NATIONAL INFORMATICS CENTRE

Request for Proposal

for

Selection of Bidder for supplying and maintaining ICT components for log management analytics

Tender Reference Number: NIC/TPS/2024/XX

Address: National Informatics Centre, A-Block, CGO Complex, Lodhi Road, New Delhi-110003

Table of Contents

1. Summary Sheet 6
2. Definitions & Abbreviations 7
   - 2.1. Definitions 7
   - 2.2. Abbreviations 10
3. Introduction 12
4. Purpose of this RFP 12
5. Scope of Work 12
   - 5.1 Detailed Scope of Work 12
   - 5.2 MIS Solution showcasing all information 13
   - 5.3 User Acceptance Testing 14
   - 5.4 Product Support (Hardware, Platform, Components and Software) 14
   - 5.5 Project Delivery Timelines 15
   - 5.6 Terms and Conditions for Proposed Infrastructure 16
   - 5.7 Training and support 17
   - 5.8 Documentation 17
   - 5.9 Roles and Responsibilities of the Bidder 17
   - 5.10 Roles and Responsibilities of the Purchaser 18
6. Service Level Agreement and Penalties 19
   - 6.1 Penalties applicable for delivery and Installation phase 19
   - 6.2 Product support SLAs 19
   - 6.3 Operational SLAs 19
7. Invitation of Bids 21
8. Bid Submission 21
   - 8.1 Overview 21
   - 8.2 Language of Bid 21
   - 8.3 Earnest Money Deposit 21
   - 8.4 Online Bid Submission 22
   - 8.5 Instructions for technical bid submission 23
   - 8.6 Instructions for financial bid submission 24
   - 8.7 General instructions for Bid submission 24
   - 8.8 Assistance to Bidders 25
   - 8.9 Address of correspondence of the Bidder 25
   - 8.10 Period of Validity of Contract/Agreement 25

8.11 Bid Security Declaration Form 26
8.12 Cost of Bid 26
8.13 Influencing the Purchaser 26
8.14 Purchaser Clarification 26
8.15 Bidder's Clarification on Tender Document 26
8.16 Amendment of Tender Document 27
8.17 Price Stability 27
8.18 Revelation of Prices 27
8.19 Security Deposit 27
9. Bid Opening 28
10. Evaluation of Bid 28
10.1 Stage 1 – Pre-qualification 28
10.2 Stage 2 – Technical Evaluation 32
10.3 Stage 3 – Evaluation of Financial Bids 33
10.4 Stage 4 – Final Bid Evaluation (Selection of Final Bidder) 33
10.5 Reasonability of Prices Received 34
10.6 Consideration of Abnormally Low Bids 34
10.7 Price Negotiation 34
10.8 Purchaser Preference Policies of the Government 34
11. Contract 35
11.1 Contract Process 35
11.2 Award of Contract 35
11.3 Scope of Contract 35
11.4 Placing of Work Order (WO) 35
11.5 Performance Bank Guarantee 36
11.6 Purchase Preference Policies of the Government 36
12. Payment Terms 38
12.1 Payment Terms 38
12.2 Payment Schedule 39
12.3 Payment against time-barred claims 40
12.4 Completion Certificate and Final payment 40
13. Other Terms & Conditions for Bidder/Bidder 43
13.1 General Conditions 43
13.2 Warranty 44

13.3 Confidentiality 44
13.4 Integrity Pact 46
13.5 Obligation to Indemnify Purchaser 46
13.6 Liquidated Damages 47
13.7 Limitation of Liability 48
13.8 Labour Laws 48
13.9 Conflict of Interest 49
13.10 Severance 49
13.11 Force Majeure 49
13.12 Events of Default by Bidder 49
13.13 Dispute Resolution /Arbitration 50
13.14 Applicable Laws 51
13.15 Adherence to safety procedures, rules, regulations & restriction 51
13.16 Micro, Small & Medium Enterprises Development Act, 2006 51
13.17 Statutory Requirements 52
13.18 Information Security 52
13.19 Continuance of Contract 53
13.20 Termination of Contract 53
13.21 Exit Management 55
13.22 Applicability of the IT Act and Rules 56
13.23 Intellectual Property Rights 56
13.24 Transfer of Project documentation and data 57
13.25 Official secrets 57
13.26 Publicity 58
13.27 Restriction under rule 144 (xi) of the GFR 2017 58
13.28 Compliance to Digital Personal Data Protection Act, 2023 58
14. Bill of Quantity (BOQ) 58
14.1 ICT Components 58
15. Technical Specifications 60
15.1 Server Type 1 60
15.2 Server Type 2 62
15.3 Server Type 3 64
15.4 Server Type 4 67
15.5 Server Type 5 70
15.6 Server Type 6 72

15.7 Server Type 7 75
15.8 Server type 8 77
15.9 Server type 9 80
15.10 Access Switches for GPU 82
15.11 Access switches for Servers 84
15.12 Core Switches 87
15.13 WAN Router 89
15.14 OOB Switch 90
15.15 OOB Aggregation Switch 92
15.16 Access Switches for Remote Locations 94
15.17 Object Storage (30PB Usable) 96
15.18 Firewall 99
15.19 Load Balancer 102
15.20 Web Application firewall 103
15.21 Network monitoring system 105
15.22 Automation 107
16. Annexures 110
Annex 1 – Declaration-Cum-Undertaking Regarding Blacklisting/ Non-Blacklisting 110
Annex 2 – Instructions to fill the Bill of Material 111
Annex 3 – Abridged Financial Bid 112
Annex 4- Detailed Financial Bid 113
Annex 5 – Bill of Materials (BoM) 114
Annex 6 – Proforma for Bank Guarantee for Security Deposit/ Contract Performance (PBG) .. 116
Annex 7 – No Deviation Certificate 118
Annex 8 – Manufacturing Authorization Form (MAF) 119
Annex 9 – Covering Letter 120
Annex 10 - Format for Bid Security Declaration Form 122
Annex 11 - Format for Integrity Pact 123
Annex 12 – Non-Disclosure Agreement 127
Annex 13 – Make In India Certificate 131

1. Summary Sheet

Tender number	
Name of the Purchaser	National Informatics Centre (NIC)
Tender type	Open tender
Tender category	Procurement
Contract Period	Two years from the date of Contract, extendable by a total period of up to two more years
Earnest Money Deposit	4 cr.
Security Deposit	Bank Guarantee as per **Annex 6,**
Period of validity of the Bid	180 days from the last date for Bid submission
Submission of pre-Bid queries	Only queries submitted on the Central Public Procurement Portal (https://eprocure.gov.in/eprocure) will be responded to in the pre-Bid meeting. However, the formal response to any query would be that published on the said portal.
Number of packets	Two-packet online Bid, as under: (a) **Packet-1:** Technical Bid (b) **Packet-2:** Financial Bid
Resubmission of Bid	Bid may be resubmitted before the last date and time for submission of the Bid.

2. Definitions & Abbreviations

2.1. Definitions

2.1.1 In this RFP, the expressions in column (2) in Table 1 shall have the meanings respectively assigned to them in the corresponding entry in column (3).

Table 1- DEFINITIONS

S. No.	Expression	Definitions
(1)	(2)	(3)
1.	Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures
2.	Authorised Representative	For the doing of any act or thing, for the purposes of the RFP or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, Bidder or Purchaser, as the case may be, may specify as its Authorised Representative in this behalf
3.	Authorised Signatory	For the affixation of signature or Electronic Signature Certificate on any document or electronic record, for the purposes of the RFP or identification of the Selected Bidder or execution of the Contract, or for any matter incidental thereto or connected therewith, such individual as the Bidder, Selected Bidder, Bidder or Purchaser, as the case may be, may specify as its Authorised Signatory in this behalf
4.	Bid	The bidding process and the proposal submitted by the selected Bidder for this RFP, including any clarifications and amendments submitted by the Bidder in response to any request made by the Purchaser in this connection
5.	Bidder	The firm participating in the Bid process pursuant to this RFP
6.	Component	An item listed under BoQ
7.	Contract Period	The period of subsistence of the Contract
8.	Contract Value	The cumulative value of Work Orders issued to the Bidder during the Contract Period
9.	Contract/Agreement	The contract or agreement entered into between the Selected Bidder and the Purchaser
10.	Financial Year	The period from the first of April till the thirty-first of March of the succeeding calendar year
11.	Go-Live	Refers to the date of installation and commencement of UAT for the supplied equipment's
12.	Implementation phase	The phase of the project before Go-Live
13.	Operational phase	The phase of the project after Go-Live

14.	Party	Includes the Bidder and the Purchaser, and the expression "Parties" shall be construed as a reference to the two taken together
15.	Purchaser	NIC, including any— (a) of its successors; (b) representative authorised by it; and assignee permitted by it
16.	Quarter	A period of three Months, reckoned from the date of Go-Live and, in respect of any period constituting less than a period of three Months in the period preceding the expiry of the Contract Period, such lesser period; and the expression "Quarterly" shall be construed accordingly
17.	Reputational Risk	Any event which may likely have the potential of negative publicity or negative public perception about the Purchaser
18.	RFP/Tender	This RFP document, including all documents, amendments and clarifications issued by the Purchaser to invite Bids from Bidders for " **Selection of Bidder for supplying and maintaining ICT components for log management analytics** "
19.	Disaster Recovery Site	NDC Hyderabad
20.	Selected Bidder	The Bidder identified by the Purchaser for entering into the Contract
21.	Service(s)	Services to be provided by the Bidder for the discharge of its obligations under the RFP and the Contract, in a manner consistent with— (a) Applicable Law; and (b) extant policies and guidelines for— (i) cybersecurity, information security and data protection procedures and practices; and (ii) prevention, response and reporting of cyber incidents, issued by the Government of India, the Purchaser, the Indian Computer Emergency Response Team (CERT-In) in the performance of functions entrusted to it by law, or the National Critical Information Infrastructure Protection Centre (NCIIPC) in respect of such Critical Information Infrastructure as may be declared as a protected system by law, including such amendments or modifications thereto as may be made from time to time
22.	**Service Provider**	**"Service Provider"** means the successful Bidder to whom this Contract has been awarded.
23.	Site Acceptance	The date of sign-off on Go-Live
24.	Total Quarterly payment	Total Payment to be made to the Bidder against invoices submitted quarterly

25.	UAT	The process of testing of the complete setup made by the Bidder for final acceptance of the Purchaser as per terms and conditions laid out in this RFP.
26.	Work Order	An order placed by the Purchaser on the Bidder for "**Selection of Bidder for supplying and maintaining ICT components for log management analytics**" NIC under the Contract **Subsequent work orders from 2nd year onwards** AMC for the supplied ICT components.

2.2. Abbreviations

Table 2- ABBREVIATIONS

S. No.	Abbreviation	Full Form/Definitions
1.	AI/ML	Artificial Intelligence/Machine Learning
2.	AMC	Annual Maintenance Cost
3.	BOM	Bill of Material
4.	BOQ	Bill of Quantity
5.	BOT	Build-Operate-Transfer
6.	CoC	Chain of Custody
7.	DAST	Dynamic Application Security Testing
8.	DB	Data Base
9.	DCO	Device Configuration Overlay
10.	DLP	Data Leakage Protection
11.	DRM	Digital Rights Management
12.	EMD	Ernest Money Deposit
13.	EPS	Event Per Second
14.	FEC	Financial Evaluation Committee
15.	GFR	General Financial Rules
16.	GOI	Government of India
17.	GTV	Gross Total Value
18.	HLD/LLD	High Level Design/Low Level Design
19.	HPA	Host Protected Area
20.	ICADR	International Centre for Alternative Dispute Resolution
21.	ICT	Information and Communication Technology
22.	IPR	Intellectual Property Rights
23.	ISO	International Organisation for Standardization
24.	ITIL	Information Technology Infrastructure Library
25.	KT	Knowledge Transfer
26.	MAF	Manufacturer's Authorization Form
27.	MeiTY	Ministry of Electronics & Information Technology
28.	MIS	Managed Information System
29.	MSE	Micro and Small Enterprises
30.	MSME	Micro, Small & Medium Enterprises
31.	NAC	Network Access Control
32.	NDA	Non-Disclosure Agreement
33.	NIC	National Informatics Centre
34.	NIC-CSG	NIC Cybersecurity Group
35.	NOC	Network Operations Centre
36.	NVME	Non-Volatile Memory Express
37.	OEM	Original Equipment Manufacturer
38.	OS	Operating System
39.	PB	Peta Byte
40.	PBG	Performance Bank Guarantee

41.	PQ	Pre-Qualification
42.	QCBS	Quality and Cost Based Selection
43.	RBI	Reserve Bank of India
44.	RCA	Root Cause Analysis
45.	RFP	Request for Proposal
46.	SAS	Serial-Attached SCSI
47.	SAST	Static Application Security Testing
48.	SCA	Software Composition Analysis
49.	SIEM	Security Information and Event Management
50.	SLA	Service Level Agreement
51.	SOAR	Security Orchestration, Automation and Response
52.	SOP	Standard Operating Procedures
53.	SSD	Solid State Drive
54.	SSO	Single Sign-On
55.	TDS	Tax Deduction at Source
56.	TEC	Technical Evaluation Committee
57.	TIP	Threat Intelligence Platform
58.	TQ	Technical Qualification
59.	UAT	User Acceptance Testing
60.	WO	Work Order
61.	ZTNA	Zero Trust Network Access

3. Introduction

3.1 NIC is a vital Information Technology entity of the Government of India, functioning as its premier IT arm. Operating under the supervision of the Ministry of Electronics and Information Technology. NIC plays a pivotal role in the advancement and execution of e-governance projects and initiatives within India. It offers a comprehensive range of services, including software development, networking infrastructure, data centre and cloud services, as well as website development and hosting. NIC is entrusted with the responsibility of developing and maintaining various government websites and portals, facilitating online services and transactions for citizens and businesses.

3.2 National informatics Centre has a vast network of offices and centres spread across the country, providing technical support and expertise to government entities. It collaborates with various stakeholders, including government agencies, public sector organisations, and industry partners, to promote innovation, efficiency, and transparency in the delivery of government services.

3.3 Overall, the National Informatics Centre plays a crucial role in the digital transformation of the Indian government, enabling efficient and accessible online services, data management, and IT solutions for the benefit of citizens and the administration. Security and sustained availability of such services being provided by NIC are critical for the performance of public duties and acts in which the public are interested. Establishment of Log Management is envisaged in this context.

3.4 The Log management solution shall be established at National Informatics Centre (NIC) in Delhi (Primary), and DR site (i.e., National Data Centre, Hyderabad) at the physical locations specified by NIC.

4. Purpose of this RFP

4.1. The Purchaser intends to select a Bidder to supply, install, integrate, configure, troubleshoot, and maintain the asked hardware and software for log management analytics for National Informatics Centre (NIC) (herein referred to as the 'Purchaser'). In this RFP, the term 'Bidder' refers to an entity submitting a proposal to the Purchaser as a response to this RFP. The term 'Bidder' is used for the agency who would be contracted to supply, install, integrate, configure, customize, troubleshoot, and maintain the hardware for Log Management analytics for National Informatics Centre (NIC), as per the terms and conditions specified in this tender.

5. Scope of Work

5.1 Detailed Scope of Work

5.1.1 Supply, install, integrate, all Components supplied through this RFP and maintain various ICT infrastructure components (such as servers, storage, object Storage, network equipment etc.)

5.1.1.1 The Bidder is responsible for providing, installing, configuring, troubleshooting, operating, and managing the supplied components for the contract period. All the solutions supplied must possess enterprise licenses without any limitations. These hardware and software delivered by

the Bidder shall exhibit high scalability and be deployed exclusively on-premises, unless stated otherwise. The Bidder must include Annual Maintenance Contracts (AMC), warranty coverage, and provision for consumables throughout the contract period.

5.1.1.2 The Bidder shall be responsible for ensuring that the agreement with Original Equipment Manufacturers (OEMs) of the provided products has the provisions for sharing vulnerability details of the supplied products well in advance, prior to their public disclosure. The Bidder shall also provide the Purchaser with the necessary information for mitigating any unpatched vulnerability identified in their products.

5.1.1.3 The Bidder shall ensure that the Proof of Delivery/Installation duly signed by the nodal officer(s) assigned by the Purchaser at required locations, with his name, date of delivery, designation, and office seal, legibly recorded, shall reach NIC Head Quarters, New Delhi within 30 days with the bills, after the date on which the item(s) was delivered / installed.

5.1.1.4 All required software and licences shall be offered as a part of the solution required to run the asked BOQ.

5.1.2 Operate, maintain the complete ICT infrastructure supplied through this RFP as per SLA (Operational phase).

5.1.2.1 The Bidder is responsible for upgrading or patching any of the deployed hardware or software and tools as necessary to meet the SLAs, without any additional cost to the Purchaser.

5.1.2.2 All ICT Infrastructure supplied as part of the contract should include required additional items like sub-components, sub-assemblies, cables, connectors, sockets, patch cords etc.

5.1.3 Support for 24x7x365 Operations

5.1.3.1 The Bidder shall ensure uptime for all components and solutions, including, but not limited to server, storage, network, system administration etc stated in the RFP document. The Bidder shall ensure that the deployed product set is supported 24x7x365.

5.1.3.2 The Bidder bears the responsibility of allocating and supplying adequate number of resources/manpower if required to fulfil the scope of work and ensure compliance to Service Level Agreements (SLAs) at no additional cost to the purchaser.

5.2 MIS Solution showcasing all information

5.2.1 The Bidder shall supply Managed Information System (MIS) reports in a format and mode that is mutually agreed upon with the Purchaser, with a periodicity that is also mutually agreed upon (such as yearly, quarterly, monthly, weekly, or daily basis). The MIS reports shall encompass various reports, including but not limited to the following—

(a) Uptime and availability of systems
(b) Incident reports encompassing disruptions, downtime, security violations etc.
(c) Any other report (related to scope) as deemed necessary by Purchaser.

5.3 User Acceptance Testing

5.3.1 The Bidder shall prepare UAT document comprising of test cases for functional and performance testing and submit the same to the Purchaser for Signoff. The Bidder shall ensure that all the test scenarios are identified and provide comprehensive coverage of all aspects. If any additional test cases are required by the Purchaser, the same shall be included by the Bidder and the revised UAT document shall be resubmitted to the Purchaser for the signoff. The signed off UAT document shall be used for the tests and the results shall be provided to the Purchaser for acceptance.

5.3.2 The UAT process shall incorporate the below indicative list of stages given below:

(a) Submission of documentations including design, architecture, configuration, troubleshooting, Standard Operating Procedure, etc.
(b) Test Planning and preparation of test scenarios and test cases
(c) Testing
(d) Reporting
(e) Reviewing
(f) Sign-off

5.3.3 The User Acceptance Testing (UAT) shall be conducted by the Bidder, after the installation, commissioning and integration has been completed in accordance with the requirements specified in the RFP, in the presence of the Purchaser and Purchaser designated agency. The Bidder shall take remedial action to rectify any deficiencies/ shortcomings observed during UAT or as indicated by the Purchaser. Bidder shall submit a duly signed UAT report for sign off by the Purchaser.

5.3.4 The Bidder shall inter-alia integrate NMS with servers, storage, network devices etc.

5.3.5 The Bidder in consultation with the Purchaser/UAT committee shall finalise the scope and use cases to be utilised/demonstrated during UAT before Go-Live. (Refer timelines)

5.3.6 The Service provider shall prepare a UAT document to showcase use cases, dashboard and demonstrate the same during UAT. The UAT shall encompass exhaustive use cases and submit the UAT document to the Purchaser for additional use cases and approval.

5.4 Product Support (Hardware, Platform, Components and Software)

5.4.1 The Bidder must ensure the product(s) supplied as part of the contract are supported from the respective OEMs for the period of the contract, and any extensions thereof, as provided for in the contract, starting from the date of completion of installation and commissioning of the product(s) delivered.

5.4.2 The Bidder is required to submit a MAF from the respective OEMs for all the hardware and software asked in the RFP as per **Annex 8**, as part of its technical Bid submission on a date prior to bid submission.

5.4.3 The licenses supplied, if any, as part of the solution deployed, shall also include timely supply and deployment of all their upgrades & updates for the entire Contract Period, and any extension thereof.

5.4.4 The Bidder must ensure that product(s) supplied as a part of the solution is/are always of the latest version and any replacement/upgrade of the product that shall ensure better delivery of Service to the Purchaser shall be made available to the Purchaser at no additional cost.

5.4.5 During the Contract Period, if the component/subcomponent goes end of life/ support during the validity of contract, then the Bidder shall upgrade the component/ sub-component with an alternative that is acceptable to the Purchaser at no additional cost to the Purchaser and without causing any performance degradation.

5.4.6 The Purchaser shall not bear any responsibility for disputes related to Intellectual Property Rights (IPR) involved in supply/use of the product(s) supplied, and which is not owned by the Purchaser. The responsibility for resolving such disputes lies solely with the respective Bidder/OEMs. IPR for any customizations performed by the Purchaser's team or by the Bidder/OEM at the insistence of the Purchaser in order to meet the requirements of the project shall be owned by the Purchaser.

5.5 Project Delivery Timelines

Table 3- PROJECT DELIVERY TIMELINES

S. No.	Product / Service Delivery	Timeline
1.	Issuance of work order (WO)	**T**
2.	Hardware and software delivery	**T+12 weeks = T1 or earlier**
3.	Implementation phase: Installation and commissioning (of complete hardware and software components (which includes , inspection, rack stack, power on, installation and configuration of bios and firmware, integration with other components, network configuration, hardening) & System Integration of all supplied platforms for supplied ICT infrastructure.	T1 + 2 weeks = T2
4.	UAT	T2 + 2 weeks = T3
5.	Go-Live	T3 +1 week = T4

5.5.1 Acceptance criteria for hardware/software supplied:
The hardware/software shall be deployed as specified deployment locations in this RFP, along with the documents including, but not limited to, the Delivery Challan/E-Way Bill, OEM test certificate(s) for the specific items delivered, sign-off by OEM for commissioning etc. The Designated nodal officer of the Purchaser at the location of deployment shall carry out basic inspection jointly with the Bidder and accept the items delivered and counter sign the accompanying OEM test certificates.
5.5.2 The Bidder shall designate a Project manager for the deployment. The Project Manager of the Bidder shall share a weekly progress report as per project timelines with the Purchaser.
5.5.3 The tech/implementation sign off criteria for each hardware and software may include demonstration of all relevant specifications as per the defined product technical specifications. This may be

verified by JRI (Joint receipt inspection) or UAT committee constituted by Purchaser for release of payment on delivery.

