/power of attorney letter from all the partner(s)) should be provided.*

ANNEXURE-I-LITIGATION IMPACT UNDERTAKING

Litigation Impact Statement

<Bidder letter head>

<Date>

<Address>

Subject:

Dear Sir,

We have read and understood the contents of the Request for Proposal and pursuant to this hereby confirm that we continue to satisfy the eligibility criteria laid out at the time of short-listing us to participate in the bidding process for Selection of agency to conduct Financial Verification.

There are no pending litigations in any court of law, which are likely to have a materially adverse impact on our ability to deliver under this selection or on our ability to provide services as contemplated in this RFP.

<Signature>
<Designation>

Duly authorized to sign the RFP Response for and on

behalf of:

Sincerely,Bidder Seal

Name Designation Signature Date

<Name and Address of Bidder>

Seal/Stamp

ANNEXURE -J- INTEGRITY PACT

TEXT OF THE PRE-CONTRACT INTEGRITY PACT

This Integrity Pact is entered into by and between CDAC, Hyderabad, acting through the_____, _____, Ministry of Electronics and Information Technology, Government of India, having its office located at Hardwar Park, Srisailam Road, Hyderabad, which expression shall, unless excluded by or repugnant to the context, deemed to include its successor/s in office or assign) of the First Part;

AND

_____, a Company incorporated under the Companies Act, 1956, having its registered office at _____ (hereinafter referred to as "bidder" which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the Second Part.

Preamble

CDAC, Hyderabad intends to award, under laid down organizational procedures, contract for _____ through an open tender process through GeM and has issued bid No._____. CDAC, Hyderabad values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/ transparency in its relations with its bidder(s) and /or Vendor(s) / Contractor(s).

In order to achieve these goals, CDAC, Hyderabad wishes to enter into this Integrity Pact with the bidder(s) for this tender process and execution of the Agreement and will appoint an <Independent External Monitor (IEM)>, who will monitor the tender process and the execution of the Agreement for compliance with the principles mentioned above.

Section 1 – Commitments of CDAC, Hyderabad

a) CDAC, Hyderabad commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

i) No employee of CDAC, Hyderabad, personally or through family members, will in connection with the bid for, or the execution of the Agreement, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

ii) CDAC, Hyderabad will during this tender process treat all bidder(s) with equity and reason. CDAC, Hyderabad will in particular, before and during this tender process, provide to all bidders the same information and will not provide to any bidder(s) confidential/ additional information

through which the bidder(s) could obtain an advantage in relation to this tender process or the Agreement execution.

iii) CDAC, Hyderabad will exclude from the process all known prejudiced persons.

b) If CDAC, Hyderabad obtains information on the conduct of any of its officers /employees which is a criminal offence under the Indian Penal Code 1860 and/or Prevention of Corruption Act 1988, or if there be a substantive suspicion in this regard, CDAC, Hyderabad will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 – Commitments of the bidder

a) The bidder commits to take all measures necessary to prevent corruption. It commits itself to observe the following principles during its participation in this tender process and during the Agreement execution.

b) The bidder will not, directly or through any other persons or firm, offer promise or give to any of CDAC, Hyderabad employees involved in this tender process or the execution of the Agreement or to any third person any material or other benefit which he/ she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during this tender process or during the execution of the Agreement.

c) The bidder will not enter with other bidder(s) into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in this tender process.

d) The bidder will not commit any offence under the Indian Penal Code 1860 and / or Prevention of Corruption Act 1988; further the bidder will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by CDAC, Hyderabad as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

e) The bidder will, when presenting its bid, disclose any and all payments it has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with this tendering process or the award of Agreement under this tendering process.

f) The bidder will not, directly or through any other person or firm, approach any Government officials, ministers, political persons public servants, or any external agencies in an effort to influence the bidding decision making process or to attain any undue favour to the bidder.

