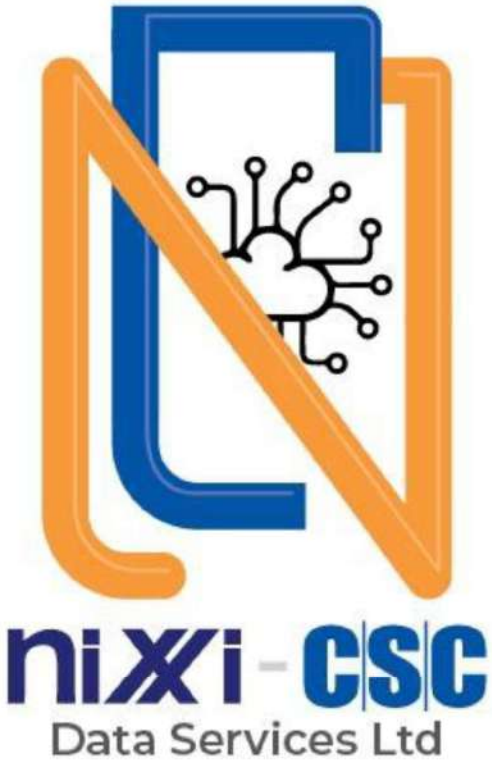


9th Floor, Statesman House,

Barakhamba Road,

New Delhi

Tender Document for IT Infrastructure for Tripura State Data Centre at Agartala

NIXI-CSC Requirement

This tender document is being issued to select an agency for delivery, installation, and commissioning of active components "**for Upcoming State Data Centre at Agartala with uptime of 99.8%**". Bids (Technical & Financial) are invited from eligible bidders which should be valid for a period of 80 days from the last date of submission. Below are the timelines:

Cost of Tender Documents

INR 5000/- to be deposited **at**

NIXI-CSC DATA SERVICES LTD.,

A/c No. 921020024655044,

IFS Code – UTIB0000007,

AXIS BANK LTD., Branch – Barakhamba Road,

Connaught Place,

NEW DELHI- 110001

Earnest Money Deposit (EMD) and Performance Bank Guarantee

The Bidder will furnish, as part of its bid, an Earnest Money Deposit (EMD) of **INR 1,25,00,000/-** which should be deposited online via RTGS and performance bank guarantee of 5% of the least awarded tender value in INR should be submitted as FDR/RTGS, to the bank account mentioned below

The performance bank guarantee should be valid for till the completion of the project days from the last date of submission of bids

Within fifteen (15) working days from the date of issuance of PO the successful Bidder shall at his own expense submit unconditional and irrevocable Performance bank guarantee (PBG) of 5% of the contract value to the NIXI-CSC. The PBG shall be from a Nationalized Bank or a Scheduled Commercial Bank in the format prescribed via FDR/Online, for the due performance and fulfilment of the contract by the bidder.

NIXI-CSC DATA SERVICES LTD.,

A/c No. 921020024655044

IFS Code – UTIB0000007, AXIS BANK LTD., Branch – Barakhamba Road, Connaught Place,

NEW DELHI- 110001

except those who are registered with the Central Purchase Organization, National Small Industries Corporation (NSIC) or the concerned Ministry or Department only (if they are registered for relevant categories/ products/ services under this tender). The bidder must submit the certification of registration with one of the given authorities along with the eligibility documents.

The EMD will be denominated in Indian Rupees and will be accepted only in form of Online line deposit via by a Nationalized/ Scheduled Bank, in favour of NIXI-CSC, New Delhi. (as mentioned above)

Unsuccessful Bidder's EMD will be discharged/ returned after award of contract to the successful Bidder. **No interest will be paid by the Purchaser on the EMD**.

The successful Bidder's EMD will be discharged upon the bidder executing the Contract. **No interest will be paid by the Purchaser on the EMD**.

Further, if for any reason, the tender floated by the purchaser is scrapped/ cancelled, EMD of the bidder's will be discharged/ returned.

Any fraudulent measures may result in cancellation of the bid response and appropriate legal action will be taken by the purchaser.

The EMD may be forfeited:

i. If a Bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid; or
ii. In the case of a successful Bidder if the Bidder fails.

- To sign the Contract in accordance with the tender; or
- To furnish online deposit for the EMD and performance bank guarantee for contract performance in accordance with the tender
- If a bidder quotes unrealistically high/ low rates in its financial bid.

Contents

INVITATION TO BID

This invitation to Bid is for **"Supply , Installation , Commissioning and Integration of active IT Infrastructure of Tripura State Data Centres (TSDC)".**
The Bidders are advised to study the tender document carefully. Submission of Bids shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications. This section provides general information about the Issuer (i.e. NIXI-CSC), important dates and addresses and the overall eligibility criteria for the Bidders.

DUE DILIGENCE

The Bidder is expected to examine all instructions, forms, terms, and specifications in this RFP and study the RFP document carefully. Bid shall be deemed to have been submitted after careful study and examination of this RFP with full understanding of its implications. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP. Failure to furnish all information required by this RFP or submission of a Bid not responsive to this RFP in each and every respect will be at the Bidder 's own risk and may result in rejection of the Bid and for which NIXI-CSC shall not be held responsible.

ISSUER

The joint venture of National Internet Exchange of India (NIXI) and CSE e-governance services Ltd herein after refers as "NIXI-CSC Data Services Centre" invites proposals for **"Supply , Installation , Commissioning and Integration of active IT Infrastructure of Tripura State Data Centres (TSDC)".** Issuer and Address for Bid Submission & Correspondence.

CEO-MD, NIXI-CSC DATA SERVICES LTD

9th Floor, B-Wing, Statesman House Barakhamba Road,

Connaught place Delhi

New Delhi DL 110001 IN

E-Mail: pdns@NIXI.in.

Key Events & Dates

Table I – Key Events & Dates

S. No	Information	Details
1.	RFP release date	25th Nov

2.	Last date for submission of written queries for clarifications	2nd Dec
3.	Date of pre-bid conference (DIT office, IT Bhavan Indiranagar, ITI Road Agartala 25th Nov 2022– 11 AM), Local contact Person Mr. Salil Das-08800661850	5th Dec
4.	Release of response to clarifications	7th Dec
5.	Bid validity period	60 days from the last date (deadline) for submission of proposals
6.	Last date (deadline) for submission of bids-by mail (pdns@nixi.in) * ** Financial bid must be password protected	9th Dec (11 am)
7.	Opening of technical bids	12th Dec (4 pm)
8.	Place, time, and date of opening of financial proposals received in response to the RFP notice	Will be intimated later

*The bidder should submit two separate files for Technical bid as well as financial bid . Hard copy of all documents, duly stamped by competent authority of the bidder must also be received at NIXI Delhi office, address given below within 1 week of the last date of submission of the soft copy of the bid via email.

** For Financial bid, the password must not be shared in any form by bidder to any NIXI-CSC official or any other personnel outside the organization, as the financial bid will be opened in front of the qualified bidders in technical evaluation at the time of financial bid opening and the respective bidders will provide their own password to NIXI-CSC officials at the time of bid opening only.

SCHEDULE OF REQUIREMENT

STATE DATA CENTRES (SDC)

Tripura has been in the verge for digital transformation and has been working recently to become a digital state in the country. The SDC shall host many e-Governance applications covering almost all government departments, Mobile tele-density, Internet penetration etc. Government of Tripura has set up the State Data Centre (SDC) in Agartala to boost the e-Governance activities of the State. Tripura State Data Centre is the Government Data Centre in

the country and has been catering operations of smart cities etc since its establishment. For achieving the full capacity of this Data Centre, Government of Tripura will start revamping it to cater 80+ rack solution. The summary status of the Data Centres are shared in the annexures.

PURPOSE

The purpose of this bid is to for **"Supply , Installation , Commissioning and Integration of active IT Infrastructure of Tripura State Data Centres (TSDC)"** (Refer Annexures for more details) respectively. The layout is given only as reference and the bidders are requested to visit the Data Centres at their own cost for better understanding of the site.

REQUIRED COMPONENTS AND SERVICES

Design, Construction of the server farm area with all required MEPC (mechanical, civil, plumbing, electrical) etc as per the guidelines stated in this RFP adhering to international standards & specifications for the equipment listed below:

PROJECT TIME SCHEDULE

The total duration of the project is for a period of 60 days from the date of release of work order including final acceptance and testing (FAT), training and submission of documentation.

INSTRUCTION TO THE BIDDERS

- **TSDC**" means Tripura State Data Centre
- **"UAT"** means User Acceptance Testing
- **"Bidder"** shall mean an Individual Company registered under the Companies Act 1956 or as defined in this document that participates in the Bidding process
- "**Representative"** shall mean the person appointed by NIXI-CSC from time to time to act on its behalf at the site for overall coordination, supervision, and project management at site
- The **"Successful bidder / Implementation Agency**" means the company with whom the order has been placed for providing Services as specified in this tender/contract and shall be deemed to include the Implementation Agency's successors, representatives (approved by NIXI-CSC), heirs, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the contract
- **"Implementation Agency's Representative"** means the person, or the persons appointed by the implementation agency from time to time to act on its behalf for overall coordination, supervision, and project management. This definition shall also include any and/or all of the employees of Bidder, their authorized agents and representatives and other personnel employed or engaged either directly or indirectly by the implementation agency for the purposes of the Contract
- **"Contract"** means the Agreement entered into between NIXI-CSC and the "Implementation Agency" as recorded in the Contract form signed by NIXI-CSC and the "Implementation Agency" including all attachments and Annexes thereto, the Tender and all Annexes thereto and the agreed terms as set out in the Bid, all documents incorporated by reference therein and amendments and modifications to the above from time to time
- **"Confidential Information"** means any information disclosed to or by any Party to this Contract and includes any information in relation to the Parties, a third party or any information with regard to any taxpayer, or any other person who is covered within the ambit of any commercial taxes legislation including any such information that may come to the knowledge of the Parties hereto / Bidder's Team by virtue of this Contract that:

By its nature or by the circumstances in which it is disclosed is confidential; or Is designated by the disclosing Party as confidential or identified in terms connoting its confidentiality; but does not include information which is or becomes public knowledge other than by a breach of this Contract

- "**The Contract Price/Value**" means the price payable to the successful bidder under the Contract for the full and proper performance of its contractual obligations
- **"Parties"** means NIXI-CSC and the successful bidder and "Party" means either of the Parties
- **"Service"** means facilities/services to be provided as per the requirements specified in this tender document and any other incidental services, such as installation, implementation, support and provision of technical assistance and other such obligations of the Successful bidder covered under the Contract.

PRE-BID CONFERENCE

NIXI-CSC shall organize a Pre-Bid Conference on the scheduled date and time. NIXI-CSC may incorporate any changes in the RFP based on acceptable suggestions received during the interactive Pre-Bid Conference. The decision of the NIXI-CSC regarding acceptability of any suggestion shall be final and shall not be called upon to question under any circumstances.
The bidders shall visit the TSDC prior to the pre-bid to have a better understanding about the existing system and location. After the bid submission date confirmation, no New Requirement/ Quires/ addition in RFP and BOQ will be entertained by NIXI-CSC.
The bidders who wish to visit sites shall give the email request to NIXI-CSC in the format given below. The request should reach NIXI-CSC at least 24 hours before the scheduled time.

Sl.no	Company	Name	Email	Mobile	Queries	Justification

AMENDMENT OF RFP DOCUMENT

At any time prior to the last date for receipt of bids, the purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, modify the Tender Document by an amendment. The amendment will be notified on NIXI-CSC portal **http://NIXI.in/notice/** and should be taken into consideration by the prospective agencies while preparing their bids.

In order to provide prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the purchaser may, at its discretion, request for extending the last date for the receipt of bids.

Purchaser at any time during the tendering process can request all the prospective bidders to submit revised technical/ financial bids and/or supplementary financial bids without thereby incurring any liability to the affected bidder or bidders

VENUE AND DEADLINE FOR SUBMISSION OF PROPOSAL

The bid proposals must be received through the specified websites (as mentioned only and that also not later than the dates specified in Events and dates section of this bid document.

PROCEDURE FOR SUBMISSION OF BIDS

MODES OF SUBMISSION

1. It is proposed to have Two E-bids for this e-tender:

I. Technical E- Bid - which includes documents for Pre-qualification Criteria and Technical proposal

II. Commercial E- Bid (Password Protected)

2. Please Note that Prices shall be indicated only in the Commercial Bid. If price is indicated in the Pre-Qualification Bid or Technical Bid, that Bid is liable to be rejected.

Bids shall be submitted only through the specified e-tendering email.

COST OF BIDDING

The Bidder shall bear all costs associated with the preparation and submission of its Bid including cost of presentation for the purposes of clarification of the Bid, if so desired by NIXI-CSC. NIXI-CSC will be in no way responsible or liable for those costs, regardless of the outcome of the tendering process.

INSTRUCTIONS FOR TENDER PROCESS

a) Bids must be submitted in two parts (Technical and Financial). Every part of bid should be in separate envelope and should be sealed (for Hard copy submission)

b) Bidder should submit their compliance against each column in technical bid.

c) Each column of financial bid should be filled up.

d) Technical compliance should be supported with relevant documents.

e) Bids should be completed in all respects, must be submitted on or before the last date specified in the schedule of events.

f) NIXI-CSC may, at its own discretion, extend the last date for submission of tenders.

g) All the bids (technical and financial) must be valid for a period of 60 days from the last date of submission of the tender for execution of contract.

h) In exceptional circumstances, prior to expiry of the original time limit, NIXI-CSC may request the bidders to extend the period of validity for a specified additional period beyond the original validity of 60 days. The request and the bidders' responses shall be made in writing. The bidders, not agreeing for such extensions will be allowed to withdraw their bids.

i) No Bid shall be modified, substituted, or withdrawn by the bidder after the due date.

j) Any alteration/ modification in the bid or additional information supplied subsequent to the bid's due date, unless the same has been expressly sought for by the authority, shall not be considered.

k) The bid submitted shall become invalid if: -

• The bidder is found ineligible.

• The bidder does not provide all the documents as stipulated in the bid document.

l) The bidder shall refer the Annexure 4 onwards to refer for more details and shall comply/adhere to those documents at the time of bid submission.

Terms and Conditions

a) Selected bidder must submit the performance bank guarantee (PBG) as per format defined in **Annexures** within stipulated days of after the receipt of notification of award of the Contract from the Purchaser

b) Selected bidders sign the agreement within Stipulated days (as shown above) from the date of receipt of PBG.

c) All equipment must be compatible with Indian electrical standards

d) NIXI-CSC, without assigning any reason can reject any tender(s), in which any prescribed condition(s) is/ are found incomplete in any respect and at any processing stage.

e) The decision of NIXI-CSC arrived during the various stages of the evaluation of the bids will be final & binding on all bidders.

f) Extra printed/ written conditions mentioned in the tender bids submitted by bidders will not be binding on NIXI-CSC.

g) Upon verification, evaluation/ assessment, if in case any information furnished by the bidder is found to be factually false/ incorrect (not supported by the documents), their total bid shall be summarily rejected.

h) NIXI-CSC will not be responsible for any misinterpretation or wrong assumption by the bidder, while responding to this tender.

i) All bidders agree with NIXI-CSC for honouring all aspects of fair-trade practices in executing the work orders placed by NIXI-CSC.

j) In the event of an empanelled company or the concerned division of the company being taken over/ bought over by another company, all the obligations and execution responsibilities under the agreement with NIXI-CSC, should be passed on for compliance by the new company in the negotiation for their transfer.

k) If the name of the product is changed for describing substantially the same in a renamed form; then all techno-fiscal benefits agreed with respect to the original product, shall be passed on to NIXI-CSC and the obligations with NIXI-CSC taken by the bidder with respect to the product with the old name shall be passed on along with the product so renamed.

l) In the case, bidder is found in breach of any condition(s) of tender or work order, at any stage during the course of service, appropriate legal action as per rules/ laws, may be initiated against the bidder and BG shall be forfeited, besides debarring, and blacklisting the bidder concerned for at least three years, for further dealings with NIXI-CSC.

m) Bidder must provide valid OEM authorization certificates for all the products quoted as well as certify that the proposed product is not declared end of sale. If the product is declared end of sale during contract period. Bidders should upgrade the equipment with same specification or higher with no cost to the purchaser.

n) The bidder must quote the products/ software's strictly as per the tendered specifications/ requirements. Complete technical details along with make, model number, complete specifications along with the quotation must be provided.

o) Any additional components, sub-components, assemblies, sub-assemblies, cables, electrical cables, connectors, sockets, required civil infrastructure that would be required to meet the desired installation requirements must be provisioned by the bidder at no additional cost to the purchaser and without any project delays.

p) The bidder must also highlight the support capabilities in India and the escalation matrix.

q) Purchaser will not be responsible for any dispute related to IPR; the entire onus for resolution will lies with the respective bidder/ OEM(s). For any customizations done by purchaser project team, the IPR remains with purchaser.

r) Purchaser reserves the right to procure the number of licenses as deemed appropriate for the software components. Purchaser reserve right to reduce or increase the required quantity.

s) Bidder must ensure that the unit price of components should include packing, forwarding, freight, insurance, installation, commissioning, warranty, or any other charges for supply at anywhere in India.

t) The bidder must follow change management procedures and security policies as suggested by purchaser time to time.

u) The bidder must co-ordinate with the other System Integrator (SI), if any, for ensuring continuity of operations. The bidder must also support the OEM in diagnosing the problems related to their systems.

v) In case any product provided by the bidder, does not meet the performance parameters mentioned by the bidder in the proposal, then the additional/ replaced appliance/ software must be immediately installed at the bidder's expense.

w) The bidder must note that the Purchaser will provide the Sign-off for delivery, installation and commissioning after successful deployment and testing of the procured components.

x) The bidder must ensure that all product set that is deployed for the proposed deployment is supported by OEM 24x7x365 backend support.

y) The bidder must ensure that no equipment's is declared as end of life/Sale while bidding and for next 5 years of product supply.

Permits, Taxes and Other Duties

The bidder shall obtain necessary road permits and pay all necessary local taxes and duties in delivering the equipment. NIXI-CSC will not be responsible for the same.

Subcontract

The Bidder may appoint a subcontractor for the execution of a certain parts of the work under this contract. The subcontracting details and documents supporting the same would be required as a part of Technical Bid. **The Bidder should ensure that there is only one level of subcontracting for the entire duration of the contract**.

The bidder should ensure that there is no discontinuity in services by the Agency or the subcontractor (due to change in sub-contractors) during the period of contract.

Prior to executing any contract or entering into any Contract or understanding with a delegate/ sub-contractor, the bidder will ensure that each delegate/ sub-contractor appointed by the bidder. executes a Deed of Adherence and a Performance Undertaking. A copy of the detailed agreement with prices blanked should be submitted to the Purchaser before submission of the first invoice.

The bidder should ensure that the delegate/ subcontractor appointed is competent, professional and possess the requisite qualifications and experience appropriate to the tasks they will perform under this contract. The bidder will also ensure that the delegate/ subcontractor appointed is certified in carrying out the designated work and is a registered organization.

Any change in the sub-contractor(s) after the arrangement is firmed up, will be made by Contractor only with the prior written information to the Purchaser.

The Bidder will be responsible and would ensure the proper commissioning and performance of the site's services or tasks, hence, the bidder will be held responsible for any non- performance or breach by delegate/ sub-contractor. The bidder indemnifies and would keep purchaser indemnified against any losses, damages, claims or such other implications arising from or out of the acts and omissions of such delegate/ sub-contractor. The bidder would be responsible for making all payments to the delegate/ sub-contractor, in respect of any work performed or task executed, and the purchaser would not be responsible for any part or full payment which is due to such delegate/ sub-contractor.

Nothing in this Contract or any delegation/ subcontract agreement hereunder should relieve the bidder from its liabilities or obligations under this Contract to provide the Services in accordance with this Contract.

Where the purchaser deems necessary, it would have the right to require replacement of any delegate/ sub-contractor with another delegate/ sub-contractor and the bidder will in such case terminate forthwith all agreements/ contracts other arrangements with such delegate/ sub-contractor and find of the suitable replacement for such delegate/ sub- contractor to the satisfaction of the Purchaser at no additional charge.

A notice will be issued 15 days in advance before removing a sub-contractor, any impact due to non-presence of person will invoke a penalty.

CLARIFICATION ON TENDER DOCUMENT

A prospective Bidder requiring any clarification on the RFP Document may submit his queries, in writing, at the mailing address and as per schedule indicated in "Invitation for Bids / Key Events and Dates" section. The queries must be submitted in the following format only to be considered for clarification:

The queries not adhering to the below-mentioned format shall not be responded.

Representatives from any OEM will not be allowed to be part of the pre-bid meeting. OEMs should also not accompany any of their system integrators or partners and are expected to submit their queries through partners for seeking clarifications.

S. No.	Page No	Clause No	Clause header	Clause details as in RFP	Query/ Clarification Required	Justification/Reason for changes required (If any)

Once answers to query/queries are published, the same queries will not be entertained further.

It is expected that the Bidder shall do their own due diligence on the question they may ask. Any changes sought must be with proper justification. Any statement such as 'specification/requirement' is not vendor neutral OR it implies to a single OEM or any such statement similar to this, must be asked with adequate and credible proof and justification.

NIXI-CSC will respond to any request for clarification to queries on the Tender Document, received not later than the dates prescribed in Invitation for Bids / Key events and dates. The clarifications (including the query but without identifying the source of inquiry) shall be replied/uploaded (with responses).