5.6 Terms and Conditions for Proposed Infrastructure

5.6.1 The scope entails the establishment of crucial components including hardware and software installations, as well as the commissioning of the supplied items. This may necessitate additional items such as sub-components, assemblies, sub-assemblies, cables, connectors, sockets, and patch cords, all of which shall be provided by the Bidder at no extra cost.

5.6.2 For technical evaluation purposes, the unpriced bill of materials (BOM) containing hardware and software components shall be included as part of the technical Bid submission. The unpriced BOM shall not deviate from the one submitted in the financial Bid, or it may lead to rejection of the Bid. Bidder to ensure that unpriced BOM submitted as part of the technical bid does not include any pricing or financial details.

5.6.3 In case any component provided by the Bidder doesn't meet the performance parameters specified by the Bidder in the proposal, then the additional/replaced component shall be immediately provided and installed at the Bidder's expense.

5.6.4 The Bidder needs to consider the high-level features and detailed functional specifications as stated in the **(Section 15: Technical Specifications)**. The specifications given are minimum. Bidders can quote equivalent or higher technical specifications to meet the requirements. The RFP and annexures together constitute the overall requirements of the solution.

5.6.5 The Bidder shall quote the products strictly as per the tendered specifications/requirements. All relevant technical details, including those relating to the make, model, specifications and salient features of the solutions and tools offered, shall be furnished with the Bid. Clause-wise compliance with the specifications/requirements, along with documentary proof and references in support of the same, shall be furnished by the Bidder.

5.6.6 Any failed disk shall be retained by the Purchaser.

5.6.7 Interoperability/compatibility of different passive components shall be responsibility of the Bidder.

5.6.8 The Bidder is required to provision for tools/ software/ hardware/ appliance that have the specified technical specifications to ensure quality.

5.6.9 Bidder shall provide necessary redundant Fiber Channel/converged switches and modules/cables (if required) for the storage solution to meet the storage port controller connectivity and performance.

5.6.10 The US Dollar foreign exchange component as specified in **Annex 5** quoted by the Bidder shall be as per RBI website (closing rate) for the foreign currency indicated (as import component) on last date of final Bid submission shall be taken as reference for Financial Bid Evaluation.

5.6.11 The costs provided shall include rates for installation, commissioning, testing, and any other related activities.

5.6.12 Unit Price shall be exclusive of the price for packaging, forwarding, freight, insurance charges, or any other logistics cost for supply at locations specified for delivery in/under this RFP.

5.6.13 Under every major heading of items, the Bidder is expected to quote the prices of all the sub items separately (components, license etc.). Bidder can use as many rows as deemed fit to fill in the details.

5.6.14 The entire solution is for on premise.

5.7 Training and support

5.7.1 As part of deliverables, the Bidder shall provide comprehensive training to the team of at least 20 officials as designated by the Purchaser on the supplied OEM components at Purchaser location. The content of such training would need to be documented and made available to all the participants and other officers of NIC.

5.8 Documentation

5.8.1 The Bidder shall be responsible for creation and maintenance of all the documentation and shared with the Purchaser as per mutually agreed format and periodicity.

5.8.2 The documentation must be consistently updated throughout the contract period, following appropriate change management procedures and version control. It is recommended to adhere to international standards and best practices, such as ISO 27001, National Institute of Standards and Technology (NIST) 800-53 when creating the documentation. The documentation shall include but not be limited to the following:

(a) Design (HLD, LLD) and Architecture
(b) Installation and Configuration
(c) Operational manuals
(d) System administration
(e) Security Hardening manual
(f) Testing manual
(g) Troubleshooting Manual
(h) Standard Operating Procedure
(i) ISO compliance documents

5.8.3 The Bidder shall be responsible for maintaining and updating all the policy documents, related to the supplied components.

5.8.4 The Bidder shall make changes to the documents as and when there is a change in the ICT infrastructure components, configuration changes or policies or as and when required by the Purchaser.

5.9 Roles and Responsibilities of the Bidder

5.9.1 The key responsibilities of the Bidder shall include, but not be limited to, the following:

5.9.2 The Bidder bears the responsibility for coordinating with OEMs of all supplied components and integration thereof and continued support during the period of contract.

5.9.3 The Bidder is required to share all internal review documents and reports used to monitor and execute the project with the Purchaser upon request and as deemed necessary.

5.9.4 The Bidder is responsible for providing all necessary logistical support if any resources are deployed at the locations of the Purchaser throughout the period of the contract.

5.10 Roles and Responsibilities of the Purchaser

5.10.1 The key responsibilities of the Purchaser shall include providing the necessary data centre hosting space and racks required for the systems.

6. Service Level Agreement and Penalties

This tender document majorly covers deliverables such as procurement of hardware and software and AMC for procured items .

a) The Work Orders for each deliverable post Go-Live may be placed separately. Additionally, the penalties will be capped at 10% of the respective work orders.
b) Prior to Go-Live a single work order may be placed.
c) In the event of any penalty incurred during the operational phase in the first year, such penalty shall be calculated based on the AMC value for the second year proposed by the bidder.

6.1 Penalties applicable for delivery and Installation phase

6.1.1 The Bidder must ensure delivery, installation and commissioning of the components and relevant software and System Integration of all Components within the required schedule as mentioned in project timelines in section 5.5 of this RFP.

6.1.2 Any delay in Go-Live as per project timelines (section 5.5) will render the Bidder liable for penalty of 0.5 % (point five percent) of the value of undelivered items per day with a maximum capping of 10% of the work order issued prior to Go-Live.

6.1.3 After the penalty reaches the capping of 10% of work order value issued prior to Go-Live as mentioned in point 6.1.2 above, the Purchaser reserves the right to cancel the work order and forfeit the security deposit and invoke bid securing declaration.

6.1.4 After Placing any work order, Bidder will give the PBG (5% percent of work order) within 20 days of the placement of work order, or Purchaser has a right to assume that Bidder is not interested in execution of the order and hence reserves the right to cancel the order and forfeit the security deposit and invoke bid securing declaration.

6.2 Product support SLAs

6.2.1 The present solution has redundant system architecture. If one of the redundant Product/Software/Equipment systems fails, the issue must be addressed with immediate response time and the same should be resolved/replaced within 24 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 maximum 0.5% (point five percent) of Work Order value per day. The penalty will be capped at 10% of the respective work order.

6.2.2 In case primary and secondary both hardware fails, the same should be resolved/replaced within 4 hours from the reporting of the second issue/problem. Any unjustified and unacceptable delay in meeting above timeline will render the Bidder liable for penalty of maximum 0.5% (point five percent) of Work Order value per day. The penalty will be capped at 10% of the respective work order.

6.3 Operational SLAs

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

the performance levels and maintain a Service uptime of 99.99% daily. The services provided by the Bidder shall be reviewed by Purchaser that shall:

6.3.1.1 Regularly check performance of the Bidder against required 99.99% SLA using NMS or similar monitoring tools.

6.3.1.2 The Bidder shall share uptime SLA reports with Purchaser using NMS or similar tools on a weekly, fortnightly and monthly basis clearly depicting daily uptime SLA compliance.

6.3.1.3 The Purchaser may choose to deploy their team/resources to review uptime and SLA.

6.3.1.4 The Purchaser may choose to inform the Bidder via email or phone for any issue or failure.

6.3.1.5 The Bidder shall discuss escalated problems, new issues and matters still outstanding for resolution. Review of statistics related to rectification of outstanding faults and agreed changes. Obtain suggestions for changes to improve the Service levels.

6.3.1.6 If the Bidder fails to maintain the uptime of 99.99% for complete Service every month a penalty of Rs.10,000 for every 5 min reduction in uptime will be applicable with a capping of 10% of payment due for AMC Work Order for that year.

6.3.1.7 SLA will be calculated on a daily basis and penalty shall be levied on quarterly basis as per the below table:

Daily uptime (in minutes)*	**Penalty (calculated on quarterly AMC order)**
>= 99.99 %	no penalty
99.99 % - 99.00 %	3%
98.99 % - 98.00 %	5%
< 98 %	7%

*In case of any single instance of 15 mins or more downtime of any component that impacts service, the Bidder shall be levied with a penalty of 5 percent on Quarterly AMC order. More than 6 instances of downtime in a quarter will levy a penalty 10% of quarterly AMC order and may invoke bid securing declaration.

6.3.1.8 Root cause analysis shall be performed by the Bidder to identify all operational issues must be shared with the Purchaser within 72 hours of the occurrence. Time extension may be granted by the Purchaser depending on the severity of the operational issue, on the request of the Bidder. For any exceptions or SLA breach beyond the control of the Bidder, the Service Provider may submit the RCA along with a justification, which may be considered by Purchaser. In case the RCA establishes that the breach on SLA was on account of Service issues as part of Bidder's scope defined in this RFP, the Bidder shall be liable for the applicable penalty.

6.3.1.9 Root Cause Analysis (RCA) shall be prepared for all incidents causing Service unavailability or disruption.

6.3.1.10 For certain incidents, RCA may be carried out by the Purchaser (or a Purchaser appointed agency), at its discretion. In case an RCA carried out by the Purchaser or by the Purchaser's authorised representative(s) reveal a finding that is at variance with the measurement done by the Service Provider as per the report given or RCA carried out by the Service Provider—

6.3.1.10.1 Such non-adherence shall be remediated by the Service Provider within 72 hours and the corresponding reports shall be rectified by the Service Provider and submitted to the Purchaser; and

6.3.1.10.2 if the finding is in variance with the measurement done, report given or RCA carried out by the Service Provider on more than two occasions, the Service Provider shall bear the cost of the RCA carried by the Purchaser, as the case may be, for every such occasion beyond the second such occasion.

7. Invitation of Bids

7.1 The invitation of Bids is for **Selection of Bidder for supplying and maintaining ICT components and for log management analytics and security Service,** for a period of two years from the date of signing of the Contract, and extendable by up to two years, as per the scope of work defined in Section 5 of this RFP.

7.2 Bidders are advised to study the RFP carefully. Submission of bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

7.3 Sealed bids prepared in accordance with the procedures enumerated in **Section 8** Bid Submission of this tender document shall be submitted not later than the date and time laid down at GeM Portal.

7.4 The tender document is not transferable.

7.5 For procedure of submission of bids refer **Section 8** of this RFP.

8. Bid Submission

8.1 Overview

8.1.1 Bidder shall adhere to the timelines as specified on GeM portal. No Bids shall be accepted post the deadline as specified as per GeM portal.

8.1.2 Bids only submitted online shall be considered for the tendering process and further evaluation.

8.1.3 Incomplete Bids may be rejected and may not be considered.

8.2 Language of Bid

8.2.1 The Bid prepared by the Bidder and all correspondence and documents relating to the Bid exchanged by the Bidder and the Purchaser, shall be written in English language.

8.3 Earnest Money Deposit

8.3.1 Earnest Money Deposit (EMD) must be submitted in the form of Bank Guarantee drawn in favour of National Informatics Centre, payable at New Delhi and shall be valid for Bid validity period as specified in factsheet from last date of submission of Bids. For the successful Bidder i.e., the Bidder, the EMD shall remain valid until the PBG (against the first WO issued by the Purchaser) is furnished by the Bidder and the same is accepted by the Purchaser. In such case, the successful Bidder i.e., Bidder shall extend the validity of the EMD for a period till the PBG is submitted and the same is accepted by the Purchaser.

8.3.2 The Earnest Money Deposit (EMD) shall be refunded without any interest accrued.

8.3.3 The Bidder must select the payment option as “offline” to pay EMD as applicable and enter details of the instrument.

8.3.4 The Bidder shall seal the original Bank Guarantee in an envelope. The address of NIC, name and address of the Bidder and the Tender Reference Number shall be marked on the envelope.

8.3.5 The Bidder shall deposit the envelope at Tender Process Section, NIC HQ. on or before the Bid submission date as per the Tender Notice.

8.3.6 In case the EMD not submitted in physical form prior to the bid submission date and time, the bid may be rejected.

8.4 Online Bid Submission

8.4.1 Online Bids (complete in all respect) must be uploaded on GeM portal as per the schedule.

8.4.2 No Bids shall be accepted post the deadline as specified in this schedule. Bids submitted online, shall only be considered for the tender opening process and further evaluation. Incomplete Bids may be rejected. The Bid security/EMD shall be accepted in the form of Account Payee Demand Draft, Fixed Deposit Receipt, Banker's Cheque or Bank Guarantee from any commercial bank in favour of National Informatics Centre, New Delhi.

8.4.3 The online Bids shall be submitted as under along with the documents specified below:

Table 4- DETAILS OF BID SUBMISSION PACKETS

Packet Number	Documents to be uploaded	File Format
Packet-1 (Technical Bid)	The file shall be saved and uploaded in a PDF file as "Packet 1_<Bidder Name>".pdf (a) Scanned copy of Covering Letter in Company Letter Head as per **Annex 9: Covering Letter for Bid** duly sealed & signed (PDF) (b) Signed and Scanned copy of Bid Securing Declaration as per **Annex 10: Format for Bid Securing Declaration Form**. (c) Scanned copy of **Original Power of Attorney letter** in a Non-Judicial Stamp Paper of at-least Rs. 100/- (d) Scanned copy of duly filled signed and stamped **Section 15: Technical Specifications** . Any deviation from the tendered specifications (except where the deviation is on account of being better specifications being offered by the Bidder) may make the Bid unresponsive. (e) Scan copy of duly filled signed and stamped **Section 10.1 Bidders Profile and Pre-Qualification Criteria** and all the supporting/mandated documents and Annexures required for eligibility criteria. (f) All the supporting documents as per **Section 10.2 Technical Evaluation.** (g) Scan copy of duly filled (Without Cost for all items) signed and stamped unpriced Bill of Material as per **Annex 5: Bill of Materials (BoM)**(without cost for all items) and technical solution along with detailed	PDF

Packet Number	Documents to be uploaded	File Format
	unpriced BOM with Model number, OEM and architecture diagram. (h) Duly filled signed and stamped copy of MAF from respective OEMs as per **Annex 8: Manufacturing Authorization Form (MAF).** (i) Duly filled signed and stamped copy of No Deviation Certificate as per **Annex 7: No Deviation Certificate** *Note: The PDF file shall not contain any details regarding the financial Bid in the explicit/implicit form and may lead to rejection of the Bid.*	
Packet -2 (Financial Bid)	Financial Bids to be uploaded as: - (a) As per BOQ: GTV Financial Bid as per **Annex 3: Abridged Financial Bid** (b) Detailed financial Bid as per **Annex 4: Detailed Financial Bid** and **Annex 5: Bill of Material (BoM)** (in .pdf format). The Detailed Financial Bid scanned pdf files, then shall be saved in a RAR 'Detailed Fin<Bidder's Name>".RAR ***Note:*** i. *Soft copy of* **Annex 3, Annex 4** & **Annex 5** *in.zip format (or as per GeM Portal provisions)* ii. *All the Bid documents duly signed by the authorised signatory of the company and stamped with company seal*	.zip

8.5 Instructions for technical bid submission

8.5.1 All the Bid documents duly signed by the authorised signatory of the company and stamped with company seal. Failure to do so may lead to rejection of the bid.

8.5.2 It shall be the sole responsibility of the Bidder to check (and double-check) the page number referencing made for supporting documents in checklist indicated under Pre-Qualification compliance and Technical Compliance Sheet. No relevant information/document shall be left, whether listed above or not.

8.5.3 All pages of the bid being submitted shall be sequentially numbered by the Bidder.

8.5.4 Relevant referencing shall be done by the Bidder, clearly indicating all page numbers where supporting documents are provided.

8.5.5 The document shall have a Table of Contents indicating page no. where supporting document are placed. All pages in the bid document shall be sequentially numbered, stamped and signed by the authorised signatory.

8.6 Instructions for financial bid submission

8.6.1 The Bidder must upload the BOQ as per the format provided in the tender document. The Bidder must adhere to terms and conditions and fill in the required details as required in BOQ.

8.6.2 The Bidder must strictly follow the prescribed format as specified in the detailed financial bid.

8.6.3 The Bidder shall quote only the GTV value in Abridged Financial Bid as derived from in Detailed Financial Bid.

8.6.4 During financial opening, only the Grand Total Value quoted by the Bidder shall be considered for determining the L1 Bidder.

8.6.5 All the bid documents shall be duly signed by the authorised signatory of the company and stamped with company seal. Failure to do so may lead to rejection of the bid.

8.6.6 Negotiations may be conducted with winning Bidder for improvement in scope, reduction in price, enhancement of warranty and advancement of delivery schedules.

8.6.7 The price finalisation after negotiation shall be kept valid during the entire period of contract and the Purchaser reserves the right to procure any quantity as deemed appropriate from the Bill of Material quoted by the Bidder.

8.7 General instructions for Bid submission

8.7.1 OEMs of the proposed solutions have to submit a MAF as per attached annexure (**Refer Annex 8**). Failure to do so may lead to rejection of the bid.

8.7.2 The Bids submitted by Fax/E-mail etc. shall not be considered. No correspondence shall be entertained on this matter.

8.7.3 Conditional Bids shall not be accepted on any ground and shall be rejected straightway. (A Bid is conditional when Bidder submits its Bid with his own conditions & stipulations extraneous to the terms and conditions specified in this tender)

8.7.4 No bids shall be accepted after the expiry of the deadline.

8.7.5 In case, the day of bid submission is declared holiday by Govt. of India, the next working day shall be treated as day for submission of bids. There shall be no change in the timings.

8.7.6 All pages of the bid being submitted shall be signed by the authorised signatory, stamped, and sequentially numbered by the Bidder irrespective of the nature of content of the documents.

8.7.7 At any time prior to the last date for receipt of bids, 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 publishing an amendment/corrigendum. The amendment shall be notified on GeM portal and shall be taken into consideration by the prospective agencies while preparing their bids. It is the responsibility of the Bidder to check website for any such notice/changes and submit its bid accordingly.

8.7.8 In order to give prospective agencies reasonable time to take the amendment into account in preparing their bids, Purchaser may, at its discretion, extend the last date for the receipt of bids. No bid may be modified subsequent to the last date for receipt of bids. No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified in the tender. Withdrawal of the bid during this interval may result in execution of bid securing declaration.

8.7.9 Printed terms and conditions of the Bidders shall not be considered as forming part of their bid. The terms and conditions of this tender shall overrule the printed terms and conditions submitted by the Bidder.

8.7.10 Bidder shall not upload any additional document other than that asked in the tender. Any additional documents uploaded shall not be considered for evaluation.

8.7.11 Bids not submitted as per the specified format and nomenclature may be rejected. The terms and conditions of this tender shall overrule the standard terms and conditions of the GeM portal, if any.

8.7.12 Ambiguous/Incomplete/Illegible Bids may be rejected. Not quoted Bids shall be considered as non-responsive and may be rejected.

8.7.13 Any alteration/ overwriting/ cutting in the Bid shall be duly countersigned.

8.7.14 Submission of the bid shall be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and required specifications in the tender document with full understanding of its implications. Failure to furnish all information required in the tender document or submission of a bid not substantially responsive to the tender document in all respects shall be at the Bidder's risk and may result in the rejection of the bid.

8.7.15 Tender process shall be over after the issuance of contract letter to the Bidder.

8.7.16 For additional instructions, refer Section 8.

8.7.17 Submission of false/forged documents shall lead to execution of Bid Securing Declaration and blacklisting of Bidder for a minimum period of 3 years from participating in Purchaser's tenders.

8.8 Assistance to Bidders

8.8.1 Any queries relating to the tender document and the terms and conditions contained therein shall be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

8.8.2 Any queries relating to the process of online bid submission or queries relating to GeM portal in general may be directed to GeM portal helpdesk.

8.8.3 Financial Prices shall not be indicated in the Technical Bid, not adhering to which shall lead to disqualification of the Bid.

8.9 Address of correspondence of the Bidder

8.9.1 The Bidder shall designate the official mailing address, place, email, phone, and fax number to which all correspondence shall be sent by the Purchaser.

8.10 Period of Validity of Contract/Agreement

8.10.1 The Contract shall be signed between Purchaser and successful Bidder based on terms and conditions of the Bid within 15 working days from the date of on which the letter of acceptance from the Purchaser is received unless the Purchaser informs otherwise. The period of validity of the agreement shall be 2 years starting from the date of Signing of contract with an extension of 2 more years (if any).

8.10.2 If it is considered necessary, the Bidder shall be required to continue delivering services as required under this Project, on the same terms and conditions or additional mutually agreeable conditions, even beyond the contract period (such period may be extended up to two more years by way of one or more extensions) till an alternate arrangement is made by the Purchaser to manage the operations.

8.11 Bid Security Declaration Form

8.11.1 The Bidders shall submit "**Bid Securing Deposit Declaration Form**" as per the format specified in **Annex 10**: **Format for Bid Securing Declaration Form** through uploaded onto the GeM Portal.

8.11.2 The bids without bid security deposit declaration form in the prescribed format as specified above, may be rejected.

8.11.3 If the bid securing declaration is not received within the specified timeframe, the Purchaser holds the right to reject the Proposal from the relevant Bidder without offering any chance for further correspondence by the Bidder concerned.

8.12 Cost of Bid

8.12.1 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 the Purchaser. The Purchaser shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the tendering process.

8.13 Influencing the Purchaser

8.13.1 Any effort by a Bidder to influence the Purchaser's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's Bid and may result in execution of bid securing declaration.

8.14 Purchaser Clarification

8.14.1 When deemed necessary, as part of Technical and financial Evaluation, during the tendering process, the Purchaser/Committee/Authorized representative and Office of NIC may seek clarifications/enquiry/supporting documents on the documents already submitted or to make presentation on any aspect from any or all Bidders which the Bidder must furnish within the stipulated time. Failing to do so may lead to rejection of the bid.

8.15 Bidder's Clarification on Tender Document

8.15.1 Bidders requiring any clarification on the Tender Document may submit their queries, on GeM portal. The queries must be submitted in the below mentioned format on the GeM portal only to be considered for clarification.