g) The bidder shall exclude, from this tender process or execution of the Agreement, all known prejudiced persons including those employees / Directors /management representatives of the bidder who have family relationships with the employees or officers of CDAC, Hyderabad.

h) The bidder shall disclose the circumstances, arrangements, undertakings or relationships that constitute, or may reasonably be considered to constitute, an actual or potential conflict of interest with its obligations specified in the tender process or under any Agreement which may be negotiated or executed with CDAC, Hyderabad. Bidder and its employees, agents, advisors and

any other person associated with the bidder must not place themselves in a position which may, or does, give rise to conflict of interest (or a potential conflict of interest) between the interests of CDAC, Hyderabad or any other interests during this tender process or through operation of the Agreement.

i) The bidder will not indulge in any corrupt, fraudulent, coercive undesirable or restrictive practice in the tender process or the execution of the Agreement.

j) The bidder will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3 – Disqualification from tender process and exclusion from future Contracts

If the bidder, during the tender process or before award or during execution of the Agreement has committed a transgression through a violation of Section 2 above, or in any other form, such as to put his reliability or credibility in question, CDAC, Hyderabad is entitled to disqualify the bidder from this tender process or decide not to award the work or terminate the awarded Agreement or blacklist the bidder.

Section 5 – Previous Transgression

a) The bidder declares that no previous transgressions occurred in the last three years with any other Central Government / State Government or Central PSU entity in India or any entity in any other country conforming to the anti-corruption approach that could justify bidder's exclusion from this tender process.

b) If the bidder makes incorrect statement on this subject or hides any material information, CDAC, Hyderabad is entitled to disqualify the bidder from this tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 – Equal treatment of all bidders

a) The bidder undertakes to demand from all subcontractors of the Vendor a commitment in conformity with this Integrity Pact, and to submit it to CDAC, Hyderabad before signing of the Agreement with CDAC, Hyderabad.

b) CDAC, Hyderabad will enter into individual Integrity Pacts with identical conditions as this one with all sub-contractors of the Vendor.

c) Only if the bidder has entered into this Integrity Pact with CDAC, Hyderabad, the bidder shall be eligible to participate in this tender process or execution of the Agreement.

d) CDAC, Hyderabad will have the right to disqualify the bidder from this tender process if the bidder does not get this Integrity Pact from bidder's authorized signatory or violate any of its provisions.

Section 7 – Criminal charges against violation bidder/ Subcontractor(s)

If CDAC, Hyderabad obtains knowledge of conduct of the bidder or its Subcontractor, or of an

employee or a representative or an associate of the bidder or Subcontractor which constitutes corruption, or if CDAC, Hyderabad has substantive suspicion in this regard, CDAC, Hyderabad will inform the same to the Chief Vigilance Officer.

Section 8 – <Independent External Monitor>

a) CDAC appoints **Ms Priti Razdan, VO CDAC** as <Independent External Monitor> for this Integrity Pact. The task of <Independent External Monitor> is to review independently and objectively, whether and to what extent the Parties comply with the obligations under this Integrity Pact.

b) <Independent External Monitor> is not subject to instructions by the representatives of the Parties and performs his functions neutrally and independently. <Independent External Monitor> shall report to **Smt. Sunita Verma Group Coordinator (R&D in IT) and Chief Vigilance Officer, C-DAC at MeitY**.

c) The bidder accepts that <Independent External Monitor> has the right to access without restriction to all project documentation of CDAC, Hyderabad including that provided by the bidder. The bidder will also grant <Independent External Monitor>, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors of the Vendor. <Independent External Monitor> is under contractual obligation to treat the information and documents of the bidder/ Subcontractor(s) of Vendor with confidentiality.

d) CDAC, Hyderabad will provide to <Independent External Monitor> sufficient information about all meetings among the parties related to the tender process or the execution of the Agreement provided such meetings could have an impact on the contractual relations between CDAC, Hyderabad and the successful bidder. The Parties offer to <Independent External Monitor> the option to participate in such meetings.