NIXI-CSC will only accept queries from direct bidder, queries from any sub-contractor, partner, OEM can raise their query via their respective bidders/SI. No direct Query from sub-contractor, partner, OEM will be accepted by NIXI-CSC and will be considered invalid for reply .

LANGUAGE OF BIDS

The Bids prepared by the Bidder and all correspondence and documents relating to the Bids exchanged by the Bidder and NIXI-CSC, shall be written in English language. Any printed literature furnished by the Bidder may be written in another language so long the same is accompanied by a duly attested English translation in which case, for purposes of interpretation of the Bid, the English translation shall govern. Price bid total value will be filled in both (number & Words) by the bidder.

DOCUMENTS COMPRISING THE BIDS

The Bid prepared by the Bidder shall comprise the following components. The Bids not conforming to the requirements shall be summarily rejected.

BID SUBMITTALS

In support of eligibility, a Bidder must submit the following documents (besides the other requirements of the tender), original copies or attested copies, as the case may be, in the absence of which the Bids are liable to be rejected. See annexures for more details regarding these documents

CONFIDENTIALITY

The RFP document is confidential and is not to be reproduced, transmitted, or made available by the Recipient to any other party. The RFP document is provided to the Recipient on the basis of the undertaking of confidentiality given by the Recipient to Company. NIXI-CSC may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same terms and conditions as this original and subject to the same confidentiality undertaking.

The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with NIXI-CSC or any of its customers, suppliers, or agents without the prior written consent of NIXI-CSC.

NO LEGAL RELATIONSHIP

No binding legal relationship will exist between any of the Recipients / Respondents and NIXI-CSC until execution of a contractual agreement.

ERRORS AND OMISSIONS

Each Recipient should notify NIXI-CSC of any error, omission, or discrepancy found in this RFP document.

ACCEPTANCE OF TERMS

A Recipient will, by responding to NIXI-CSC RFP, be deemed to have accepted the terms as stated in the RFP.

NORMALIZATION OF BIDS

The NIXI-CSC may go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that, shortlisted bidders are more or

less on the same technical ground. After the normalization process, if NIXI-CSC feels that any of the Bids needs to be normalized and that such normalization has a bearing on the price bids; the NIXI-CSC may at its discretion ask all the technically shortlisted bidders to re-submit the technical and commercial bids once again for scrutiny.

AUTHORIZED SIGNATORY

The selected bidder shall indicate the authorized signatories who can discuss, signnegotiate, correspond and any other required formalities with the NIXI-CSC, with regard to the obligations. The selected bidder shall submit, a certified copy of the resolution of their Board, authenticated by Company Secretary, authorizing an official or officials of the company to discuss, sign with the NIXI-CSC, raise invoice and accept payments and also to correspond. **The bidder shall furnish proof of signature identification for above purposes as required by the NIXI-CSC.**

SERVICE LEVELS

The services of the vendor, to be selected through this tender, shall be required to provide the Annual Maintenance Services contract duty certified by OEM supplier of respective equipment / hardware/software / services/ support services (The highest level of support contract available with OEM) and periodic Audit services after tender finalization and AMC of basic IT infrastructure equipment after warranty expiry as per the details below:

a) Maintenance, Safety and Operations of the multi-layer Physical Security for the products, devices, systems, equipment's, and IT infrastructure that shall be delivered over the period of time.
b) Support for Data Centre, IT Infrastructure Operations, and maintenance on 24x7x365 basis by qualified engineers/ personnel for a period of at least five years, ensure at least 99.98% uptime availability.
c) Preventive Maintenance activities for the IT infrastructure products, devices, equipment's etc should be performed regularly on semi-annually basis to prevent unexpected failures in the future. The Preventive Maintenance report shall be submitted to NIXI-CSC. Which shall highlight, suggest, guide about the device, products health, problems, issues (if any) and recommendations in case the device is not functioning properly or changing the device etc.
d) The selected SI shall deploy manpower in case a downtime/ critical failure occurs (so local presence is a must for the SI/OEM). Periodic visits need to be catered to the TSDC site by the engineer for backend support, preventive maintenance etc.
e) The response time commitment from the OEMs required is 6 Hrs in the event of any breakdown and the resolution time maximum 10 hrs to 24 Hours.

Although the support contract need to be valid for 5 Yrs , The Bidder will include the initial 1 Year Annual Maintenance Services contract duty certified by OEM supplier of respective equipment / hardware/software / services/ support services (The highest level of support contract available with OEM) into the BOQ , with remaining 4 Yrs of recurring per year maintenance services , which will be paid every year in advance without any increase into the AMC cost for next 4 Yrs ,

SERVICE LEVEL AGREEMENT

PURPOSE OF THIS AGREEMENT

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service, which shall be provided by the SI to NIXI-CSC for the duration of this contract.

The benefits of this SLA are to:

a) Trigger a process that applies NIXI-CSC and the SI management attention to some aspect of performance when that aspect drops below an agreed upon threshold, or target makes explicit the expectations that NIXI-CSC has for performance Helps NIXI-CSC control the level and performance of SI services.

b) The SI and NIXI-CSC shall maintain a monthly contracts to monitor the performance of the services being provided by the SI and the effectiveness of this SLA. This Service Level Agreement is between the SI and NIXI-CSC.

DEFINITIONS

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

"**Availability**" shall mean the time for which the services and facilities offered by the SI are available for conducting operations from the MEPC and Non-IT equipment's hosted in the Data Centre.

"**Downtime**" is the time the services and facilities are not available to NIXI-CSC and excludes the scheduled outages/ maintenance planned in advance for the Data Centre.

"**Support**" shall mean the SI's 24x7x365 centre which shall handle Fault reporting, Trouble Ticketing, and related enquiries during this contract.

"**Incident**" refers to any event / abnormalities in the functioning of the Data Centre MEPC, Non-IT Equipment / Services that may lead to disruption in normal operations of the Data Centre services.

DESCRIPTION OF SERVICES PROVIDED

The SI will provide following services for Maintenance including, (but not limited to) OEM support based AMC* of all IT Infrastructure into the scope of this RFP , for the establishment of (NIXI-CSC) TSDC Data Centre at the proposed site.

*Highest level of OEM provided onsite support , preferably 24x7x365 support .

DELIVERY, INSTALLATION AND COMMISSIONING OF EQUIPMENT

a) The bidder should agree to deliver, install, and commission all the equipment at the specific location as identified by NIXI-CSC. NIXI-CSC shall reject the component/ equipment supplied if it does not comply with the specifications or does not function properly after installation. The bidder shall replace the non-

functioning or defective equipment or its spares immediately and ensure proper functioning of all equipment.

b) The bidder must ensure delivery, installation and commissioning of the components and relevant software and System Integration of all Components within 12 weeks.

Any unjustified and unacceptable delay in delivery and installation schedule as given, of this section will render the bidder liable for liquidated damage of maximum 0.1% (point one percent) of PO value per day with a maximum capping of 10%.

WARRANTY AND AMC CLAUSE

a) All quoted items should be at least 5 Years on-site comprehensive warranty from the date of its successful installation and acceptance at the site, including free spare parts, kits etc. During this period, all the parts of the product shall be considered as non-consumable and bidder shall have to maintain all spare parts at no extra cost, if required.

b) Bidder must ensure at least 5 Years AMC*. AMC* shall be on the same terms and conditions as applicable for warranty. Bidder will quote initially 1 year cost separately for AMC (renewable every year in advance for next 4 years without any increase in AMC cost for next 4 years .

c) During this period, besides service/ maintenance of hardware & system Software and all driver software up-gradation, patches shall also be provided at no extra cost.

d) Since the required solution is required in high availability, if one of the redundant product/ software/ equipment systems fails, the issue must be addressed with immediate response time and the same must be resolved/ replaced within 6 hours from the reporting of the incident/ issue/ problem. Any unjustified and unacceptable delay in meeting above timeline will render the bidder liable for penalty of Rs.1000/- per extra 10 minutes.

e) The bidder shall ensure that that there is a back-to-back agreement with OEM to meet hardware and software support during this period (Agreement document to be attached).

f) During the period of support/ warranty, the bidder shall:

I. Support the entire hardware/ software of equipment

ii. Diagnose the hardware/ software faults and rectify the hardware/ software faults detected

iii. Repair and replace the faulty parts/ part thereof

iv. Upkeep the software periodically including implementation of patches, if required

v. Periodically analyse the health of various components of system

vi. Bidder shall carry out support activities as per requirement of NIXI-CSC

vii. Should update all licenses, patch, and software with latest version

g) Repair and Maintenance:

I. The bidder shall station their Technical Support Engineers (TSEs), for providing services to NIXI-CSC at their identified office

ii. The bidder shall ensure the availability of spare parts at different locations to meet the criteria of turnaround time for fault restoration/ faulty unit repair etc.

iii. The bidder shall ensure that all the TSEs are competent and responsible engineers and are capable of giving all types of necessary technical/ assistance to NIXI-CSC representatives in respect of all the hardware and software components of equipment as well as capable of attending faults/ resolving problems whenever needed.

iv. The bidder shall also ensure availability of experts in case of non-rectification of the faults by TSEs.

v. The bidder shall make the arrangements for taking out the faulty items from NIXI-CSC nodes after replacing them with new working spare, during support period.

vi. The bidder shall bear the entire cost including freight, insurance etc. and other incidental charges related to replacement of faulty items. It shall also include any interconnecting cables like power cables, networking cables, fibre cables etc.

vii. In case the faulty equipment/ card/ part is replaced, the replaced equipment/ card/ part shall become the property of NIXI-CSC, and the defective will become the property of bidder.

SERVICE LEVEL AGREEMENTS & TARGETS

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The SI shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels.

The services provided by the SI shall be reviewed by NIXI-CSC shall:
a) Check performance of the SI against this SLA over the review period and consider any key issues of the past period's performance statistics including major incidents, service trends, etc.
b) Discuss escalated problems, new issues and matters still outstanding for resolution.
c) Review of statistics related to rectification of outstanding faults and agreed changes.
d) Obtain suggestions for changes to improve the service levels.

In case desired, NIXI-CSC may initiate an interim review to check the performance and the obligations of the SI. The SLA may be reviewed and revised in accordance with the procedures, SLA Change Control. The procedures will be used if there is a dispute between NIXI-CSC and the SI on what the performance targets should be.
The SLA has been logically segregated in the following categories:
a) Performance Related Service Levels
b) Support Services related for the Data Centre infrastructure
c) Compliance & reporting Procedures
d) Periodic Facility Audits

The following measurements and targets shall be used to track and report performance on a regular basis. The targets shown in the following table are applicable for the duration of the contract.

AVAILABILITY MEASUREMENTS

	Type of Infrastructure	**Measurement**	**Expected Service Level**
Critical	Environmental Infrastructure	Availability of Critical Environmental Infrastructure Elements.	99.982%
key	Environmental Infrastructure	Availability of Key Environmental Infrastructure Elements	99.982%

PERIODIC FACILITY AUDITS

Though NIXI-CSC would also conduct their own audits at the time of supplying, testing, installation, commissioning, basis, surprise checks can be conducted anytime and for any number of times. Any non-compliance observed in the IT-during the surprise checks, audits would also qualify the SI for a penalty. The penalty would be levied on an additive basis and the accumulated total would be deducted from the payment due to the SI in the month in which surprise checks were conducted.

Note: Safety procedures and protocols to be adhered at all times when working on site.

SLA CHANGE MANAGEMENT PROCEDURE

General SLA Procedure

It is acknowledged that this SLA may change as NIXI-CSC 's functional requirement evolve over the course of the contract period. This document also defines the following management procedures:

a) A process for negotiating changes to the SLA.

b) An issue management process for documenting and resolving difficult issues.

c) NIXI-CSC and SI management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

d) Any changes to the levels of service provided during the term of this Agreement will be requested,

Documented and negotiated in good faith by both parties. Either party can request a change. Changes will be documented as an addendum to this SLA and, subsequently, the Contract.

If there is any confusion or conflict between this document and the Tender (and its addenda), the Tender will supersede. SLA Change Process The parties may amend this SLA by mutual agreement in accordance with terms of this contract. Changes can be proposed by either party. The SI can initiate an SLA review with the NIXI-CSC. Normally, the forum for negotiating SLA changes will be NIXI-CSC 's monthly meetings. Unresolved issues will be addressed using the issue management process.

e) The SI shall maintain and distribute current copies of the SLA document as directed by NIXI-CSC. Additional copies of the current SLA will be made available at all times to authorized parties.

ESCALATION PROCEDURE

The bidder need to submit the escalation procedure as part of the plan , design ,delivery , supply , implementation , integration and maintenence teams ,

CONTACT MAP

Escalation Level	**Contact Details**	**SI Representative with Managers Contact Details**
Level 1:		

Level 2:		
Level 3:		

MAINTENANCE

The Bidder will supply the devices with 1 year OEM support (igest level onsite support , preferably 24X7X365 days) as part of the bid and the same support will be renewal for next 4 years on yearly basis via per year advance payment without any increase in maintenence charges , either from SI or from OEM ,

SI shall provide information for the following:

- SI/OEM

Acceptance of SLA IN WITNESS WHEREOF, the parties hereto have caused this Service Level Agreement to vide Tender No. ……. Dated …….. to be executed by their respective authorized representatives.

For and on behalf of SI:

For and on behalf of NIXI-CSC:

PRE-QUALIFICATION CRITERIA

The Bidder must possess the requisite experience, strength, and capabilities in providing the services necessary to meet the requirements as described in the RFP document. The Bids must be complete in all respects and shall cover the entire scope of work as stipulated in the tender document. The invitation to Bid is open to all Bidders who qualify the eligibility criteria as given below:

The Bidder also need to provide the self-compliance sheet as part of the bid process

Table 1: Pre-Qualification compliance

S. No	Criteria	Document required	Compliance (yes / no)
1.	The Bids shall be submitted only by the sole Bidder; no consortium is allowed in this Bid	Declaration in this regard needs to be submitted	

2.	The Bidder shall furnish, as part of its Bid, an Earnest Money Deposit (EMD) as specified	Payment shall be made as specified	
3.	(a) The Bidder shall be an established company registered under the Companies Act, 1956 or Limited liability partnership firm act 2013 and in operation for at least 5 years as on 31.03.2022 and shall have their registered offices in India. (b) The company must be registered with appropriate authorities for all applicable statutory duties/taxes. (c) The Bidder must have a local presence in North-East or should establish a local presence within 30 days from the award of contract.	(a) Valid documentary proof of: ● Certificate of incorporation ● Certificate of Commencement ● Certificate consequent to change of name, if applicable (b) Valid documentary proof of: ● GST Registration number ● Income Tax registration/PAN number ● Income Tax returns for the financial years 2018-19, 2019-20 and 2020-21. ● (c) Valid documentary proof of: ● Local presence/ Declaration regarding the establishment of local presence within the desired time.	
4.	The Bidder shall have a positive net worth in each of the following years FY 2018-19, 2019-20, 2020-21, and 2021-22. Note: State/ Central PSUs are exempted from the positive net worth.	A certified document by the Chartered Accountant stating the net worth for each year specified.	
5.	The average annual financial turnover of the bidder during the last three years ending 31.03.2022 should be at least Rs. 100 Crores.	Audited balance sheet for the financial year 2018-19, 2019-20, 2020-21, and 2021-22	
6.	*Bidder should have successfully completed implementation of similar projects in Data Centres in India, during the last five years ending on 31 March 2022. i. Three completed projects costing not less than Rs. 20 Crores each or ii. Two completed projects costing not less than Rs. 30 Crores each or iii. One completed project costing not less than Rs. 40 Crores *This criteria is only applicable for pre- qualification, but the bidders are encouraged to submit more projects than the pre-qualification criteria to get maximum marks for technical bid marking as defined into Technical Qualification of the	1. Work orders confirming year and area of activity. 2. Completion certificate from the customer. 3. No work order for supply of one of the packages will qualify for eligibility.	

	RFP (stage 2 Technical qualifications section no 2)		
7.	The Bidder shall not be under a Declaration of Ineligibility for corrupt or fraudulent practices or blacklisted with any of the Central / State Government agencies.	Declaration in this regard by the authorized signatory of the Bidder	
8.	Certificate by authorized signatory confirming acceptance of all tender terms and conditions	Declaration on the company letter head by the signing authority	
9.	Authorization of signatory for the purpose of this tender	Power of Attorney	
10.	OEM Local presence: The OEM of major equipment Precision AC, Diesel Generator, UPS proposed by the bidder must have a service centre in North-East.	Declaration from OEM to be provided	
11.	The bidder should have successfully executed build of at least 2 Data Centers comprising of 1000 Sq. ft. or more area. Out of these two Data Centers, The bidder should successfully have setup and has maintained, managed one Data Centre having more than 1000 sq. ft. which is primarily consisting of Data Centre Network, Campus Network, compute network, HCI, hypervisor, cloud Mgmt., EMS, Network Security, content security, Load balancing etc. **Note**: A. Bidder 's in house Data Centers shall not be considered. Bidders who have built their own Internet Data Centre (DC) for commercial use will be considered.	• Copy of Client Certification for successful completion and commissioning • For IDC bidder certificate from client mentioning area of Data Centre occupied. PO & Installation report.	

12.	The OEM quoted by the bidder should have at least one manufacturing unit registered in India. The Products offered by the OEM should have presence in any one of the Data Centre environments in India	A document in this regard from the client is to be submitted.	

Note:

a) The bid documents uploaded shall be properly aligned with page numbers and index. Relevant portions, in the documents submitted in pursuance of eligibility criterion mentioned above, shall be highlighted.

b) Bidders must ensure that all required documents have been uploaded along with the bid to justify eligibility.

c) Bidder must comply with all the above-mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. Photocopies of relevant documents / certificates should be submitted as proof in support of the claims made. NIXI-CSC reserves the right to verify /evaluate the claims made by the vendor independently. Any decision of NIXI-CSC in this regard shall be final, conclusive, and binding upon the bidder.

d) Please refer to Annexures for Declarations asked above.

GENERAL INFORMATION ABOUT THE BIDDER

Details of the Bidder (Company)		
1.	Name of the Bidder	
2.	Address of the Bidder	
3.	Status of the Company (Public Ltd / Pvt. Ltd)	
4.	Details of Incorporation of the Company	Date:
Ref.#		
5.	Details of Commencement of the Business	Date:
Ref.#		
6.	Valid GST registration no.	
7.	Permanent Account Number (PAN)	
8.	Name & Designation of the contact person to whom all reference shall be made regarding this tender	
9.	Telephone No, (with STD code)	
10.	Email of the contact person:	
11.	Fax No. (with STD code)	

12.		Website		
13.		Financial Details (as per audited Balance Sheets) in crore)		
14.	Year	2018-19	2019-20	2020-21* /2021-22
15.	Net Worth			
16.	Turn over			
17.	PAT			

EVALUATION CRITERIA

Evaluation will be carried out in three steps i.e. pre-qualification , technical evaluation and financial evaluation. Bidder has to qualify in technical evaluation for being eligible for financial evaluation.

a. Technical evaluation will be based on various parameters as mentioned below.

i. Experience

ii. Turnover

iii. Technical capabilities (Technical solution submitted)

Absence of non-compliance or non-submission of technical supporting documents may lead to rejection of bid. No relaxation is permitted in eligibility conditions after submission of bids.

b. The financial evaluation will done as mentioned below. Bid will evaluate the total of cost of equipment and OEM support cost for 1 years. The total costs will include the cost of hardware/ software/ AMC / Installation with applicable taxes. The Bidder will supply the devices with 1 year OEM support and the same support will be renewal for next 4 years on yearly basis at the same charges.

Bidder should be financially competent to undertake the project without any delay/hindrance and should have positive net worth.

EVALUATION PROCESS

i. NIXI-CSC shall constitute a Tender Evaluation Committee to evaluate the responses. The Tender Evaluation Committee shall evaluate the responses to the TENDER and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids.

ii. The decision of the Tender Evaluation Committee in the evaluation of bids shall be final. No correspondence will be entertained outside the process of evaluation with the Committee. The Tender Evaluation Committee may ask for meetings or presentation with the Bidders to seek clarifications or conformations on their bids.

iii. The Tender Evaluation Committee reserves the right to reject any or all bids. Each of

the responses shall be evaluated as per the criteria and requirements specified in this TENDER.

The steps for evaluation are as follows:

STAGE 1: PRE-QUALIFICATION

- NIXI-CSC shall validate the "TENDER Document fee& Bid Security/Earnest Money Deposit (EMD)".
- If the contents of the RFP Bid are as per requirements, NIXI-CSC shall open the "Pre-Qualification Bid". Each of the Pre-Qualification condition mentioned into the RFP is MANDATORY. In case, the Bidder does not meet any one of the conditions, the bidder shall be disqualified.
- Technical and Financial bids for those bidders who don't pre-qualify will not be opened. Financial bid will not be opened for those bidders, who don't qualify the technical evaluation. Bid Security shall be returned to the unsuccessful bidders.
- The SI should add at least minimum projects to qualify into the Pre-Qualification but more and more similar projects to be submitted to get maximum marks into the Technical Qualification Criteria.

STAGE 2: TECHNICAL EVALUATION

- "Technical bid" will be evaluated only for the bidders who succeed in Stage 1 (PRE-QUALIFICATION).
- NIXI-CSC will review the technical bids of the short-listed bidders to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at NIXI-CSC's discretion.
- The bidders' technical solutions proposed in the bid document shall be evaluated as per the requirements specified in the TENDER and technical evaluation framework as mentioned into the RFP.
- Each Technical Bid will be assigned a technical score out of a maximum of 100 marks. Only the bidders who get an Overall Technical score of 70% or more in the Technical Evaluation Framework as given in the RFP will qualify for commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid.