Table 5- FORMAT FOR SEEKING CLARIFICATIONS

S.No.	Date	Clause	Page No.	Existing Clause	Queries / Change Requested	Organization
<S. no.>	*<Date of query submission>*	*<Specific Clause No. ex: 8.2.1.1>*	*<Page No of Clause>*	*<Clause to be written as per tender>*	*<Query>*	*<Name of Organization>*

8.15.2 The Purchaser shall not respond to any queries not adhering to the above-mentioned format. All queries on the Tender Document shall be received on or before as prescribed by the Purchaser in **Section 1: Summary Sheet** of this tender document. Purchaser's response (including the query but without identifying the source of inquiry) would be uploaded in the GeM portal. Bidders are responsible for duly checking the website for any clarifications.

8.16 Amendment of Tender Document

8.16.1 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 shall be notified on GeM portal and shall be taken into consideration by the prospective agencies while preparing their Bids.

8.16.2 In order to provide prospective Bidders reasonable time to take the amendment into account in preparing their Bids, the Purchaser may, at its discretion, extend the last date for the submission of bids.

8.17 Price Stability

8.17.1 To ensure the stability in prices provided by Bidder to the Purchaser during the tenure of 2 years (maximum 4 years in case of contract extension) starting from the date of acceptance, below mentioned conditions should not influence the Price quoted by the Bidder.

8.17.2 During the delivery of product, no product should be manufactured more than 1 year from the date of supply.

8.17.3 During the delivery of product, no product should be end of life/sale wherever, there is such a case the Bidder will be required to replace it with the next compatible product in line (having specifications either equal or better) which is not end of life/sale. Further during the tenure of the empanelment, if the product goes end of life/ sale, the Bidder should propose next version or product line that is replacing the quoted product and that should be provided to the Purchaser at not a price more than the previous cost.

8.17.4 The Bidder will ensure that the product supplied should not be end of support for 4 years from the date of supply of equipment.

8.17.5 In the case of CPU, hard-disk speed, memory speed, memory size etc., Bidder should provide the latest to the Purchaser after due approval of the Purchaser.

8.18 Revelation of Prices

8.18.1 Prices in any form or by any reason before opening the financial bid shall not be revealed, failing which the offer shall be liable to be rejected.

8.19 Security Deposit

8.19.1 The Bidder shall submit the security deposit in the form of Bank Guarantee for the equivalent amount of EMD (Format as per **Annex 6**) from a Commercial bank in favour of NIC, New Delhi with validity three years from the date of Contract.

8.19.2 Bidder shall be required to submit Security Deposit (in the form of bank guarantee) within 15 working days of issuance of letter/email by Purchaser for award of contract unless the Purchaser informs otherwise.

8.19.3 In the event wherein the Empanelment is extended by the Purchaser beyond two years, the Bidder shall ensure renewal of Security Deposit (in the form of bank guarantee) within 30 calendar days of issuance of letter of intent for extension of contract by the Purchaser.

8.19.4 Purchaser shall have the right to forfeit the security deposit if the Bidder fails to meet the terms and conditions of the tender document or fails to perform any other obligation under the contract, fails to execute the work orders issued by Purchaser.

8.19.5 Apart from this Purchaser also reserves the right to terminate the contract of the Purchaser in case of repeated default and invoke Bid security declaration.

9. Bid Opening

9.1 A technical evaluation committee (TEC) shall be formed for opening and evaluation of the technical Bids. Decision of the committee would be final and binding upon all the Bidders.

9.2 A financial evaluation committee (FEC) shall be formed for opening & evaluation of financial bid.

9.3 Purchaser shall download the Bids from GeM portal.

9.4 The Bids shall then be passed on to the duly constituted Technical Evaluation Committee (TEC).

9.5 The TEC shall open the technical Bids and shall evaluate the technical Bids as defined in the tender.

9.6 Financial Bids of only those Bidders whose Bids are found qualified in both Pre-Qualification (PQ)& Technical Qualification (TQ) criteria shall be opened for further evaluation.

9.7 Financial Bids, original and revised, if any, of only the technically qualified agencies, shall be opened on a notified date and time.

9.8 The financial Bids shall then be passed on to the duly constituted Financial Evaluation Committee (FEC) for evaluation, which shall evaluate the technically qualified Bids as per **Section 10**.

10. Evaluation of Bid

10.1 Stage 1 – Pre-qualification

10.1.1 Purchaser shall validate the "Earnest Money Deposit (EMD)".

10.1.2 If the EMD meets the requirements, Purchaser shall assess the documents pertaining to the "Pre-Qualification Criteria". It is mandatory to fulfil each of the conditions stated in the Qualification criteria. If the Bidder fails to satisfy any of the condition, Purchaser reserves the right to disqualify the Bidder.

10.1.3 A technical evaluation committee will be formed for evaluation of the bids. Decision of the committee would be final and binding upon all the Bidders.

10.1.4 It is mandatory to fulfil each of the conditions stated in the Pre-Qualification Criteria. If the Bidder fails to satisfy any of the conditions, Purchaser reserves the right to disqualify the Bidder.

10.1.5 Documentary evidence for compliance to each of the pre-qualification criteria must be enclosed along with the references as required.

10.1.6 Relevant portions, in the documents submitted in pursuance of eligibility criterion specified above, shall be highlighted and all pages of the Bid document shall be serially numbered.

10.1.7 Undertaking for subsequent submission of any of the above document shall not be entertained under any circumstances. However, Purchaser reserves the right to seek required/additional documents (in case the Bidder finds any issue, with due justification, in submitting the documents) and/or seek clarifications on the already submitted documents.

10.1.8 All documents shall be submitted electronically in PDF format unless specified.

10.1.9 Pre-Qualification Evaluation comprises of Bidder's profile and Pre-qualification criteria as mentioned in the tables below:

Table 6- BIDDER'S PROFILE

S. No.	Criteria	Documents to be Provided
1.	Name of the Company	
2.	Date of Incorporation in India	
3.	Registration No	
4.	Complete Address in India (with PIN Code)	
5.	Name and Designation of the Contact Person	
6.	Contact Person Phone/Mobile No: Email Address:	
7.	Telephone Number	
8.	Goods and Service Tax (GST) No.	
9.	PAN No.	
10.	Total Manpower in India	
11.	Whether Bidder is blacklisted/ or any Litigation Arbitration/ proceeding (Yes/ No)	

Table 7- PRE-QUALIFICATION CRITERIA

S. No.	Criteria	Mandatory Documents to be Provided
1.	Authorization of signatory for the purpose of this tender	Scanned copy of Original Power of Attorney letter in a Non-Judicial Stamp Paper of at-least Rs.100/- **AND any one of the following documents** 1. Board Resolution in Letter Head in original in case of Registered Limited Companies 2. Original Authorization in Letter Head in case of Partnership Firm 3. Original Self Certificate in Letter Head in case of Proprietorship naming/indicating the person authorized to sign the bid

S. No.	Criteria	Mandatory Documents to be Provided
		(PDF)
2.	**Legal Entity** The Bidder should be an established Information Technology company registered under the Companies Act, 1956/2013 or LLP firm/ Partnership firm under Partnership Act 1932 and in operation for at least 5 years as on 31.03.2024 and should have their registered offices in India. The company must be registered with appropriate authorities for all applicable statutory duties/taxes.	Valid documentary proof of: 1. Certificate of incorporation with certificate consequent to change of name, if applicable 2. Certificate of Commencement 3. Copy of Memorandum of Association 4. GST Registration certificate 5. PAN Details 6. Income Tax returns for the last three financial years
3.	**Not Blacklisted** The Bidder, as on the date of bid submission is not under blacklisting period /active debarred list by NIC/NICSI or any of the Central or state Government Organization / Public Sector Undertaking /Autonomous Body etc. The Bidder should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice on the date of submission of the bid.	Self-certification duly signed by authorized signatory** on company letter head. (Refer **Annex 1:** Declaration-Cum-Undertaking Regarding Blacklisting/ Non-Blacklisting)
4.	**Annual Turnover** The Bidder must have an annual turnover of at-least (INR) 500 Cr. in following financial years the F.Y 2021-2022 , 2022-23 and 2023-24 for which audited annual financial statements are available.	The annual turnover certified by the statutory auditor /chartered accountant/ company secretary; audited balance sheets & Profit & loss accounts report to be provided for last 3 years ending on 31st March of the previous financial year.
5.	**Relevant Projects** The Bidder must have work order received for Similar ICT Infrastructure setup/ O&M in a single work order from any Govt./PSU/State Govt in last **five completed financial years** (2023-24, 2022-23, 2021-22, 2020-21 and 2019-20). • One project of value 50 crores or	**Documents required in case of Completed project:** Copy of work order/Agreement + Completion certificate/ Satisfactory report **Documents required in case of Ongoing project:** Copy of work order/Agreement + satisfactory report/ contract agreement supported with relevant documentary evidence for the design parameters and the

S. No.	Criteria	Mandatory Documents to be Provided
	more • Two projects of value 25 Crores or more	go live/milestone completion certificates by the client. <u>Work order without above certificate shall not considered.</u> Alternatively, in the case of NDA, Bidder shall submit a declaration signed by the Authorized Signatory/CA/CS** of the Bidder mentioning details of such clients along with supporting documents. However, in case if any content in the supporting document is masked, NIC/NICSI reserves the right to call for original document.
6.	**Net Worth** The Bidder must have positive net worth during the last 3 financial years (i.e. 2021-22, 2022-23 & 2023-24). And the net worth of the Bidder should not have been eroded by more than 30% in last 3 financial years ending on 31st March 2024.	Audited balance sheets for the last 3 financial years i.e. 2021-22,2022-23 & 2023-24 where financial turnover is segregated. Every sheet shall be duly certified by a CA or accounting firm stating net worth, Turnover and Profit/Loss for last 3 financial years.
7.	**OEM MAF** Bidder shall provide valid OEM Authorization certificate for all the products quoted as well as certify that the proposed product is not declared end of sale. All software provided and used for the project must be of enterprises level with backlining from OEMs with highest level support	Documentary evidence such as Manufacturers Authorization Form (MAF) from all OEMs whose products are being quoted viz. Duly filled signed and stamped copy of MAF form from respective OEMs as per <u>Annex 8</u> or in any format addressing all the content of <u>Annex 8</u>
8.	**Certifications** The Bidder must have at the following certifications: a) ISO 27001:2015/2013 b) ISO 20000-1:2018 c) ISO 9001:2015	Valid Copy of the Certifications
9.	**Registered Office** The Bidder should have a project/local office	An undertaking in this regard must be provided by the Bidder on its company letter

S. No.	Criteria	Mandatory Documents to be Provided
	in the Consignee Locations New Delhi.	head (having address and contact person details of project/local office) duly signed and stamped by the authorized signatory.
10.	The Bidder must comply with IT Act 2000 (including 43A)	Undertaking/Self-certification duly signed by authorized signatory** on company letter head.
11.	Bid Securing Declaration	Bid Securing Declaration as per Annex 10
12.	The Bidder shall submit a **covering letter** indicating that all terms and conditions mentioned in the tender document have been assessed carefully and shall be adhered to throughout the course of selection.	Original Covering letter as per Annex 9 Covering Letter, duly signed by authorized signatory and on company's letter head with stamp.
13.	Bidder should provide back-to-back support from OEM for a period of 5 years from the date of award of Site Acceptance.	Undertaking from Bidder
14.	The Bidder should have at least 100 (hundred) full time Technical Support professionals on its permanent roll in India and preferably at least 25 (twenty five) full time Technical Support Professionals in Delhi/NCR who have current and relevant OEMs proposed in the solution skills, competency/Certification if supported by OEM.	Certified by the Statutory Auditor or Company Secretary/ Authorized signatory of the firm/ HR head
15.	Make In India certificate	Annex 13

10.2 Stage 2 – Technical Evaluation

10.2.1 Only those Bidders who qualify all Pre-Qualification (PQ) Criteria requirements shall be qualified for technical Bid evaluation.

10.2.2 The TEC reserves the right to reject a Product/ Service if it is of an opinion that the offered product/ Service does not match the technical requirements/ objectives specified in tender document.

10.2.3 Bidders are required to comply with the Technical Specifications as mentioned in Tender and no deviation will be accepted.

10.2.4 Bidders shall submit the technical specification compliance sheet as a part of technical Bid as specified in Section 15: Technical Specifications of the tender document.

10.2.5 Bidder shall submit unpriced Bill of Material along with technical Bid as per Annex 5.

10.2.6 Bidder shall submit reference to the relevant document/datasheet for each technical compliance

wherever required.

10.2.7 If required, the Purchaser may seek clarifications from any or all Bidder(s) at this stage. The Purchaser would determine the Bidders that qualify for the next phase after reviewing the clarifications provided by the Bidder(s).

10.2.8 Bids that are technically qualified would only be taken up for financial evaluation.

10.2.9 Technical Presentation/Demonstration/POC may be required and shall be a part of the process for evaluation of the Bids.

10.3 Stage 3 – Evaluation of Financial Bids

10.3.1 Financial Bids submitted by only those Bidders, who have qualified the Pre-Qualification criteria and technical evaluation shall be eligible for further evaluation.

10.3.2 The Financial Bids of only those Bidders short listed from the Technical Bids by TEC shall be opened electronically in the presence of their representatives on a specified date and time to be intimated to the respective Bidders by Tender Process Section of NIC, and the same shall be evaluated by a duly constituted Finance Evaluation Committee (FEC).

10.3.3 Bidders quoting incredibly low or unrealistic high cost of items leading to unrealistic GTV with a view to subverting the tender process shall be rejected straight away by FEC and may invoke Bid Securing Declaration clause for such vendor.

10.3.4 The lowest quoting Bidder (L1) will be determined as mentioned below:

i) Initially Abridged Financial Bid as per "Annex 3: Abridged Financial Bid" will be opened for all the technically qualified Bidders on a specified date.

ii) The Detailed Financial Bid of only the lowest quoting Bidder shall be opened. On evaluation, if its detailed financial bid is found in order, it shall be declared as L1 Bidder else, the detailed financial bid of the next lowest quoting Bidder shall be considered for the same process and so on until L1 Bidder is identified. NIC reserves the right to reject the Bids of such Bidders whose bid are opened for L1 identification and not found in order as mentioned above.

iii) The L1 Bidder will be the Bidder with the lowest Gross Total Value (GTV) among all the quoted GTV in the Abridged Financial Bids (Annex 3) and its Detailed financial bid (Annex 4 and Annex 5) is in order.

10.4 Stage 4 – Final Bid Evaluation (Selection of Final Bidder)

10.4.1 The detailed financial bid (Annex 4 and 5) will be opened only for the selected Bidder having lowest GTV.

10.4.2 The first ranked Bidder will be selected as the final Bidder (L1) only when there is no discrepancy in the detailed financial bid. In case of any deviations/ discrepancy, the Purchaser reserves the right to disqualify the first ranked Bidder and select the subsequent second ranked Bidder as per the process mentioned above and so on until a Bidder is identified with no deviations and discrepancies.

10.4.3 Further, in the event of any mismatch in the GTV value provided at Annex 3 (Abridged financial bid) and total of Annex 5 (Bill of Material) of the Bidder, the following criteria shall be adopted to remove the discrepancy between these two values:

(a) When Grand Total Value given in Annex 3 (Abridged Financial Bid) is greater than the Grand Total Value given in Annex 5 (Bill of Material). The value given in Annex 5(Bill of Material) shall be taken as the value for Annex 3(Grand Total Value).

(b) When Grand Total Value given in Annex 3 (Abridged Financial Bid) is less than the Grand Total Value given in Annex 5 (Bill of Materials). The value given in Annex 5 (Bill of Materials) shall be replaced with the value given Annex 3 (Abridged Financial Bid) and the item-wise value for each item Annex 5 (Bill of Material) shall be reduced on Pro-Rata basis and consequently unit values shall be worked out.

10.4.4 Lack of competition shall not be determined solely on the basis of the number of Bidders. Even when only one Bid is submitted or a single bid remains as a result of technical or financial evaluation, the bid of the said Bidder will be evaluated as per tender terms and conditions and contract would be awarded if considered suitable.

10.4.5 Any decision taken by NIC, or the evaluation committee shall be final and binding on the Bidder. All the Bidders are required to agree to this clause and must sign an undertaking accepting this clause without any conditions.

10.5 Reasonability of Prices Received

10.5.1 The Purchaser may evaluate whether the GTV, and/or any of its components mentioned in Annex 5 (Bill of Materials), received as part of the bid are reasonable. If the prices received are considered abnormally low or unreasonably high, the Purchaser reserves its right to reject any or all bids, or abandon/ cancel the tender process and issue another tender for identical or similar services.

10.6 Consideration of Abnormally Low Bids

10.6.1 An Abnormally Low Bid is one in which the GTV, or any of its components including manpower, appears so low that it raises substantive concerns as to the Bidder's capability to perform the contract at the offered price. The Purchaser may in such cases seek written clarifications from the Bidder, including detailed price analyses of its GTV, and/or any of its components, concerning scope, schedule, allocation of risks and responsibilities, and any other requirements of the RFP. If, after evaluating the price analyses, the Purchaser determines that Bidder has substantively failed to demonstrate its capability to deliver the contract at the offered price, the Purchaser may reject the Bid/ proposal, and evaluation may proceed with the subsequent second ranked Bidder and so on.

10.7 Price Negotiation

10.7.1 The Purchaser reserves its right to negotiate the price with the lowest quoted Bidder (L1), who is techno-commercially suitable for delivery of Services.

10.8 Purchaser Preference Policies of the Government

10.8.1 The Purchaser reserves its right to grant preferences to eligible Bidders under various Government Policies/directives (policies relating to Make in India; MSME; Start-ups etc.).

11. Contract

11.1 Contract Process

11.1.1 The Bidder has to agree for honouring all tender conditions, SLAs and adherence to all RFP terms and conditions in executing the Work Orders placed by Purchaser.

11.1.2 Purchaser reserves the right to cancel this tender or modify the requirement, at any stage of Tender process cycle.

11.1.3 Purchaser also reserves the right to modify/relax any of the terms & conditions of the tender by declaring / publishing such amendments in a manner that all prospective vendors / parties to be kept informed about it.

11.1.4 Purchaser, without assigning any further reason can reject any tender(s), in which any prescribed condition(s) is/are found incomplete in any respect and at any processing state.

11.1.5 Purchaser also reserves the right to award Work Orders on quality / technical basis, which depends on quality, capability, and infrastructure of the Bidder.

11.2 Award of Contract

11.2.1 The acceptance of the tender shall be intimated to the successful Bidder by Purchaser/ through a letter/email. Purchaser would be the sole judge in the matter of award of contract and the decision of Purchaser shall be final and binding.

11.2.2 The Bidder shall sign the Contract as per tender terms and conditions with Purchaser within 15 working days of award of contractor such other extended time period approved by the Purchaser.

11.2.3 If the Bidder does not submit the duly filled proforma for contract within 15 working days unless the Purchaser informs otherwise, the Purchaser reserves the right to cancel the offer and invoke the execution of Bid securing declaration as per Annex 10 - Format for Bid Security Declaration Form**.**

11.2.4 Period of the contract shall be two years from the date of singing of contract and shall be extendable by another two years. Work Order shall be issued on yearly basis (or as deemed appropriate by the Purchaser).

11.3 Scope of Contract

11.3.1 Scope of the Contract shall be as defined in the tender document.

11.3.2 The Bidder is required to provide such services, support and infrastructure as the Purchaser or Purchaser's Technical Representative may deem proper and necessary, during the term of this contract.

11.4 Placing of Work Order (WO)

11.4.1 The Purchaser reserves the right to procure any quantity as deemed appropriate from the Bill of Material quoted by the Bidder placed at **Annex 5**. Work Orders shall be issued on yearly basis, or as deemed appropriate by the Purchaser.

11.4.2 Objection, if any, to the Work Order must be reported to the Purchase by the Bidder within five (5) working days counted from the date of issuance of Work Order for modifications, otherwise it shall

be assumed that the Bidder has accepted the Work Order. This is applicable in case of electronic delivery of Work Order also.

11.4.3 On the receipt of the Work Orders, the Bidder shall obtain all the necessary documents for timely delivery of the goods.

11.4.4 The details of Bill of Materials (BoM) submitted through Annex 5 are only for rate discovery of individual components, platform. The Purchaser reserves the right to use these discovered rates to place additional Work Orders for any of the components over and above the contract price.

11.5 Performance Bank Guarantee

11.5.1 The Bidder is required to ensure submission of Performance Bank Guarantee (PBG) equivalent to 5 % (Five Percent) of the Work Order value issued by the Purchaser in accordance with the proforma given at **Annex 6: Proforma for Bank Guarantee for Contract Performance**. PBG must be furnished within 20 days of issue of WO or as informed by the Purchaser. In the event of default/delay in submission of PBG within the stipulated time, the Bidder shall be liable for a penalty amounting to 0.3% (Zero Point three Percent) of the WO value per day delay/default with a maximum penalty capping of 10% of Work order value. Beyond the maximum capping of 10% of Work Order value, in respect of the first WO issued under the contract, the Purchaser reserves the right to forfeit the Security Deposit, terminate the contract.

11.5.2 PBG shall be in the form of an unconditional and irrevocable Bank Guarantee/ e-Bank Guarantee from a Commercial bank in the name of National Informatics Centre (NIC), New Delhi.

11.5.3 The Performance Bank Guarantee shall remain valid for a period of 90(Ninety) days beyond the date of completion of all contractual obligations of the supplier for that Work Order.

11.5.4 The Performance Bank Guarantee must be submitted within 15 working days of award of subsequent Work Orders or as informed by the Purchaser.

11.5.5 In the event of default/delay in submission of PBG within the stipulated time, the Bidder shall be liable for a penalty amounting to 0.3% (Zero Point three Percent) of the WO value per day delay/default with a Maximum penalty capping of 10% of Work Order value.

11.5.6 Beyond the maximum capping of 10% of WO value, the Purchaser reserves the right to forfeit any PBG and terminate the contract.