e) As soon as <Independent External Monitor> notices, or believes to notice, a violation of this Integrity Pact, he will so inform CDAC, Hyderabad and request CDAC, Hyderabad to discontinue or take corrective action, or to take other relevant action. <Independent External Monitor> can in this regard submit non-binding recommendations. Beyond this, <Independent External Monitor> has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

f) <Independent External Monitor> will submit a written report to CDAC, Hyderabad within 8 to 10 weeks from the date of reference or intimation to him by CDAC, Hyderabad and, should the occasion arise, submit proposals for correcting problematic situations.

g) If <Independent External Monitor> has reported to CDAC, Hyderabad, a substantiated suspicion of an offence under relevant Indian Penal Code 1860 and Prevention of Corruption Act 1988, and CDAC, Hyderabad has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, <Independent External Monitor> may also transmit this information directly to the Central Vigilance Commissioner, Government of India.

h) The word 'Monitor' would include both singular and plural.

Section 9 – Pact Duration

a) This Integrity Pact begins when both Parties have legally signed it. It expires for the successful bidder 12 months after the last payment under the Agreement, and for all other bidders, 6 months after the execution of the Agreement with the Vendor.

b) If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/ determined by CDAC, Hyderabad.

Section 10 – Other provisions

a) This Integrity Pact is subject to Indian Law, place of performance and jurisdiction is the Office of CDAC, Hyderabad first above written, i.e. Hyderabad.

b) Changes and supplements of this Integrity Pact as well as termination notices need to be made in writing. Parties acknowledge that side agreements have not been made.

c) Should one or several provisions of this Integrity Pact turn out to be invalid, the remainder of this Integrity Pact remains valid. In this case, the Parties will strive to come to an agreement to their original intentions.

For & On Behalf of CDAC	For & On Behalf of the bidder
(Official Seal)	(Official Seal)
Signature: Signature:	
Name: _____	Name: _____
Place: _____	Place: _____
Date: _____	Date: _____
Witness:	Witness:
(Name Signature & Address):	(Name Signature & Address):

ANNEXURE -K- LAND BORDER SHARING

(To be submitted in Original on Letterhead-For All the items separately)

Date:

The Director,
Centre for Development of Advanced Computing (C-DAC) Plot
No: 6&7, Hardware Park,
Sy. No.1/1, Srisailam Highway,
Hyderabad – 501510.

Subject: Undertaking by **Supplier** for tender no. **.....** for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution **at C- DAC.**

Dear Sir,

We have read the clause mentioned in Office Memorandum No. F.No.6/18/2019-PPD of Public Procurement Division Department of Expenditure Ministry of Finance dated 23rd July 2020 and Order (Public Procurement No. 1) No. F.No.6/18/2019-PPD of Public Procurement Division Department of Expenditure Ministry of Finance dated 23rd July 2020 and further Order/OMs regarding restrictions on procurement from a bidder of a country which shares a land border with India. In view of this; we certify that

a) We are not from a country sharing land border with India and any registration as mentioned in said OM is not applicable to us.

OR.

b) We are registered with the competent authority as mentioned in said OM. The copy of registration No.xxx dt.xxx is enclosed.

Signature & company seal

Name
Designation
Email
Mobile No.

ANNEXURE - L - LOCAL CONTENT DECLARATION

(To be given by Statutory Auditor / Cost Auditor / Cost Accountant / CA for tender value above Rs.10 crores)

To
Centre for Development of Advanced Computing
Hyderabad

SUBJECT: …….
Tender Reference No. …….

I _____ S/o, D/o, W/o _____, Resident of _____ do hereby solemnly affirm and declare as under that:

I will agree to abide by the terms and conditions of subject tender terms & conditions issued by C-DAC.

1. The information furnished hereinafter is correct to best of my knowledge and belief and I undertake to produce relevant records on demand by C-DAC for the purpose of verifying the Local Content (LC).