- The Bidder's technical solution proposed in the Technical Evaluation bid shall be evaluated as per the evaluation criteria in the following table.

S No.	Evaluation Criteria	Total Marks	Minimum Technical qualification Marks
1.	Company profile and financial Standing	15	60
2.	Past Experience/Projects Bidder should have successfully completed implementation of similar projects in Data Centres in India, during the last five years ending on 31 March 2022.	Max 45	
	i. Total Value of projects more than as 120 crore as per the defined criteria of the projects into PQ (pre-Qualification criteria defined in stage 1: pre-qualification section 6)	45	
	ii. Total Value of projects more than as 80 crore and less than 120 crores as per the defined criteria of the projects into PQ (pre-Qualification criteria defined in stage 1: pre-qualification section 6)	40	
	iii. Total Value of projects less than 80 crores as per the defined criteria of the projects into PQ (pre-Qualification criteria defined in stage 1: pre-qualification section 6)	35	
3.	Proposed Solution, Approach, Methodology	15	
4.	Technical presentation and Demo	10	
5.	Providing Capacity building, Training Methodology , Maintenance & Support	15	10
	Total	**100**	**70**

- Qualification Minimum absolute technical score to qualify for commercial evaluation is 70 marks out of total 100 marks and also the bidder should get minimum of 70% of marks in each of above- mentioned evaluation criteria.
- NIXI-CSC reserves the right to check/validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the additional

requisite support must be provided by the Bidder.

STAGE 3: COMMERCIAL EVALUATION

- All the technically qualified bidders will be notified to participate in Commercial Bid opening process.
- The commercial bids for the technically qualified bidders shall then be opened on the notifieddate and time and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at NIXI-CSC 's discretion.
- Commercial Bids that are not as per the format provided in Annexures shall be liable for rejection.
- The bid price shall inclusive of all taxes and levies and shall be in Indian Rupees with clear breakup of base price along with taxes (without GST).
- Mentioning compliance for each line item of BOM is mandatory.
- Bidder would not leave blank in any of the line item of BoM.
- The Bid Security amount shall be returned to those who don't qualify the financial evaluation stage and after PBG shall be submitted by the Successful Bidder.

SHORT LISTING

The bidder needs to qualify as per eligibility criteria. Only eligible bidders will be qualified for the Technical evaluation process, to be qualified for commercial bid opening. Only those bidders who achieve technical requirements mentioned in scope of work would be short-listed for commercial bid evaluation.

The Commercial Bids of only technically qualified bidders will be opened and evaluated by NIXI-CSC, and the evaluation will take into account the following factors:

1. The optimized TCO identified in the commercial bid would be the basis of the entire outflow of NIXI-CSC for undertaking the scope of work. NIXI-CSC will consider the TCO over a seven-year period starting from the date of going live in production. Any further infrastructure or hardware (electrical components) required to meet the performance criteria of NIXI-CSC as stated in the RFP, during the tenure of the project, would be at the cost of the Bidder.
2. The bidder will be solely responsible for complying with any applicable Export / Import Regulations. NIXI-CSC will no way be responsible for any deemed Export benefit that may be available to the bidder.
3. In case there is a variation between numbers and words; the value mentioned in words would be considered.
4. The OEM needs to provide Unit costs would be provided for components and services; unit rates would be considered for the TCO purposes.
5. In the event the vendor has not quoted or mentioned the component or services required, for evaluation purposes the highest value of the submitted bids for that component or service

would be used to calculate TCO. For the purposes of payment and finalization of the contract, the value of the lowest bid would be used.

ENTIRE AGREEMENT

The agreement will be between NIXI-CSC and the bidder (including all backend agreements of bidder with OEM and third parties) constitutes the entire agreement between the "Parties" with respect to the matters addressed herein and can only be modified through a written instrument signed and agreed with consensus-ad-idem by both parties

a) **Governing Law and Jurisdiction**: This agreement shall be construed and governed in accordance with the laws of India. Further, in case of any dispute is between the parties, the same shall be referred to the arbitration and shall be decided as per the provisions of the Arbitration & Conciliation Act, 1996 (amended and updated as of date) with arbitration seat/ venue at New Delhi. Any appeal or petition against the arbitration award/ final order/ judgment shall be filed in and decided by courts in New Delhi, India.

CONFIDENTIALITY AND SECURITY

The selected bidder and their personnel will not, either during the term or after expiration of this contract, disclose any proprietary or confidential information relating to the services, contract or business or operations of NIXI-CSC without the prior written consent of NIXI-CSC.

b. The bidder will ensure that no information about the software, hardware, and database, the policies of NIXI-CSC is taken out in any form including electronic form or otherwise, from the client site.

INDEMNITY

a. The selected bidder shall indemnify NIXI-CSC from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising, or incurred inter alia during and after the Contract period out of:

b. Any negligence or wrongful act or omission by the selected bidder or any third party associated with selected bidder in connection with or incidental to this Contract or.

c. Any breach of any of the terms of this contract by the selected bidder, the selected bidder's team or any third party

d. Any infringement of patent, trademark/ copyright arising from the use of the supplied goods and related services or any party thereof

e. The selected bidder shall also indemnify the purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, service provided as mentioned in any Intellectual Property Rights and licenses.

LIMITATION OF LIABILITY

a. Neither Party shall be liable to the other Party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.

b. Except in the case of gross negligence or wilful misconduct on the part of the selected bidder or on the part of any person acting on behalf of the selected bidder executing the work or in carrying out the services, the selected bidder, with respect to damage caused by the selected bidder including to property and/ or assets of NIXI-CSC shall regardless of anything contained herein, not be liable for any direct loss or damage that exceeds (A) the contract value or (B) the proceeds the selected bidder may be entitled to receive from any insurance maintained by the selected bidder to cover such a liability, whichever of (A) or (B) is higher. For the purposes of this clause, "gross negligence" means any act or failure to act by a Party which was in reckless disregard of or gross indifference to the obligations of the Party under the contract and which causes harmful consequences to life, personal safety, or real property of the other Party which such Party knew or would have known if it were acting as a reasonable person, would result from such act or failure to act. Notwithstanding the foregoing, gross negligence shall not include any action taken in good faith for the safeguard of life or property. "Wilful Misconduct" means an intentional disregard of any provision of this Contract which a Party knew or should have known if it were acting as a reasonable person, would result in harmful consequences to life, personal safety or real property of the other Party but shall not include any error of judgment or mistake made in good faith.

c. This limitation of liability slated in this Clause, shall not affect the selected bidder's liability, if any, for direct damage by selected bidder to a Third Party's real property, tangible personal property or bodily injury or death caused by the selected bidder or any person acting on behalf of the selected bidder in executing the work or in carrying out the Services.

FORCE MAJEURE

If at any time, during the continuance of the agreement, the performance in whole or in part by either party of any obligation under the agreement is prevented or delayed by reasons beyond the control of a party such as war, hostility, acts of public enemy, civil commotion, sabotage, fires, floods, explosions, epidemics quarantine restrictions, strikes, natural calamities, lockouts, pandemic, acts of state or acts of God (hereinafter referred to as "events"), provided notice of happenings of any such event is duly endorsed by the appropriate authorities/chamber of commerce in the country of the party giving notice, is given by party seeking concession to the other as soon as practicable, but within 21 days from the date of occurrence and termination thereof, neither party shall, by reason of such event, be entitled to terminate the empanelment/contract, nor shall either party have any claim for damages against the other in respect of such non-performance or delay in performance, and deliveries under the empanelment/contract shall be resumed as soon as practicable after such event has come to an end or ceased to exist, provided further, that if the performance in whole or in part or any obligation under the empanelment is prevented or delayed by reason of any such event for a period exceeding 60 days, NIXI-CSC may at its option, terminate the empanelment. Neither Party shall be liable for any failure or delay in the performance of its obligations under the contract or Work Orders hereunder to the extent such failure or delay or both is caused, directly, without fault by such Party, by reason of such event. NIXI-CSC shall, however, be responsible to pay the bidder for the services successfully rendered to the satisfaction of NIXI-CSC under the work orders/ purchase orders issued pursuant to the contract.

EVENTS OF DEFAULT BY BIDDER

The failure on the part of the bidder to perform any of its obligations or comply with any of the terms of this Contract should constitute an Event of Default on the part of the bidder. The events of default as mentioned above may include inter-alia the following:

a) the bidder has failed to perform any instructions or directives issued by the Purchaser which it deems proper and necessary to execute the scope of work under the Contract, or

b) the bidder/ bidder's Team has failed to confirm with any of the Service/Facility Specifications/standards as set out in the scope of work of this Tender document or has failed to adhere to any amended direction, modification or clarification as issued by the Purchaser during the term of this Contract and which the Purchaser deems proper and necessary for the execution of the scope of work under this Contract.

c) the bidder has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the Tender, and this Contract.

d) The bidder/ bidder's Team has failed to comply with or is in breach or contravention of any applicable laws.

e) Failure of the successful Bidder to comply with the requirement of this clause shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD/Security Deposit. In case of exigency, if the Purchaser gets the work done from elsewhere, the difference in the cost of getting the work done will be borne by the successful Bidder subject to maximum of 10% of the value of the goods/services for which alternative option is sorted to.

TERMINATION OF THE CONTRACT

A Notice shall be given 30 days curing period in advance to the selected bidder before termination of the contract.

The contract maybe terminated within 30 business days if the Bidder does not perform its obligations as mentioned in the Contract or commits an Event of Default and fails to cure such default within 30 days of receiving a written notification from the Purchaser notifying it of such default, the same would constitute the breach of the Contract and the Purchaser shall have the right to terminate or withdraw the Contract. Such cancellation of contract on account of non-performance by the Bidder would entitle the Purchaser to forfeit the performance security.

Further the purchaser may terminate this agreement on 30 business days' notice to the bidder under the following conditions as well:

a) If the bidder becomes insolvent, bankrupt, or enters receivership, dissolution, or liquidation, the other party may terminate this agreement with immediate effect; or

b) There is or becomes any Law that makes the performance of the terms of this agreement illegal or otherwise prohibited; or

c) Any Governmental Authority issues an Order restraining or enjoining the transactions under this agreement; or

d) In case purchaser finds illegal use of hardware and software tools that are dedicated to purchaser only

e) Under any other justified circumstance

In the event of termination, Purchaser may Invoke the Performance Performance bank guarantee/Security Deposits, recover such other direct costs and other amounts towards direct damages from the selected bidder that may have resulted from such default and pursue such other rights and/or remedies that may be available to the Purchaser under law.

In any case of Termination, the Purchaser shall be liable to pay the bidder for all the goods and services accepted as per the milestone till the effective date of termination.

EXIT MANAGEMENT

The exit management requirements as elaborated below must be read in conjunction to and in harmony with related clauses of this tender.

a) Given the critical nature of the service, it is imperative that a well-defined exit management strategy be made ready which will enable easy transition of activities when the contract expires/ is truncated. Accordingly, the bidder shall submit an exit management plan, which will focus on the key activities it will perform to ensure that a seamless transition of knowledge and activities be possible, and the same shall be evaluated. The exit management plan will be based on the plan proposed by the bidder in its technical proposal. The final exit management plan will have to be mutually agreed upon by both NIXI-CSC and the bidder. The bidder shall understand that ensuring a smooth transition at the end of the project period is a key requirement from NIXI-CSC. The bidder needs to update the exit management plan on half yearly basis or earlier in case of major changes during the entire contract duration. While proposing the exit management plan, the bidder shall ensure that the subsequent points are taken care of.

b) At the end of the contract period or during the contract period or contract termination, if any other agency is identified or selected for providing services related to the scope of work as in the contract, the bidder shall ensure proper and satisfactory transition is made to the other agency. In case NIXI-CSC wants to take over the project itself, then bidder has to ensure proper transition to the team designated by NIXI-CSC.

c) All risks during transition stage shall be properly documented by bidder and mitigation measures be planned in advance and recorded in the exit management plan so as to ensure smooth transition without any service disruption.

d) The bidder shall provide all knowledge transfer of the system to the satisfaction of NIXI-CSC as per the specified timelines.

DISPUTE RESOLUTION

a) The Bidder and NIXI-CSC shall endeavour their best to amicably settle, by direct negotiation, all disputes arising out of or in connection with the empanelment.

b) In case any dispute between the Parties, does not settle by negotiation, the same may be resolved exclusively by arbitration and such dispute may be submitted by either party for arbitration. Arbitration shall be held in New Delhi and conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory modification or re- enactment thereof. Each Party to the dispute shall appoint one arbitrator each and the third to be appointed by the MeitY, Government of India.

c) The "Arbitration Notice" should accurately set out the disputes between the parties, the intention of the aggrieved party to refer such disputes to arbitration as provided herein, the name of the person it seeks to appoint as an arbitrator with a request to the other party to appoint its arbitrator within 45 days from receipt of the notice. All notices by one party to the other in connection with the arbitration shall be in writing and be made as provided in this tender document.

d) Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides. The Bidder shall not be entitled to suspend the Service/s or the completion of the job, pending resolution of any dispute between the Parties and shall continue to render the Service/s in accordance with the provisions of the Contract/Agreement notwithstanding the existence of any dispute between the Parties or the subsistence of any arbitration or other proceedings.

CORRUPT AND FRAUDULENT PRACTICES

As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy:

Corrupt Practice‖ means the offering, giving, receiving, or soliciting of anything of values to influence the action of an official in the procurement process or in contract execution

AND

Fraudulent Practice means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the NIXI-CSC and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive he NIXI-CSC of the benefits of free and open competition.

The NIXI-CSC reserves the right to reject a proposal for award if it determines that the bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

The NIXI-CSC reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

LIMITATION OF LIABILITY

Bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for

a. IP Infringement indemnity.

b. Bodily injury (including Death) and damage to real property and tangible property caused by Bidder/s' gross negligence. For the purpose of this section, contract value at any given point of time, means the aggregate value of the purchase orders placed by NIXI-CSC on the Bidder that gave rise to claim, under this RFP.

c. Bidder shall be liable for any indirect, consequential, incidental, or special damages under the agreement/ purchase order.

PREVIOUS TRANSGRESSION

The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER 'S exclusion from the tender process.

The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

FALL CLAUSE

The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present bid in last 1 year , in respect of any other Ministry/Department of the Government of India or PS U and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

FACILITATION OF INVESTIGATION

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

LAW AND PLACE OF JURISDICTION

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

OTHER LEGAL ACTIONS

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

STATEMENT OF PURPOSE

NIXI-CSC Data Services Limited (hereby called/referred as "Issuer") invites competitive sealed technical and commercial proposal from eligible, reputed, qualified organizations with sound technical and financial capabilities for Integration, Revamping, Supplying, Installation, Implementation, Testing and Commissioning of a Public Cloud Solution in the Data Centre/Server Farm at TSDC Agartala, Tripura having previous experience in designing and successfully Implementing, similar type of projects for Data Centres /Companies /Institutes /Government /PSUs etc.

The Issuer proposes to deploy a new Public cloud solution that shall be used by Government Organisations, Non-Government Organisation and Public Sector that in the existing 3200sq. ft (approx.) data centre/server farm facility, considering the growth requirement for next 7 years with the latest State-of-Art technology, design and equipment. This deployment should comply with latest (IT) Data Centre standards to provide High availability and connectivity of the hosted services at TSDC, resilient to outages, safety, and security. The successful bidder shall appropriately estimate and design a total solution for the Data Centre/ Server Farm, including but not limited to rack placement design with stacking of the racks with chassis comprising of a Public Cloud Solution consisting of Datacentre Network, Compute, Storage, Virtualization, Cloud Management, Automation, Orchestration, Security Hardware and Software Solutions (such as IPS, firewalls (internal/external), etc.) along with integration and coupling of the hardware components/equipment/infrastructure together with software infrastructure. The successful bidder shall refer this document to meet the expected requirements and further plan out an optimal solution. The design is to be done in such a way that not all 80 racks will be deployed at once. Only few of the racks will be populated along with the computation racks as per the BoQ.

SCOPE OF WORK

The Scope of Work shall be with a single bidder, it is and will be the selected Systems Integrator (SI)/bidder's complete responsibility to supply, install, execute, commission, test and maintain the project until Go-Live (where the Data Centre becomes fully operational/available for end customers/Issuers use). The deployment of the public cloud solution having features (but not limited to) automation, orchestration, scalability and rapid elasticity, virtualisation, IAAS, PAAS, SAAS, cloud management, cloud portal, resiliency, DR, security, multi-tenancy, etc. The SI shall also be responsible for providing annual maintenance (AMC) for 1 year OEM support and the same support will be renewal for next 5 years on yearly basis at the same charges at-least which is commenced after Go-Live, but not limited to the following:

• The Systems Integrator (SI)/ Successful Bidder is advised to do a detailed site survey/site analysis/site visit before starting the execution and quoting the prices (as per the requirements). The Systems Integrator (SI)/ Successful Bidder are free to inspect the site prior to submitting their proposals.

• The Successful Bidder shall prepare detailed deployment design/plan documents (both hard and soft copy) and shall submit the same for approval and also do necessary changes required/listed/told/approved by the owners.

• The Systems Integrator (SI)/Bidder shall prepare the rack diagram/layout/drawing after understanding the bid, the requirement of the client and then start work accordingly. The approval for the rack diagram/layouts/drawings to be taken before starting the work. All execution related drawings such as

rack diagram/layout/drawings, etc. shall be prepared by the SI and submitted for approval before starting any work.

• Supply of necessary components: The Systems Integrator (SI) shall supply the materials and equipment as required. In case, it is identified that certain components are required for necessary functionality but not included in the Tender BoQ, SI should include such equipment in the bid value, quote for them as "any other item." The SI shall note that the specification provided is the minimum requirement and the SI shall procure better equipment if it is required to meet the service levels mentioned in this RFP.

• Supply, Installation, Integration and Commissioning of equipment/components/materials to be taken care by the Systems Integrator (SI). The Successful Bidder shall install, integrate, and commission the activities as per approved deployment design. All the work shall be done in a conscientious manner as per the guidelines and best industry practices. The system shall be subjected to inspection at various stages. Local regulation / codes shall be followed at all times. The Successful Bidder shall follow all Standard Safety Regulations, norms, and best practices while working.

• The successful Bidder shall not cause any damage to the existing data centre, Government buildings /other premises and the property, and will perform restoration if any damage occurs. Trenches, path-cutting, etc. will be back-filled and restored to the original condition immediately after laying of the conduit/cable. The Successful bidder shall seal conduits, entrance holes and cut-outs where the cabling/wiring etc. has been installed with suitable sealing material.

• The successful Bidder has to prepare and submit a delivery report including details of all components supplied. The authorities will validate the delivery report.

• The selected bidder should take all necessary Statutory/ regulatory approvals from the respective authorities.

• The SI must prepare a pre-installation and a post-installation checklist and get the same approved from the consultant/ PMC/Issuer and install the equipment as per the agreed norms.

• The commissioning check list has to be prepared by the SI and an approval has to be sought.

• The SI must handover all the documents such as drawings, designs, warranty certificate, manuals, data sheets, back-ups etc. to the client before Go-Live.

• The selected SI/bidder shall also dispose all trash/garbage/junk properly within 24 hours. No trash should be stored/placed/dumped inside the Data Centre or in the Building and shall be stored/ placed/dumped/thrown at a designated spot/place/area provided by the Issuer/Owner etc.

• if the SI may engage a third-party for its guidance, support, assistance etc. for performing the mentioned tasks. The accountability of the third-party vendors who are guiding. supporting, assisting etc. shall be under the scope of SI and SI only. Any mistake, error, wrong work done, delay etc. by Third party shall cause the SI to be liable, accountable for its actions.

• **Network Management:** The objective of this service is to ensure continuous operation and upkeep of the LAN (& WAN) infrastructure at the DC including all active and passive components. The services to be provided for Network Management include:

- Ensuring that the network should be resilient and highly available.
- Attending to and resolving network failures and issues.
- Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.

- Configuration and backup of network devices/ equipment including documentation of all configurations, OS-Backup, etc.
- The solution should be capable of monitoring of the network to spot the problems immediately.
- Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, LAN links and routers, etc.

• **Application Monitoring**: It should include monitoring of:

- Web Services
- Application Server
- Database Server
- Middleware
- Others

• **Backend Services:** The selected bidder is required to maintain and support all the Backend Services implemented at the DC. The services include:

- Directory Services
- Database Services
- User rights & policies

• **Directory Services:** It should include the following services:

- Domain management.
- Group management.
- User management.
- Implementation of policies and standards

• **Backup / Restore Services**

- Backup of Application and Database as per the defined policies.
- Backup of storage as per the defined policies.
- Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies as defined by the Client.
- Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis.
- Media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets (onsite and offsite).
- 365x24x7 support for file and volume restoration requests at the Data Centre. The successful bidder shall be responsible for restoration of services at the DR site. Necessary arrangement for restoration of services at DR Site shall be done. (However, TSCA will provide all the necessary infrastructure for the same.)
- Off-site Backup (DR) – Data (backup) meant for Offsite locations will be handed over by DCO in secured manner to designated officer(s) of Client or TSCA. TSCA will be responsible for maintaining the Off-site location.