11.5.7 Performance Bank Guarantee would be returned only after successful completion of tasks assigned to Bidder for respective WO and only after adjusting/ recovering any dues recoverable/ payable from/ by the Bidder on any account under the contract.

11.5.8 The PBG shall be released (without any accrued interest) after the completion of all tasks (deliverables) as assigned in the WO.

11.6 Purchase Preference Policies of the Government

Unless otherwise stipulated in the RFP, the Procuring Entity reserves its right to grant preferences to the following categories of eligible Bidders under various Government Policies/ Directives:

1) **Class I Local Suppliers** under Public Procurement (Preference to Make in India) Order 2017" (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised from time to time.

2) **Bidders from Micro and/or Small Enterprises (MSEs)** under Public Procurement Policy for the Micro and Small Enterprises (MSEs) Order, 2012 as amended from time to time.

3) **Start-ups Bidders** under Ministry of Finance, Department of Expenditure, Public Procurement Division OM No F.20\212014-PPD dated 25.07.2016 and subsequent clarifications; and/ or
4) **Any other category of Bidders**, as per any Government Policies, announced from time to time, if so provided in the RFP.

11.6.1 Make in India Order

Orders issued by the Government of India regarding eligibility to participate and for purchase preference to "Local Suppliers" to encourage 'Make in India' and promote manufacturing and production of goods and services in India shall apply to this procurement, as detailed below.

(a) Categories of Local Suppliers

Bidders/Contractors are divided into three categories based on Local Content. Local content in the context of this policy is the total value of the Service procured (excluding net domestic indirect taxes) minus the value of imported content in the Service/ incidental Goods (including all customs duties) as a proportion of the total value, in percent):

i. 'Class-I local Supplier' with local content equal to or more than 50%.

ii. 'Class-II local Supplier' with local content equal or more than 20%, but less than that applicable for Class-I local Supplier.

iii. 'Non - Local Supplier' with local content less than that applicable for Class-II local Supplier, in sub-clause above.

(b) Eligibility Restrictions based on Reciprocity

If so stipulated in the Tender Document, entities from such countries identified as not allowing Indian companies to participate in their Government procurement shall not be allowed to participate on a reciprocal basis in this tender. The term entity of a country shall have the same meaning as under the FDI Policy of DPIIT as amended from time to time.

(c) Thresholds

i. Local content for eligibility for Class-I; Class-II local Suppliers and Non-local Suppliers shall be 50% and above; 20% and above but less than 50%; and less than 20%, respectively.

ii. Minimum local content for eligibility to participate shall be 20%,
iii. The margin of purchase preference shall be 20%

(d) Purchase preference to Class-I local Suppliers

i. Among all technically qualified bids, in the Stage 3 – Evaluation of Financial Bids (Selection of LQ1 Bidder), the lowest bid shall be termed as LQ-1. If LQ 1 is 'Class-I local Supplier'.

ii. If LQ-1 is not 'Class-I local Supplier', the lowest Bidder among the 'Class- I local Supplier' shall be invited to match the LQ-1 price subject to Class- I local Supplier's quoted price falling within the margin of purchase preference, such 'Class-I local Supplier' shall be termed as LQ-1 subject to matching the LQ-1 price.

iii. If such lowest eligible 'Class-I local Supplier' fails to match the LQ-1 price, the 'Class-I local Supplier' with the next higher and so on, bid within the margin of purchase preference shall be invited to match the LQ-1 price. If none of the 'Class-I local Supplier' within the margin of purchase preference matches the LQ-1 price, the non-local supplier with lowest bid shall be termed as LQ-1.

11.6.2 Verification of local content and violations:

(a) The 'Class-I local Supplier'/ 'Class-II local Supplier' at the time of tender, bidding, or solicitation shall be required to indicate the percentage of local content and provide selfcertification that the item offered meets the local content requirement for 'Class-I local Supplier'/ 'Class-II local Supplier', as the case may be.

(b) The 'Class-I local Supplier'/ 'Class-II local Supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) certifying that the Bidder qualifies as class-I or class-II Bidder as per Annex 13

(c) Bids with false declarations regarding Local contents shall be rejected as responsive, in addition to punitive actions under the MII orders and for violating the Code of Integrity as per the RFP . The Bidder may also invoke bid securing declaration incase of voilation.

(d) Purchaser reserves the right to seek any clarification/document/certification w.r.t compliance with MII orders referred above till the time of completion of tender process.

12. Payment Terms

12.1 Payment Terms

12.1.1 A pre-received bill (three copies) shall be submitted in the name of "NATIONAL INFORMATICS CENTRE" at NIC, New Delhi.

12.1.2 Bidder has to install the complete solution and prepare the installation report as per the prescribed format (to be shared by the Purchaser at the time of installation) and get it signed by the Authorised

Representative with date and stamp. For the overall project commissioning, the Bidder shall submit UAT report for sign off by the Purchaser.

12.1.3 If the Bidder fails to deliver as per the project timelines, penalty as mentioned in tender, shall be applicable.

12.1.4 All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the latest Income-Tax Act.

12.1.5 Payment against Work Order shall be done as per payment schedule specified in the tender.

12.1.6 Payment shall be done after deduction of all applicable penalties, as per Service Level Agreement (as defined in Section 6 of the RFP), the SLAs shall be measured on monthly basis.

12.2 Payment Schedule

TABLE 12: PAYMENT SCHEDULE

S No.	Billing Cycle	Payment Milestone
1	Complete delivery of Hardware & Software as per BoM and Inspection thereof.	70% cost of delivered hardware. Penalties shall be deducted as per delivery timelines mentioned in RFP.
2	Post successful installation of the deployed hardware	As per **5(B) Table for Implementation**
3	After 1 month of Go-Live, and UAT acceptance	Remaining 30% cost of deployed hardware. Penalties shall be deducted as per timelines mentioned in RFP.
4	Annual maintenance Cost for supplied ICT components. The AMC payment will commence from the second year as the hardware and software are under warranty in the first year	Purchaser will release the payment to the Bidder quarterly in arrears, subsequent to the receipt of invoice and certificate at the end of quarter. **Penalties shall be deducted as per SLA/Uptime mentioned in the RFP**

12.2.1 Payments shall be made subject to the following—

(c) Adherence to project delivery timelines.

(d) Payment shall be released on deployment of all hardware and software components specified in the respective Work Order.

(e) The contract period and any extensions thereof for the software licenses and hardware warranty shall be from the date of Go-Live.

(f) The Bidder shall provide all necessary documentation related to the Services consumed and any other documents as demanded by the Purchaser. Invoice without any of the said documents shall be deemed incomplete and not acceptable.

(g) The Purchaser shall release the payment for Services rendered and accepted, subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the contract and meet SLA requirements.

(h) For release of payment for any license, subscription or AMC of the supplied Hardware or Software the Bidder shall share the required documents from the respective OEM indicating that the subscriptions have been renewed.

(i) The amount will be as per the unit rate amount specified in Bill of Material. Payments will be released only on satisfactory acceptance of the deliverables for each task and after deduction of penalty if any for each task as per the schedule mentioned.

(j) Payment shall be released by the Purchaser against the invoices raised by Bidder within 30 calendar days given all the relevant documents are submitted timely and are complete in all reference.

(k) Installation Payments "Remaining 30% cost of deployed hardware" to be released after successful integration and Go-live and duly approved by the UAT committee constituted by the Purchaser

12.3 Payment against time-barred claims

12.3.1 All claims against the Purchaser shall be time-barred after a period of 3 years, reckoned from the date on which the payment falls due, unless the payment claim has been under correspondence. The Purchaser shall be entitled to reject such claims.

12.3.2 In respect of any claim where the same is raised without furnishing the documents as required under the contract and the Purchaser, as a result, it is not in position to claim input tax credit under the applicable law(s) governing taxation, the Bidder shall not be entitled to payment of such input tax credit amount as the Purchaser would not be in position to claim.

12.4 Completion Certificate and Final payment

12.4.1 Completion Certificate:

Upon a written intimation from the Bidder, the Purchaser shall issue a certificate of completion duly indicating the date of completion after satisfying itself of the following. The Purchaser may also issue such a certificate indicating the date of completion concerning any part of the Service (before the completion of the whole of Service), which has been completed to the satisfaction of the Purchaser:

(a) that the whole of the Services to be done under the provisions of the contracts have been completed or when any such certificate is given in respect of part of a Service, such part shall be considered completed.

(b) that they have been inspected by him since their completion and found to be in good and substantial order,

(c) that such completed services have satisfactorily passed any final test or tests that may be prescribed,

(d) that all properties, works and things, removed, disturbed, or damaged in consequence of the Services have been adequately replaced and

(e) that the Purchaser has returned in good condition, all assets loaned or hired from the Purchaser (if any) and has given a satisfactory account of payments made to or retained by the Purchaser for such loaned/ hired assets,

(f) that the Bidder has made good and satisfied in conformity with the contract all expenses and demands:

i. incurred by or made upon by the Purchaser.

ii. for or in respect of damages or losses from or in consequence of the services.

12.4.2 Approval Only by Completion Certificate:

No certificate other than completion certificate referred to in sub-clause above shall be deemed to constitute approval of any Service or other matter in respect of which it is issued or shall be taken as an admission of the due performance of the Bidder or any part thereof or of the accuracy of any claim or demand made by the Bidder or of additional varied Services having been ordered by the Purchaser nor shall any other certificate conclude or prejudice any of the powers of the Purchaser.

12.4.3 Cessation of Procuring Entity's Liability

After the issue of Completion Certificate, the Purchaser shall not be liable to the Bidder for any matter arising out of or in connection with the contract for the delivery of the Services, unless the Bidder shall have claimed in writing in respect thereof before the issue of the Completion Certificate for Service in Contract.

12.4.4 Unfulfilled Obligations

Notwithstanding the issue of Completion Certificate for Service, the Bidder and the Purchaser shall remain liable for the fulfilment of any obligation incurred under the provision of the contract before the issue of the Completion Certificate for services, which remains unperformed at the time such certificate is issued. The contract shall be deemed to remain in force till the nature and extent of any such obligations are determined.

12.4.5 Final Payment

The Bidder shall submit a Final bill on the Purchaser's certificate of completion regarding the services. The Final payment shall be made as per the following calculations to the Bidder after receiving a clear "No Claim Certificate" signed from it:

(a) the total quantity of Service executed by the Bidder upto the completion date based on the Purchaser's or its representative's certified measurements.

(b) priced at the rates in the Price Schedule in the contract and for extra works under change management process.

(c) necessary adjustment for any payments already made or retained

(d) any deduction which may be made under the contract,

(e) a complete account of all claims Bidder may have on the Purchaser, and the Purchaser gave a certificate in writing that such claims are correct.

12.4.6 No Claim Certificate and Release of Contract Securities:

The Bidder shall submit a 'No-claim certificate' to the Purchaser in such form as shall be required by the Purchaser after the Services are finally admeasured and before the final payment/ PBG are released. The Purchaser shall release the contractual securities without any interest if no outstanding obligation, asset, or payments are due from the Bidder. The Bidder shall not be entitled to make any claim whatsoever against the Purchaser under or arising out of this Contract, nor shall the Purchaser entertain or consider any such claim, if made by the Bidder, after he/she shall have signed a "No Claim" Certificate in favour of the Purchaser. The Bidder shall be debarred from disputing the correctness of the items covered by the "No Claim" Certificate or demanding a clearance to arbitration in respect thereof.

12.4.7 Post Payment Audit:

Notwithstanding the issue of Completion Certificate and release of final Payment, the Purchaser reserves the right to carry out within 180 days (unless otherwise stipulated in the contract) of such completion/ final payment, a post-payment audit and/ or technical examination of the Services and the final bill including all supporting vouchers, abstracts etc. If any over-payment to the Bidder is discovered due to such examination, the Purchaser shall claim such amount from the Bidder.

12.4.8 Signature on Receipts for Amounts:

Every receipt for money, which may become payable, or for any security which may become transferable to the Bidder, the contract, shall if signed in the partnership name by any one of the partners of a Bidder's firm, be a suitable and sufficient discharge to the Purchaser in respect of the sums of money or security purported to be acknowledged thereby. In the event of death of any Bidder contractor, partners during the pendency of the contract, every receipt by anyone of the surviving constituents shall be suitable and sufficient discharge as aforesaid. Nothing in this Clause shall be deemed to prejudice or effect any claim that the Purchaser may hereafter have against the legal representative regarding any breach of any contract conditions by any Bidder partner/member so dying. Nothing in this clause shall be deemed to prejudice or effect the respective rights or obligations of the Bidder partners/ members and the legal representatives of any deceased Bidder partners/ members.

12.4.9 Defects Liability Period

(a) the Bidder warrants that the Services have been delivered as per description, scope/ quantum, performance standards and quality outlined in the contract. This Defect Liability shall be in effect for a period stipulated in the contract (or if not specified for

ninety (90) days) from completing the Services. The contract shall be deemed alive during this period, even if final payment and/ or Performance Guarantee has been released.

(b) During the Defects Liability Period, upon discovering any deficiencies in outputs/ outcomes attributable to a shortfall in scope/ quantum, performance standards and quality of the performed Services, the Purchaser shall give written notice to the Bidder.

(c) Upon receiving such notice, the Bidder shall, within 21 days (or within any other period, if stipulated in the contract), expeditiously remedy or reperform the Services or parts thereof, free of cost, at the site.

(d) If the Bidder, having been notified, fails to rectify/ replace the defect(s) within 21 days (or within any other period, if stipulated in the contract), it shall amount to breach of Contract, and the Purchaser shall proceed to take such remedial action(s) as deemed fit by it as detailed.

13. Other Terms & Conditions for Bidder/Bidder

13.1 General Conditions

13.1.1 As a matter of policy and practice and on the basis of Notification published in Gazette of India dated 14th March 1998, it is clarified that services and supplies of the Bidder selected through this tender can be availed by National Informatics Centre (NIC). The Bidder which shall be called Bidder, shall be obliged to render services to Purchaser as per the Work Order.

13.1.2 Consortium is not allowed.

13.1.3 The Bidder/OEM shall undertake to provide support for the supplied solution for entire contract period and any extension thereof (including 5-year OEM warranty & support starting from the date of final acceptance of the solution).

13.1.4 Any deviation in bid terms and conditions may lead to rejection of the bid.

13.1.5 In case the Bidder is found in-breach of any condition(s) of tender or supply order, at any stage during the course of supply/ installation/commissioning or warranty period, the legal action as per rules/laws, shall be initiated against the Bidder, EMD/Security Deposits shall be forfeited and bid securing declaration may be invoked.

13.1.6 Any attempt by Bidder to bring pressure towards Purchaser's decision-making process, such Bidders shall be disqualified for participation in the present tender and may result in invoking bid securing declaration.

13.1.7 Printed conditions specified in the tender Bids submitted by Bidders shall not be binding on Purchaser. All the terms and conditions for the supply, testing and installation, payment terms, penalty etc. shall be as those specified herein and no change in the terms and conditions by the Bidders shall be acceptable. Alterations/overwriting, if any, in the tender Bids shall be attested properly by the Bidder, failing which, the tender shall be rejected.

13.1.8 Upon verification, evaluation / assessment, if in case any information furnished by the Bidder is found to be false/incorrect, their total Bid shall be summarily rejected and no correspondence on the same, shall be entertained.

13.1.9 Purchaser shall not be responsible for any misinterpretation or wrong assumption by the Bidder, while responding to this tender.

13.1.10 Bid Security/EMD of the unsuccessful Bidders shall be returned to the respective Bidders at the earliest after expiry of the final Bid validity and latest on or before the 30th day after the award of the contract results. However, in case of two packet Bidding, EMD of unsuccessful Bidders during first stage i.e., technical evaluation, shall be returned within 30 days of declaration of results of first stage i.e., technical evaluation.

13.1.11 Any equipment or its components supplied by the Bidder/OEM must comply to the land border restrictions of Clause 13.27 of this tender document.

13.2 Warranty

13.2.1 The Bidder warrants that all the Goods are new, unused, and of the most recent or current models, and that they incorporate all recent improvements in design and materials, unless provided otherwise in the Contract.

13.2.2 The Bidder further warrants that the Goods shall be free from defects arising from any act or omission of the Supplier or arising from design, materials, and workmanship, under normal use in the conditions prevailing in the country of final destination.

13.2.3 Unless otherwise specified in the Other terms and conditions, the warranty shall remain valid for twelve (12) months after the Goods, or any portion thereof as the case may be, have been deployed and accepted at the final destination indicated in the scope of work in this tender, or for eighteen (18) months after the date of shipment from the port or place of loading in the country of origin, whichever period concludes earlier.

13.2.4 The Purchaser shall give notice to the Bidder stating the nature of any such defects together with all available evidence thereof, promptly following the discovery thereof. The Purchaser shall afford all reasonable opportunity for the Bidder to inspect such defects.

13.2.5 Upon receipt of such notice, the Bidder shall expeditiously repair or replace the defective Goods or parts thereof at no cost to the Purchaser.

13.2.6 If having been notified, the Bidder fails to remedy the defect within the specified period, the Purchaser may proceed to take within a reasonable period such remedial action as may be necessary, at the Bidder's risk and expense and without prejudice to any other rights which the Purchaser may have against the Bidder under the Contract.

13.3 Confidentiality

13.3.1 All documents, data, associated correspondence or other information furnished by or on behalf of the Purchaser to the Bidder, in connection with the contract, whether such information has been furnished before, during or following completion or termination of the contract, are confidential and shall remain the property of the Purchaser and shall not, without the prior written consent of Purchaser neither be divulged by the contractor to any third party, nor be used for any purpose other than the procurement, maintenance or other services and work required for the performance of this Contract. If advised by the Purchaser, all copies of all such information in original shall be returned on completion of the Bidder's performance and obligations under this contract.

13.3.2 The Bidder shall not use Confidential Information, the name, or the logo of the Purchaser except for the purposes of providing the Service as specified under this contract.

13.3.3 The term "Confidential Information", as used herein, shall mean all business strategies, plans and procedures, proprietary information, software, tools, processes, methodologies, data and trade secrets, and other confidential information and materials of the Purchaser, its affiliates, their respective clients or suppliers, or other persons or entities with whom they do business, that may be obtained by the Bidder from any source or that may be developed for the Purchaser as a result of the Contract Agreement.

13.3.4 The Bidder shall be responsible for providing a signed NDA by its antecedents, delegates, to the Purchaser. The Bidder shall be held responsible for any breach of the NDA by its antecedents, delegates, or sub-contractors. The Bidder and all the deployed resources if any shall sign the NDA with reference to "THE OFFICIAL SECRETS ACT, 1923".

13.3.5 The provisions respecting confidentiality shall not apply to the extent, but only to the extent, that the information or document is:

(a) already known to the Bidder free of any restriction at the time it is obtained from the Purchaser,

(b) subsequently learned from an independent third party free of any restriction and without breach of this provision.

(c) is or becomes publicly available through no wrongful act of the Bidder or any third party.

(d) is independently developed by the Bidder without reference to or use of any Confidential Information of the Purchaser/organisation; or

(e) is required to be disclosed pursuant to an applicable law, rule, regulation, government requirement or court order, or the rules of any stock exchange (provided, however, that the Bidder shall advise the Purchaser of such required disclosure promptly upon learning thereof in order to afford the Purchaser a reasonable opportunity to contest, limit and/or assist the Bidder in crafting such disclosure).

13.3.6 The Bidder must ensure to provide the signed NDA in case of change in antecedents, delegates, and the sub-contractors from time-to-time.

13.3.7 The Bidder shall notify the Purchaser promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of the Purchaser.

13.3.8 The Bidder shall not use Confidential Information (CCTV records, Biometric Records, etc.), the name or the logo of the Purchaser except for the purposes of providing the Service as specified under the contract.

13.3.9 The Bidder may only disclose Confidential Information in the following circumstances—

(a) with the prior written consent of the Purchaser.

(b) to a member of the Bidder's Team ("Authorised Person") if:

(i) The Authorised Person needs the Confidential Information for the performance of obligations under the contract.

(ii) The Authorised Person is aware of the confidentiality of the Confidential Information and is obliged to use it only for the performance of obligations under the contract

13.3.10 The Bidder shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality contract with the members of the partners and other Systems Integrator's team members to the satisfaction of the Purchaser.

13.3.11 The Bidder shall treat all the information provided by Purchaser such as IP schema, DC and Cloud architecture, block diagrams, manuals, policies, procedure, guidelines, employee details etc. (but not limited to) as top-secret information and shall not disclose the information without explicit written permission for the same by Purchaser.

13.3.12 The obligations under this clause shall survive for three years from termination or expiration of this Contract/agreement.

13.3.13 The Work Order/contract with the organisation may define more stringent confidentiality obligations depending on the nature of information / data being shared. In such event, the more stringent obligations shall prevail.

13.4 Integrity Pact

13.4.1 In compliance with the Central Vigilance Commissioner Circular No. 06/05/21 dated 3rd June 2021 regarding adaptation of Integrity Pact- Revised Standard Operating Procedure to ensure transparency, equity and competitiveness in public procurement, the Bidder(s) are required to sign an Integrity Pact with Purchaser.

13.4.2 The pact essentially is an agreement between the Bidder(s) and the Purchaser, committing the persons/Officials of both sides, not to resort to any corrupt practices in any aspect/stage of the contract. Only those Bidders, who commit themselves to such a pact with the Purchaser, would be considered competent to participate in the bidding process.

13.4.3 The Bidders are required to submit the signed Integrity pact along with the Technical Bid, failing which, the Bids would not be considered for evaluation for such Bidders and may get disqualified. The format for the integrity pact is attached as Annex 12: Format for Integrity Pact.

13.4.4 The Integrity pact shall be applicable from the date of Bid submission or from the date when the Purchaser sends signed copy of the Integrity Pact to the Bidder, whichever is later. Further, any violation of Integrity pact would entail disqualification of the Bidder(s) and forfeiture of EMD.