2. The LC for all inputs which constitute the said Goods /Services/Works has been verified by me and I am responsible for the correctness of the claims made herewith against the subject tender participation by M/s_____(Bidding Firm name).

3. In the event of the LC of the Goods/Services/Works mentioned herein is found to be incorrect and not meeting the prescribed LC norms, based on the verification by C-DAC (or) appropriate authority, I/my firm will be liable as under clause 9(f) of Public Procurement (Preference to Make in India) Order 2017.

4. I agree to maintain all information regarding my claim for LC in the Company's record for a period of 2 years and shall make this available for verification to any statutory authorities.

5. The details of LC claim by M/s_____(Bidding Firm name):
   a) Goods /Services/Works for which the certificate is produced:
   b) Percentage of LC claimed: ……..%
   c) Type of Supplier (Class-I/Class-II):……
   d) Name and contact details of the unit of the manufacturer/Service Station:

Note: "Local Content" means the amount of value added in India which shall, be the total value of the item being offered minus the value of the imported content in the item (including all customs duties) as a proportion of the total value, in percent. The bidders cannot claim services such as transportation, insurance, installation, commissioning, training and after sales service support like AMC/CMC etc as local value addition.

Certified by the Auditors,
(Name of the Auditors)
CA Membership Number……

ANNEXURE - M

BIDDER DETAILS

<Letter Head>

Details of the bidder Organization	
Name	
Address in Delhi:	
Address of offices in India	
Date of commencement of legal practice/services	
Other Relevant Information	
Mandatory Supporting Documents: a. Copy of the Certificate of Incorporation issued by Registrar of Companies. In case of Partnership firm, duly signed and notarized copy of the partnership deed or a Certificate of Registration issued by the Registrar of Firms; or in case of a sole proprietorship, a GST registration certificate and/or PAN number. b. Supporting documentary proof for having office / branch in Delhi /National Capital Region. c. Relevant sections of Memorandum of Association of the company or filings to the stock exchanges to indicate the nature of business of the company. d. Copy of board resolution (or) Power of attorney authorizing the bid signatory in support of Annexure-IV "Authorization Letter".	

CERTIFICATE

I,<*name of the bidder*>,certify that the details submitted by me are true and no information is false orincorrect.

Date:

Name:

Signature:

(Seal)

ANNEXURE – N

DRAFT NDA

This Non Disclosure Agreement ("Agreement") is made effective from this day of [month year]between [agency name] having office at [address of agency] and Centre for Development of Advanced Computing, Noida, a constituent unit of C-DAC, a Scientific Society under the Ministry of Electronics and Information Technology, Government of India, registered under the Societies Registration Act, 1860 and Bombay Public Trust Act, 1950, having its registered office at Savitribai Phule Pune University Campus, Ganesh Khind, Pune-411007 and place of business at C-56/1, Anusandhan Bhawan, Sector-62, Noida 201309 (hereinafter referred to as "Client")

(Client and [agency name] shall be individually referred to hereinafter as a "Party" and collectively as the "Parties")

WHEREAS, the Client has appointed [agency name] for rendering < consultancy> services during the period commencing from <ddmmyy> to < ddmmyy>

WHEREAS, the parties hereto are willing to execute this Agreement in order to protect certaininformation to be disclosed to each other for the aforesaid purposes.

NOW, THEREFORE, in consideration of the recitals set forth above and the covenants set forth herein, the Parties agree that:

1. It is hereby agreed that the discretion applied at the time of disclosure would provide thebest protection of Confidential Information of either Party. Accordingly, a Disclosing Partyshall ensure that only those Confidential Information which serve the engagement objectives shall be disclosed as per an agreed procedure to the identified individuals at therecipient"send.