• **Network passive cabling work:**

- Network cabling for the entire area must be done by SI/Bidder.
- The network cabling will be for both fibre and copper (CAT6A).

- The network cables and connectors should be procured in abundance for having redundancy in case of faulty cables/ defects/improper crimping/ improper clamping/changing of connectors etc. The different tools/components/equipment
- Network cabling will also be done for the DC OPTS, Staging, Reception and the user or support area and Network devices like network switches, DCIM servers, storage etc., has to be considered for the NON-IT Infrastructure LAN.

• **Physical Infrastructure Management and Maintenance Services:**

All the IT devices installed in the Data Centre as part of the physical infrastructure shall be centrally and remotely monitored and managed on a 24x7x365 basis via industry leading infrastructure management solution deployed to facilitate monitoring and management of the Data Centre Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

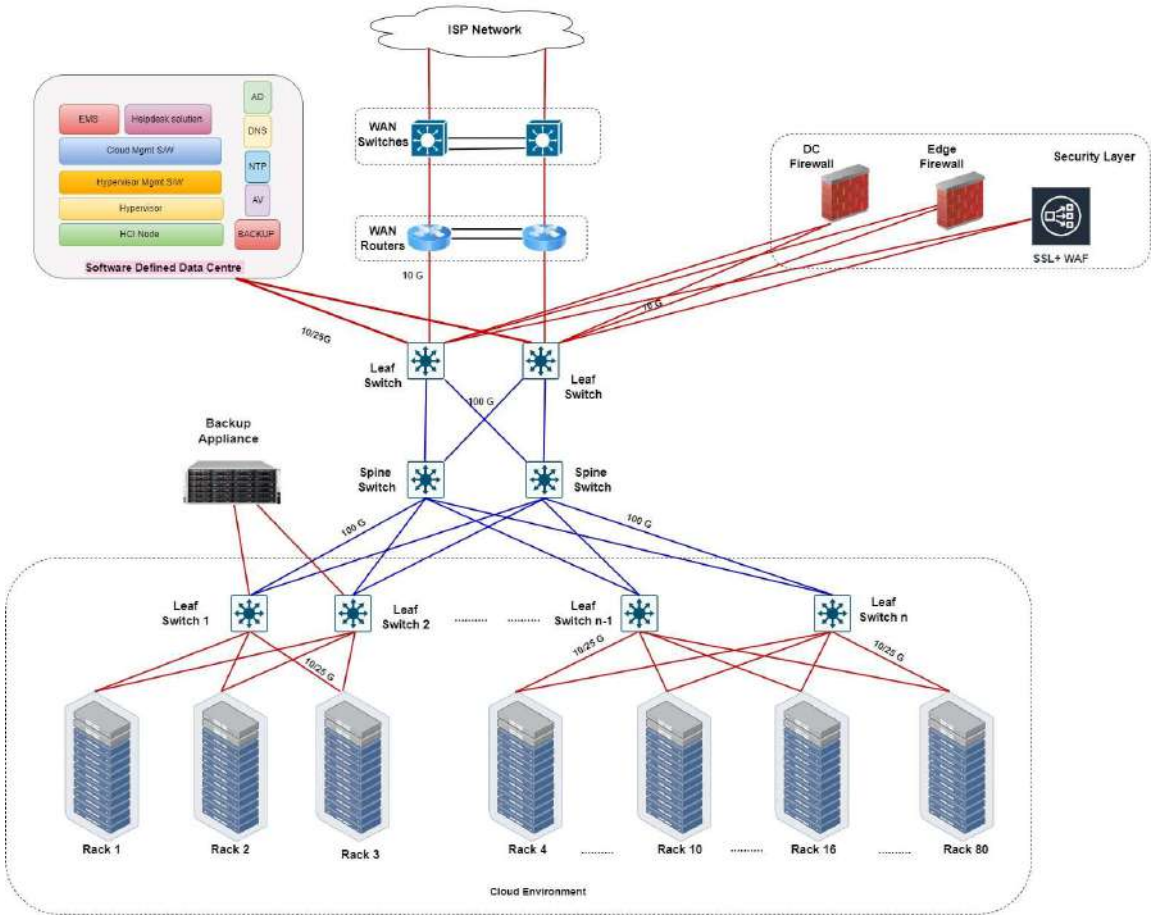
- Proactive and reactive maintenance, repair, and replacement of defective components (IT and Non-IT/ Hardware and Software etc.). The cost for repair and replacement shall be borne by the selected bidder.
- The selected bidder shall have to stock and provide adequate onsite and offsite spare parts and spare components to ensure that the SLA is met for the entire contract period. To provide this service it is important for the selected bidder to have necessary back-to-back arrangement with the respective OEMs / vendors. For this, the bidder may directly contact OEMs.
- Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected bidder fails to meet these standards, penalty will be imposed on DCO, as specified in the SLA.
- The selected bidder shall also maintain log/records of all maintenance activities for the new DC equipment/components and shall maintain a logbook on-site that may be inspected by Clients at any time during contract period.

Professional Services

- Provisioning of Professional Services to include (but not limited to) Managed Maintenance Support, Network Audit, Network Optimisation, Documentation, Training, OEM Support, Project Planning and Management etc.

TSDC HIGH LEVEL ARCHITECTURE

A high-level solution architecture design for Cloud based Data Centre that will to be built at TSDC is shown below.



TECHNICAL AND FUNCTIONAL REQUIREMENTS

The minimum compliance requirement for the DC IT Infrastructure is mentioned below:

Hyper Converged Infrastructure Type 1

RFP Clause	Technical Specifications	Compliance (Yes/No)
01	The proposed HCI solution should have all flash nodes, each proposed node should have 40TB as raw capacity (excluding cache disks) and minimum 10TB as usable capacity (excluding cache disks) & considering storage optimization. The cluster must be configured with minimum replicas of data. The bidder needs to ensure the OEM recommended cache disk to capacity disk ratio for the best performance	
02	In all flash nodes the proposed cache drive shall be of NVMe/SAS read intensive SSD with high endurance and support for 4TBW per day or better	
03	In all flash nodes the proposed capacity drive shall have interface type as NVMe/SAS mixed use SSD. The bidder/OEM can propose the capacity drive of any size, but it should meet the minimum requirement of 40TB raw capacity per node	
04	The proposed HCI hardware nodes should be 2RU form factor	
05	Each proposed HCI hardware should have minimum 2 processors, each processor should have 64 Cores with base clock speed 2.4 GHz or better, L3 cache 192 MB or better, TDP 240 or better.	
06	Each proposed HCI hardware should have RAM populated using 64 GB or higher DDR4 Module @ 2700 MHz or better. Each node should have total 1024GB of RAM or better	
07	Each proposed HCI hardware 2* Quad port 10G SFP + /25G SFP+ network adaptor with 10G SFP + SR modules populated in all available ports	
08	The proposed HCI hardware should support features such as Intelligent Platform Management Interface Version 2, secure boot, UEFI shell, PXE boot, SNMP v2 & v3, HTML 5 GUI, CLI, SMTP, XML API/redfish API, Virtual console, energy star, TPM 2.0, PCIe 3.0 compliance	
09	The proposed HCI hardware should have redundant hot swappable high efficiency power supplies, redundant fan modules, Trusted Platform Module 2.0, 2* USB 3.0 ports, One VGA/Display/KVM port, one out of band management port, 2* 10G RJ 45 ports, 2* PCIe 3.0 slots ,2* M2 SSD slots	
10	The proposed solution should support deduplication, compression, and encryption in all flash configuration	
11	The proposed solution should leverage any of industry standard hypervisor like ESXi/ Hyper-V/ KVM/RHEV/AHV	
12	The proposed solution should be able to support different generation of Intel/AMD x86 processors in the same cluster	

13	The proposed solution should have feature to distribute the replicas to HCI nodes in different rack/fault domain	
14	The proposed solution should support addition of compute/storage only nodes in the existing cluster	
15	The proposed solution should support minimum 16 nodes in single cluster	
16	The proposed solution should support simultaneous two node failure in the cluster	
17	The proposed solution should be able to connect to external 3rd party SAN & NAS storage into the HCI cluster for capacity expansion	
18	The proposed solution should support checksum of data to ensure data integrity & to enable automatic detection and reproposed solution of errors.	
19	The proposed solution should be 100% software defined	
20	The proposed solution should run on industry standard x86 servers	
21	The proposed solution should be able to independently scales storage and compute as and when needed without any downtime.	
22	The proposed solution should support native File, Block, Object Storage, Data at rest encryption and Data in transit encryption	
23	The proposed solution should support monitoring via SNMPv3 and email alerting via SMTP	
24	The proposed solution should be a tested and validated solution to run MS SQL, PostgreSQL, MongoDB, OpenStack, Virtual machines, Windows Server OS, RHEL OS & Containers	
25	The proposed solution should have centralized configuration & monitoring GUI for the HCI proposed solution	
26	The proposed should integrate with any 3rd party SSO solution/AD/LDAP/ any third-party Identity & Access Management solution	
27	The proposed HCI software solution OEM should be mentioned in the latest Gartner Magic Quadrant for HCI solution.	
28	The proposed Software & Hardware OEM for the HCI solution should have at least 5 Years warranty & 24x7x365 support	
29	The proposed Software & Hardware OEM for the HCI solution should have at least 3 successful deployments in any Indian government vertical. The OEM/bidder need to share the valid proof for the same	
31	All the required licenses for the hypervisor, HCI software, HCI Management software should be supplied as part of the solution	
32	The proposed Software and Hardware OEM for HCI solution should be minimum 5-year-old organization and should have the corporate/support offices in India	
33	The proposed HCI software should be certified for FIPS 140-2, PCI-DSS, HIPAA, KMIP compliant key managers, GDPR and FISMA compliance	

Hyperconverged Infrastructure Type 2

RFP Clause	Technical Specifications	Compliance (Yes/No)
01	The proposed HCI solution should have all hybrid nodes, each proposed node should have 40TB as raw capacity (excluding cache disks) and minimum 10TB as usable capacity (excluding cache disks) without considering any storage optimization. The cluster must be configured with 2 replicas of data. The bidder needs to ensure the OEM recommended cache disk to capacity disk ratio for the best performance	
02	In all hybrid nodes the proposed cache drive shall be of NVMe/SAS read intensive SSD with high endurance and support for 4TBW per day or better	
03	In all hybrid nodes the proposed capacity drive shall have interface type as NVMe/SAS mixed use SSD. The bidder/OEM can propose the capacity drive of any size, but it should meet the minimum requirement of 40TB raw capacity per node	
04	In hybrid nodes the proposed capacity drive shall have interface type as 12G SAS mixed use HDD. The bidder/OEM can propose the capacity drive of any size, but it should meet the minimum requirement of 40TB Raw capacity per node	
05	The proposed HCI hardware nodes should be 2RU form factor	
06	Each proposed HCI hardware should have minimum 2 processors, each processor should have 64 Cores with base clock speed 2.4 GHz or better, L3 cache 192 MB or better, TDP 240 or better.	
07	Each proposed HCI hardware should have RAM populated using 64 GB or higher DDR4 Module @ 2700 MHz or better. Each node should have total 1024GB of RAM or better	
08	Each proposed HCI hardware 2* Quad port 10G SFP + /25G SFP+ network adaptor with the 10G SFP + SR modules populated in all available ports	
09	The proposed HCI hardware should support features such as Intelligent Platform Management Interface Version 2, secure boot, UEFI shell, PXE boot, SNMP v2 & v3, HTML 5 GUI, CLI, SMTP, XML API/redfish API, Virtual console, energy star, TPM 2.0, PCIe 3.0 compliance	
10	The proposed HCI hardware should have redundant hot swappable high efficiency power supplies, redundant fan modules, Trusted Platform Module 2.0, 2* USB 3.0 ports, One VGA/Display/KVM port, one out of band management port, 2* 10G RJ 45 ports, 2* PCIe 3.0 slots ,2* M2 SSD slots	
11	The proposed solution should leverage any of industry standard hypervisor like ESXi/ Hyper-V/ KVM/RHEV/AHV	
12	The proposed solution should be able to support different generation of Intel/AMD x86 processors in the same cluster	
13	The proposed solution should have feature to distribute the replicas to HCI nodes in different rack/fault domain	
14	The proposed solution should support addition of compute/storage only nodes in the existing cluster	

15	The proposed solution should support minimum 16 nodes in single cluster	
16	The proposed solution should support simultaneous two node failure in the cluster	
17	The proposed solution should be able to connect to external 3rd party SAN & NAS storage into the HCI cluster for capacity expansion	
18	The proposed solution should support checksum of data to ensure data integrity & to enable automatic detection and reproposed solution of errors.	
19	The proposed solution should be 100% software defined	
20	The proposed solution should run on industry standard x86 servers	
21	The proposed solution independently scales storage and compute as and when needed without any downtime.	
22	The proposed solution should support native File, Block, Object Storage, Data at rest encryption and Data in transit encryption	
23	The proposed solution should support monitoring via SNMPv3 and email alerting via SMTP	
24	The proposed solution should be a tested and validated solution to run MS SQL, PostgreSQL, MongoDB, OpenStack, Virtual machines, Windows Server OS, RHEL OS & Containers	
25	The proposed solution should have centralized configuration & monitoring GUI for the HCI proposed solution	
26	The proposed should integrate with any 3rd party SSO solution/AD/LDAP/ any third-party Identity & Access Management solution	
27	The proposed HCI software solution OEM should be mentioned in the latest Gartner Magic Quadrant for HCI solution in last 3 years .	
28	The proposed Software & Hardware OEM for the HCI solution should have at least 5 Years warranty & 24x7x365 support	
29	The proposed Software & Hardware OEM for the HCI solution should have at least 3 successful deployments in any Indian government vertical. The OEM/bidder need to share the valid proof for the same	
30	All the required licenses for the hypervisor, HCI software, HCI Management software should be supplied as part of the solution	
31	The proposed Software and Hardware OEM for HCI solution should be minimum 5-year-old organization and should have the corporate/support offices in India	
32	The proposed HCI software should be certified for FIPS 140-2, PCI-DSS, HIPAA, KMIP compliant key managers, GDPR and FISMA compliance	

Virtualisation

S. No.	**Specification**	**Compliance (Y/N)**
1	**Hypervisor**	
1.1	Hypervisor shall allow heterogeneous support for Docker, Kubernetes, guest Operating Systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu, and CentOS) and latest versions.	

1.2	Hypervisor shall have the capability to create the VMs form virtual machine template	
1.3	Hypervisor shall allow taking snapshots of the virtual machines to be able to revert back to an older state if required.	
1.4	Hypervisor should be able to boot from iSCSI, FCoE, and Fibre Channel SAN.	
1.6	Hypervisor should have the ability to thin provision disks to avoid allocating all storage space upfront. Full monitoring capabilities and alerts to prevent from accidentally running out of physical storage space.	
1.7	Hypervisor should support live Virtual Machine migration	
1.8	Hypervisor should have the ability to live migrate VM files from one storage array to another without any VM downtime. Support this migration from one storage protocol to another. (ex. FC, iSCSI, NFS, DAS).	
1.9	Hypervisor shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optimal control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
1.10	Hypervisor shall have High Availability capabilities for the virtual machines in the sense if in case one server fails all the Virtual machines running on that physical server shall be able to migrate to another physical server running same virtualization software. The feature should be independent of Operating System Clustering and should work with FC/ iSCSI SAN and NAS shared storage	
1.11	Hypervisor should have the ability to manage virtual switches at a cluster level that can span an entire cluster and is VM mobility aware. It should support features Net Flow and Port mirror and protocols Link Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP)	
1.12	Hypervisor must support built-in storage multi-pathing.	
1.13	Hypervisor should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.	
1.14	Hypervisor should allow configuring each virtual machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address.	
1.15	Hypervisor must support NIC teaming for load sharing and redundancy	
1.16	Hypervisor shall allow creating virtual switches that connect virtual machines.	
1.17	Hypervisor shall support configurations of 802.1 q VLANs which are compatible with standard VLAN implementations from other vendors.	
1.18	Hypervisor should allow dynamic adjustment of the teaming algorithm so that the load is always balanced across a team of physical network adapters.	
1.19	Hypervisor shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines.	
1.20	Hypervisor shall allow RAM over-commitment that allows configuring virtual machine memory in such a way that safely exceeds the physical server memory.	

1.21	Hypervisor shall allow usage of remote devices which allow installation of software in a virtual machine running on a server from the CDROM of a desktop.	
1.22	Hypervisor should provide support for Microsoft , Oracle Cluster or any other leading OEM Services between virtual machines.	
1.23	Hypervisor should provide solution to automate and simplify the task of managing hypervisor installation, configuration, and upgrade on multiple physical servers.	
1.24	Hypervisor should support 3rd party backup and recovery software for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents	
1.25	The bidder should factor the hypervisor licenses for all the HCI nodes mentioned in the HCI requirement and hypervisor remote technical support 24*7*365 days for at least 5 Years	
1.26	The proposed hypervisor should support vTPM for virtual machines, should prevent the guest operating systems from Ransomware, Denial of Service attack and any other vulnerabilities	
1.27	The proposed hypervisor should support firewall to control, secure the hypervisor and guest virtual machines, Automation and orchestration, REST API, Software Defined Network, Hot Add virtual devices (vCPU, Memory, vNIC), Role-based access control.	
2	**Hypervisor Management Software**	
2.1	Hypervisor management software console shall provide a single view of all virtual machines, Containers, Kubernetes cluster, allow monitoring of system availability and performance and automated notifications with real-time alerts	
2.2	The Hypervisor management software should be able to perform quick, as-needed deployment of additional hypervisor hosts. This automatic deployment should be able to push out update images, eliminating patching and the need to schedule patch windows.	
2.3	Hypervisor management software console shall provide capability to monitor and analyse virtual machines, Containers, Kubernetes clusters, server utilization and availability with detailed performance graphs	
2.4	Hypervisor management software console shall maintain a record of significant configuration changes and the administrator who initiated them	
2.5	Hypervisor management software console shall provide the Manageability of the complete inventory of virtual machines, Containers, Kubernetes cluster, and physical servers with greater visibility into object relationships	
2.6	Hypervisor management software should provide a global search function to access the entire inventory of multiple instances of virtualization management server, including virtual machines, hosts, datastores and networks, anywhere from within Virtualization management server.	
2.7	Hypervisor management software should support user role and permission assignment (RBAC) and 3rd party SSO integration	
2.8	Hypervisor management software should allow you to deploy and export virtual machines	

2.9	Hypervisor management software should allow reliable and non-disruptive migrations for Physical/ Virtual machines running Windows and Linux operating systems to virtual environment	
2.10	Hypervisor management software should include provision for automated host patch management with no VM downtime.	
2.10.1	The proposed hypervisor management software should have the sufficient licenses to manage all the HCI nodes asked this RFP and remote technical support 24*7*365 days for at least 5 Years	
3	**Cloud Solution**	
3.1.0	The solution should be able to manage physical, bare metal and virtualized platforms	
3.1.1	The solution should support multi-vendor virtual platforms such as VMWare, Hyper-V, RHeV, KVM, Citrix hypervisor, AHV	
3.1.2	The solution should have capability to provide IaaS, PaaS, DaaS, SaaS	
3.1.3	The bidder should integrate the proposed and existing load balancers, Network devices, Firewalls, IDAM/SSO solution, Hypervisor management software, Storage, Backup solution, Enterprise Management System, physical servers, patch management solution, Help Desk system/ticketing system to automate the manual Day1 and Day2 tasks. The proposed cloud solution OEM should only perform the integration services	
3.1.4	The bidder should factor the necessary licenses and support (24*7*365 for at least 5 years) for the proposed cloud solution	
3.1.5	The bidder must quote appropriate licenses to enable and meet the mentioned features in the Cloud solution requirement which will hosted on top of all HCI nodes asked in the SOR section.	
3.1.6	The Cloud Automation and management engine should provide pre-built / out of box workflows and templates, enabling ease and timeliness in configuration and setup. Additionally, it should also provide pre-built interfaces into popular authentication engines such as LDAP, Active Directory etc.	
3.2.1.0	**Multi-Tenancy**	
3.2.1.1	Should support multiple organizations /Departments/ Business Units to have logically and /or physically isolated environments within a cloud instance, spanning physical infrastructures such as host servers, networks, subnets, storage etc.	
3.2.1.2	To permit controlled access to end users and administrators within business units.	
3.2.2	Should be able to talk to Cluster controllers of virtual platforms through a set of well documented, tested and fully exposed APIs.	
3.2.3	Should support all logical and physical configurations of underlying virtual and physical infrastructure.	
3.2.4	Should support both high availability, distributed deployment, and Disaster recovery (failover, failback) within the Cloud Control & management components	
3.2.5	To allow hierarchical setup, control and access to global cloud administrators, business units administrators, system architects and operations, within the boundaries of the multi-tenancy.	