13.5 Obligation to Indemnify Purchaser

13.5.1 For breach of IPR Rights

(a) The Bidder shall indemnify and hold harmless, free of costs, the Purchaser and its employees and officers from and against all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which may arise in respect of the Services provided by the Bidder under this Contract, as a result of any infringement or alleged infringement of any patent, utility model, registered design, copyright, or other Intellectual Proprietary Rights (IPR) or trademarks, registered or otherwise existing on the date of the contract arising out of or in connection with:

   i. Any design, data, drawing, specification, or other documents or Services provided or designed by the Bidder for or on behalf of the Purchaser.
   ii. The sale by the Purchaser in any country of the services/ products produced by the Services delivered by the Bidder, and
   iii. The delivery of the Services by the Bidder or the use of the Services at the Purchaser's Site

(b) Such indemnity shall not cover any use of the Services or any part thereof other than for the purpose indicated by or to be reasonably inferred from the contract, neither any infringement resulting from the use of the Services or any part thereof, or any Service/ products produced thereby in association or combination with any other Service, equipment, plant, or materials not delivered by the Bidder.

(c) If any proceedings are brought, or any claim is made against the Purchaser arising out of the matters referred above, the Purchaser shall promptly give the Bidder a notice thereof. At its own expense

and in the Purchaser's name, the Bidder may conduct such proceedings and negotiations to settle any such proceedings or claim, keeping the Purchaser informed.

(d) If the Bidder fails to notify the Purchaser within twenty-eight (28) days after receiving such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its behalf at the risk and cost to the Bidder.

(e) At the Bidder's request, the Purchaser shall afford all available assistance to the Bidder in conducting such proceedings or claim and shall be reimbursed by the Bidder for all reasonable expenses incurred in so doing.

13.5.2 For Losses and Damages Caused by Bidder

(a) The Bidder shall indemnify and keep harmless the Purchaser, from and against, all actions, suit proceedings, losses, costs, damages, charges, claims, and demands of every nature and description brought or recovered against the Purchaser because of any act or omission or default or negligence or trespass of the Bidder, his agents, or employees despite all reasonable and proper precautions may have been taken, during the execution of the Services. The Bidder shall make good at his own expense all resulting losses and/ or damages to:

   i. the Services themselves or
   ii. any other property of the Purchaser or
   iii. the lives, persons, or property of others

(b) In case the Purchaser is called upon to make good such costs, loss, or damages, or to pay any compensation, including that payable under the provisions of the Workmen's Compensation Act or any statutory amendments thereof; the amount of any costs or charges including costs and charges in connection with legal proceedings, which the Purchaser may incur about it, shall be charged to the Bidder. All sums payable by way of compensation under any of these conditions shall be considered as reasonable compensation to be applied to the actual loss or damage sustained and whether or not any damage shall have been sustained.

(c) The Purchaser shall have the power and right to pay or to defend or compromise any claim of threatened legal proceedings, or in anticipation of legal proceedings being instituted consequent on the action or default of the Bidder, to take such steps as may be considered necessary or desirable to ward off or mitigate the effect of such proceedings, charging to Bidder, as aforesaid, any sum or sums of money which may be paid and any expenses whether for reinstatement or otherwise which may be incurred and the propriety of any such payment, defence or compromise, and the incurring of any such expenses shall not be called in question by the Bidder.

13.6 Liquidated Damages

13.6.1 The delivery dates, timetables, milestones and other requirements specified in the RFP and this contract are binding on the Bidder and the Bidder agrees to accomplish the user requirement specified and Scope of Work under this contract as per the Timelines specified in the RFP.

13.6.2 If the Bidder fails to achieve the Timelines or the Service Levels due to reasons solely attributable to the Bidder, the Purchaser shall be entitled to recover from the Bidder the liquidated damages as per the SLAs specified in Section 6 of this RFP.

13.6.3 In the event Bidder is not solely responsible for such failure in Timelines and Service Levels, the Purchaser shall have the right to determine such extent of fault and liquidated damages in consultation

with the Bidder and any other party it deems appropriate. In such cases, the proportionate Liquidated Damage as mutually determined shall be levied.

13.6.4 Recovery of liquidated damages shall not be the sole and exclusive remedies available to the Purchaser and the Bidder shall not be relieved from any obligations by virtue of payment of such liquidated damages. Liquidated damages shall be capped at 10% of the respective work orders. If the liquidated damages cross the cap on liquidated damages specified herein, the Purchaser shall have the right to terminate the contract for default and consequences for such termination as provided in this contract shall be applicable.

13.7 Limitation of Liability

13.7.1 Except in cases of criminal negligence or willful misconduct, the aggregate liability of the Bidder to the Purchaser, whether under the contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the Bidder to indemnify the Purchaser concerning IPR infringement.

13.8 Labour Laws

13.8.1 The Bidder shall, and hereby agrees to, comply with all the provisions of Indian Labour Laws and industrial laws in respect of the resources employed thereof.

13.8.2 Wherever necessary, the Bidder shall apply for and obtain license as provided under Contract Labour (Regulation and Abolition) Act, 1970, and strictly comply with all the terms and conditions that the licensing authority may impose at the time of grant of license. The Purchaser shall not be held responsible for any breach of the license terms and conditions by the Bidder.

13.8.3 The Bidder shall be solely responsible for the payment of wages to the deployed resources and ensure its timely payment thereof.

13.8.4 The Bidder shall duly maintain a register giving particulars of the deployed resources, nature of work, rate of wages, etc.

13.8.5 The Bidder shall also ensure compliance to the following labour legislations:

(a) Minimum Wages Act
(b) Employees Provident Fund Act
(c) Employees State Insurance Act
(d) Workmen's Compensation Act, if the ESI Act does not apply
(e) Maternity Benefit Act
(f) Code on Wages 2019,
(g) The Industrial Relations Code 2020,
(h) The Social Security Code 2020, and
(i) The Occupational Safety, Health and Working Conditions Code 2020
(j) Any other laws, as applicable, time to time

13.8.6 The Bidder shall be solely responsible to adhere to all the rules and regulations relating to labour practices and Service conditions of its workmen and at no time shall it be the responsibility of Purchaser.

13.8.7 The resources if asked under this tender and deployed by the Bidder shall be on pay roll and full-time employee of the Bidder.

13.9 Conflict of Interest

13.9.1 The Bidder shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

13.10 Severance

13.10.1 In the event any provision of this Contract is held to be invalid or unenforceable under the applicable law of India, the remaining provisions of this Contract would remain in full force and effect.

13.11 Force Majeure

13.11.1 For the purposes of this RFP, "Force Majeure" means an event which is beyond the reasonable control of a Party, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, landslide, fire, explosion, storm, tempest, flood, hurricane, cyclone, lightning, thunder, other adverse weather conditions, volcanic eruption, pandemic, quarantine, plague, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by government agencies.

13.11.2 Force Majeure shall not include any event that is caused by the negligence or intentional action of a Party or its agents or its employees, or any event which a diligent Party could reasonably have been expected to have considered at the time of the conclusion of the Contract and to have avoided or overcome in the carrying out of its obligations hereunder, through exercise of reasonable skill and care.

13.11.3 Force Majeure shall not include insufficiency of funds or failure to make any payment required hereunder.

13.11.4 If at any time, during the term of the Contract, the performance in whole or in part by any Party of any obligation hereunder is prevented or delayed by reasons of occurrence of Force Majeure events as defined above, and notice of such occurrence is duly furnished by such Party, seeking concession, to the other, as soon as practicable, but within 21 days from the date of such occurrence, and satisfies the party adequately of the measures taken by it, no Party shall, by reason of that event, be entitled to terminate the Contract, nor shall any Party have any claim for damages against the other Parties in respect of such non-performance or delay in performance, and deliveries under the Contract shall be resumed as soon as practicable after such event has come to an end or ceased; and the decision of the Purchaser as to whether the deliveries have resumed or not shall be final and conclusive.

13.12 Events of Default by Bidder

13.12.1 The failure on the part of the Bidder to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the Bidder. The events of default as specified 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 conform 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 has failed to comply with or is in breach or contravention of any applicable laws of India.

13.12.2 Failure of the successful Bidder to comply with the Tender requirements shall constitute sufficient grounds for the annulment of the award and forfeiture of the 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 shall be borne by the Bidder.

13.13 Dispute Resolution /Arbitration

13.13.1 Amicable settlement

The Parties shall, in good faith, endeavour to settle amicably all disputes arising out of or in connection with this Agreement or interpretation thereof.

13.13.2 Dispute Resolution

(a) Any dispute, difference, or controversy whatsoever, howsoever arising under or out of or in relation to this Agreement (including its interpretation) between the Parties, and so notified in writing by any Party to another Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure set forth in this tender.

(b) The Parties agree to use their best efforts for resolving all Disputes arising under or in respect of this Agreement promptly, equitably and in good faith, and further agree to provide each other with reasonable access during normal business hours to all non-privileged records, information and data pertaining to any Dispute.

(c) Any Dispute which is not resolved amicably by conciliation as provided in paragraph 13.15, shall be finally decided by reference to Arbitration.

(d) This Agreement and the rights and obligations of the Parties shall remain in full force and effect, pending the award in any Arbitration proceedings hereunder.

13.13.3 Conciliation

In the event of any Dispute between the Parties, any Party may call for amicable settlement, and upon such reference, the nominated persons shall meet not later than 10 days from the date of reference to discuss and attempt to amicably resolve the Dispute. If such meeting does not take place within the said period of 10 days, or the Dispute is not amicably settled within 15 days of the meeting, or the Dispute is not resolved as evidenced by the signing of written terms of settlement within 30 days of the notice in writing referred to in Section 13 or such longer period as may be mutually agreed upon by the Parties, any Party may refer the Dispute to Arbitration in accordance with the provisions of Section 13.

13.13.4 Arbitration

(a) Without prejudice to the right of the Purchaser to terminate the Contract and pursue other remedies thereunder, if a dispute, controversy or claim arises out of or relates to the Contract, or breach, termination, or invalidity thereof, and if such dispute, controversy or claim cannot be settled and

resolved by the Parties through discussion and negotiation, then the Parties shall refer such dispute to sole Arbitrator appointed with the mutual consent of the Purchaser and the Bidder. The Arbitration proceedings shall be conducted in English and a written order shall be passed. The venue of the Arbitration shall be Delhi. The Arbitration shall be held in accordance with the provisions of the Arbitration and Conciliation Act, 1996. The Parties agree to have their dispute(s) or difference(s) resolved in terms of section 29B of the said Act.

(b) The Arbitration award shall be final, conclusive and binding upon the Parties and judgement may be entered thereon, upon the application of either Party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of Arbitration, including fees and expenses of the Arbitrator, shall be shared equally by the Parties, unless the award otherwise provides.

(c) The courts in Delhi shall have exclusive jurisdiction in relation to this Contract.

13.14 Applicable Laws

13.14.1 The Bidder shall be governed by the laws of India and shall include any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, byelaw, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on or until the date of the execution of the Agreement, and during the subsistence thereof, that the Purchaser may get into with the Bidder, applicable to the Project.

13.15 Adherence to safety procedures, rules, regulations & restriction

13.15.1 Bidder shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. Purchaser's employee shall also comply with safety procedures/policy.

13.15.2 The Purchaser shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

13.15.3 Bidder shall also adhere to all security requirement/regulations of the Purchaser during the execution of the contract.

13.15.4 Access to the Purchaser's Data centre shall be strictly restricted in the following manner:

13.15.5 No access to any person except one explicitly authorised by the Purchaser shall be allowed entry. Even if granted, access shall be restricted to system/equipment necessary to run the engagement and access to any other equipment must be strictly precluded by necessary means, locks, video surveillance, etc.

13.15.6 No access to any employee of the Bidder, except the essential staff who has genuine work-related need, shall be furnished. All such access shall be logged in a loss-free manner for permanent record with unique biometric identification of the employee to avoid misrepresentations or mistakes.

13.16 Micro, Small & Medium Enterprises Development Act, 2006

13.16.1 If a Bidder falls under the Micro, Small & Medium Enterprises Development Act, 2006, then a copy of the valid certificate must be provided to the Purchaser. Further, the Bidder must keep Purchaser informed of any change in the status of the company or any other legal entity.

13.16.2 Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME) or are registered with the Central Purchase Organisation or the concerned Ministry or Department are liable to get following benefits.

(a) Issue of tender sets free of cost (Zero Tender Fee)

(b) Exemption from payment of earnest money (Zero EMD)

13.16.3 The Bidder is required to submit a copy of the registration certificate to Purchaser. Further, the Bidder must keep Purchaser informed of any change in the status of the company or any other legal entity.

13.17 Statutory Requirements

13.17.1 During the tenure of the contract nothing shall be done by the Purchaser in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange, etc.

13.17.2 The Bidder and their personnel/representative shall not alter / change / replace any hardware component proprietary to the Purchaser and/or under warranty or AMC of third party without prior consent of the Purchaser.

13.17.3 The Bidder and their personnel/representative shall not without consent of the Purchaser install any hardware or software not purchased / owned by the Purchaser.

13.18 Information Security

13.18.1 The Bidder shall not carry and/or transmit any material, information, layouts, diagrams, storage media or any other goods/material in physical or electronic form, which are proprietary to or owned by the Purchaser, out of extended location premises without prior written permission from the Purchaser.

13.18.2 Bidder acknowledges that Purchaser proprietary information or materials, whether developed by Purchaser or being used by Purchaser pursuant to a license Work Order with a third party (the foregoing collectively referred to herein as “proprietary information”) are confidential and proprietary to Purchaser; and Bidder agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorised use or disclosure thereof, which care shall not be less than that used by Bidder to protect its own proprietary information. Bidder recognizes that the good shall of Purchaser depends, among other things, upon Bidder keeping such proprietary information confidential and that unauthorised disclosure of the same by Bidder could damage Purchaser and that by reason of Bidder’s duties hereunder. Bidder may come into possession of such proprietary information, even though Bidder does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by the contract. Bidder shall use such information only for the purpose of performing the said services.

13.18.3 Bidder shall, upon termination of the contract for any reason, or upon demand by Purchaser, whichever is earliest, return any and all information provided to Bidder by Purchaser, including any copies or reproductions, both hardcopy and electronic. Any proprietary tools of the Bidder, if any used for the project and Bidders Pre-existing IPR will remain with the Bidder.

13.18.4 The authorised signatory of the Bidder shall sign the NDA with reference to this tender “The Official Secrets Act, 1923” within 7 days and submit the same along with the acceptance of the Work Order letter.

13.19 Continuance of Contract

13.19.1 Notwithstanding the fact that settlement of dispute(s) (if any) under arbitration may be pending, the parties hereto shall continue to be governed by and perform the work in accordance with the provisions under the Scope of Work to ensure continuity of operations.

13.20 Termination of Contract

Purchaser reserves the right to suspend any of the services and/or terminate the agreement in one or more of the following circumstances by giving 90 days' notice in writing:

13.20.1 Termination process

Upon occurrence of an event of default as set out in above clauses, Purchaser shall deliver a default notice in writing to the other party which shall specify the event of default and give the Bidder an opportunity to correct the default. At the expiry of notice period, unless the party receiving the default notice remedied the default, the party giving the default notice may terminate the agreement.

13.20.2 Termination for insolvency, dissolution, bribery

(a) The Contract may be terminated by the Purchaser and the deposits/guarantees in possession of the Purchaser (Security Deposit and the Performance Bank Guarantee) may be forfeited in case a public officer is bribed by the Bidder or the Bidder becomes insolvent or in case of dissolution/winding up of Bidder, provided that such termination shall not prejudice or effect any right of action or remedy which has accrued thereafter to Purchaser.

(b) In case of Contract termination for reasons specified in Section 13, the Purchaser reserves the right to recover any dues payable by the Bidder from any amount outstanding to the credit of the Bidder, including on account of any pending bills and/or by invoking the Performance Bank Guarantee and/or the Security Deposit in possession of the Purchaser and the remaining amount may be paid to the liquidator/Bidder, as applicable.

13.20.3 Termination for default/breach

Purchaser may without prejudice to any other remedy for breach of contract, (including forfeiture of security deposit and/or, Performance Bank Guarantee) by written notice of default sent to the Bidder, terminate the contract in whole or in part after sending a notice to the Bidder in this regard. Further, Purchaser may afford a reasonable opportunity to the Bidder to explain the circumstances leading to such a breach and may increase the time limit for curing such breach before terminating the contract. Any notice served pursuant to this Clause shall give reasonable details of the breach. Following conditions shall be considered as breach of contract:

(a) If the Bidder fails to accept the Work Order(s).

(b) The Bidder/Bidder's Team has failed to conform 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 goes into liquidation, voluntarily or otherwise.

(d) The Bidder/Bidder's Team has failed to comply with or is in breach or contravention of any applicable laws.
(e) If the Bidder fails to deliver services within the time period specified in the Work Orders granted by Purchaser.
(f) If the Bidder fails to meet any other terms and conditions under the contract.

13.20.4 Termination for convenience

Purchaser may by written notice, sent to the Bidder, terminate the Work Order and/or the Contract, in whole or in part at any time of its convenience. The notice of termination shall specify that termination is for Purchaser's convenience, the extent to which performance of work under the work-order and/or the contract is terminated and the date upon which such termination becomes effective. Purchaser reserves the right to cancel the remaining part and pay to the Bidder an agreed amount for partially completed Services.

13.20.5 Termination for violation of law/agreement

(a) In the event of any content found to be in violation of any law or direction of statutory authority or found to be in contravention of Intellectual Property Rights (IPR) etc., Purchaser may suspend / terminate the Agreement. The Purchaser reserves the right to terminate the Agreement for any breach or non-observance or non-fulfilment of Agreement conditions that may come to its notice through complaints or as a result of the regular monitoring. Notwithstanding any other rights and remedies provided elsewhere in the agreement, upon termination of the Agreement:
(b) Neither Party shall represent the other Party in any of its dealings.
(c) The expiration or termination of the Agreement for any reason whatsoever shall not affect any obligation of either Party having accrued under the Agreement prior to the expiration or termination of the Agreement and such expiration or termination shall be without prejudice to any liabilities of either Party to the other Party existing at the date of expiration or termination of the Agreement.
(d) Purchaser reserves the right to terminate the Contract in the event of data breach or stealing of data or unauthorised access.
(e) Payments for all satisfactorily completed services till the time of termination shall be made to the Bidder in the event of termination.

13.20.6 Consequences of termination

(a) In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], Purchaser shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from the termination/breach, and further allow the next successor Bidder to take over the obligations of the erstwhile Bidder in relation to the execution/continued execution of the scope of the Contract.
(b) Nothing herein shall restrict the right of the Purchaser to invoke the Bidder's PBG and/or Security Deposit, enforce the indemnity as defined under Section 13, and pursue such other rights and/or remedies that may be available to the Purchaser under law or otherwise.

(c) The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

(d) In case of termination, all hardware, software, tools and any other components for which the payment has been made by the Purchaser shall be the property of the Purchaser.

(e) Post the termination notice, the Bidder shall provide support, as per the exit management provisions hereunder.

13.21 Exit Management

13.21.1 The Bidder may also prepare a structured & detailed exit management plan along with the technical proposal as part of its Bid. Post signing of the contract, the exit management plan shall be finalized by the Bidder in consultation with the Purchaser.

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

13.21.3 Given the critical nature of the Service, it is imperative that a well-defined exit management strategy be made ready which shall enable easy transition of activities when the contract expires/ is truncated.

13.21.4 Accordingly, the Bidder shall submit an exit management plan within two months of Go-Live, which shall focus on the key activities it shall perform to ensure that a seamless transition of knowledge and activities be possible, and the same shall be evaluated. The exit management plan shall be based on the plan proposed by the Bidder in its technical proposal. The final exit management plan shall have to be mutually agreed upon by Purchaser and the Bidder.

13.21.5 The Bidder shall understand that ensuring a smooth transition at the end of the project period is a key requirement from Purchaser. The Bidder needs to update the exit management plan on half yearly basis or earlier or whenever required by Purchaser in case of major changes during the entire contract period. While proposing the exit management plan, the Bidder shall ensure that the subsequent points are taken care of.

13.21.6 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 Purchaser wants to take over the project itself, then Bidder has to ensure proper transition to the team designated by Purchaser.

13.21.7 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.

13.21.8 The Bidder shall provide all knowledge transfer of the system to the satisfaction of Purchaser as per the specified timelines.

13.21.9 The exit management period starts:

(a) In case of expiry of Contract, at least 12 Months prior to the date when the Contract comes to an end, or

(b) In case of termination of Contract, on the date when the notice of termination is sent to the Bidder.

13.21.10 The exit management period ends on the date agreed upon by the Purchaser or 12 Months after the beginning of the exit management period, whichever is earlier. In case of termination 12 Months exit period applies there also until Purchaser decides otherwise.

13.22 Applicability of the IT Act and Rules

13.22.1 Adherence to IT Laws and Government Regulations

The solution should comply to standards (ISO 27001:2013, ISO 22301:2019, ISO 20000- 1:2018, etc.) and regulations as notified by Government of India from time-to-time including but not limited to IT Act 2000 and its subsequent amendments, Digital Personal Data Protection Act 2023, RBI Guidelines, Ministry of Electronics and Information Technology (MEITY), CERT-In, NCIIPC, NIC, etc. Bidder need to ensure that offered solution as part of project scope and ensuing policies and procedures to have strict compliance to all cyber/information security policies, procedures and regulation and its subsequent updates issued by Government of India or its authorized agencies during the entire Project duration.

13.23 Intellectual Property Rights

13.23.1 Subject to the other provisions contained in this Clause, the Bidder shall agree that all deliverables created or developed by the Bidder, specifically for the Purchaser, together with any associated copyright and other intellectual property rights, shall be the sole and exclusive property of National Informatics Centre (Purchaser).

13.23.2 The Purchaser shall acknowledge that:

(a) In performing services under the Contract, the Bidder may use Bidder's proprietary materials including without limitation any software (or any part or component thereof), tools, methodology, processes, ideas, know-how and technology that are or were developed or owned by the Bidder prior to or independent of the services performed hereunder or any improvements, enhancements, modifications or customization made thereto as part of or in the course of performing the services hereunder, ("the Bidder's Pre-Existing IP").

(b) Notwithstanding anything to the contrary contained in the Contract, the Bidder shall continue to retain all the ownership, the rights title and interests on all the Bidder's Pre-Existing IP and nothing contained herein shall be construed as preventing or restricting the Bidder from using the Bidder's Pre-Existing IP in any manner.