2. Recipient agrees to protect Confidential Information received from the Disclosing Partywith at least the same degree of care as it normally exercises to protect its own proprietary information of a similar nature. Recipient agrees to promptly inform the Disclosing Party ofanyunauthorised disclosure of the Disclosing Party"s Confidential Information.

3. In the case of Confidential Information that is disclosed only orally, Disclosing Party shall, within seven days after such disclosure, deliver to the Receiving Party a brief written description of such Confidential Information; identifying the place and date of such oral disclosure and the names of the representatives of the Receiving Party to whom such disclosure was made. It is expected that such information will bear a legend or label of "Confidential" or

other similar designation manifesting intent that the information is confidential ("ConfidentialInformation").

4. The restrictions set forth in this Agreement on the use or disclosure of Confidential Information shall not apply to any information which:

a. is independently developed by the Recipient ; or
b. is rightfully received free of restriction from another source having the right to so furnish suchinformation; or
c. has become generally available to the public; or
d. at the time of disclosure to the Recipient was rightfully known to such party or its affiliated companies free of restriction as evidenced by documentation in its possessions; or
e. the non-Disclosing Party agrees in writing to be free of such restrictions; or

is required to be furnished to any authority, department, office or body by a decree, order or authorization of law.

5. Each Party shall use Confidential Information of the other Party which is disclosed to it only for the purpose of this Agreement and shall not disclose such Confidential Information to anythird party, without the other Party's prior written consent, other than to [agency name] subcontractors and to each other's employees on a need-to- know basis.

6. All information shall remain the property of the Disclosing Party and shall be returned upon written request or upon the Recipient's determination that it no longer has a needfor such information except that both parties may retain copies of the Confidential Information, to the extent required to comply with applicable legal and regulatory requirements.

7. The Parties agree that during the existence of the term of this Agreement, neither Party shall solicit directly or indirectly the employees of the other Party.

8. The term of this Agreement shall be xxxx from the date of its execution by both Parties.Both the parties shall jointly review this Agreement after end of xxxx and shall extendit for xxxxx at a time if mutually agreed upon by both the parties

9. The authorised representatives from [agency name] side shall be –
a. <xx>

10. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by in accordance with the Arbitration and Conciliation Act, 1996. Any claim for losses under this Agreement shall be restricted to direct losses only.

11. This Agreement constitutes the entire understanding between the Parties hereto as to the information and merges all prior discussions between them relating thereto. No amendment ormodification of this Agreement shall be

valid or binding on the Parties unless made in writingand signed on behalf of each of the Parties by their respective authorised officers orrepresentatives.

12. The Parties agree that the laws of India, other than its conflict of laws provisions, shallapply inany dispute arising out of this Agreement.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed as ofthedate set forth above.

For and on behalf of	For and on behalf of
Sig.:	Sig.:
Name:	Name:
Title:	Title:
Place:	Place:

Witness:
Signature:
Name:
Title

ANNEXURE - O
CHECKLIST

Sr	Description	Page No (s)
1	Annexure – I Technical Bid Summary	
2	Annexure – II Technical Bid Compliance	
3	Annexure – III Price Break-up Format	
4	A copy of Certificate of Incorporation, Partnership Deed / Memorandum and Articles of Association / any other equivalent document showing date and place of incorporation, as applicable, in support of eligibility criteria.	
5	Copies of PAN and GST registration certificates, as applicable.	
6	The detailed technical solution offered as per format given in **Section – V.**	
7	The copies of audited Profit and Loss Accounts **OR** the certificate from a Chartered Accountant certifying the annual sales turnover of the bidder for the last 3 financial years. (Average Annual Financial Turnover of Rs. 180 Crores during the last three financial years ending 31st March 2023)	
8	Other documents necessary in support of eligibility criteria, product catalogues, brochures etc.	
9	Bidder must have executed successfully at least two projects of similar nature / complexity in India, each costing not less than Rs. 25 Cr.	
10	Bid Security Declaration, as per **Annexure – A.**	
11	Compliance Letter, as per **Annexure – B.**	
12	The undertakings from the Principal Manufacturers (OEMs) of equipment/ items offered as per **Annexure – C.**	
13	Technical Solution offered Annexure – D	
14	Acceptance Letter Annexure – E	
15	Undertaking for Non-Deviation Annexure - F	