3.2.6	The cloud setup created should be such that it is Self Service/SSO portal would be used to deploy the infrastructure underneath it. The solution should provide a workload aware deployment mechanism. The service levels defined in the cloud setup would enable users to choose the service levels and thereby choose the infrastructure to be deployed. There needs to be a logic built-in which would be deployed using these service levels, to deploy the apps to the closest infrastructure available to the Purchaser's Data Centre location.	
3.3	**Templates Orchestration & Automation, Self-Service Portal**	
3.3.1	The proposed solution should have capability to deals with definition of standard units of consumption of resources, of giving end users the choice selecting appropriate configurations, and of having an "orchestration" and "automation" engine that will quickly and efficiently carry out the process of provisioning the appropriate resources.	
3.3.2	The end user should be able to choose the following from the self-service portal	
3.3.2.1	Virtual machine services of Different type (Windows Server, RHEL, ubuntu, Suse,) and different size (Small, Medium, Large, Extra-large) and also there should be an option for end user to request for the customized requirement	
3.3.2.2	Storage services (Block, object, File)	
3.3.2.3	Web Application services such as IIS, Apache, GitHub, WordPress, etc.,	
3.3.2.4	Database services such as MS SQL, My SQL, EDB, PostgreSQL, Oracle RAC, MongoDB, etc.,	
3.3.2.5	Server Load balancer services	
3.3.2.6	Firewall services	
3.3.2.7	IDAM/SSO Services	
3.3.2.8	Backup services	
3.3.2.9	Container and Kubernetes services	
3.3.2.10	DNS Services	
3.3.2.11	Web hosting services	
3.3.2.12	VDI services	
3.3.2.13	SaaS and PaaS Services	
3.3.2.14	SSO/IDAM Services	
3.3.3	**Workflows for Lifecycle Management**	
3.3.3.1	Initial provisioning	
3.3.3.2	Change management – Increase / decrease in resources, change in timespan, retiral, archival etc.	
3.3.4	Self-Service Portal, Authentication, Automation & Orchestration	
3.3.4.1	The ability to let end-users and administrators log in into a "Self-Service" portal, whereby various templates, catalogs, and actions are presented as menu items.	
3.3.4.2	The ability to authenticate and validate portal users and their roles by authenticating against IAM/ LDAP / Active Directory within the Cloud data repository.	
3.3.4.3	The ability to selectively display only items pertinent to the portal users' role definition, while respecting BU multi-tenancy boundaries.	

3.3.4.4	Interaction via an elegant and intuitive UI, with the ability to customize selected areas for branding/organisation's logos and critical information display.	
3.3.4.5	The ability to allow users to select actions, templates and apply attached workflows and hierarchical approvals before automating completion of such actions.	
3.3.4.6	Actions to be performed shall include, but are not limited to, provisioning and change management of physical and virtual resource, VM templates, Clones, etc of migrating applications across physical infrastructure, of addition/changes to personnel, roles & responsibilities etc.	
3.3.5	**Cloud Management – Monitoring and Reporting**	
3.3.5.1	Define thresholds based on capacity and performance	
3.3.5.2	Define & generate dashboards that report on health of System.	
3.3.5.3	Include the ability to monitor infrastructure resources & application availability and to provide a facility to take appropriate corrective action.	
3.3.5.4	Monitor and report on performance and capacity utilization metrics with the option to filter such reports based on various parameters like resource type, Data Centre location, etc.	
3.3.5.5	Leverage information for optimal utilization and capacity planning – retiring idle VMs, reclaiming resources, analysis on utilization and consumption of resources, maintaining adequate headroom etc.	

Backup Solution

S. No	**Backup Solution**	**Compliance (Y/N)**
1	The proposed backup solution should support various platforms such as IaaS, SaaS, PaaS, Physical, Virtual and Container	
2	The backup solution should support backup and restore of various sources such as Windows, Unix, Linux, MS SQL, My Sql, DB2,PostGreSQL, EDB, MongoDB, Oracle RAC, SAP HANA, Splunk, SAP S/4HANA, MS Exchange, MS Share Point, Active Directory, Oracle enterprise business suite, Hadoop, Windows & Linux File system, Gluster FS, NFS shares, CIFS shares, SMB shares, Macintosh File System, Virtualized platform (ESXi, Hyper-V, RHEV, AHV, Citrix Xen, Oracle VM), OpenShift, Kubernetes & Docker , Amazon S3, Amazon EFS, Azure blob, Azure File Storage, Azure Data Box, Oracle Cloud Object Storage, Red Hat Ceph Storage, Google Cloud Storage, etc.	
3	The backup solution should include the backup software and backup disk-based appliance	
4	The proposed license for the backup solution should have 600TB capacity-based license	
5	The backup solution should be FIPS 140-2, FedRAMP, CIS, TLS 1.3 certified	
6	The proposed backup solution should support Encryption in transit and rest, Role-based access control, Auditing, Rest API, Html 5 GUI Access, CLI, industry leading 3rd party IDAM & Key management solution	

7	The backup solution should have the ability to backup data from one server platform and restore it from another server platform to eliminate dependence on a particular machine and for Disaster Recovery purposes.	
8	The backup solution should support cloud-native backup, disaster recovery to cloud, multi-tier backup copies, vTPM platform support, Agent less backup support for ESXi, Hyper-V, RHEV, AHV, KVM	
9	The backup solution should support automated scheduled replication to remote site for facilitating Disaster Recovery copy of backup data	
10	The backup software should be able to encrypt the backed-up data using 256- bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be factored in the proposed solution.	
11	The backup software should support wizard-driven configuration and modifications for backups and devices	
12	The backup software should support industry standard Common Device Interface for advanced device reporting and handling.	
13	The backup software should have firewall support.	
14	The backup software should support deduplicated backup and recovery for Hyper-V using VSS at the host (parent partition) to protect both the host and guest (child partition).	
15	The backup software should have in-built scheduling system and also support check-point restart able backups.	
16	The backup software should support backup / recovery of raw SCSI volumes	
18	The backup software should support NDMP multiplexing of NDMP and non NDMP data to the same tape and should also support NDMP backup to disk.	
19	The backup software should support backup and restore of NDMP data to media server attached tape/ Backup Appliance.	
20	The backup software must provide support for online backup for Databases such as MS SQL, Oracle, Exchange, DB2, Informix, Sybase, and MySQL with out-of-box agents.	
21	The backup software should support more than 1 worker/storage/media server which works as worker to receive backup data from clients and write data to tape.	
22	The backup software should support Hardware and storage array-based snapshot backup for off host zero downtime and zero load on the primary backup client.	
23	The backup software should support data movement directly from the backup client to the disk target without passing through the backup server.	
24	Provide a policy driven data-protection mechanism through scheduled backup and recovery.	
25	Provide a single and centralized management console and dashboard for data protection and reporting.	
26	Provide advanced management, reporting, alerts, and troubleshooting features. Backup of data to be taken via server-free backup methodology for physical and virtual servers, so that local recovery is quicker in case any application data is required.	

27	The backup solution should support replication of data between two similar backup appliance This will ensure that there are two copies of all data backups to provide recoverability in case of disasters.	
28	The solution should assure that the storage has online replica of production data volumes for instant recovery for up to 24 hours.	
29	The online replicas should be used for enabling server-free backups to a backup storage.	
30	The solution should provide online full and incremental backups for File and Application servers and popular databases like Oracle, SAP, DB2 or other databases	
31	The solution should provide Image Level backups and granular recovery for Virtual Environments without installation of any agents inside the virtual machines.	
32	The proposed backup appliance should have minimum 500GB usable capacity in RIAD 6, 8*16/32G FC Ports with 8*16G FC SFP populated from day 1, 8*10/25G SFP+ Ports with 8*10G SFP+ SR populated from day 1, no single point of failure in terms of power supply, controller, fan modules.	
33	Server Free Backup Methodology. The solution should be based on server-free backup methodology for reducing the impact of backup process on the production servers. The Bidder must provide all necessary software/hardware components to facilitate server-free backups.	
34	Online Backup from Databases and Applications: The Purchaser requires online backups for the production databases hosted in Data Centres. The bidders have to facilitate the required agents and software modules from the backup application to integrate with respective databases.	
35	Disk to Disk Backups for Medium- and Long-Term Retention. Purchaser wants to implement backup-to-disk solution using disk-based backup appliances to simplify operations and improve overall backup/restore performance. The solution should consist of Enterprise backup software and disk-based backup appliances. The backup appliance must provide global de-duplication of data across all devices / LUNs configured to drive backup storage efficiency. Backups will be retained on de-duplication enabled disk appliance based on following policy schedule: - Seven daily incremental backups for 1 week. Four weekly full backups for 1 month. Twelve monthly full backups for a period of 1year.	
36	Use of Source and Target Based De-duplication for Backups. In order to improve the backup performance and reduce the disk footprint for storing backup data, the disk-appliance solution proposed by the Bidder must support inline global de-duplication and must integrate with the backup software to facilitate client direct backups to the backup disk with source based de-duplication to reduce data transfer over IP and FC Networks.	

Licences (OS & DB)

S. No	**Licences (OS & DB)**	Compliance (Y/N)
1	Supply, Installation, Configuration & Comprehensive Warranty/ Subscription Support of supplied Databases, Operating Systems, Servers, associated components etc.	
2	Obtaining, installation, completion, and commissioning certificate (Sign-Off) from the nodal/ designated officer/personal.	
3	Products shall be supplied with ready-to-use condition along with all Software Drivers, Manuals and Media etc.	
4	During the Warranty/ Subscription Support period, the OEM available patches, fixes, upgrades etc. must be available for download from OEM site for Operating systems, Database, and related tools.	
5	All the required Operating Systems & Database licenses etc. to be factored and needs to be supplied from Day 1 for the compliance and completion of the project. And no open-source software/application/license product should be used.	
6	Databases should be platform independent and function in multiple operating systems like Linux/Unix/ Windows environment with 64-bit support.	
7	Operating Systems preferred Microsoft: Windows Server 2022 Data centre Edition; Linux based: RedHat Enterprise Server and preferred Databases: Microsoft SQL Enterprise / Oracle Database.	
8	Licensed Antivirus solution that manages advance data centre security for handling today's sophisticated threats and attacks while having minimalistic impact on performance of the data centre.	
9	Backup Scheduling tool, Management tool, DB and Instance level monitoring tool and Reporting features tool implementation as per the implementation plan. Historical data of performance and other parameters Daily, Weekly, Monthly, Yearly, and as per Custom time period. The output data can be exported to excel, pdf etc.	
10	Database should have Auto-partitioning and Scalability features. Database should provide Parallel Distributed Query Engine. Database should have Data Locality Awareness. Database should have support for both SQL and NoSQL APIs.	
11	Database should provide Multi-site Clusters with Active Geographical Replication. Database should provide Online Scaling and Schema Upgrades. Database should provide a Cluster Manager for cluster administration.	
12	Database should provide Memory optimized tables for low latency and real-time performance. Database should provide Auto-sharing for high read and write scalability. Database should be based on Distributed, Multi-Master, Shared-nothing design etc.	
13	Integration with mail system for mail notification and auto report scheduling	
14	Database should provide Synchronous and asynchronous replication with integrated failover and recovery.	

15	Database Support: Database with 24x7 Technical Support, from OEM for management, monitoring, auditing, security tooling and bundled package Subscription which include all Database Features, Tools, Platform, Upgrades for monitoring DBA activities for future enhancement.	
16	On-Site Training on the product and functionality features (overall and installed features at site) to be provided by OEM or OEM Authorized Partner for at-least/minimum 3 Days.	
17	One month technical and operational support by the implementation team (partner) from the date of FAT.	

DC-EMS

S.No.	**Specifications**	**Compliance (Y/N)**
01	EMS tool should have a capability of drawing the entire topology of the network with the immediate neighbour's so that in case of root cause, it can be helpful to reach on final outcome of root cause	
02	The tool should be SNMP v1, v2, v3 and MIB II compliant.	
03	EMS tool should have a capability of the Automatic Discovery, Topology drawing, real-time and trend reporting on the network resources in the environment along with this module should be aimed to provide unified management and central repository.	
04	The tool should tightly integrate with the helpdesk management system for automatic updating of the incident tickets.	
05	The tool should automatically discover and update itself with the configuration changes in the device and the re-indexing of the ports.	
06	EMS tool should have a capability of perform the root cause analysis for any fault that may occur in the network infrastructure and send the notification in the form of alarms to the respective end user console.	
07	EMS tools should have a feature of limited/ control connectivity to enterprise SMS gateway with the proper queuing options for the alarms/alert's delivery on to the server/host owner.	
08	EMS tool should have a capability of merging the alarms to a single alarm on intelligence basis, for e.g. In case of router failure, instead of generating lots of single alarm for all of connecting devices to router, it should be capable of generating single alarm for the router connectivity by correlating the corresponding alarms.	
09	EMS tool should have a capability of Role management access to the concerned group /users with their separate topology option. So that concerned team of any single project can also monitor their services/ hosts.	
10	EMS tool should have a feature of identifying and monitoring configurations of single Network devices (switches, routers, and hub) and device families that comprise a network. It also can be captured network device configurations and stored them in the tool database. It should have a feature of Comparing running and start-up configuration of network devices.	

11	EMS tool necessarily should have a feature of HA High Availability with the distributed cluster support.	
12	EMS tool should have the capability of graphical report generation for calculation of outage, total no of discovered devices, deleted devices and availability for Service Level Agreements.	
13	The proposed solution must provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.	
14	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: • Event filtering • Event Deduplication • Event aggregation	
15	The proposed solution must support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system, and application infrastructures.	
16	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.	
17	The solution should classify events based on business impact	
18	The solution should allow creation of correlation or analytics rules for administrators	
19	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms	
20	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes.	
21	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message	
22	The system shall support the following log formats for log collection: o Windows Event Log o Syslog o Access Log Data o Application Log data o Any Custom Log data o Text Log (flat file)	
23	The solution must provide pre-defined log correlation rules to detect suspicious behaviour.	
24	The solution must support real-time and scheduled alerting timeline while creating a log policy to catch specific log pattern	
	Server Performance Monitoring, Management and Reporting Tool	
25	The tool should be capable of real time monitoring the app services/daemons that constitute an application and the underlying infrastructure responsible for the delivery of the service. it should also be capable of process monitoring.	
26	Tool agents (deploy on to OS) can be in the form of agent and agentless.	

27	The tool should be for monitoring availability, utilization and latency of all finite hardware and software resources that are allocated to be consumed by applications (servers, database, NTP services, app, storage, service desk, etc.).	
28	It should be capable of Forward system and application faults to SNMP-based network management systems (EMS).	
29	Tool should be capable of Server's log file monitoring with the feature such that if any matching pattern is logged then automated mail could be triggered to concerned staff.	
30	Tool should have a capability of Lightweight Footprint of agents and patches with a highly optimized and low percent of CPU and memory utilization. It should also be multi-platform support.	
31	Reporting tool should have the feature of generating the graphical Reports for CPU/Memory utilization, Availability, page fault, storage, and CPU load average etc. for the hosts with the report scheduling feature.	
32	Reporting tools should be capable of generation of trend reports for the proactive resource's prediction also with the feature of summarized reports for Root cause. it should also have the feature of User Account Creation for the Enterprise Projects and group wise. Hence the specified Enterprise user can generate the reports on the web using the intranet.	
33	This tools should have the capabilities of out the box integration with EMS and the Helpdesk Software with the minimal efforts.	

Datacentre Network Solution: (Spine-Leaf)

S.NO.	**Technical Specifications**	**Compliance (Yes/No)**
	SPINE SWITCH	
1	The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and/or control plane. Issues with any of the plane should not impact the functioning of the switch. All the switches should be from same OEM	
2	Switch should be chassis based with every payload slot providing wire speed throughput for the required number of interfaces. The switch should have control plane and/ or forwarding plane redundancy for maximum uptime.	
3	The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch	
4	The switch should not have any single point of failure like CPU, supervisor, switching fabric power supplies and fans etc. should have 1:1/N+1 level of redundancy	
5	Switch should support total aggregate minimum 24 Tbsp. minimum of switching capacity	

6	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch	
7	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification/IPV6 ready	
8	Switch should support upgradation of the operating systems of the switch without disturbing the traffic flow. There should not be any impact on the performance in the event of the software upgrade/downgrade. Similarly, It should also support patching of selected process/processes only without impacting other running processes	
9	Switch should support non-blocking, wire speed performance per line card	
10	Switch should be rack mountable and support side rails, if required	
11	Switch should have adequate power supplies for the complete system usage with all slots populated and used, providing N+1 redundancy	
12	Switch should support Jumbo Frames up to 9K Bytes	
13	Interfaces must support 1/10/25/40G/100G	
14	Spine switch shall have minimum 24 x 100G QSFP+ port per card. Each Spine switch shall be loaded with at least 2-line cards from Day-1.	
15	100G QSFP+ or better optical modules should be provided fully populated on all line cards on all spine switches.	
16	The Switch should support non-blocking Layer 2 switching and Layer 3 routing. Switch should support VLAN tagging (IEEE 802.1q)	
17	Switch should support at least 64K ARP entries and 100K MAC Addresses.	
18	Switch should support IEEE Link Aggregation and Ethernet Bonding or equivalent functionality to group multiple ports for redundancy. Switch should support 300 LAG groups and 8 ports per LAG or better.	
20	Switch should support Layer 3 routing protocols like Static, IS-IS, OSPF, OSPF v3 from day 1 for the solution with minimum 32K or better IPv4 or IPv6 unicast routes and minimum 8K IPv4 or IPv6 multicast routes.	
21	Switch should support both IPv4 and IPv6 protocols like BGP, BGP+, IGMP v1, v2, v3, IGMP snooping, PIM SM/DM, PIM SSM, MPLS, IS-IS etc.	
22	Switch should support minimum 512 VRF instances	
23	The switch should support uninterrupted forwarding operation for OSPF, BGP etc. routing protocol to ensure high availability during primary controller failure	
24	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre.	
25	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)	
26	Switch should support Open Flow/Open Day light/Open Stack controller	
27	Switch should support Data Centre Bridging	
28	Control plane denial-of-service (DoS) protection.	

29	Support for broadcast, multicast, and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities.	
30	Filtering based on source and destination address, Port based, VLAN based and routed filters.	
31	Quality of Service- Switch should support minimum 4 number of hardware queues per port with support for 802.1 P and Strict Priority Queuing.	
32	Switch should be SNMP v1, v2, v3, SSH, telnet, LLDP, CLI enabled and should have Out of Band Management port.	
33	Switch should support port mirroring feature for monitoring network traffic. SPAN, RSPAN, ERSPAN	
34	Should support tools like Python, Puppet, Rest-API for automation.	

LEAF SWITCH OFC		
1	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy	
3	Switch support in-line hot insertion and removal of different parts like modules/power supplies/fan tray etc. should not require switch reboot and disrupt the functionality of the system	
4	Switch should support the complete STACK of IP V4 and IP V6 services. Switch must have IPv6 phase 2 ready logo certification/IPV6 ready.	
5	Switch should be rack mountable and support side rails if required	
6	Switch should have adequate power supply for the complete system usage with all slots populated and used and provide N+1 redundant	
7	Switch should support minimum 1.4 Tbsp. of switching capacity. Switch should support minimum 96,000 no. of MAC addresses	
8	Switch should support VLAN tagging (IEEE 802.1q), Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S)	
9	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel, LAG etc.	
10	Minimum 48 * 1/10/25G Downlink Fiber Optical Interfaces	
11	Minimum 6 * 40G/100G Uplink Fiber Optical Interfaces	
12	25G/10G SFP+ or better optical modules should be provided fully populated on all interfaces of leaf switches. 4x100G QSFP+ or better optical module should be provided with each Leaf switch.	
13	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface	
14	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy. Should support at-least 40 LAG groups and 16 ports per LAG or better.	

15	Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third-party switch or server. Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host	
16	Switch should support Jumbo Frames up to 9K Bytes	
17	Support for broadcast, multicast, and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
18	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)	
19	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine -Leaf architecture to optimise the east - west traffic flow inside the data centre	
20	Switch should support Open Flow/Open Day light/Open Stack controller	
21	Switch should support Data Centre Bridging	
22	Switch should support minimum 1000 VRF instances	
23	Switch should support both IPv4 and IPv6 protocols like Static Routing, OSPF, IS-IS, BGP, BGP+, IGMP v1, v2, v3, IGMP snooping, PIM SM/DM, PIM SSM, MPLS, IS-IS etc. The switch should support 12,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	
24	Control plane denial-of-service (DoS) protection.	
25	Quality of Service -Switch should support minimum 8 number of hardware queues per port with support for 802.1 P, Strict Priority Queuing.	
26	Filtering based on source and destination address, Port based, VLAN based and routed filters.	
27	Quality of Service. Switch should support minimum 4 number of hardware queues per port with support for 802.1 P and Strict Priority Queuing.	
28	Switch should be SNMP v1, v2, v3, SSH, telnet, LLDP, CLI enabled and should have Out of Band Management port.	
29	Switch should support port mirroring feature for monitoring network traffic. SPAN, RSPAN, ERSPAN	
30	Should support tools like Python, Puppet, Rest API etc for automation.	

DCN: Data Centre Networking

	DCN FABRIC	
1	Programmability & SDN controller: DC Fabric must provide open scripting interface from the central management appliance / SDN Controller for configuring the entire fabric. Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol	
2	Fabric must provide deeper visibility into the fabric in terms of latency and packet drop between VM to VM, VM to Physical server and vice versa, Leaf to another leaf etc. Should provide pervasive visibility of traffic across the entire data centre infrastructure, including servers and extending all the way to processes. Should provide complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the network.	
3	Network Fabric should have the Clos Architecture defined using Spine, Leaf.	
4	Network Fabric should support Configuration roll-back and check point	
5	Allows workload mobility anywhere in the DC	
6	Full cross-sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active	
7	Fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale	
8	Add as many Leafs as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.	
9	Fabric must auto discover all the hardware and auto provision the fabric based on the policy.	
10	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.	
11	Fabric must support Role Based Access Control in order to support Multi - Tenant environment	
12	Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.	
13	Fabric must provide RBAC policies and support AAA using Local User authentication, External RADIUS, External TACACS+, External LDAP, External AD	
14	Fabric must support true multi - tenancy	
15	Fabric should support scale up and scale out without any service disruption	
16	Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change	

17	Fabric must provide Centralised Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring, and provisioning the entire Fabric.	