(c) If any of the Bidder's Pre-Existing IP or a portion thereof is incorporated or contained in a deliverable under the Contract, the Bidder hereby grants to the User Department/Purchaser a non-exclusive, perpetual, royalty free, fully paid up, irrevocable license of the deliverables with the right to sublicense through multiple tiers, to use, copy, install, perform, display, modify and create derivative works of any such deliverables and only as part of the deliverables in which they are incorporated or embedded.

(d) Purchaser being the owner of all the IPs created in the deliverables, except the Pre- Existing IPs of the Bidder used in the development and deployment, shall have exclusive rights to use, copy, license, sell, transfer, share, deploy, develop, modify or any such act that the organisation/Purchaser may require or find necessary for its purpose. The IP rights of the Purchaser shall indefinitely subsist or continue in all future derivatives of the deliverables.

(e) The Bidder or its deployed resources shall have no claims whatsoever on the deliverables and all the IPs created in deliverables except its Pre-Existing IPs for which it shall grant all authorizations to the organisation/Purchaser for use as detailed in the Clause (c) above.

(f) Except as specifically and to the extent permitted by the Bidder, the organisation/Purchaser shall not engage in reverse compilation or in any other way arrive at or attempt to arrive at the source

code of the Bidder's Pre-Existing IP, or separate Bidder's Pre-Existing IP from the deliverable in which they are incorporated for creating a standalone product for marketing to others.

(g) The organisation/Purchaser shall warrant that the materials provided by the organisation/Purchaser to Bidder for use during development or deployment of the application shall be duly owned or licensed by the organisation/Purchaser.

(h) The Purchaser's contractual rights to use the Standard Software or element of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with relevant licence to a legally constituted successor organisation (e.g., a reorganisation of a public entity formally authorised by the government or through a merger acquisition of a private entity).

13.24 Transfer of Project documentation and data

13.24.1 Before the expiry of the exit management period, the Bidder shall deliver relevant records and reports pertaining to the Project and its design, implementation, operation, and maintenance including all operation, maintenance records and manuals pertaining thereto and complete as on the divestment date.

13.24.2 The Bidder shall provide the Purchaser with a complete and up to date list of the documents, data and relevant system details to be transferred to the Purchaser within 30 days of start of Exit Management Period.

13.24.3 The Bidder shall pass on to the Purchaser, the subsisting rights in any licensed products on terms not less favourable to the Purchaser, than that enjoyed by the Bidder.

13.24.4 Even during the Exit Management period, the Bidder shall continue to perform all their obligations and responsibilities as stipulated under the contract, and as may be proper and necessary to execute the Scope of Work in terms of the RFP, to execute an effective transition and to maintain business continuity.

13.24.5 All solutions provided by Bidder under the scope of the RFP should be /interoperable during the transfer/hand over at time of exit/contract termination. No proprietary Service is to be used/implement by the Bidder. Any customization/ tools/ effort required for smooth transfer of documentation and data arising out of interoperability issue will be borne by the Bidder.

13.24.6 All equipment and solutions utilised to deliver the project scope should have valid Service contract and should not be under end of life/end of support during contract period.

13.24.7 The Bidder shall share the details of all existing Service contracts and agreements executed with current vendors, sub-contractor, Service Provider to Purchaser on yearly basis.

13.25 Official secrets

13.25.1 The Service Provider shall ensure and inform all persons employed by it in any works in connection with the Contract that the Official Secrets Act, 1923 shall apply and continue to apply to them even after execution and expiry of the Contract or resignation by any employee and that they shall be bound to not disclose any information regarding this Contract to any third party. The Service Provider shall bring to the notice of the Purchaser any information found to be leaked or disclosed. Where such leakage or disclosure is brought to the notice of the Purchaser or the Purchaser detects any leakage or disclosure during the Contract Period (including any period for which the Contract is extended) or after its expiry, the person concerned as well as the Service Provider shall be liable for penal action. The Purchaser shall

have the liberty to terminate the Contract without notice, thereby invoking the exit management provisions of this Agreement.

13.26 Publicity

13.26.1 The Bidder shall not publicize any information pertaining to this Project or the Purchaser without seeking prior written consent of the Purchaser.

13.27 Restriction under rule 144 (xi) of the GFR 2017

13.27.1 Any Bidder or its OEM from a country which shares a land border with India will be eligible to bid in this RFP only if the Bidder is registered with the Competent Authority (i.e., Registration Committee constituted by Department for Promotion of Industry and Internal Trade (DPIIT)). Further, any Bidder (including Bidder from India) having specified Transfer of Technology (ToT) arrangement with an entity from a country which shares a land border with India, shall also require to be registered with the same Competent Authority. Please refer to the Govt. notifications provided at https://doe.gov.in/procurement-policy-divisions for details & updates [under Rule 144 (xi) of the General Financial Rules 2017]. The Bidder shall submit a certificate to this effect. If such certificate, given by a Bidder whose bid is accepted is found to be false, this would be a ground for debarment and further legal action in accordance with the law.

13.28 Compliance to Digital Personal Data Protection Act, 2023

13.28.1 Bidder shall ensure all the personal data is stored in compliance with Digital Personal Data Protection Act, 2023. The Bidder shall also ensure that personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and the access privileges to the back-end data segment are limited to the minimum necessary set of authorised users and are protected with multi-factor authentication.

14. Bill of Quantity (BOQ)

14.1 ICT Components

Table 8- BOQ

S. No.	Description	Quantity to be supplied
1.	Server Type 1	30
2.	Server Type 2	10
3.	Server Type 3	6
4.	Server Type 4	5
5.	Server Type 5	2
6.	Server Type 6	10
7.	Server Type 7	2
8.	Server type 8	10
9.	Server type 9	2
10.	Access Switches for GPU	10
11.	Access Switches for Servers	14

12.	Core Switches	4
13.	WAN router	2
14.	OOB Switch	8
15.	OOB Aggregation Switch	2
16.	Access Switches for Remote Locations	2 Per location total 10
17.	Object Storage (30 PB net usable)	1
18.	Firewall	2
19.	Load Balancer	10
20.	Web Application firewall	2
21.	Network Monitoring System	1
22.	Automation 300 end points	1

Note:

(a) All the supplied ICT components shall be provided with full feature and functionality, without any licensing restrictions/limitations. For delivering on the required SLA, each supplied solution shall include the required hardware, compute, storage, network, and other software licenses and other ICT equipment.

15. Technical Specifications

15.1 Server Type 1

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	Form Factor: The server hardware must be maximum 6U Rack Mountable system.	
2.		All the servers provided should be identical in all specifications including model , make form factor etc.	
3.	Processors	The system should be provided with a dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon Gold / Platinum scalable series Latest Gen with a minimum of 48 cores, 96 threads, 2.4+ GHz base frequency, and minimum 30 MB cache per cpu.	
		Option 2: AMD LatestGen EPYC with a minimum of 48 cores, 96 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
4.	Memory RAM	The system should be supplied with minimum 1.5 TB of DDR4/DDR5 RAM	
5.		It should have memory slots available for future expansion.	
6.	Expansion Slots	4 *dual-port 10G SFP+ & 2*1G/10G RJ45	
7.		The system should have a minimum of 4 PCIe x8 Full Height Expansion slots.	
8.		It should also have a minimum of 2 PCIe x16 Full Height Expansion Slots.	
9.		All expansion slots must support Gen 3.0 or above.	
10.	RAID Controller	The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 4GB Cache	
		The RAID controller should support RAID levels 'O', '1 ', '10', '5', '50', '6', and '60'.	
11.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements:	
		Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
12.	Storage	The server should have a minimum of 80 internal / DAS disks with capacities 20+ TB (minimum) Enterprise HDDs	
13.		The Hot-Plug disks should be Enterprise HDD, SAS 12+ Gb/s Connectivity, 7200+ RPM and a 3.5-inch form factor.	

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
14.		Performance HW Raid controller= RAID 0, 1,5,6 ,10, 50, 60, SATA / SAS-3 connectivity, 4+ GB cache, battery or flash backed protection, for the disks.	
15.		All 60 HDDs should be connected to the performance HW raid controller and should be able to configure a sing le RAID volume of RA ID 60 with all the disks.	
16.	Accessories	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
17.		Baseboard management console with dedicated RJ45 interface, (IPMl), Browser (HTML5) based Server Console access over HTTPS	
18.	Power Supply	The server must have hot-swappable redundant power supplies	
19.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit iii) All Systems Management including server, power, update and IPMI should be done from single management console iv) Systems Management should support 2 factor authentication. v) Should have virtual Media support with all required Licenses. vi) Remote KVM vii) Server Health Logging viii) Out of Band Management	
20.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgrades, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. vii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc.) viii) Real-time-out-of-band hardware performance monitoring & alerting	

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy based security v) Server should provide server intrusion detection vi) Rapid OS Recovery, dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery, Real time firmware security scanning	
21.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating iii) System on predefined security breach Secure/Automatic BIOS recovery iv) Network Card secure firmware boot	
22.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OS & Hypervisior vendor	

15.2 Server Type 2

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	The server hardware must be a maximum 2U Rack Mountable system.	
2.		All the servers provided should be identical in all specifications including model , make form factor etc.	
3.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon EPYC scalable series Latest Gen with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen EPYC with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
4.	Memory (RAM)	The system should be provided with 128 GB DDR4/DDR5	
5.		It should have a memory slots available for future expansion.	
6.	NIC	2*dual-port 10G SFP+ & 2*1G/10G RJ45	
7.	RAID Controller:	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels 'O', '1 ', '5', '6'.	

		The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 8GB Cache	
8.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
9.		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
10.	Storage:	The server should have a minimum of 4 disks with minimum capacities 20+ TB Enterprise HDDs	
11.		The Hot-Plug disks should be Enterprise HDD, SAS 12+ Gb/s Connectivity, 7200+ RPM and a 3.5-inch form factor.	
12.		All 4 HDDs should be connected to the performance HW raid controller and should be able to configure a single RAID volume of RAID 6 with all disks.	
13.	Accessories	The System includes a requirement for a Rai ls Kit to facilitate rack mounting.	
14.		Baseboard management console with dedicated RJ 45 interface, (IPMI) Browser (HTMLS) based Server Console access over HTTPS	
15.	Power Supply	The server must have hot-swappable redundant power supplies	
16.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management vii) All Systems Management including server, power, update and IPMI should be done from single management console. viii) Systems Management should support 2 factor authentication.	
17.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites.	

		ii) Automated infrastructure management for patch upgrades, version upgrades, etc. iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. lthe user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) viii) Real-time-out-of-band hardware performance monitoring & alerting	
18.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy-based security v) Server should provide server intrusion detection vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
19.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach iii) Secure/Automatic BIOS recovery iv) Network Card secure firmare boot	
20.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OS & Hypervisior vendor	

15.3 Server Type 3

S. No.	Server Requirements	Specifications	Compliance (Yes/No)

1.	Form Factor	The server hardware must be a maximum 2U Rack Mountable system.	
2.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon scalable series Latest Gen with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen EPYC with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
3.	Memory (RAM)	The system should be configured with 256 GB DDR4/DDR5 memory	
4.		It should have memory slots available for expansion.	
5.	Expansion Slots	2*dual-port 10G SFP+ & 2*1G/10G RJ45	
6.	RAID Controller	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels 'O', '1 ', '5', '6'. The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 8GB Cache	
7.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
8.		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
9.	Accessories:	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
10		Baseboard management console with dedicated RJ 45 interface, (IPMI), Browser (HTMLS) based Server Console access over HTTPS	
11	Power Supply	The server must have hot-swappable redundant power supplies.	
12	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management vii) All Systems Management including server, power, update and IPMI should be done from single management console.	

		viii) Systems Management sholud support 2 factor authentication.	
13	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgrades, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) ix) Real-time-out-of-band hardware performance monitoring & alerting	
14	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy-based security v) Server should provide server intrusion detection vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
15	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach iii) Secure/Automatic BIOS recovery iv) Network Card secure firmare boot	
16	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OS & Hypervisior vendor	

15.4 Server Type 4

S. No.	Server Requirements	Specifications	Compliance (Yes/ No)
1.	Form Factor	The server hardware must be a maximum 10U Rack Mountable system.	
2.	Processors	2* intel Xeon Platinum 8352Y 32 core 2.2 GHz Max turbo Frequency 3.4 Ghz cache 48 MB ,205 TDP	
3.	Memory (RAM)	The system should be provided with minimum of 2TB of DDR4/DDR5 RAM.	
4.		It should have memory slots available for expansion.	
5.		The server must be capable of supporting up to 1536 GB of DDR4/DDR5	
6.	Expansion Slots	The system should have a minimum of 4 PCIe x8 Full Height Expansion slots	
7.		2x25 G Dual port cards	
8.		4xConnectX 7 200 Gb/sec NDR 200 IB dual port (8*100/400 Gig)	
9.		It should also have a minimum of 2 PCIe x16 Full Height Expansion Slot.	
10.		All expansion slots must support Gen 3.0 or Higher.	
11.	Bootable Storage System	It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity, Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 nos of SSDs, sequential, Block size 64KB, Queue depth 64: 400+ MB/sec - Total read speed after RAID 1 with 2 nos of SSDs, sequential, Block size 64KB, Queue depth 64: 900+ MB/sec	
12.	Storage	The server should have a minimum Internal / External capacity of minimum 144 TB in Raid 6 for Data	
13.		The Hot-Plug disks should be SAS 7.2K RPM with a 12Gbps interface and a 3.5-inch form factor.	
14.		All HDDs should be connected to HW raid controller and should be able to configure a single virtual volume of raid 6 / raid 5 with all the disks	
15.	Accessories	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
16.		Baseboard management console with dedicated RJ45 interface, (IPMI), Browser (HTML 5) based Server Console access over HTTPS	
17.	Power Supply	The server should have hot-swappable redundant power supplies.	

18.	GPU Requirements (Number of GPUs: 8 unit of GPU in each server)	Minimum Specification of the GPU model (NVIDIA H100 or any higher NVIDIA model with a memory capacity of at least 80GB	
		Performance (FP16): 1,979 Tera FLOPS or more	
		ECC Protection: Supported	
19.	Infini band	Required infini band switches to be provided with the server	
20.	Management Platform	The proposed software management platform should be able to handle CPU and GPU based workloads with a central console Software Management platform should provide both container and virtualization for GPUs and CPUs in conjunction. Software Platform should have operator framework for various applications and runtimes Software Platform should have capabilities to scan runtimes vulnerabilities Software Platform should provide MLOPS capability out of the box with 24 x 7 support from OEM The AI/ML Platform must give the provision to optimize the performance of your compute intensive data science models using GPU & HPU acceleration & must support various hardware accelerators such as NVIDIA, Intel, AMD for GPU flexibility for current and future needs.	
21.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management	

22.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgardes, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) ix) Real-time-out-of-band hardware performance monitoring & alerting	
23.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy based security v) Server should provide server intrusion detection	
24.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating iii) System on predefined security breach iv) Secure/Automatic BIOS recovery v) Network Card secure firmware boot	
25.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OS & Hypervisior vendor	

15.5 Server Type 5

S. No.	Server Requirements	Specifications	Compliance (Yes/ No)
1.	Form Factor	The server hardware must be a maximum 10U Rack Mountable system.	
2.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon gold / Platinum scalable series Latest Gen with a minimum of 28 cores, 56 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest generation with minimum of 28 core, 56 threads 2.4 GHz base frequency and 128 MB cache.	
3.	Memory (RAM)	The system should be provided with minimum of 2TB of DDR4/DDR5 RAM.	
4.		It should have memory slots available for expansion.	
5.		The server must be capable of supporting up to 1536 GB of DDR4/DDR5	
6.	Expansion Slots	The system should have a minimum of 4 PCIe x8 Full Height Expansion slots	
7.		2x25 G Dual port cards	
8.		4xConnectX 7 200 Gb/sec NDR 200 IB dual port (8*100/400Gig)	
9.		It should also have a minimum of 2 PCIe x16 Full Height Expansion Slot.	
10.		All expansion slots must support Gen 3.0 or Higher.	
11.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1. It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
12.	Storage	The server should have a minimum Internal / External capacity of 256 TB in raid 6	
13.		The Hot-Plug disks should be SAS 7.2K RPM with a 12Gbps interface and a 3.5-inch form factor.	
14.		All HDDs should be connected to HW raid controller and should be able to configure a single virtual volume of raid 6 / raid 5 with all the disks	

15.	Accessories	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
16.		Baseboard management console with dedicated RJ45 interface, (IPMl), Browser (HTML 5) based Server Console access over HTTPS	
17.	Power Supply	The server should have hot-swappable redundant power supplies.	
18.	GPU Requirements (Number of GPUs: 8 unit of GPU in each server)	Minimum Specification of the GPU model (NVIDIA H100 or any higher NVIDIA model with a memory capacity of at least 80GB	
		Performance (FP16): 1,979 Tera FLOPS or more	
		ECC Protection: Supported	
19.	Infini band	Required infini band switches to be provided with the server	
20.	Management Platform	The proposed software management platform should be able to handle CPU and GPU based workloads with a central console Software Management platform should provide both container and virtualization for GPUs and CPUs in conjunction. Software Platform should have operator framework for various applications and runtimes Software Platform should have capabilities to scan runtimes vulnerabilities Software Platform should provide MLOPS capability out of the box with 24 x 7 support from OEM The AI/ML Platform must give the provision to optimize the performance of your compute intensive data science models using GPU & HPU acceleration & must support various hardware acclerators such as NVIDIA, Intel, AMD for GPU flexibility for current and future needs.	
21.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management	

22.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgardes, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagonistic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) ix) Real-time-out-of-band hardware performance monitoring & alerting	
23.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy based security v) Server should provide server intrusion detection	
24.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating iii) System on predefined security breach iv) Secure/Automatic BIOS recovery v) Network Card secure firmware boot	
25.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OEM	

15.6 Server Type 6

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	The server hardware must be maximum 6U Rack Mountable system.	

2.		All the servers should be identical in make, model and form factor	
3.	Processors	The system should support a dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon / Platinum scalable series Latest Gen with a minimum of 48 cores, 96 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen Epyc with a minimum of 48 cores, 96 threads,	
		2.4+ GHz base frequency, and 30+ MB cache.	
4.	Memory (RAM):	The system should be provided with 1.5 TB of DDR4/DDR5 RAM.	
5.		It should have memory slots available for expansion.	
6.		The server must be capable of supporting up to 1536 GB of DDR4/DDR5 Memory.	
7.	Expansion Slots	The system should have a minimum of 4 PCIe x8 Full Height Expansion slots.	
8.		It should also have a minimum of 2 PCIe x16 Full Height Expansion Slots.	
9.		All expansion slots must support Gen 3.0 or higher	
10.		4*dual-port 10G SFP+ & 2*1G/10G RJ45	
11.	RAID Controller	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels 'O', '1 ', '10', '5', '50', '6', and '60'.	
12.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
13.		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
14.	Storage	The server should have a minimum 80 disks Internal / External capacity.	
		Each disk to be of min 20 TB size	
		TheadditionL Hot-Plug disks should be SAS 7.2K RPM with a 12Gbps interface and a 3.5-inch form factor.	
		Performance HW Raid controller= RA ID 0, 1,5,6,10, 50, 60, SATA/SAS-3. connectivity, 4+ GB cache, battery or flash backed protection, for the disks.	

		All HDDs should be connected to HW raid controller and should be able to configure a single virtual volume of raid 6 / raid 5 with all the disks	
15.	Accessories	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
16.		Baseboard management console with dedicated RJ45 interface, (IPMl), Browser (HTML 5) based Server Console access over HTTPS	
17.	Power Supply	The server must feature dual power hot-swappable redundant power supplies	
18.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management vii) All Systems Management including server, power, update and IPMI should be done from single management console viii) Systems Management should support 2 factor authentication	
19.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgardes, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagonistic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc.) ix) Real-time-out-of-band hardware performance monitoring & alerting	

20.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy based security v) Server should provide server intrusion detection vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
21.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach iii) Secure/Automatic BIOS recovery iv) Network Card secure firmare boot	
22.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OEM	

15.7 Server Type 7

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	The server hardware must be a maximum 2U Rack Mountable system.	
2.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon scalable series Latest Gen with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen EPYC with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
3.	Memory (RAM)	The system should be configured with 512 GB DDR4/DDR5 memory	
4.		It should have memory slots available for expansion.	
5.	NIC	2*dual-port 10G SFP+ & 2*1G/10G RJ45	
6.	RAID Controller	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels ‘O’, ‘1 ‘, ‘5’, ‘6’. The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 8GB Cache	

7.		The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
8.	Boot Storage Subsystem	It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
9.	Accessories:	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
10.	Storage:	The server should have minimum of 4 disks with 20TB+ Enterprise HDD The Hot-Plug disks should be Enterprise HDD, SAS 12+ Gb/s Connectivity, 7200+ RPM and a 3.5-inch form factor. All 4 HDDs should be connected to the performance HW raid controller and should be able to configure a single RAID volume of RAID 6 with all disks	
11.		Baseboard management console with dedicated RJ 45 interface, (IPMI), Browser (HTMLS) based Server Console access over HTTPS	
12.	Power Supply	The server must have hot-swappable redundant power supplies.	
13.	Management Features-1	(i) Remote power on/Shutdown of server. (ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port (iii) Should have virtual Media support with all required Licenses. (iv) Remote KVM (v) Server Health Logging (vi) Out of Band Management (vii) All Systems Management including server, power, update and IPMI should be done from single management console. (viii) Systems Management should support 2 factor authentication	

14.	Management Features-2	(i) Management of multiple Servers from single console with single source of truth for multiple sites. (ii) Automated infrastructure management for patch upgrades, version upgrades, etc (iii) Simplified management with analytics driven actionable intelligence. (iv) Platform inventory and health status (v) Server utilization statistics collection (including firmware updates and diagnostic tools) (vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. (vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. (viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) (ix) Real-time-out-of-band hardware performance monitoring & alerting	
15.	Security Features-1	(i) Secure Boot (Firmware and BIOS Level Security) (ii) Provision to lock the system on breach (iii) Hardware root of trust/Dual Root of Trust (iv) Server should provide policy-based security (v) Server should provide server intrusion detection (vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
16.	Security Features-2	(i) Provision for Cryptographic firmware updates (ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach (iii) Secure/Automatic BIOS recovery (iv) Network Card secure firmware boot	
17.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OS & Hypervisior vendor	

15.8 Server type 8

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	The server hardware must be a maximum 2U Rack Mountable system.	