16	Non – Blacklisting Annexure – G	
17	Authority Letter Annexure - H	
18	Litigation Impact Annexure – I	
19	Integrity Pact Annexure – J	
20	Land Border Sharing Annexure – K	
21	Local Declaration Annexure – L	
22	Bidder Details Annexure – M	
23	Draft NDA Annexure – N	
24	Check List Annexure – O	

ANNEXURE - P
PROFORMA OF BANK GUARANTEE
(on non-judicial paper of appropriate value)

To,
Centre for Development of Advanced Computing (C-DAC)
Plot No: 6&7, Hardware Park,
Srisailam Highway,
Hyderabad – 501510

BANKS GUARANTEE NO:
DATE:

Dear Sir(S)

This has reference to the Purchase Order No. Dated been placed by Centre for Development of Advanced Computing(C-DAC), Hyderabad on M/s (Name & Address of vendor) for Implementation of Turnkey Solution for Establishing Private Cloud with Software Defined Components for Compute, Storage, Network and Security at DC & DR locations along with Replication Solution (description of items) at C-DAC, site.

The conditions of this order provide that the vendor shall,

Arrange to deliver the items listed in the said order to the consignee, as per details given in said order, and

Arrange to install and commission the items listed in said order at client's site, to the entire satisfaction of C-DAC and

Arrange for the comprehensive warranty service support towards the items supplied by vendor on site as per the warranty clause in said purchase order.

M/s (Name of Vendor) has accepted the said purchase order with the terms and conditions stipulated therein and have agreed to issue the performance bank guarantee on their part, towards promises and assurance of their contractual obligations vide the Supply Order No. _____M/s. __(name of vendor) holds an account with us and has approached us and at their request and in consideration of the promises, we hereby furnish such guarantees as mentioned hereinafter.

C-DAC shall be at liberty without reference to the Bank and without affecting the full liability of the Bank hereunder to take any other undertaking of security in respect of the bidders obligations and / or liabilities under or in connection with the said contract or to vary the terms vis-a – vis the bidder or the said contract or to grant time and or indulgence to the bidder or to reduce or to increase or otherwise vary the prices or the total contract value or to forebear from enforcement of all or any of the obligations of the bidder under the said contract and/or the remedies of C-DAC under any security now, or hereafter held by C-DAC and no such dealing(s) with the bidder or release or forbearance whatsoever shall have the effect of releasing the bank from its full liability of C-DAC hereunder or of prejudicing right of C-DAC against the bank.

This undertaking guarantee shall be a continuing undertaking guarantee and shall remain valid and irrevocable for all claims of C-DAC and liabilities of the supplier arising up to and until _____(date)

This undertaking guarantee shall be in addition to any other undertaking or guarantee or security whatsoever the that C-DAC may now or at any time have in relation to its claims or the

supplier's obligations/liabilities under and / or in connection with the said contract and C-DAC shall have the full authority to take recourse to or enforce this undertaking guarantee in preference to the other undertaking or security (ies) at its sole discretion and no failure on the part of C-DAC in enforcing or requiring enforcement of any other undertaking or security shall have the effect of releasing the bank from its full liability hereunder.