Firewalls

S.NO.	**Technical Specifications**	**Compliance (Yes/No)**
	(EXTERNAL) EDGE FIREWALL	
1	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest three years Magic Quadrant for Firewall published by Gartner	
2	Firewall must have integrated redundant power supply	
3	Firewall must support at least 25,000,000 concurrent sessions	
4	Firewall must support at least 250,000 connections per second	
5	Firewall should support at least 40 VRFs	
6	Firewall should support stateful inspection, URL Filtering, L7 application detection and Blocking	
7	Firewall should support NAT, PAT, Dynamic NAT, Dynamic PAT, Destination based NAT including NAT64 and DNS64.	
8	NGFW must support 3DES/AES IPsec VPN throughput of at least 5Gbps	
9	Firewall Should support Site to Site IPSEC Tunnel with IKEv1 and IKEv2 for 10000 remote gateways	
10	Firewall must support at least 1000 vlans	
11	Firewall should support at least 40Gbps of IPv4 Stateful Throughput with AVC and Next-Gen Firewall features.	
12	Firewall should support Active-Active and Active Standby High Availability	
13	Firewall must support operating in routed & transparent mode. must be able to set mode independently for each context in multi-context mode.	
14	Firewall must support 10 virtual firewalls from day one & support licensed based scalability up to 100 virtual firewalls as & when required with licenses	
15	Firewall Should support IPSEC and SSL encryption/Decryption	
16	Firewall must support Nat-T for IPsec VPN	
17	Firewall must support pre-shared keys & Digital Certificates for VPN peer authentication	
18	Firewall shall support stateful session maintenance in the event of a fail-over to a standby unit. Firewall must replicate Nat translations, TCP, UDP connection states, ARP table, ISAKMP & IPsec SA's, SIP signalling session	
19	Firewalls should be provided with Redundant Power Supplies	
20	Firewalls should have at least 12*1G RJ45 ports, 12 *10G Fiber SFP+ ports, 4*40G QSFP+ ports	
21	Firewall must provide application inspection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP, SQLNET	
22	Firewall module must support security policies based on (IPv4 and IPv6)	

23	Firewall solution must provide protection against botnets.	
24	Firewall must support creating access-rules with IPv4 & IPv6 objects simultaneously	
25	Firewall must support operating in routed & transparent mode. must be able to set mode independently for each context in multi-context mode.	
26	The Firewall must support Link Aggregation Control Protocol 802.3ad	
27	Optical modules should be provided fully populated on all interfaces of Next-Gen Firewall.	
28	25 IPSEC SSL VPN licenses with third part SSL certificate.	

S.NO.	**Technical Specifications**	**Compliance (Yes/No)**
	(INTERNAL) DC FIREWALL	
1	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the last three years Magic Quadrant for Firewall published by Gartner	
2	Firewall must have integrated redundant power supply	
3	Firewall must support maximum 30,000,000 concurrent sessions with AVC/Application Security	
4	Firewall must support at least 400,000 connections per second, with AVC	
5	Firewall should support at least 40 VRFs	
6	Firewall should support stateful inspection, URL Filtering, L7 application detection and Blocking	
7	Firewall should support NAT, PAT, Dynamic NAT, Dynamic PAT, Destination based NAT including NAT64 and DNS64.	
8	NGFW must support 3DES/AES IPsec VPN throughput of at least 20Gbps	
9	Firewall Should support Site to Site IPSEC Tunnel with IKEv1 and IKEv2 for 10000 remote gateways	
10	Firewall must support at least 4096 VLANS	
11	Firewall should support at least 80Gbps of IPv4 Stateful Throughput with AVC and Next-Gen Firewall features.	
12	Firewall should support Active-Active and Active Standby High Availability	
13	Firewall must support operating in routed & transparent mode. must be able to set mode independently for each context in multi-context mode.	
14	Firewall must support 10 virtual firewalls from day one & support licensed based scalability up to 100 virtual firewalls as & when required with licenses	
15	Firewall Should support IPSEC and SSL encryption/Decryption	
16	Firewall must support Nat-T for IPsec VPN	
17	Firewall must support pre-shared keys & Digital Certificates for VPN peer authentication	
18	Firewall shall support stateful session maintenance in the event of a fail-over to a standby unit. Firewall must replicate Nat translations, TCP, UDP connection states, ARP table, ISAKMP & IPsec SA's, SIP signalling session	
19	Firewalls should be provided with Redundant Power Supplies	
20	Firewalls should have at least 12*1G RJ45 ports, 8*10G Fiber SFP+ ports, 8*40G QSFP+ ports	

21	Firewall must provide application inspection for DNS, FTP, HTTP, SMTP, ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP, SQLNET	
22	Firewall module must support security policies based on (IPv4 and IPv6)	
23	Firewall solution must provide protection against botnets.	
24	Firewall must support creating access-rules with IPv4 & IPv6 objects simultaneously	
25	Firewall must support operating in routed & transparent mode. must be able to set mode independently for each context in multi-context mode.	
26	The Firewall must support Link Aggregation Control Protocol 802.3ad	
27	Optical modules should be provided fully populated on all interfaces of Next-Gen Firewall.	
28	Maximum VPN Peers: 5,000	

Intrusion Protection System

S.NO.	**Technical Specifications**	**Compliance (Yes/No)**
	NIPS: Network Intrusion Protection System	
1	The IPS solution must be a purpose-built dedicated appliance (not a subset of firewall or UTM appliance)	
2	The device must operate in transparent (Bridge) mode	
3	The device must have separate dedicated interface for management	
4	The device must have inbuilt internal Redundant Power Supply (RPS) with no additional cost	
5	The device must have functionality of hardware-based fail-open & Software Fail Open. NIPS must also have fail-open feature which must allow traffic to pass through uninterrupted when power failure occur on the NIPS.	
6	The IPS solution must support IDS (Inline detection mode) as well as IPS (Intrusion Prevention Mode)	
7	The single device must have minimum Inspected throughput of 80 Gbps for all kinds of real-world traffic in case of Active-Active in HA or Active-Passive mode.	
8	Must have minimum 16 x 10G monitoring interface (with fully populated SFP - SR modules) with fail-open capability	
9	Latency must be < 60 microseconds. must support at least 30,000,000 concurrent connections	
10	The device must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes,	
11	The device must use prevention techniques and provide zero-day protection against worms, Trojans, spyware, key loggers, and other malware from penetrating the network.	

12	The device must perform traffic inspection based on: Signatures, Protocol anomaly, Behaviour anomaly, Reputation	
13	The device must accurately detect the following Attack categories: -	
	Malformed traffic, Invalid Headers, DoS	
	Vulnerability exploitation	
	Zero-day and unknown attacks – desirable	
	URL obfuscation	
14	The device must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
15	The device must provide advanced DOS/DDOS protection and not just signatures based employing a combination of threshold-based and self-learning, profile-based detection techniques, volume based and exploits signatures to detect DoS and DDoS attacks	
16	The device must support vulnerability based and exploit-based signatures. It must detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability)	
17	The device must handle following traffic inspection& support:	
	IPv6, IPv4, MPLS, Tunnelled: 4in6, 6in4, 6to4	
	Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection	
	Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation	
	Rate-based threats, Statistical anomalies	
18	The device must have the ability to identify/block individual applications (e.g. Facebook or skype) running on one protocol (e.g. HTTP or HTTPs)	
19	The device must prevent SSL protocol-based attacks	
20	Protect against IPv6 based attacks	
21	The device must support Block attacks based on: IP reputation, DNS Inspection, Geo-location, URL Inspection	
22	The device must support for File reputation/type on the basis of application protocol including Http, Https, FTP, SMB (no file must be sent to cloud)	
23	The device must support for Blocking of file by geographical source or destination	
24	The device must have the ability to block connection to or from outside based on the reputation of the IP address that is trying to communicate with the network using OEM own threat intelligence.	
25	The device must protect against vulnerability in: Web applications, Databases.	
26	The device must protect against DOS attacks based on: Heuristic-based detection	
27	The device must have the feature of Self-learning profile-based detection / Network Behaviour Analysis	
28	The device must have the feature for creating user-defined signature.	

29	The device must support active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done and its logging.	
30	The device must support a wide range of response actions: Block traffic, Allow traffic, Monitor / Log traffic	
31	The IPS solution shall provide source reputation-based analysis. It must support source lookup for file, Ip, domain reputation.	
32	The device must support Packet capture, User defined scripts, Email alert, SNMP alert, Syslog alert,	
33	The device must have facility to enable/disable each individual signature. Each signature must allow granular tuning.	
34	The device must allow policy to be assigned per device, port, VLAN tag, IP address/range.	
35	The IPS solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant by Gartner	

Load Balancer and Controller + WAF

Sr. No	**LOAD BALANCER / APPLICATION DELIVERY CONTROLLER CAPABILITIES**	**Compliance (Yes/No)**
1	The Load Balancer/ADC should have Layer 4 and Layer 7 load balancing should support the following	
1.1	Throughput (L4): 40 Gbps with future scalability of 100%	
1.2	Throughput (L7): 20 Gbps with future scalability of 100%	
1.3	Should support 10K SSL terminations per second with 2048-bit keys (each request is new handshake)	
1.4	L4 Concurrent connections: 14M	
1.5	L4 Connections Per Second: 120,000	
1.6	L7 Requests Per Second: 2,40,000	
1.7	Max. Compression Throughput 5Gbps with future scalability of 100%	
1.8	Should have minimum 8x10GE and 8x1GE interfaces.	
2	The solution should have the following Load Balancer / ADC algorithms	
2.1	Round-Robin	
2.2	Weighted Round-Robin	
2.3	Least Connections	
2.4	Fastest Response	
3	Server Load Balancer should support following Server Persistency Methods	
3.1	Source-IP	
3.2	Hash IP	
3.3	Hash IP/Port	
3.4	Hash Header	
3.5	Hash Query	
3.6	Persistent Cookie	
3.7	Rewrite Cookie	

3.8	Insert Cookie	
3.9	Hash Cookie	
3.10	Embedded Cookie	
3.11	RADIUS Attribute	
3.12	SSL Session ID	
4	Server Load Balancer should support following Health Check Algorithms	
4.1	ICMP	
4.2	TCP	
4.3	TCP Echo	
4.4	HTTP	
4.5	HTTPS	
4.6	DNS	
4.7	RADIUS	
4.8	RADIUS Accounting	
4.9	SMTP	
4.10	POP3	
4.11	IMAP4	
4.12	FTP	
4.13	TCP Half Open	
4.14	TCP SSL	
4.15	SNMP	
5	Server Load Balancer should support Layer 7 Load Balancing of well-known protocols: -	
5.1	HTTP	
5.2	HTTPS	
5.3	TCP	
5.4	UDP	
5.5	FTP	
5.6	RADIUS	
6	The solution must support URL re-write to ensure delivery secure content through HTTPS protocol and support the following actions:	
6.1	Request modifications	
6.2	Insert header	
6.3	Delete header	
6.4	Modify header	
7	The system should have the ability to graph service level statistics such as number of connections, requests	
8	The solution should have a web-based administration.	
9	The solution should have exportable logs for access, audit, network, Server failures, etc.	
10	The solution should be delivered as a hardware, virtual or cloud-based appliance.	
11	The virtual appliance should support all major hypervisors such as:	
11.1	Microsoft Hyper-V	
11.2	Citrix Xen	

11.3	VMWare ESXi	
12	The solution should have configurable dashboards.	
13	The solution should provide a RESTful Application Programming Interface (API)	
14	The solution should have integrated AAA support for LDAP and Radius.	
15	The solution should have the ability to compress Web traffic to reduce network requirement.	
16	The solution should have the ability to reduce back-end Web server load and increase Web server performance by caching Web content	
17	The solution should support One-Arm with Reverse and Transparent proxy mode deployment scenarios & Direct Server Return.	
18	High Availability - The solution should provide comprehensive and reliable support for high availability mode. It should be able to be deployed in Active-Active or Active-Passive mode.	
19	The solution should support virtualisation, supporting up to 10 virtual instances and scalable up to 30.	
20	The solution should support communication link for real-time configuration synchronization and during run time to keep consistence configuration on both units.	
21	The solution should support built in failover decision/health check conditions.	
	Network Management	
22	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend	
23	The solution should support data centre level redundancy with built-in Global Server Load Balancing (GSLB) based on the following	
23.1	Priority - provides alternate location for accessing resource in the event that the primary server fails	
23.2	Geo IP - directs requests to the geographically closet server location	
23.3	Region – requests from a certain region are directed to the data centre that supports that region	
24	The solution should have support for multiple VLANs with tagging capability	
25	The solution should support IEEE 802.3ad link aggregation for bonding links to prevent network interfaces from becoming a single point of failure	
26	The solution should support Multi-level virtual service policy routing – Static, default.	
27	The solution should support Dynamic Routing protocols like RIPv2, OSPF and BGP	
28	It should have the capability of rate shaping & QoS Support.	
29	The solution should support monitoring of the Load Balancer / ADC via SNMP.	
30	The solution should support SNMP traps.	
	SSL Capabilities	
31	The solution should have SSL offload capabilities.	
32	The solution should support minimum 15000 transactions per second (TPS).	

33	The solution should support minimum 2 Gbps Bulk Encryption Rate.	
34	The solution should support Key Lengths of 512 Bit, 1024/2048 bits or higher.	
35	The solution should have the ability to receive encrypted data on the front-end and pass clear text to the back-end servers	
36	The solution should have advanced encryption capabilities that support Perfect Forward Secrecy (PFS) with ECDSA and RSA and allow for the selection of various ciphers to encrypt messages	
37	The solution should have SSL certificate management like Certificate & Key Importing, Auto/Manual Enrolment & Renewal of Certificates and Keys.	
38	The solution should support time stamped certificate revocation lists. SSL accelerator should have the capability of verifying the revocation status of Client Certificates by using the following:	
38.1	a. Online Certificate Status Protocol (OCSP)	
38.2	b. Certificate Revocation List (CRL)	
39	The solution should have the capability to add policies to allow for client authorization and authentication	
40	**Web Application Firewall Capabilities**	
41	The solution should have abuse detection, tracking, Profiling and should support Abuse response and real time incident management.	
42	The solution should protect against OWASP Top 10 common attacks such as:	
42.1	SQL Injections	
42.2	Cross-site Scripting (XSS)	
42.3	Cross-Site Request Forgery (CSRF)	
43	The solution should have DDoS prevention that can granularly control the number of requests to throttle or drop traffic based on IP or client	
44	The solution must protect web application against Cookie Poisoning, cookie injection, command injection.	
45	The solution must protect web application against buffer overflow and layer7 DDOS attacks.	
46	The solution must protect web application against parameter tampering and must have inbuilt controls to block invalid files, filtering of sensitive words in HTTP request and response.	
47	The solution should be able to detect suspicious application errors that indicate abuse including illegal and unexpected response codes.	
48	The solution should be able to detect when an attacker is attempting to request files with suspicious extensions, prefixes, and tokens	
49	The solution should support creation of the policies for HTTP/HTTPS headers to ensure critical infrastructure information is not exposed. Response and request headers can be stripped, mixed, or filtered	
50	The solution should be able to detect and prevent attackers from finding hidden directories. inbuilt security control to limit the action of crawling and scanning	
51	The solution should be able to detect attempts to abuse non-standard HTTP/HTTPS methods such as TRACE.	

52	The solution should be able to detect attempts to manipulate application behaviour through query parameter abuse. Solution must support behaviour analysis to detect and prevent day on attacks	
53	The solution should maintain a profile of known application abusers and all of their malicious activity against the application	
54	The solution should support network-based security controls including ACL 's, IP blacklist/whitelist and URL blacklist/Whitelist.	
55	The solution should support Anti-DDOS protection with SYN flood, UDP flood, ICMP flooding, command, and control protection	

WAN Routers

1	**DC Router Specifications**	**Compliance (Yes/No)**
1.1	Router should have modular configuration so that different modules can be added to it and shall also have modular Operating System with redundant AC power supplies and Redundant Control Plane card from day 1.	
1.2	The operating system of the router shall have a microkernel-based architecture	
1.3	Should support redundant CPU for high availability	
1.4	Router should be provided with 1+1 route processor, 1+1 or 1+N switch fabric and 1+1 or 1+N power supply redundancy	
1.5	Failure of one switch fabric card shall not degrade the performance & capacity of routers. Failure of one switch fabric card shall not degrade the per line card available bandwidth	
1.6	Should have power supply redundancy. There should not be any impact on the router performance in case one of the power supplies fails	
1.7	All interface modules, power supplies should be hot swappable for high availability	
1.8	Router should have minimum 16 x 1G Copper based, 18x 1/10GE Fiber based ports spread across multiple line cards should be provided. Should be scalable to support up to 40Gig or better ports with maximum distance of 10KM and 40KM without any additional regenerators	
1.9	Router should have minimum 4 interface slots.	
1.10	Router should support at least two free slots for future expansion	
1.11	Router should support minimum 100 Gbps full duplex throughput and 1.4 Bpps of performance for IPv4 and IPv6.	
1.12	Router should support RIB capacity of 4 Million IPv4, IPv6, 4K L3VPN VRF and 4K VPLS routing-instances and MAC scaling of 1 million MAC.	
1.13	Router should support services like L2VPN, L3VPN and VPLS.	
1.14	Router should support Static Route, Default Route, RIPv2, OSPFv2 & OSPFv3, BGPv4, PBR and IS-IS.	

1.15	Should have Multicast routing protocols IGMPv1, v2, v3, PIM-SM (RFC2362) and PIMSSM, MSDP, IGMP v2 snooping	
1.16	Router should support VXLAN/NVGRE or equivalent for Data Centre Interconnect.	
1.17	Router should support following MPLS features – LDP, Layer 2 VPN technologies with LDP signalling, Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection.	
1.18	Router should support IPv6 QoS and Traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, MPLS EXP, DSCP	
1.19	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter	
1.20	Router should have 4 level of scheduling for HQOS	
1.21	The router shall support IEEE 802.3ad link aggregation of minimum of 8 links within a single bundle.	
1.22	Router should have capability of mapping of address and port using encapsulation as well as translation mechanism for IPv4 to IPv6 migration functionalities.	
1.23	Router should have a console for Out-of-band Management.	
1.24	Router should be manageable through Local Console & Aux Port, Telnet and SSHv2.	
1.25	Router should support SNMP v1, v2 and v3 and RMON features.	
1.26	Support Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc	
1.27	Time based & Dynamic ACLs for controlled forwarding based on time of day for offices	
1.28	Support per-user Authentication, Authorization and Accounting through RADIUS or TACACS	
1.29	MD-5 route authentication for RIP, OSPF and BGP	
1.30	Multiple privilege level authentications for console and telnet access through Local database or through an external AAA Server	
1.31	Support for monitoring of Traffic flows for Network planning and Security purposes	
1.32	Display of input and output error statistics on all interfaces	
1.33	Router shall support System & Event logging functions as well as forwarding of these logs onto a separate Server for log management.	
1.34	Router should be minimum common criteria EAL3/NDPP/NDcPP certified.	