2.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon scalable series Latest Gen with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen EPYC with a minimum of 32 cores, 64 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
3.	Memory (RAM)	The system should be configured with 512 TB DDR4/DDR5 memory	
4.		It should have memory slots available for expansion.	
5.	NIC	2*dual-port 10G SFP+ & 2*1G/10G RJ45	
6.		The system should have minimum 4 * PCIe x8 full height expansion slots , it should also have minimum 2 PCIe x16 full height expansion slots all the slots must support Gen 3.0.	
7.	RAID Controller	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels 'O', '1 ', '5', '6'. The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 8GB Cache	
8.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
9.		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
10.	Accessories:	The System includes a requirement for a Rails Kit to facilitate rack mounting.	
11.	Storage:	The server should have minimum of 80 TB with minimum 20 TB+ Enterprise HDD in raid 6 The Hot-Plug disks should be Enterprise HDD, SAS 12+ Gb/s Connectivity, 7200+ RPM and a 3.5-inch form factor. All 4 HDDs should be connected to the performance HW raid controller and should be able to configure a single RAID volume of RAID 6 with all disks	
12.		Baseboard management console with dedicated RJ 45 interface, (IPMI), Browser (HTMLS) based Server Console access over HTTPS	
13.	Power Supply	The server must have hot-swappable redundant power supplies.	

14.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management vii) All Systems Management including server, power, update and IPMI should be done from single management console. viii) Systems Management sholud support 2 factor authentication via e-mail	
15.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgrades, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) ix) Real-time-out-of-band hardware performance monitoring & alerting	
16.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy-based security v) Server should provide server intrusion detection vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
17.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach iii) Secure/Automatic BIOS recovery iv) Network Card secure firmare boot	

18.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OEM	

15.9 Server type 9

S. No.	Server Requirements	Specifications	Compliance (Yes/No)
1.	Form Factor	The server hardware must be a maximum 2U Rack Mountable system.	
2.	Processors	The system should be provided with dual-socket configuration. The processor options include:	
		Option 1: Intel Xeon scalable series Latest Gen with a minimum of 28 cores, 56 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
		Option 2: AMD Latest Gen EPYC with a minimum of 28 cores, 56 threads, 2.4+ GHz base frequency, and 30+ MB cache.	
3.	Memory (RAM)	The system should be configured with 1 TB DDR4/DDR5 memory	
4.		It should have memory slots available for expansion.	
5.	NIC	2*dual-port 10G SFP+ & 2*1G/10G RJ45	
6.		The system should have minimum 4 * PCIe x8 full height expansion slots , it should also have minimum 2 PCIe x16 full height expansion slots all the slots must support Gen 3.0.	
7.	RAID Controller	The server must be equipped with a Performance RAID Controller. The RAID controller should support RAID levels ‘O’, ‘1 ‘, ‘5’, ‘6’. The server must be equipped with a dedicated Performance Hardware RAID Controller with minimum 8GB Cache	
8.	Boot Storage Subsystem	The system must have a Boot Storage subsystem configured with Redundant Hardware RAID 1.	
9.		It should include 2 Enterprise SAS SSDs/M.2 NVME with each SSD meeting the specified technical requirements: Minimum of 960GB Capacity ,Mixed Use (Read+Write Intensive) - Total write speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 400+ MB/sec - Total read speed after RAID 1 with 2 no:s of SSDs, sequential, Block size 64KB, Queue depth 64 : 900+ MB/sec	
10.	Accessories:	The System includes a requirement for a Rails Kit to facilitate rack mounting.	

11.	Storage	The server should have minimum of 256 TB disks with minimum 16TB+ Enterprise HDD The Hot-Plug disks should be Enterprise HDD, SAS 12+ Gb/s Connectivity, 7200+ RPM and a 3.5-inch form factor. All 4 HDDs should be connected to the performance HW raid controller and should be able to configure a single RAID volume of RAID 6 with all disks	
12.		Baseboard management console with dedicated RJ 45 interface, (IPMI), Browser (HTMLS) based Server Console access over HTTPS	
13.	Power Supply	The server must have hot-swappable redundant power supplies.	
14.	Management Features-1	i) Remote power on/Shutdown of server. ii) Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port iii) Should have virtual Media support with all required Licenses. iv) Remote KVM v) Server Health Logging vi) Out of Band Management vii) All Systems Management including server, power, update and IPMI should be done from single management console. viii) Systems Management sholud support 2 factor authentication via e-mail	
15.	Management Features-2	i) Management of multiple Servers from single console with single source of truth for multiple sites. ii) Automated infrastructure management for patch upgrades, version upgrades, etc iii) Simplified management with analytics driven actionable intelligence. iv) Platform inventory and health status v) Server utilization statistics collection (including firmware updates and diagnostic tools) vi) Solution should be open and programmable providing Rest API, SDK for programming languages like Python, power shell scripts etc. vii) Should have customizable dashboard to show overall faults/heath/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. viii) The user should be flexibility to select name for dashboards and widgets (viz. health, utilization etc) ix) Real-time-out-of-band hardware performance monitoring & alerting	

16.	Security Features-1	i) Secure Boot (Firmware and BIOS Level Security) ii) Provision to lock the system on breach iii) Hardware root of trust/Dual Root of Trust iv) Server should provide policy-based security v) Server should provide server intrusion detection vi) Rapid OS Recovery , dynamically enabled USB ports, digitally signed firmware updates, automatic BIOS recovery , Real time firmware security scanning	
17.	Security Features-2	i) Provision for Cryptographic firmware updates ii) Capability to stop execution of Application/Hypervisor/Operating lSystem on predefined security breach iii) Secure/Automatic BIOS recovery iv) Network Card secure firmare boot	
18.	OS & Hypervisior compatibility	• Canonical Ubuntu Server LTS • Microsoft Windows Server with Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi The Support should be available on the website of the respective OEM	

15.10 Access Switches for GPU

S.No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	**General Requirement**	The Switch should support non-blocking architecture, all proposed ports must provide wire speed line rate performance	
2.		Switch should support the complete STACK of IP V4 and IP V6 services.	
3.		All relevant licenses for all the features and scale should be quoted along with switch	
4.		Switch should be part of same VXLAN EVPN fabric comprising of both GPU access switches as well as server access switches	
5.	**Hardware and Interface Requirement**	The proposed Switch should provide 32 * 400G QSFP-DD ports with support for 200G/100G/40G . Switch should be populated with minimum 20*400G QSFP-DD and 6*100G QSFP transceiver	
6.		Switch should have console port for local management & management interface for Out of band management	
7.		Switch should have adequate power supplies for the complete system usage and providing N+1 power supply redundancy	
8.	**Performance Requirement**	Switch should support minimum 500 VRF instances with route leaking functionality	
9.		The switch should support minimum 200K IPv4 LPM routes	

10.		The switch proposed should have minimum 120 MB Packet Buffer	
11.		The switch should support 8k multicast routes	
12.		Switch should support a minimum of 25 Tbps BW	
13.	**Network Virtualization Features**	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
14.		Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center	
15.	**Layer 2 Features**	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
16.		Switch should support VLAN Trunking (802.1q)	
17.		Switch should support minimum 150K no. of MAC addresses	
18.		Switch should support VLAN tagging (IEEE 802.1q)	
19.		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
20.		Switch should support layer 2 extension over VXLAN across all Data Center to enable VM mobility & availability	
21.		The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
22.		Switch should support static and dynamic routing	
23.		Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Support Multicast Source Discovery Protocol (MSDP) Switch should support Multicast routing	
24.	**Quality of Service**	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)	
25.		Switch should support for different type of QoS features for real time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
26.		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	

27.	**Security**	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
28.		Switch should support for external database for AAA using:	
29.		a. TACACS+	
30.		b. RADIUS	
31.		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
32.	**Manageability**	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
33.		Switch should provide remote login for administration using Telnet and SSHv2	
34.		Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP v3 with Encryption	

15.11 Access switches for Servers

S. No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	**Solution Requirement**	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2.		Switch should support the complete STACK of IPv4 and IPv6 services.	
3.		Switch Should be fully populated	
4.		The Switch used have the capability to function in line rate for all ports	
5.	**Hardware and Interface Requirement**	Minimum 48 ports support 1/10/25 Gbps SFP/SFP+/SFP28 ports for host connectivity and 6* 40/100G ports for Core/Spine connectivity. The proposed switch should support native 25G and should be populated with 48*25G Multimode fiber transceivers for downlink connectivity & 4*100G ports with multimode 100G Transceivers, for uplink connectivity.	
6.		Switch should have console port for local management & management interface for Out of band management	
7.		1 RU fixed form factor	
8.		Switch should be rack mountable and support side rails if required	
9.		Switch should be provided with power redundancy	

10.	**Performance Requirement**	Modular OS with dedicated process for each routing protocol	
11.		Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	
12.		Switch should support minimum 500 VRF instances with route leaking functionality	
13.		The switch should support minimum 200k IPv4 routes	
14.		The Switch should support intelligent buffer management with a minimum buffer of 32MB.	
15.		The switch should have MAC Address table size of 90k	
16.		The switch should support 8K multicast routes	
17.		Switch should support 64 nos of ECMP paths	
18.		Switch should support minimum 3 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity)	
19.	**Network Virtualization Features**	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
20.		Switch should support VXLAN and EVPN symmetric IRB/Asymmetric IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center	
21.	**Layer 2 Features**	Switch should support Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) and VLAN Trunking (802.1q)	
22.		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
23.		Switch should support minimum 90k of MAC addresses	
24.		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
25.		Switch should support layer 2 extension over VXLAN across all DataCenter to enable VM mobility & availability	
26.		The Switch should support DC Briding i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Explicit Congestion Notification (ECN).	
27.		The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
28.	**Layer 3 Features**	Switch should support static and dynamic routing	

29.		Switch should support multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
30.		Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM	
31.		Support Multicast Source Discovery Protocol (MSDP)	
32.		IGMP v1, v2 and v3	
33.	**Quality of Service**	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)	
34.		Switch should support for different type of QoS features for reaL time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
35.		Switch should support Rate Limiting - Policing and/or Shaping	
36.		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
37.	**Security**	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
38.		Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
39.		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
40.		Switch platform provide the capability to should support MAC Sec (802.1AE) encryption in hardware or MAC Filter or MAC ACL	
41.		Switch should support Dynamic ARP Inspection or similar feature to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol	
42.		Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	

43.		Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port or should support storm control (broadcast, unicast , multicast)	
44.	**Manageability**	Switch must have Switched Port Analyzer (SPAN)/ mirror with minimum 4 active session	
45.		Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
46.		The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	
47.		All the components should be from same OEM for ease of management and interoperability	

15.12 Core Switches

S.No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	General Requirement	The Switch should support non-blocking architecture, all proposed ports must provide wire speed line rate performance	
2.		Switch should support the complete STACK of IP V4 and IP V6 services.	
3.		All relevant licenses for all the features and scale should be quoted along with switch	
4.		Switch and optics should be from the same OEM	
5.		Switch should be part of same VXLAN EVPN fabric comprising of both GPU Access Switches as well as Server Access Switches.	
6.		Switch should run same OS as other Access/Leaf switches as part of the overall solution with single management and monitoring plane.	
7.	Hardware and Interface Requirement	The proposed Switch should provide minimum 64 * 400G QSFP-DD ports with support for 200G/100G/40G . Switch should be populated with minimum 40*400G QSFP-DD and 24*100 QSFP transceivers.	
8.		Switch should have console port for local management & management interface for Out of band management	
9.		Switch should have adequate power supplies for the complete system usage and providing N+1 power supply redundancy	
10.	Performance Requirement	Switch should support minimum 500 VRF instances with route leaking functionality	

11.		The switch should support minimum 200K ipv4 and ipv6 LPM routes	
12.		The Switch should support intelligent buffer management with a minimum buffer of 120MB.	
13.		The switch should support 8k multicast routes	
14.		Switch should support a minimum of 50 Tbps BW	
15.	Network Virtualization Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN	
16.		Switch should support VXLAN and EVPN symmetric IRB for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data center	
17.	Layer2 Features	Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
18.		Switch should support VLAN Trunking (IEEE 802.1q)	
19.		Switch should support minimum 200K no. Of MAC addresses	
20.		Switch should support VLAN tagging (IEEE 802.1q)	
21.		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
22.		Switch should support layer 2 extension over VXLAN across all datacenter to enable VM mobility & availability	
23.		The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
24.		Switch should support static and dynamic routing	
25.		Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Support Multicast Source Discovery Protocol (MSDP) Switch should support Multicast routing	
26.	Quality of Service	Switch system should support 802.1P classification and marking of packet using: a. Cos (Class of Service) b. DSCP (Differentiated Services Code Point)	
27.		Switch should support for different type of qos features for ream time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
28.		Switch should support to trust the qos marking/priority settings of the end points as per the defined policy	
29.	Security	Switch should support control plane Protection from unnecessary or dos traffic by control plane protection policy	
30.		Switch should support for external database for AAA using:	
31.		A. TACACS+	
32.		B. RADIUS	

33.		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
34.	Manageability	Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
35.		Switch should provide remote login for administration using Telnet and sshv2	
36.		Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP v3 with Encryption	

15.13 WAN Router

S.No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	**General Requirement**	The Proposed Router should support multi-core Processor, internal redundant field replaceable power supply (from Day1).	
2.	**Hardware and Interface Requirement**	Router should have minimum 20 x 10G and 6 x 40 / 100G QSFP28 LAN / WAN Interface loaded with 10 x 1 G Multimode Fiber SFP, 10 x 10G Multimode Fiber SFP+, 4 x 40G QSFP28 and 2 x 100G QSFP56	
3.	**Performance Requirement**	Router should have minimum IP forwarding throughput of 500 gbps	
4.		The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should able to create GRE tunnel.	
5.		The router should support 300 Gbps of IPSEC Bandwidth	
6.		Router should support VRF level segmentation with min support for 4000 VRF segments	
7.		Router should support IGMP v1/v2/v3 and PIM multicast routing	
8.	**Layer3 Features & Security**	Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunneling , MPLS, RSVP, DHCP, L2 and L3 VPN, BFD, Segment routing, EVPN and VxLAN from Day 1	
9.		The Router should support Zone Based Firewall feature or an external appliance for the same functionality can be provided.	
10.		Shall have 802.1p class of Service and marking, classification, policing and shaping.	

11.		Should support advanced encryption algorithms like AES-256 and AES-GCM	
12.		The router should be able to support Hierarchical QoS. QoS should be supported both at Physical and sub-interface level	
13.	**Manageability**	Router should support SSHv2, SNMPv2c, SNMPv3 and NTP	
14.		Routers should support AAA using RADIUS and TACACS+	
15.		Should have extensive support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss.	
16.		Router should support monitoring of network traffic with application-level insight with deep packet visibility.	
17.		Router should have ability to track SNMP, Syslog, interface counters or IP SLA	
18.	**Certification**	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	
19.		Router shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
20.		Router/Router's Operating System should be tested and certified for EAL 3/NDPP or above under Common Criteria Certification	
21.		Router should be IPv6 Certified/IPv6 logo ready.	

15.14 OOB Switch

S.No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	General Features	Switch should be 1U and rack mountable in standard 19" rack.	
2.		Switch should support internal field replaceable unit redundant power supply from day 1.	
3.		Switch should have minimum 2 GB RAM and 2 GB Flash.	
4.		Should be fully populated	
5.		Switch should have dedicated slot for modular stacking or should support virtual stacking, in addition to asked uplink ports. Should support for minimum 40 Gbps of stacking throughput with minimum 2 switch in single stack	

6.	Performance	Switch shall have minimum 176 Gbps of switching fabric and 130 Mpps of forwarding rate.	
7.		Switch shall have minimum 16K MAC Addresses and 250 active VLAN.	
8.		Should support minimum 3K IPv4 routes or more	
9.		Switch shall have 1K or more multicast routes.	
10.		Switch should support netflow/jflow/sflow or equiv. for traffic monitoring	
11.		Switch should support 128 or more STP/VSTP/MSTP Instances.	
12.		Switch should have 4MB or more packet buffer.	
13.	Functionality	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.	
14.		Switch must have functionality like static routing, RIP, PIM, OSPF, PBR and QoS features from Day1.	
15.		Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	
16.		Switch shall have 802.1p class of Service, marking, classification, policing and shaping and eight egress queues.	
17.		Switch should support management features like SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+	
18.		Switch should support IPv6 Binding Integrity Guard/DHCPv6 snooping,IPv6 RA Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	
19.		Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128/MAC ACLs on hardware for all ports.	
20.		During system boots or OS upgrades, the system's software should be checked for integrity.	
21.	Interface	Switch shall have 48 nos. 10/100/1000 Base-T ports and additional 4 nos. 10 uplinks ports.	

22.	Certification	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	
23.		Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
24.		Switch / Switch's Operating System should be tested for EAL 2/NDPP or above under Common Criteria Certification.	

15.15 OOB Aggregation Switch

S.No.	Parameters/Category	Specification	Compliance (Yes/No)
1.	**Hardware and Form factor Specifications**	The proposed switch should be of 1RU form Factor	
2.		The switch should have minimum of 24 nos. 1G/10G/25G SFP28 Ports and additional 2 nos. of 40G/100G QSFP+/QSFP28 ports	
3.		Switch should provide redundant power supplies from Day-1	
4.		Switch should provide redundant fans from Day-1	
5.		Switch should be provided with AC power supply and India power cords	
6.		The switch should have 16 GB of DRAM and 16GB of Flash memory to store image and logs	
7.		Proposed switch should be enterprise grade switch	
8.		Switch should have dedicated slot for modular stacking or should support virtual stacking, in addition to asked uplink ports	
9.		Switch should have atleast 400 Gbps stacking performance.	
10.		Switch should be provided with necessary stacking module and cables from day-1 or switch should support virtual stacking to support at least 2 switches in a single stack.	
11.		Switch should support 2 members in stack	
12.		Switch should support cross-stack etherchannel/ MC-LAG.	
13.		Switch should support event manager scripts	
14.	**Performance Parameters**	The switch should support non-blocking switching bandwidth up to 2000 Gbps (without considering stacking bandwidth)	
15.		The switch should support wire-speed Forwarding Rate up to 1000 Mpps	
16.		Switch should be able to support 24000 IPV4 Routes or 18000 IPV6 routing entries.	

17.		Switch should support minimum 1000 Switched Virtual Interfaces.	
18.		The switch should support Jumbo frames of 9198 bytes	
19.		The switch should support 32000 Unicast MAC addresses	
20.		Switch shall support application visibility and traffic monitoring using netFlow/sflow/jflow entries.	
21.		Switch should have 16MB or more packet buffer.	
22.	**General Features**	Switch should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z	
23.		Switch must have functionality like static routing, Static Routes,PIM, PBR and QoS features from Day1	
24.		Switch should support advanced functionalities like VXLAN, VRFs, OSPF	
25.		Should be fully populated	
26.		Switch shall have 802.1p class of Service, marking, classification, policing and shaping and eight egress queues.	
27.		Switch should support management features like SSH, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS.	
28.		Switch should support IPv6 Binding Integrity Guard/DHCPv6 snooping, IPv6 RA Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	
29.		Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec/MAC ACL on hardware for all ports.	
30.		Switch should provide a feature that enable hardware and software authenticity assurance for supply chain trust and strong mitigation against attacks that compromise software and firmware by providing capabilities image signing or Secure Boot etc.	
31.	**Environment and Certifications**	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	
32.		IPv6 Certified from Day 1	
33.		Switch shall conform to EN 55032 Class A/B or CISPR32 Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	
34.		Operating temperature of 0°C to 40°C.	
35.		Switch or Switch's Operating System should be tested for EAL 2/NDPP/NiAPP or above under Common Criteria Certification.	