We _____ (Name of Bank) hereby agree and irrevocably undertake and promise that if in your (C-DAC's) opinion any default is made by M/s _____(Name of Vendor) in performing any of the terms and /or conditions of the agreement or if in your opinion they commit any breach of the contract or there is any demand by you against M/s _____(Name of Vendor), then on notice to us by you, we shall on demand and without demur and without reference to M/s _____(Name of Vendor), pay you, in any manner in which you may direct, the amount of Rs. _____/- (Rupees _____ Only) or such portion thereof as may be demanded by you not exceeding the said sum and as you may from time to time require. Our liability to pay is not dependent or conditional on your proceeding against M/s _____ (Name of Vendor) and we shall be liable & obligated to pay the aforesaid amount as and when demanded by you merely on an intimation being given by you and even before any legal proceedings, if any, are taken against M/s _____(Name of Vendor)

The Bank hereby waives all rights at any time inconsistent with the terms of this undertaking guarantee and the obligations of the bank in terms hereof shall not be anywise affected or suspended by reason of any dispute or disputes having been raised by the supplier (whether or not pending before any arbitrator, Tribunal or Court) or any denial of liability by the supplier or any order or any order or communication whatsoever by the supplier stopping or preventing or purporting to stop or prevent payment by the Bank to C-DAC hereunder.

The amount stated in any notice of demand addressed by C-DAC to the Bank as claimed by C-DAC from the supplier or as suffered or incurred by C-DAC on the account of any losses or damages or costs, charges and/or expenses shall as between the Bank and C- DAC be conclusive of the amount so claimed or liable to be paid to C-DAC or suffered or incurred by C-DAC, as the case may be and payable by the Bank to C-DAC in terms hereof.

You (C-DAC's) shall full liberty without reference to us and without affecting this guarantee, postpone for any time or from time to time the exercise of any of the powers and rights conferred on you under the contact with the said M/s _____(Name of Vendor) and to enforce or to forbear from endorsing any power or rights or by reason of time being given to the said M/s _____ (name of Vendor) which under law relating to the sureties would but for the provisions have the effect of releasing us.

You will have full liberty without reference to us and without affecting this guarantee, postpone for any time or from time to time the exercise of any of the powers and rights conferred on you under the contract with the said M/s _____(Name of Vendor) and to enforce or to forbear from endorsing any power or rights or by reason of time being given to the said M/s _____ (Name of Vendor) which under law relating to the sureties would but for the provisions have the effect of releasing us.

Your right to recover the said sum of Rs. _____/- (Rupees _____only) from us in manner aforesaid will not be affected/ or suspended by reason of the fact that any dispute or disputes have been raised the said M/s _____(Name of Vendor) and/ or that any dispute or disputes are pending before any officer, tribunal or court or Arbitrator.

The guarantee herein contained shall not be determined or affected by the liquidation or winding up, dissolution or change of constitution or insolvency of the said M/s _____(Name of Vendor) but shall in all respects and for all purposes be binding and operative until payment of all dues to C-DAC in respect of such liability or liabilities.

Our liability under this guarantee is restricted to Rs._____/- (Rupees _____Only). Our guarantee shall remain in force until unless a suit action to enforce a claim under guarantee is filed against us within six months from (which is date of expiry of guarantee) all your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there under.

We have power to issue this guarantee in your favour under Memorandum and Articles of Association of our Bank and the undersigned has full power to do under the power of Attorney dated.

Notwithstanding anything contained herein:

A. Our liability under this guarantee shall not exceed Rs_____ (in words)

B. This bank guarantee shall be valid up to _____ & unless a suit for action to enforce a claim under guarantee is filed against us within 1 month from the date of expiry of guarantee. All your rights under the said guarantee shall be forfeited and we shall be relieved and discharged from all liabilities there after i.e. after one month from the date of expiry of this Bank guarantee

C. We are liable to pay the guaranteed amount or any parts thereof under this bank guarantee only and only if you serve upon us a written claim or demand or before _____

D. The Bank guarantee will expire on 2 Months beyond the warranty period of 5 Years (the period of 62 months) from the date of successful installations of the items in the order) _____

SEAL OF THE BANK

Authorised Signatory
Granted by the Bank

Yours faithfully,

For (Name of Bank)

(END OF DOCUMENT)