Campus-NOC Switch

1	**Campus/NOC Switch Specifications**	
1.1	Switch should have 40 X 10/100/1000Base-T autosensing ports complying to IEEE 802.3, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto negotiation on each port with 4 x SFP+ uplink ports	
1.2	All copper-based ports will be POE ports 802.3af compliant @15.4 Watts.	
1.3	Switch should support stacking with dedicated stacking ports whenever required in future. Stacking bandwidth should be min 80 Gbps with dedicated stacking ports	
1.4	Switch should support link aggregation across multiple switches in a stack.	
1.5	Stack should support automatic upgrade when the master switch receives a new software version. The switch should support configurable egress buffer allocation for different queues on the stack ports	
1.6	Should support stacking of minimum of eight switches	
1.7	Switch should support IPv4 and IPv6 from day One	
1.8	Switch should have non-blocking switching fabric of minimum 88 Gbps or more and should have Forwarding rate of minimum 65 Mpps.	
1.9	Switch should support power supply redundancy	
2	**Layer-2 Features**	
2.1	IEEE 802.1Q VLAN tagging with support for minimum 255 active VLANs and 4k VLAN ids	
2.2	Should support for minimum 16k MAC addresses	
2.3	Switch should support Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) and Multiple Spanning Tree Groups and Protocol (MSTP or 802.1s).	
2.4	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping	
3	**Connectivity**	
3.1	802.3ad based standard port/link aggregation, Jumbo frames, storm control	
3.2	Switch should support up to 4000 configurable VLANs (IEEE 802.1Q) with 4000 VLAN IDs.	
4	**Security**	
4.1	The switch should support up to 400 IPv4 & IPv6 Security ACEs	
4.2	Switch should support MAC address-based filters / access control lists (ACLs) on all switch ports	
4.3	Switch should support Port as well as VLAN based Filters / ACLs.	
4.4	Switch should support RADIUS and TACACS+ for access restriction and authentication.	
4.5	Secure Shell (SSH) Protocol, HTTP and DoS protection	
4.6	Should support DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)	
4.7	RADIUS change of authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA serve to reinitialize authentication and apply to the new policies.	
4.8	The switch support IPV6 first hop security using common function across the OEM's such as IPV6 RA guard, DHCP Guard, Neighbour Discovery, IPV6 Snooping	
5	**QoS Features.**	

5.1	Switch should support classification and scheduling as per IEEE 802.1 P on all ports	
5.2	Switch should support DiffServ as per RFC 2474/RFC 2475	
5.3	Switch should support QoS configuration on per switch port basis support four hardware queues per port	
6	**Management Features**	
6.1	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.	
6.2	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.	
6.3	Switch should support TELNET and SSH Version-2 for Command Line Management	
6.4	Switch should support 4 groups of embedded RMON (history, statistics, alarm, and events)	
6.5	Support for Unidirectional Link Detection Protocol (UDLD) to detect unidirectional links caused by incorrect fibreoptic wiring or port faults and disable on fibre-optic interfaces	
6.6	Should support DHCP Server feature to enable a convenient deployment option for the assignment of IP addresses in networks that do not have without a dedicated DHCP server.	
6.7	Switches should support Energy Efficient Ethernet (EEE) (IEEE 802.3az standard) to reduce power consumption in Ethernet networks during idle periods. The switch should provision to save power by entering low power idle (LPI) mode during periods of low utilization.	
7	**Certifications**	
7.1	Switch should be EAL3/NDPP certified.	
7.2	Switch should be RoHS (with lead exemption) and WEEE certified.	
7.3	Switch should be UL 60950-1, IEC 60950-1, EN 60950-1, EN60825-1 certified	

OOB Switch

1	**OOB Switch Specifications**	
1.1	Switch should have 40 X 10/100/1000Base-T autosensing ports complying to IEEE 802.3, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto negotiation on each port with 4 x SFP+ uplink ports	
1.2	Switch should support stacking with dedicated stacking ports whenever required in future. Stacking bandwidth should be min 80 Gbps with dedicated stacking ports	
1.3	The switch should Pre-Provision stack-member configuration – configure stack member interfaces even before adding the member. Useful for replacing the RMA stack member and should also support Faster stack convergence <100ms	
1.4	Switch should support link aggregation across multiple switches in a stack.	
1.5	Stack should support automatic upgrade when the master switch receives a new software version. The switch should support configurable egress buffer allocation for different queues on the stack ports	
1.6	Should support stacking of minimum of eight switches	
1.7	Switch should support IPv4 and IPv6 from day One	
1.8	Switch should have non-blocking switching fabric of minimum 88 Gbps or more and should have Forwarding rate of minimum 65 Mbps.	
1.9	Switch should support power supply redundancy	
2	**Layer-2 Features**	
2.1	IEEE 802.1Q VLAN tagging with support for minimum 255 active VLANs and 4k VLAN ids	
2.2	Should support for minimum 8k MAC addresses	
2.3	Switch should support Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) and Multiple Spanning Tree Groups and Protocol (MSTP or 802.1s).	
2.4	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping	
3	**Connectivity**	
3.1	802.3ad based standard port/link aggregation, Jumbo frames, storm control	
3.2	Switch should support up to 4000 configurable VLANs (IEEE 802.1Q) with 4000 VLAN IDs.	
4	**Security**	
4.1	The switch should support up to 500 IPv4 & IPv6 Security ACEs	
4.2	Switch should support MAC address-based filters / access control lists (ACLs) on all switch ports	
4.3	Switch should support Port as well as VLAN based Filters / ACLs.	
4.4	Secure Shell (SSH) Protocol, HTTP and DoS protection	
4.5	Should support DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)	
4.6	RADIUS change of authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA serve to reinitialize authentication and apply to the new policies.	
4.7	The switch support IPV6 first hop security using common function across the OEM's such as IPV6 RA guard, DHCP Guard, Neighbour Discovery, IPV6 Snooping	

5	**Management Features**	
5.1	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.	
5.2	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.	
5.3	Switch should support TELNET and SSH Version-2 for Command Line Management	
5.4	Switch should support 4 groups of embedded RMON (history, statistics, alarm, and events)	
5.5	Support for Unidirectional Link Detection Protocol (UDLD) to detect unidirectional links caused by incorrect fibreoptic wiring or port faults and disable on fibre-optic interfaces	
5.6	Should support DHCP Server feature to enable a convenient deployment option for the assignment of IP addresses in networks that do not have without a dedicated DHCP server.	
5.7	Switches should support Energy Efficient Ethernet (EEE) (IEEE 802.3az standard) to reduce power consumption in Ethernet networks during idle periods. The switch should provision to save power by entering low power idle (LPI) mode during periods of low utilization.	
6	**Certifications**	
6.1	Switch should be EAL3/NDPP certified.	
6.2	Switch should be RoHS (with lead exemption) and WEEE certified.	
6.3	Switch should be UL 60950-1, IEC 60950-1, EN 60950-1, EN60825-1 certified	

Structured cabling for entire Data Centre:

SI / Bidder to consider Multimode OM4 fibre cable to provide backbone connectivity between Spine and leaf switches (100G) and between Core & access SAN switches. Connectivity between server/storage to leaf (10/25G) and access SAN switch will also be provisioned on multimode OM4 fibre cable. Data Centre structured cabling involves following activities:

- Supply, installation, testing and commissioning of all fibre/copper panels, Network/Server Rack dressing, laying of cables (Copper STP [CAT6A] & Fibre), terminations at both end and other passive components for approx. 80 racks.
- Cable laying will be through metal raceways, PVC conduits, overhead ladder / tray, and other relevant activities.
- Laying of STP copper Cable in raceways includes proper bunching and tagging for different Cables including color coding. (if required)
- Preliminary continuity Testing & Ferruling at both end for each cable unique identity.
- Termination, Installation, Fixing of Port Jack Panels including proper Dressing of Cables. Proper routing of Patch Cords in Racks, Jack Panels, and wire/ cable manager with tagging of Mounting Cords.
- Network rack shall be with proper cable management, Ladder, Vertical & Horizontal Wire Manager etc.
- Fibre termination and Management System and Fibre routing also has to be included in the scope.
- OLTS Scanning of laid Copper/Fibre Cables for the performance testing of Installed Cabling System with EIA/TIA specified parameters.

- Cabling system shall include factory-terminated system components which can be quickly mated to form an end-to-end optical link between patching locations and/or equipment ports.
- Cabling system shall be a modular solution and should offer a greater degree of flexibility in managing equipment moves, adds, or changes.
- Bidder shall submit the certificate from fibre glass OEM stating bend insensitive glass is supplied for all the cables in this project and also attenuation report of fibre core used.
- Fibre cable & jumper shall have OM4 fibre with bend insensitive fibre Trunk cable and jumper.
- There should be at least 25-year product warranty and Application Assurance for passive components.
- Cables should have no joints or splices, all foil should necessarily be grounded at all terminations.
- Under no circumstance hand labelling of the cables will be accepted, No hand punching shall be allowed without proper tools. Labelling and Punching should be done as per TIA/EIA standards.
- Any cable that does not meet TIA/EIA specifications should be repaired or replaced at the bidder's expense.
- Each outlet shall be tested for satisfactory operation based on certification parameters valid for the entire warranty period of at least 25 years or more as applicable.
- All outlets in the Facility be clearly marked, labelled & documented for future reference.
- The Bidder Provision of additional Passive nodes shall do maintenance of the LAN Passive components whenever required and shall also need to be provided based on requests.
- Cable layout plan should be submitted as part of the technical bid.
- Network cabling will also be done for the DC OPTS, Staging, Reception and the user or support area and Network devices like network switches, DCIM servers, storage etc., has to be considered for the Non-IT Infrastructure LAN.

Ticketing / Helpdesk Solution

S.NO.	Technical Specification	Compliance (Yes/No)
1	**Helpdesk Solution**	
1.1	Introduction. A helpdesk solution shall be provided for is an incident logging and tracking system. It shall provide multi-purpose support tools that can be used across the Purchaser's organization to manage processes such as technical helpdesks, Subscriber services, and trouble management.	
2	**Functional Requirements**	
2.1	Bidder shall provide for helpdesk licenses for handling all concurrent users as per dimensioning parameters. The bidder should assess the help desk load for the volumetric given in this tender in terms of user base accessing this help desk and provide the additional licenses if required.	
2.2	System shall have LDAP support.	
2.3	System shall have web interface for users, Purchasers and other administrators which shall support all the helpdesk functionalities including analysis and reporting	
2.4	System shall be ITILv3 (Information Technology Infrastructure Library) compliant. Verifiable proof that the helpdesk is ITILv3 compliant shall be submitted.	
2.5	System shall manage the relationships between user problems and network and services events.	

2.6	It shall provide workflow, business and IT process orchestration and automation.	
2.7	It shall support single sign-on feature and shall store single sign on credentials.	
2.8	It shall provide integrated authentication and authorization for agent roles and applications by means of Enterprise Single Sign-On.	
2.9	The system shall provide the web-based self-care functionality for the NOC personnel.	
2.10	The system must support access to data using a common business logic layer in SOA Compliant architecture.	
2.11	Native support for Web services and Purchaser-defined XML schemas should makes it easy to integrate form data with many back-end systems using Web services.	
2.12	Trouble ticketing system shall be able to extract all incidents, resolution progress reports.	
2.13	Helpdesk system should provide capability to interface with the Inventory Management System.	
2.14	Trouble ticket shall be tracked in the helpdesk system till the cause of the outage has been detected, repaired and the service restored.	
2.15	In case the outage is self-healing, the event management system shall notify the help desk system and clear the trouble ticket automatically.	
2.16	Whenever a problem is reported by an end user, a unique trouble ticket ID shall be generated by the system. This shall be intimated to the help desk analyst at the NOC, so that they can track the status on the basis of this ID.	
2.17	It shall be possible for NOC staff to submit and check the status of reported problems through web interface.	
2.18	The system shall automatically track, log, and escalate user interactions and requests.	
2.19	NOC personnel shall be able to view, change the status of the calls, reassign / transfer the trouble tickets to other NOC personnel or technical specialist through the web interface.	
2.20	It shall be able to generate various customized Service Level Reports e.g. Open Call Reports, Closed Call Reports, Problem Area / Location specific Reports.	
2.21	It shall have the capability for accepting queries through various sources including telephone, email, or web interface.	
2.22	It shall provide case categorization capabilities for the NOC personnel to categorize incoming requests and problems etc using category quickly and consistently, type, urgency level and item menus etc.	
2.23	Duplicate Case Tracking. Support staff should be able to associate multiple instances to a single problem and tie the resolution of multiple cases to the resolution of one case.	
2.24	System shall check for tickets status and escalation and notify the management or next level of support staff based on predefined Service Level Agreement (SLA) which shall include criteria like service application, severity, and Purchaser etc.	
2.25	It shall be possible for the queries and escalations to be assigned to NOC personnel groups or individual NOC personnel.	
2.26	It shall have bulletin board to allow NOC personnel, Managers and Administrators to post and review messages about critical issues. It shall be possible to track the time spent on specific case.	
2.27	Trouble ticketing system shall be able to escalate and track problems to the support agencies external to Army.	

2.28	Trouble ticketing system shall interface with SLA and Performance management systems to account for the period of network or service unavailability.	
2.29	Life cycle of the case or trouble ticket shall include phases like opening, suspension, closing and archiving which shall be tracked by the system.	
2.30	Assignment, routing, and escalation of trouble ticket shall be both automated and manual and shall be based on pre-defined rules. Rules shall include the case of escalation when estimated time to repair is not met.	
2.31	The trouble tickets shall be attached to a workflow wherever there are multiple steps required for resolution.	
3	**Reporting and Workflow**	
3.1	System shall provide predefined reports for the proposed components.	
3.2	System shall have the capability to access and query the database.	
3.3	System shall provide the ability for an administrator to customize its workflow via point-and-click capabilities.	
3.4	Shall provide the ability for a NOC personnel /administrator to customize his GUI using a point-and-click interface to add and change windows, objects, and fields in windows	
3.5	System shall provide the ability to integrate the application with web portal, EMS, etc using XML etc	
3.6	Workflow shall be able to perform notification via email, SMS, etc.	
3.7	System shall have the capability to attach documents along with the trouble ticket.	
3.8	System shall provide approval engine so that any customized applications developed could incorporate the hierarchy, role based, level-based ad-hoc approval structure. Shall include notification and escalation capability if approval is not performed.	
3.9	It shall integrate with Single Sign On for all helpdesk applications on the portal by integration with directory services/equivalent. It shall enable Trimmed-UI where the NOC personnel will only see what access rights he has.	

SIEM

S. No.	Technical Specifications	Compliance (Yes/No)
1	**Security Information/Incident & Event Management Software**	
1.1	The SIEM platform should be based on a Hardened Operating System as an appliance solution.	
1.2	The SIEM solution licensing should be by the number of events per second (EPS), and the license must allow incoming events from unlimited number of assets, considering the limit of events per second. License must be factored for 30,000 EPS.	
1.3	The SIEM solution should not require the addition of agents or software on the monitored assets, except if the asset being monitored does not provide any means native log shipping.	
1.4	The SIEM solution must possess native connectors for all the assets within the scope of work as part of this RFP.	

1.5	For assets not natively supported, the SIEM solution should provide the collection of events through customization of connectors or similar integration; Must support event collection using at least the following industry standards: syslog, OPSEC, WMI, SDEE, ODBC, JDBC, FTP, SCP, HTTP, text file, CSV, and XML file.	
1.6	The SIEM solution must supply own API and graphical tools for creating new connectors or similar parsing solution. Please Specify.	
1.7	The SIEM receiver or log collection component must be able to store the data locally if communication with centralized Correlators is unavailable.	
1.8	The SIEM must allow sending crude/raw event for storage and should support online log management up to 1 year for forensic analysis.	
1.9	The solution should provide support for IPv6.	
1.10	The solution must allow correlating events and alerts to existing data in lists (watch list), also allows the creation of new and editing existing lists, both as an automated and manual. Must allow creation of static or dynamic Lists.	
1.11	The SIEM solution should support RADIUS and Active Directory for Authentication.	
1.12	The solution should provide a single pane of glass view for all events and incidents across the organisation and should provide Real Time Analysis and Reporting.	
1.13	The proposed SIEM Solution should be at least FIPS 140-2, Level 2 Validated.	
1.14	The SIEM platform should not require a separate RDBMS for log collection, web server or any kind of application software for its installation.	
1.15	The solution should be highly available and redundant. There should not be any single point of failure.	
	Log Collector/Receiver Systems at NDC, DRDC & RDCs	
2	**Log Collection**	
2.1	The SIEM solution should support Integration with Existing Firewalls, IPS, Antivirus Solution, Gateways routers, switches etc.	
2.2	The SIEM solution should be able to collect logs via the following ways as inbuilt into the solution: SYSLOG, OPSec, Agent-Less WMI, SDEE, Calls to MS-SQL Systems via ODBC, FTP, SCP, etc.	
2.3	The solution should provide the capability to integrate with the storage solution being implemented as part of this tender, to store events for historical reporting and analysis.	
2.4	The SIEM solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	
2.5	The SIEM solution should provide for a data store which is compressed via aggregation logic. The solution should provide for data compression.	
2.6	The solution should be highly available and redundant. There should not be any single point of failure.	
	SIEM Correlation System	
3	**Correlation**	
3.1	The SIEM solution should provide content aware correlation against data collected from multiple devices across the network.	
3.2	The SIEM solution must support the ability of integrating with offline threat intelligence system with information from global risks and use the information collected in this system in the correlation of events. .	

3.3	The solution should have pre-defined correlation rules out of the box, so as to provide correlation on the fly. Specify number of pre-defined correlation rules available out of the box.	
3.4	The solution should integrate with the proposed Identity and Access Management being deployed as part of this RFP.	
3.5	The SIEM solution should take the vulnerability information from the Vulnerability Assessment solution and correlate with existing enterprise-wide countermeasures and also correlate with the global threat intelligence feeds to prioritize security risks.	
3.6	The SIEM must allow the creation of an unlimited number of new correlation rules, as well as the customization of existing rules.	
3.7	The SIEM solution should provide a formula of threat which should be customized to allow increasing or decreasing the level of risk with at least the following types of correlation:	
3.7.1	Geo Location Based correlation	
3.7.2	Historical Based Correlation	
3.7.3	Vulnerability Based Correlation	
3.8	The relative risk of each activity should be calculated based on values assigned by the Asset Administrator.	
3.9	The solution should support segregation of activities based on levels of risk for the Purchaser organization. For example, Very high, high, medium, low, and very low.	
3.10	The SIEM solution must support multiple mechanisms of correlation and the correlated events from these, to carry out activities of correlation and located centrally.	
3.11	The solution should be able to decode an entire application session up to Layer 7, providing a full analysis of everything from the underlying protocols and session integrity.	
3.12	The solution should include pre-built detection rules for regulated and sensitive data.	
3.13	The solution should be highly available and redundant. There should not be any single point of failure.	
	SIEM Alerting, Reporting, Querying, Dashboard, and Incident Management System	
4	**Reporting/Dashboard/Event Viewer/Incident Management**	
4.1	The solution should provide pre-defined and customizable report templates.	
4.2	The SIEM solution should provide support for Incident Management Workflow.	
4.3	The SIEM solution should be able to integrate with a Trouble Ticketing system.	
4.4	The SIEM solution should support integration with the proposed Vulnerability Assessment solution.	
5	**Log Aggregation and Normalization.**	
5.1	Logs collected from all the devices should be aggregated as per the user configured parameters. Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.	
6	**Log Archival**	
6.1	Logs collected from all the devices should be stored in a non-tamper able format on the archival device in the compressed form. For correlation and	

	report generation purpose, past 01-year log data should be available online. Solution being provided should be scalable and user configurable to cater to the future requirement of the organisation.	
6.2	Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Purchaser at no extra cost.	
7	**Log Correlation**	
7.1	Collected Logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. The correlation rules should be predefined and also user configurable. Correlation rules should be customized by the bidder on regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.	
7.2	**Alert Generation**. Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS, Syslog, SNMP as per user configurable parameters.	
8	**Event Viewer/ Dashboard/ Reporting/ Incident Management System**	
8.1	SIEM solution should provide web-based facility to view security events and security posture of network and register incidents at the National/Regional SOC. Solution should have drill down capability to view deep inside the attack and analyse the attack pattern. Dashboard should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc. Dashboard should have Role Based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level. Solution should provide various reports based on user configurable parameters and standard compliance reports like PCI-DSS, ISO27001, SOX, IT Act, and regulatory reports.	
8.2	Bidder shall customize Incident Management/Dashboard/Reports for the Purchasers needs and will modify the same as per the changing requirement of the organisation.	
8.3	The SIEM solution should provide centralized visibility and monitoring/reporting interface to detect advance patterns of attacks and an overall security visibility across the entire IT security landscape. SIEM solution should integrate event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and extensible compliance reporting all in a single set of technology. This solution would collect and perform correlation on all logs, events and flows from various IT devices such as Routers, Switches, Firewalls, Network IPS, Server Security solutions, and host of other IT and Telecom domain equipment.	

Schedule Of Requirement

1. Vendors are required to offer only one option in terms of Make/Model as part of the Technical Bid.

2. Adequacy. Any additional items, hardware, software, licenses, accessories, cables, connectors, patch cords etc not specifically asked by the Purchaser but essential to achieve 100% functionality as given in

this tender, shall be supplied by the bidder at no additional cost. The bidder shall hence ensure that all items required to meet complete operational and functional requirements of the network are included as part of the technical and commercial bid. In case, the same is discovered during implementation, the bidder shall provide the same to the Purchaser at no additional cost.

3. Documentation. Complete technical literature in English with detailed connection diagram of various sub-components and other details of the system shall be provided for all equipment. All aspects of installation, operation, troubleshooting, and maintenance shall also be covered in the handbooks.

4. License. All licenses for software shall be unlimited and provided for the required validity period (5years/7years/lifetime) and free updates/upgrades/patches during Warranty and AMC period.

S. No.	Item Description	Units	Quantity
1	**CUSTOMER RELATIONSHIP MANAGEMENT**		
1.1	Ticketing /Helpdesk Solution	Set	01
2	**DATACENTRE HARDWARE AND SOFTWARE**		
2.1	Data Centre HCI solution	Set	01
2.1.1	Hyper Converged Infrastructure Type 1	Nos	20
2.1.2	Hyper Converged Infrastructure Type 2	Nos	40
2.2	Data Centre Networking Solution		
2.2.1	Data Centre WAN Router	Nos	02
2.2.2	Data Centre WAN Switches	Nos	02
2.2.3	Core LAN Switch (Spine)	Nos	02
2.2.4	Top of Rack Switch (Leaf)	Nos	20
2.3	Data Centre Security Hardware		
2.3.1	Network Intrusion Prevention System	Nos	2
2.3.2	Host Intrusion Prevention System	Lot	1
2.3.3	External Firewall	Nos	2
2.3.4	Internal Firewall	Nos	2
2.3.5	SSL Accelerator + SLB + WAF	Nos	2
2.4	Data Centre Backup Solution	Lot	1
2.5	Data Centre IT Software		
2.5.1	Virtualization Software	Lot	01
2.5.2	Cloud Management Solution	Lot	01
2.5.3	Antivirus Management Server	Lot	01
2.5.4	Antivirus Endpoint Licenses	Nos	2000
2.5.5	Windows Server 2022 (or latest) Datacentre Edition (2 core pack) Note: The bidder should not consider these licenses to provide the required solution as per RFP, if any such license is required that has to be factored by the bidder as part of the proposed solution. Pay per Use Mode	Nos	256
2.5.6	Red Hat Enterprise Linux Server VDC subscription license (latest edition) Note: The bidder should not consider these licenses to provide the required solution as per RFP, if any such license is required that has to be factored by the bidder as part of the proposed solution. Pay per Use Mode	Nos	256

2.5.7	Database Software: MS SQL Server enterprise edition licenses (2 core pack); 2019 or latest edition	Nos	16
2.6	Data Centre EMS	Lot	01
2.7	Additional Items (if any)	Lot	As per Req.
3	**SIEM**	**Lot**	**01**
3.1	Security Information and Event Management Solution including Licensing, Installation and Configuration Cost		
3.1.1	Log Collector/Receiver Systems at NDC and DRDC		
3.1.2	Log Collector/Receiver Systems RDCs		
3.1.3	Log Management System (including Normalization, Parsing, Indexing and Categorizing Functions)		
3.1.4	SIEM Correlation System		
3.1.5	SIEM Archiving System		
3.1.6	SIEM Alerting, Reporting, Querying, Dashboard, and Incident Management System		
3.2	Vulnerability Assessment: Hardware/appliance Solution		
3.2.1	Licenses for Servers		
3.2.2	Licenses for Network Devices		
3.2.3	Licenses for Database Instances		
3.3	Cyber Threat Intelligence Feeds		
3.4	Additional Items (if any)		
4	**IDENTITY AND ACCESS MANAGEMENT SOLUTION – Pay per use model**	**Lot**	**01**
4.1	Additional Items (if any)		
5	**CAMPUS NETWORKING (Routing & Switching)**		
5.1	Campus/NOC Switch	Nos	2
5.2	OOB Switches	Nos	<= 2
5.3	Supply, Installation, Commissioning of Structured Cabling complete with accessories	Lot	As per Reqd.
6	**Network Management System (EMS)**	Lot	01
7	**MISC. IT HARDWARE, TRAINING & OFFICE EQUIPMENT**		As per requirement.
8	**AMC for all Hardware and software for at least 5 years**	lot	1

Milestone

S.no.	Milestone	% Of amount
1)	Project plan, Designing and approval as per SOW	10%
2)	On delivery of products	40%
3)	On installing and commissioning of the BOQ material	20%
4)	On Acceptance & Handover (UAT, KT, As built, SOP, device credential OEM hardware warranty certificate)	10%
5)	Validation of Complete implementation which is to be scheduled at least 1 Year post Milestone 4 completion	20%

*Sign-off to be taken after every milestone from client

40% payment will be made on delivery of items at any specified site in India as per the following process:
a) The bidder will deliver the items at designated locations as per the purchase order and obtain signature with date and stamp on delivery proof (s) of the concerned user.

b) The bidder will submit a copy of proof of delivery duly signed by the purchaser project coordinator, with his name, date of delivery, designation, and office seal, legibly recorded, should reach NIXI-CSC.

c) The bidder will submit the bills along with original excise duty gate pass or invoice & original delivery certificate to NIXI-CSC. Performance Performance bank guarantee will also be required to be submitted at the time of bill submission for payment to be made.

d) Penalty if any, will be imposed as per the tender document

Payment for Product Support (AMC)
It is understood that all post sales services which include hardware and software patches are covered in warranty and therefore AMC will start after the completion of warranty period of 1 years.

PENALTY CLAUSE

Product Delivery:
a) The bidder must ensure delivery, installation and commissioning of the components and relevant software as mentioned in the tender document.

b) Any unjustified and unacceptable delay in delivery and installation schedule as given, of this section will render the bidder liable for liquidated damage of maximum **0.1% (point one percent) of PO value per day with a maximum capping of 10%.**

c) After Placing the order, the bidder will give the BG within 10 days, or NIXI-CSC has a right to assume that the vendor is not interested in execution of this order and hence reserve the right to cancel the order forfeit the BG (equivalent to EMD) and take legal action.

d) Proof of Delivery/ Installation duly signed by the user/purchaser Project Coordinator, with his name, date of delivery, designation, and office seal, legibly recorded, should reach NIXI-CSC Head Quarters, New Delhi within 30 days with the bills, after the date on which the item(s) was delivered / installed.

Product Support SLA's:

a) If one of the redundant Product/Software/Equipment **(not impacting Data Centre operations)** systems fails, the issue must be addressed with immediate response time and the same should be resolved/replaced within **8 hours** from the reporting of the incident/issue/problem.

b) Any unjustified and unacceptable delay in meeting above timeline will render the agency liable for **penalty of Rs.1000/- per extra 10 minutes**.

c) In case primary and secondary both **(impacting Data Centre operations)** fail leading to service failure, the same should be resolved/replaced within **1 hours** from the reporting of the incident/issue/problem.

d) Any unjustified and unacceptable delay in meeting above timeline will render the agency liable for **penalty of Rs.10,000/- per extra 10 minutes**.

ANNEXURES

ANNEXURE 1

PRE-QUALIFICATION CRITERIA

Evidence submitted as per Pre-Qualification Criteria will be examined by Pre-Qualification technical evaluation committee (TEC) and if not found relevant, more time would be given to resubmit the evidence, failing to do so bidder will be rejected. “TEC shall have the right to ask for more details if not convinced”.

Sr. No.	**Pre-Qualification Criteria**	**Supporting Documents Provided**
1		
2		
3		

ANNEXURE 2

FORMAT FOR RESPONSE TO THE TENDER: PRE-QUALIFICATION BID

This section provides the outline, content, and the formats that the Bidders are required to follow in the preparation of the Pre-Qualification Bid

Pre-Qualification Bid Letter

To

CEO-MD, NIXI-CSC DATA SERVICES LTD

9th Floor, B-Wing, Statesman House Barakhamba Road,

Connaught place Delhi

New Delhi DL 110001 IN

E-Mail: pdns@NIXI.in

Sir,

Subject: "Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)": Tender No: <**Tender Reference Number**> Dated <dd/mm/yyyy> We, the undersigned Bidders, having read and examined in detail all the Tender documents do hereby propose to provide the services as specified in the Tender document number <**Tender Reference Number**> Dated <dd/mm/yyyy> along with the following:

a) Earnest Money Deposit (EMD)

b) We have paid an EMD of Rs. 1,25,00,000/- through the Bank. This EMD is liable to be forfeited in accordance with the provisions mentioned above.

Contract Performance Performance bank guarantee: We hereby declare that in case the contract is
awarded to us, we shall submit the contract performance performance bank guarantee as per compliance
to the General terms Conditions mentioned in this RFP and Contract document.

We hereby declare that in case the contract is awarded to us, we shall submit the Contract Performance Performance bank guarantee Bond.

We hereby declare that our Bid is made in good faith, without collusion or fraud and the information contained in the Bid is true and correct to the best of our knowledge and belief.

We understand that our Bid is binding on us and that you are not bound to accept a Bid you receive.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Printed Name
Designation
Seal
Date:
Business Address:

ANNEXURE 3

Declaration of Acceptance of Terms & Conditions in the RFP

To
CEO-MD, NIXI-CSC DATA SERVICES LTD

9th Floor, B-Wing, Statesman House Barakhamba Road,

Connaught place Delhi

New Delhi DL 110001 IN

E-Mail: pdns@NIXI.in

Sir,

I have carefully gone through the Terms & Conditions contained in the RFP document [No. ……..] For **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"** I declare that all the provisions of this RFP/Tender Document are acceptable to my company. I further certify that I am an authorized signatory of my company, and I am, therefore, competent to make this declaration.

Yours faithfully,

(Signature of the Bidder)

Printed Name

Designation

Seal

Date:

Business Address:

ANNEXURE 4

Declaration Regarding Clean Track Record

To
CEO-MD, NIXI-CSC DATA SERVICES LTD

9th Floor, B-Wing, Statesman House Barakhamba Road,

Connaught place Delhi

New Delhi DL 110001 IN

E-Mail: pdns@nixi.in

Sir,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No._____] For **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"** for the period of the project. I hereby declare that my company has not been debarred/blacklisted by any Government / Semi-Government organizations in India. I further certify that I am competent officer in my company to make this declaration.

Yours faithfully,

(Signature of the Bidder)

Printed Name-

Designation-

Seal-

Date: -

Business Address:

ANNEXURE 5

Format for Response to Tender: Technical Bid

Technical Bid Letter

To

CEO-MD, NIXI-CSC DATA SERVICES LTD

9th Floor, B-Wing, Statesman House Barakhamba Road,

Connaught place Delhi

New Delhi DL 110001 IN

E-Mail: pdns@nixi.in

Sir,

Subject For **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"** Reference: Tender No: <Tender Reference Number> Dated <dd/mm/yyyy>

We, the undersigned Bidders, having read and examined in detail all the Tender documents do hereby propose to provide the services as specified in the Tender document number <Tender Reference Number> Dated <dd/mm/yyyy> along with the following:

Earnest Money Deposit (EMD):

We have paid an EMD of ₹1,25,00,000/- through the portal/bank. This EMD is liable to be forfeited in accordance with the provisions of - General Conditions of the Contract.

Deviations:

We declare that all the services shall be performed strictly in accordance with the Tender documents except for the variations, assumptions, and deviations, all of which have been detailed out exhaustively in the following statements, irrespective of whatever has been stated to the contrary anywhere else in our **Tender:**

Statement of Deviations from Tender Terms and Conditions is as specified in General Terms and Conditions

Further we agree that additional conditions or assumptions, if any, found in the Tender documents other than those stated in deviation schedule shall not be given effect to.

Contract Performance Guarantee Bond:

We hereby declare that in case the contract is awarded to us, we shall submit the Contract Performance Guarantee Bond in the form prescribed in the RFP.

Bid Validity Period:

We agree to abide by this Bid for a period of 60 days after the date fixed for Bid opening or for any further period for which Bid validity has been extended and it shall remain binding upon us, and Bid may be accepted at any time before the expiration of that period.

We hereby declare that our Bid is made in good faith, without collusion or fraud and the information contained in the Bid is true and correct to the best of our knowledge and belief.

We understand that our Bid is binding on us and that you are not bound to accept a Bid you receive.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Printed Name

Designation

Seal

Date:

Business Address:

ANNEXURE 6

OEM Authorisation Letter

To
CEO-MD, NIXI-CSC DATA SERVICES LTD
9th Floor, B-Wing, Statesman House Barakhamba Road,
Connaught place Delhi
New Delhi DL 110001 IN
E-Mail: pdns@nixi.in

Sub: Product Compliance with the tender specifications
Ref: Tender No.:
This is to certify that the bidder M/s _____ (name of bidder) is representing us, M/s _____ (name of OEM) for _____ (name of product category) for the above referred tender no., for **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"**.
Ref:
WHEREAS <Name of the Original Equipment Manufacturer> who are official producers of <Name of Products intended for this Tender> and having production facilities at <Address of Mfg. Facility> do hereby authorize <Name of the bidder with complete address> (hereinafter, the "Bidder") to submit a bid of the following Products produced by us, for the Supply and Technical Support Requirements during execution period and after sales, service upto minimum 7 years from the date of completion of work.
When resold by <Name of the bidder>, these products are subject to our applicable standard end user warranty terms of 3 years and AMC for 3 years post warranty period is over
We assure you that in the event of <name of the Bidder> not being able to fulfil its obligation as our Service Provider in respect of our standard Warranty Terms we would continue to meet our Warranty Terms as prescribed in the NIXI-CSC terms.
We confirm that the products quoted are on our current product list and are not likely to be discontinued within 7 years from the day of this letter. We assure availability of spares for the products for the next Seven years.
We also confirm that any bidder who offer our products without our authorization as above, NIXI-CSC at its discretion may decide to disqualify the bidder and we will have no objection in this regard. Further, in such case we confirm that such bidder will not be authorized to bid for our products in any of the RFP call by NIXI-CSC in future.
We confirm that the technical compliance submitted by <Name of the bidder> has been duly endorsed by us with stamp and signature.

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:
(**Note: This letter of authority must be on the letterhead of the Manufacturer and duly signed by an authorized person not below capacity of General Manager/Business unit head or Equivalent)**

ANNEXURE 7

Format for Response to Tender: Commercial Bid

Commercial Bid Letter

To
CEO-MD, NIXI-CSC DATA SERVICES LTD
9th Floor, B-Wing, Statesman House Barakhamba Road,
Connaught place Delhi
New Delhi DL 110001 IN
E-Mail: pdns@nixi.in

Subject: For **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"**
Reference: Tender No:<Tender Reference Number>Dated<dd/mm/yyyy>
Dear Sir,
Having examined Request For Proposal (RFP) number ---------- ---------- ---------- dated ---------- the receipt of which is hereby acknowledged, we, the undersigned, offer "Design, Engineering, Supply, Installation, Testing and Commissioning of Air-conditioning, UPS and iPDU" in full conformity with the said RFP, for a total project cost of Rs …… (Rupees …… only). The above amount is in accordance with the Price Schedules herewith made part of this bid as per the Commercial bid template.
We undertake that we shall carry out audit activities in conformity with the bidding documents (and as amended from time to time) for a total cost as provided in the Commercial bid if the contract is awarded to us.

We declare that we have studied RFP and are making this proposal with a stipulation that you shall award us Contracts, either in part or whole, **"Procurement of IT Infrastructure of Tripura State Data Centres (TSDC)"** (meaning as realized in RFP) including all other services specified in the Contract Documents.

We have read the provisions of RFP and confirm that these are acceptable to us. All necessary clarifications, if any, have been sought for by us and duly clarified in writing, by NIXI-CSC. We understand that any other ambiguous clauses in the RFP, if any, are subject to interpretation NIXI-CSC.

We further declare that additional conditions, variations, deviations if any, found in the proposal other than those listed in Attachment pertaining to any rebates offered, shall not be given effect to.
We undertake, if our bid is accepted, to commence the work on the project immediately upon your Notification of Award to us, and to achieve Completion within the time stated in the Bidding Documents.
If our bid is accepted, we undertake to execute all contractual documents and provide all securities & guarantees as required in the bid document (and as amended from time to time).
We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act".

We agree to abide by this bid, consisting of this letter, the tender fee, EMD, Technical bid and Commercial bid, for a period of bid validity from the date fixed for submission of bids as stipulated in the RFP, and it shall remain binding upon us and may be accepted by you at any time before the expiration of that period.

Until the formal order is placed and final Contract is prepared and executed between us, this bid, together with your written acceptance of the bid and your notification of award, shall constitute a binding contract between us.

(Signature of the Bidder)
Printed Name
Designation
Seal
Date:
Business Address:
Witness:
Address:

ANNEXURE 8

Performance bank guarantee

5% of total quoted amount in tender as performance performance bank guarantee, which will be renewed after one year during AMC. Below is the format of performance bank guarantee: -

We _____ bank do hereby undertake to pay the amounts due and payable under this guarantee without any demur merely or a demand from '_____ ' (name of entity for whom performance bank guarantee is given) stating that the amount claimed is due by way of loss or damage caused to or would cause to or suffered by '(name of entity for whom performance bank guarantee is given) by reason of any breach by the said tenderer(s) of any of the terms or conditions contained in the said tender or by reason of the said tenderer's failure to keep the tender open. any such demand made on the bank shall be conclusive as regards the amount due and payable by the bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding

__ (Rs. _____ only).

We_____ bank further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the finalization of the said tender and that it shall continue to be enforceable till the said tender is finally decided and order placed on the successful tenderer and/ or till all the dues of (name of Entity for whom Performance bank guarantee is given) under/or by virtue of the said tender have been fully paid and its claims satisfied or discharged or till a duly authorized officer of (name of Entity for whom Performance bank guarantee is given) certified that the terms and conditions of the said tender have been fully and properly carried out by the said tenderer(s) and accordingly discharges the guarantee.

Unless a demand or claim under this guarantee is made on us in writing on or before the _____to include 3 months claim over and above the period mentioned in the paragraph for the validity of the performance bank guarantee in the tender we shall be discharged from all liability under this guarantee thereafter.

We _____ bank, lastly undertake not to revoke this guarantee during its currency except with the previous consent of _____ (name of Entity for whom Performance bank guarantee is given) in writing.

Dated _____day of _____2022. Corporate Seal for Bank

ANNEXURE 9

IMPLEMENTATION SCHEDUILE (AT THE TIME OF BID SUBMISSION)

Work Description	**Time of Delivery**
Site inspection	
Initiation of procurement of the identified components as part of the BOM	
Design, HLD,	
Design LLD	
Supply and Installation of BoQ Material	
DC build completion and go-live	
Acceptance testing	
KT, AS build and SOP submission	
Others (if any)	

For……..

Designation:

(Signature and seal of authorized person)

Work Description	**Time of Delivery**
Site inspection	
Initiation of procurement of the identified components as part of the BOM	
Design, HLD,	
Design LLD	
Supply and Installation of BoQ Material	
DC build completion and go-live	
Acceptance testing	
KT, AS build and SOP submission	
Others (if any)	

For……..

Designation:

(Signature and seal of authorized person)

ANNEXURE 10

All the bidders need to submit this compliance sheet , duty stamped and signed by respective company authority along with the bid .

S No.	IT RFP SECTIONS	Compliance (Yes (Y)/No (N))
1	INVITATION TO BID	
2	DUE DILIGENCE	
3	ISSUER	
4	Key Events & Dates	
5	SCHEDULE OF REQUIREMENT	
6	STATE DATA CENTRES (SDC)	
7	PURPOSE	
8	REQUIRED COMPONENTS AND SERVICES	
9	PROJECT TIME SCHEDULE	
10	INSTRUCTION TO THE BIDDERS	
11	PRE-BID CONFERENCE	
12	AMENDMENT OF RFP DOCUMENT	
13	VENUE AND DEADLINE FOR SUBMISSION OF PROPOSAL	
14	PROCEDURE FOR SUBMISSION OF BIDS	
15	MODES OF SUBMISSION	
16	COST OF BIDDING	

17	INSTRUCTIONS FOR TENDER PROCESS	
18	Terms and Conditions	
19	Permits, Taxes and Other Duties	
20	Subcontract	
21	CLARIFICATION ON TENDER DOCUMENT	
22	LANGUAGE OF BIDS	
23	DOCUMENTS COMPRISING THE BIDS	
24	BID SUBMITTALS	
25	CONFIDENTIALITY	
26	NO LEGAL RELATIONSHIP	
27	ERRORS AND OMISSIONS	
28	ACCEPTANCE OF TERMS	
29	NORMALIZATION OF BIDS	
30	AUTHORIZED SIGNATORY	
31	SERVICE LEVELS	
32	SERVICE LEVEL AGREEMENT	
33	PURPOSE OF THIS AGREEMENT	
34	DEFINITIONS	
35	DESCRIPTION OF SERVICES PROVIDED	
36	DELIVERY, INSTALLATION AND COMMISSIONING OF EQUIPMENT	
37	WARRANTY AND AMC CLAUSE	
38	SERVICE LEVEL AGREEMENTS & TARGETS	
39	AVAILABILITY MEASUREMENTS	
40	PERIODIC FACILITY AUDITS	
41	SLA CHANGE MANAGEMENT PROCEDURE	
42	PENALTIES	
43	ESCALATION PROCEDURE	
44	CONTACT MAP	
45	MAINTENANCE	
46	PRE-QUALIFICATION CRITERIA	
47	GENERAL INFORMATION ABOUT THE BIDDER	
48	EVALUATION CRITERIA	
49	EVALUATION PROCESS	
50	STAGE 1: PRE-QUALIFICATION	
51	STAGE 2: TECHNICAL EVALUATION	
52	STAGE 3: COMMERCIAL EVALUATION	
53	SHORT LISTING	
54	ENTIRE AGREEMENT	
55	CONFIDENTIALITY AND SECURITY	
56	INDEMNITY	
57	LIMITATION OF LIABILITY	
58	FORCE MAJEURE	
59	EVENTS OF DEFAULT BY BIDDER	
60	TERMINATION OF THE CONTRACT	

61	EXIT MANAGEMENT	
62	DISPUTE RESOLUTION	
63	CORRUPT AND FRAUDULENT PRACTICES	
64	PREVIOUS TRANSGRESSION	
65	FACILITATION OF INVESTIGATION	
66	LAW AND PLACE OF JURISDICTION	
67	OTHER LEGAL ACTIONS	
68	STATEMENT OF PURPOSE	
69	SCOPE OF WORK	
70	TSDC HIGH LEVEL ARCHITECTURE	
71	TECHNICAL AND FUNCTIONAL REQUIREMENTS	
72	Hyper Converged Infrastructure Type 1	
73	Hyperconverged Infrastructure Type 2	
74	Virtualisation	
75	Backup Solution	
76	Licences (OS & DB)	
77	DC-EMS	
78	Datacentre Network Solution: (Spine-Leaf)	
79	DCN: Data Centre Networking	
80	Firewalls	
81	Intrusion Protection System	
82	Load Balancer and Controller + WAF	
83	WAN Routers	
84	Campus-NOC Switch	
85	OOB Switch	
86	Structured cabling for entire Data Centre:	
87	Ticketing / Helpdesk Solution	
88	SIEM	
89	Schedule Of Requirement	
90	Milestone	
91	PENALTY CLAUSE	
92	ANNEXURES	
93	ANNEXURE 1	
94	ANNEXURE 2	
95	ANNEXURE 3	
96	ANNEXURE 4	
97	ANNEXURE 5	
98	ANNEXURE 6	
99	ANNEXURE 7	
100	ANNEXURE 8	
101	ANNEXURE 9	