15.16 Access Switches for Remote Locations

S. No.	Parameters/ Category	Specification	Compliance (Yes/No)
1.	**Solution Requirement**	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2.		Switch should support the complete STACK of IPv4 and IPv6 services.	
3.		The Switch used have the capability to function in line rate for all ports	
4.	**Hardware and Interface Requirement**	Minimum 24 ports support 1/10/25 Gbps SFP/SFP+/SFP28 ports for host connectivity and 6* 40/100G ports for Core/Spine connectivity. The proposed switch should support native 25G and should be populated with 24*25G Multimode fiber transreceivers for downlink connectivity & 4*100G ports with multimode 100G Trancievers, for uplink connectivity.	
5.		Switch should have console port for local management & management interface for Out of band management	
6.		1 RU fixed form factor	
7.		Switch should be rack mountable and support side rails if required	
8.		Switch should be provided with power redundancy	
9.	**Performance Requirement**	Modular OS with dedicated process for each routing protocol	
10.		Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP)	
11.		Switch should support minimum 500 VRF instances with route leaking functionality	
12.		The switch should support 350k IPv4 LPM routes	
13.		The Switch should support intelligent buffer management with a minimum buffer of 32 MB.	
14.		The switch should have MAC Address table size of 90k	
15.		The switch should support 8K multicast routes	
16.		Switch should support 64 nos of ECMP paths	
17.		Switch should support minimum 1 Tbps of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non-blocking capacity)	
18.	**Network Virtualization Features**	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
19.		Switch should support VXLAN and EVPN symmetric IRB/Asymmetric IRB for supporting Spine – Leaf	

		architecture to optimize the east - west traffic flow inside the data center	
20.	**Layer2 Features**	Switch should support Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S) and VLAN Trunking (802.1q)	
21.		Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
22.		Switch should support minimum 90k of MAC addresses	
23.		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
24.		Switch should support layer 2 extension over VXLAN across all DataCenter to enable VM mobility & availability	
25.		The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC),-Explicit Congestion Notification (ECN).	
26.		The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	
27.	**Layer 3 Features**	Switch should support static and dynamic routing	
28.		Switch should support multi instance routing using VRF/ VRF Edge/ Virtual Router routing and should support VRF Route leaking functionality	
29.		Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM	
30.		Support Multicast Source Discovery Protocol (MSDP)	
31.		IGMP v1, v2 and v3	
32.	**Quality of Service**	Switch system should support 802.1P classification and marking of packet using: a. CoS (Class of Service) b. DSCP (Differentiated Services Code Point)	
33.		Switch should support for different type of QoS features for real time traffic differential treatment using a. Weighted Random Early Detection b. Strict Priority Queuing	
34.		Switch should support Rate Limiting - Policing and/or Shaping	
35.		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
36.	**Security**	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	

37.		Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
38.		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding	
39.		Switch should support IP Source Guard to prevents a malicious hosts from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN	
40.		Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port or should support storm control (broadcast, unicat , multicast	
41.	**Manageability**	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session on physical interface /Port Channel , VLAN interfaces	
42.		Should have Open APIs to manage the switch through remote-procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS after secure authentication for management and automation purpose.	
43.		The Switch Should support monitor events and take corrective action like a script when the monitored events occur.	
44.		All the components should be from same OEM for ease of management and interoperability	

15.17 Object Storage (30PB Usable)

S. No.	Specification	Compliance (Yes/No)
1.	Usable Net Capacity of Object Storage (PB): 30 PB - Net capacity is the amount of storage that will be available for storage of data after all system overheads are accounted for including but not limited to data protection, metadata, space required for objects pending garbage collection, and best practices for maximum recommended fill rate, including fill levels requiring special growth requirements on the object storage system.	
2.	Object storage solution must be able scale up to at least 200PB with addition of disks and/or storage nodes	
3.	Industry standard with maximum 42U racks to be utilized.	
4.	Number of Chassis/Nodes (Number): Minimum 8. If multiple nodes per chassis are utilized, then failures tolerance will be measured at chassis level	

5.	Minimum Number of LFF Drive Slots per Node (Number): 50	
6.	Max Weight per Rack: 1000 kg	
7.	Standby Power Consumption of System (Watt): Max 7000 per rack.	
8.	Max Power Consumption of System (Watt): Max 8000 Watt per rack.	
9.	Regardless of object size the number of tolerable concurrent storage node / disk failures occurring concurrently one by one for both data and metadata: any 3 storage chassis/storage nodes/storage enclosures or any 3 disk failures or any combination of any 3 storage chassis/storage nodes/storage enclosure/disks.	
10.	Proposed object storage should be fully distributed, asymmetrical, and scale-out architecture allowing multi-site active/active architecture.	
11.	Object storage should maintain the authenticity and integrity of objects using hash keys such as MDS/SHA-1/SHA-2 with self-healing and auto-configuration features as well.	
12.	The solution must support data at rest encryption along with data in transit encryption capabilities based on AES-256-SHA.	
13.	Object storage data and metadata must be independently scalable to ensure ability to fully utilize all hardware resources.	
14.	Scaling of all system component must be accomplished without any Service downtime or risk of data loss.	
15.	The proposed object storage solution should support the efficient storage of object sizes from a few kilobytes to 1TB. If space reclaim after deletion is impacted, then add-on capacity must be supplied to reach net space usable required capacity.	
16.	Object storage must support distributed Erasure Coding and/or Replication to support required fault tolerance. Local RAID for data or metadata protection must not to be utilized.	
17.	Object storage must have certified SEC Rule 17a-4(f) compliance.	
18.	Proposed object storage should not allow users to access data via system-console login to the cluster's nodes and it should be used only for management.	
19.	Object storage S3 API GET operation must support AWS S3 API GET operation conditionals including ETag and modified/unmodified conditionals.	
20.	Object storage must support prevention of sensitive metadata attributers such as object creation timestamp by any manner.	
21.	Object storage must disallow or be configurable to prevent the modification of the object data. In case object modification is necessary it must only be provided by the creation of a new object with updated metadata including time stamps. The original object shall remain intact.	
22.	Object storage must provide for logging of all operations and authentication attempts with a retention period of 2 years. Log forwarding functionalities should be present.	

23.	Object storage system shall have built-in self-healing, automatic failure detection, global namespace with active data access and modification. Storage nodes should be allowing fine grained vertical expansion disks and/or RAM and/or networking. Object storage system must allow for horizontal expansion by addition of nodes. Vertical and horizontal expansion must be able to be accomplished non-disruptively.	
24.	Specialized ToR 25GbE or higher switched should be provided.	
25.	Selected Bidder must provider redundant H/W Load balancer hardware load balancer as required to integrate object storage, sized to offer the asked throughput. Selected Bidder must ensure that load balancer supplied must be scalable.	
26.	Object storage solution must provide a built-in dashboard for capacity, object count, bandwidth usage, etc.	
27.	Object storage solution must provide REST API support for advanced monitoring and management.	
28.	Object storage solution shall be sized by number of storage nodes and disk type and capacity to provide for concurrent sustained throughput of at least 35 GBps for GET operations and 35 GBps for PUT operations for the 30PB of net usable capacity	
29.	Object storage system must support multiple configurations of storage nodes including different generations, configuration, disk types.	
30.	Relevant documentation of the REST API for data ingestion, retrieval, monitoring and management should be provided the OEM.	
31.	Scope of supply must include installation, commissioning & integration together with all necessary software to make the system fully functional as intended. Installation and configuration must be performed on-site by OEM professionals.	
32.	The selected Bidder should arrange for Training (8-10 participants) of the proposed technologies from the proposed object storage product OEM's own certified trainers.	
33.	The selected Bidder shall supply Software and services as per schedule of Requirements and in accordance with minimum functional & technical specifications as provided in the requirement sections. Design and Implementation of the storage cluster with underlying software components should be certified by OEM professionals.	
34.	The Defined Storage Bidder should have local presence and should have world-wide 24/7 support.	
35.	Selected Bidder must certify that object storage system, hardware and software, shall not be end of sale support during the period of delivery , but not less than 6 years from data of supply, or Bidder must replace it with the next compatible with next product in line (having specifications either equal or better) which is not end of support/sale at no cost, including data migration.	

15.18 Firewall

S. No	Specification	Compliance (Yes/No)
1.	The NGFW must be modular based architecture to meet the requirements defined below within the single appliance	
2.	Licensing: should be per device license for Unlimited users for Firewall / VPN (IPsec & SSL) and other features. There should not be any user/IP/host-based licenses	
3.	Support for Virtualization (i.e. Virtual Systems / Virtual Domains)	
4.	The proposed NGFW should be provided with a dedicated Central Management and Reporting Solution from the same OEM either in Physical or Virtual Form Factor	
5.	The platform should be based on real-time, secure field operating system with EAL4+/NDPP certification	
	Interface and Connectivity Requirements	
6.	Minimum 4 x 1/10 Gig Copper interfaces and Minimum 10 x 1/10Gig SFP/SFP+ with fully populated 10G SFP+ SR transceivers from day 1	
7.	Minimum 2X 40/100 Gig Ports with required 2*40G SR and 2*100G SR transceivers from day 1	
8.	Dedicated 2*HA ports with active optical cable in addition to requested data ports, OOB, Console Management and USB Port	
9.	The platform should support the standards-based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth	
	Performance Requirements	
10.	The Proposed Solution must be provided with least 50 Million Layer 4 TCP concurrent sessions or minimum 20 Million Concurrent HTTP sessions from day 1	
11.	The Proposed Solution must be provided with at least 2 Million Layer 4 New TCP connections/sessions per second or at least 700,000 New Layer 7 HTTP sessions per second from day 1	
12.	The NGFW appliance should provide NGFW throughput of minimum 60 Gbps considering 100 % Application traffic mix by enabling Layer 7 inspection and logging enabled from day 1	
13.	The proposed solution should support a minimum of Threat Prevention throughput of 45 Gbps (Threat Protection performance is measured with Application Control/AVC, IPS, antivirus, antispyware, Sandboxing, and logging enabled) considering 100% application traffic mix from day 1.	
14.	Should support for minimum 10000 gateway to gateway VPN tunnels.	
15.	Should support for minimum 20000 clients to gateway VPN tunnels.	
16.	Appliance should support Virtualization (i.e. Virtual Systems / Virtual Domains/Virtual Instances) with 25 minimum instances provisioned from day 1. The virtual system should have all the features as of physical device	
17.	The proposed solution should be Rack mountable with maximum 6U Rack space	
18.	All the performance benchmarking values defined throughput, and performance should be offered within the same appliance.	

19.	The firewall should have a Redundant Hot Swappable power supply modules along with redundant fan modules	
20.	The proposed appliance should have minimum 480 GB SSD for storage in RAID 1 apart from Logging storage provisioned centrally for Logging/Reporting	
	Network/Routing Requirements:	
21.	Static routing, Policy based Routing/Forwarding and Dynamic Routing (RIP, OSPF, BGP) must be supported for both IPV4 and IPV6	
22.	Multicast Routing must be supported	
	Firewall Features Requirement:	
23.	The Firewall/Firewall OS should be ICSA Labs certified or EAL 4 certified and should also be certified under Common Criteria program (global) or TEC Certified or certified under the Indian Common Criteria Certification Scheme(IC3S) that has been set up by the Ministry of Electronics and Information Technology (MeitY) program	
24.	It should be possible to operate the firewall in “bridge mode” or “transparent mode” apart from the standard NAT mode	
25.	The Firewall must provide NAT functionality, including PAT.	
26.	Should support “Policy-based NAT”	
27.	The Firewall should provide advanced NAT capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP	
28.	Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc	
	Authentication Requirements:	
29.	Support for authentication for Users and Firewall Administrators (Local and Remote – RADIUS/ TACACS+ & LDAP), RSA SecureID, PKI / Digital Certificate based two-factor Authentication or other Token based products.	
	High Availability Requirements:	
30.	The device must support Active-Active as well as Active-Passive redundancy.	
31.	The Firewall must support Stateful failover between the appliances in case of HA deployment	
32.	Should support VRRP or equivalent and Link Failure Control	
	Encryption / VPN Requirements	
33.	The VPN functionalities should be integrated within firewall including IPSEC and SSL TLS. Should support the following protocols: 3DES, MD5, SHA-1 & SHA-256 authentication, Diffie-Hellman Group 1, Group 2, Group 5 & Group 14, Internet Key Exchange (IKE) v1 and IKE v2 algorithm, and AES 128, 192 & 256 (Advanced Encryption Standard)	
34.	IPSec VPN should support Xauth over RADIUS and RSA SecurID or similar product.	
35.	Should have integrated SSL VPN with no user license restriction. Required licenses to be provided by the Bidder from day 1 if the product does not follow the required licensing policy	
36.	Should support SSL Two-factor Authentication with Digital Certificates	
37.	Should support Windows and MAC OS for SSL-VPN and licenses should be provisioned from day 1 for remote VPN users	

38.	Should support NAT within IPSec/SSL VPN tunnels	
	Other Requirements	
39.	Should Support Packet Capture/sniffer to capture and examine the contents of individual data packets that traverse the firewall appliance for troubleshooting, diagnostics and general network activity	
40.	The proposed system should have integrated Traffic Shaping / QoS functionality	
41.	Should be able to support Geo-IP block. It should be able to block country wise traffic.	
42.	The proposed solution should maintain the audit trail for the management activities of individual users and administrators accessing and using the application	
43.	Solutions should provide for Role-Based Access Control (RBAC) and provide access based on the least privilege criteria	
44.	The proposed solution should comply with FIPS-140-2 standard for cryptographic modules	
45.	The proposed firewall should have protection for at least 20000 IPS signatures excluding custom and feature to add custom signatures	
46.	The proposed solution should have capability to protect against fileless based attacks, and never-before-seen phishing and JavaScript attacks inline. Solution should be capable to use both signature based and ML based signature less technology to protect against Phishing, Ransomware and other HTML based attacks	
47.	The proposed firewall should allow creation of custom categories according to different needs around risk tolerance, compliance, regulation, or acceptable use	
48.	The proposed firewall should have a vast categorization database where websites are classified based on site content, features, and safety	
49.	The proposed firewall should support DNS security in inline mode	
50.	DNS security capabilities should block known Bad domains and predict with advanced machine learning technology and should have global threat intelligence of at least 10 million malicious domains if needed for any future considerations	
51.	The proposed firewall should support prevention against DNS tunneling which are used by hackers to hide data theft in standard DNS traffic by providing features like DNS tunnel inspection, DOT, DOH and prevent against DGA and Dynamic DNS based attacks.	
52.	The proposed firewall support prevention against new malicious domains (newly registered domains) and enforce consistent protections for millions of emerging domains. The Solution must be able to do real-time inspection of both the DNS request and DNS response to stop DNS hijacking in near real time	
53.	The proposed Management solution must allow policy rule creation for application control, user-based control, host profile, threat prevention, Anti- virus, file filtering, content filtering, QoS and scheduling.	
54.	Should support on device and centralized management with on firewall administration. NGFW should have capability for Admin-level commits or change management workflow	

55.	The proposed solution should be provided with IPS, Anti-Spyware, AV , URL filtering and DNS security features mentioned above bundled from day 1 for 5 years	

15.19 Load Balancer

S.no	Feature Specifications	Compliance (Yes/No)
1.	Should support Layer-4 Load Balancing inc. UDP and TCP	
2.	Should support Layer-7 Load Balancing inc. TLS	
3.	Should support various health check mechanisms like detection of uptime of specific TCP/UDP	
4.	Should support packet error rate monitoring and response delays to identify priority for data Service, ICMP check, ARP check, etc forwarding.	
5.	Should support detection of ICMP Destination Unreachable packets for UDP packets to identify failed delivery	
6.	Should support configurable and automated retransmission of packets/data on failed delivery (as per above points) to another server	
7.	Should support configurable health check parameters	
8.	Should support Sticky Sessions for client to have session persistence	
9.	Should be capable of forwarding alerts for failed deliveries, retransmissions, etc	
10.	Should provide capability to extensively monitor the traffic based on source/destination, data type and other packet parameters.	
11.	Should support TLS protocols like TLS 1.2, TLS 1.3 among others with secure cipher suites.	
12.	Should be capable of being configured in High Availability mode - Active-Active and Active-Passive	
13.	Server load balancer should have plug-in to integrates with container orchestration environments to dynamically create L4/L7 services on LB, and load balance network traffic across the services.	
14.	The Controller for Kubernetes lets you manage your LB device from Kubernetes or OpenShift using either environment's native CLI/API	
15.	The proposed solution should have inbuild HTTP to MQTT Parser. The proposed solution should provide certificate based authentication between IOT devices and Load Balancer.	
16.	Server Load Balancer should support SQL-based querying for the following databases for health checks: • Oracle • MSSQL • MySQL • PostgreSQL • DB2	
17.	All log management servers should be connected across DC through GSLB functionality.	

18.	DNS and GSLB capability to understand records like A, AAAA,CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, TXT	
19.	Supports DNS SEC eg digitally sign DNS answers. This enables the resolver to determine the authenticity of the response, preventing DNS hijacking and cache poisoning. These signed DNS responses can be used in conjunction with the dynamic DNS system to enable global server load balancing.	
20.	The solution must have in-built function Vulnerability scanner and / or support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support all the common web application vulnerability assessment tolls (Web application scanners) including Acunetix, Qualys, Rapid 7,IBM Appscan etc. to virtually patch web application vulnerabilities.	
21.	Solution should support single-sign on in future.	
22.	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions.	
	Technical Requirements	
23.	Application throughput L7: 25Gbps	
24.	Layer 4 concurrent sessions :20 Million .	
25.	SSL Bulk Throughput: 15 Gbps.	
26.	Load Balancing Capacity : 10-20 Hosts .	
27.	Network Interface : 4 x 10G SFP+ and 4 x 1G copper, 1x1G RJ-45 Management Port	
28.	Configuration mode: HA Active-Active.	

15.20 Web Application firewall

S.no	Feature Specifications	Compliance (Yes/No)
1.	Should provide robust protection against OWASP Top 10 vulnerabilities and provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	
2.	Should include rate limiting capabilities.	
3.	Should support white-list and black-list mode rule configuration, per application	
4.	Should offer advanced bot protection	
5.	Should support IP whitelisting/blacklisting	
6.	Should feature advanced application layer protocol security.	

7.	Should support custom rule creation and tuning.	
8.	Should support High Availability in Active-Active and Active-Passive modes .	
9.	Should support ECC as well as RSA for TLS.	
10.	Should provide Geo-IP blocking capabilities.	
11.	Should support configurable content caching.	
12.	Should offer real-time threat intelligence updates.	
13.	Should include Anti-DDoS protection.	
14.	Should offer API protection. WAF must provide inbuilt capability of API security including support for uploading swagger file and inspect.	
15.	Should allow for session fixation protection.	
16.	Should support TLS protocols like TLS 1.2, TLS 1.3 among others with secure cipher suites.	
17.	Should provide comprehensive logging, reporting and log forwarding capabilities.	
18.	Should have native parsing of GraphQL traffic to allow WAF Attack Signatures to be applied. Should have GraphQL policy template and content profile as a part of the Application Security Policy.	
19.	System should support inbuilt ability or integration with any 3rd party solution to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.	
20.	The Solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks including stress-based DOS and Heavy URL attacks. The solution must support all the common web application vulnerability assessment tools (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM Appscan, etc (or) Equivalent Gartner vulnerability assessment tools to virtually patch web application vulnerabilities. Necessary logs to be generated for audit and compliance.	
21.	The solution must distinguish between browsers and bots which are able to execute Java script by using advanced techniques such as browser capability challenge and CAPTCHA challenge. Necessary logs to be generated for audit and compliance.	
22.	The solution should be able to "clock" error responses to hide sensitive server related information in the response body and response headers. It should also facilitate hiding/masking sensitive parameters in logs policy wise. Solution should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration.	

23.	The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system.	
24.	Solutions Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions.	
	Technical Requirements:	
25.	L4 Connections/second : 1000K Connections/Sec.	
26.	HTTPS/L7 Requests: 2000k Requests/Sec	
27.	L7 Throughput : 80Gbps	
28.	SSL Performance (for ECC) : 50k transactions/sec, with 40Gbps SSL throughput	
29.	Network Interface : 4 x 10G SFP+ and 2 x 40G/100G, 1x1G RJ-45 Management Port.	

15.21 Network monitoring system

S. No.	Technical Specifications	Compliance (Yes/No)
1.	The Monitoring Solution should provide Network Fault Management, Network Performance Management, Server Performance Monitoring, and unified Dashboard & Reporting	
2.	Should be able to monitor servers , networking devices and other components mentioned in the BOQ.	
3.	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Reporting and analytics	
4.	The proposed NMS must provide comprehensive monitoring capabilities for a diverse network environment which includes automatic discovery, health assessment, and performance tracking of various physical and virtual devices like Layer-2 and Layer-3 switches, routers, firewalls, load balancers, servers both physical and virtual, storage systems and other IP-enabled devices, a unified dashboard should provide clear visibility into their overall health and performance of entire infrastructure.	
5.	The solution shall provide future scalability of the whole system without major architectural changes.	
6.	The proposed solution must not use any third-party database (including RDBMS and open source) to store data to provide full flexibility and control on collected data.	
7.	Should support various data gathering methods including SNMP, JMX, IPMI, agent-based and probe based.	
8.	The platform must provide complete cross-domain visibility of IT infrastructure issues	
9.	Should be capable of monitoring various network services including http, ssh, etc.	

10.	Should be capable of monitoring web services using custom probes like http response status codes and basic html matching.	
11.	Should support monitoring of custom SNMP fields.	
12.	Should support both SNMP polling and SNMP traps for monitoring network events such as alerts for critical port status changes, with configurable frequency.	
13.	The solution must support custom dashboards for different role users such as Management, admin, and report users	
14.	The solution must support custom query-based widget with multiple visualization methods including Chart, Gauge, Grid, Top N list etc. to visualize and represent collected data with ease.	
15.	The solution should provide superior view of infrastructure health across system,networks, application and other IT Infrastructure components into a consolidated, central console	
16.	The solution must provide agentless and agent-based method for managing the nodes and have the capability of storing events / data locally if communication to the management server is not possible due to some problem. This capability will help to avoid losing critical events.	
17.	The proposed solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be to set polling interval as low as 1 second with low overhead on target server infrastructure	
18.	The proposed solution platform shall provide a single integrated solution for comprehensive monitoring of the wired, wireless access, security access control devices, or any pingable devices and rich visibility into connectivity and performance assurance issues.	
19.	Should support template based configurations including pre-configured templates for quickly setting up monitoring for new devices.	
20.	The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices.	
21.	The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.	
22.	The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status	
23.	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 based on event pairing, event sequencing etc.	
24.	The proposed solution should have multiple alerting feature based in predefined events to get the notification via email, sms and third-party systems	
25.	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 suppression, event aggregation and event annotation	
26.	The proposed solution should provide alert console with alert summary such as no. of correlated alert, network alert, server alert, virtualization alert, cloud alert, application alert ,etc.	
27.	The system must have provision to overlay alert on reported metric to understand alert triggering behaviour across multiple drill down pages	
28.	Should provide a flexible alerting system that can trigger notifications based on predefined events, via email, SMS, or custom scripts, among other methods.	
29.	The solution should be capable of running in Linux platform and should be 64-bit application to fully utilize the server resources on which it is installed	
30.	OEM Should provide support for 5 Years with all upgrades and updates during the contract Period.	
31.	OEM Should provide on Site Configuration and Training for minimum 3 Days (for 8-10 participants) Training along with the Training Material.	
32.	Should provide capabilities to run in High Availability	
33.	Data retention to be supported for at least 5 years.	

15.22 Automation

S. No.	Technical Specifications	Compliance (Y/N)
1	The software should be able to deploy application in any set of OS for automation.	
2	The offered automation software should support Configuration Management and Application Deployment	
3	The offered software should be open standard/open source/enterprise ready in nature with L1-L3 based 24x7 support from OEM, updates, and upgrades for the project period.	
4	The software should support tasks to be perform in one or many hosts simultaneously.	
5	The automation software should support Multi-tier Orchestration	
6	The platform should support OS native connection protocol like SSH, winrm and there should be agentless communication with the end points to save resources	
7	Proposed software should be offered with Yet-Another-Markup-Language capability	
8	The automation software should have dashboard for providing heads-up display for everything going on in your automation environment.	
9	Proposed solution should show host and inventory status; all the recent job activity and a snapshot of recent job runs	
10	The proposed solution should support the Patch automation functionality.	

11	Solution scripts should run stream in real time. Automates across to play and tasks complete, broken down by each machine, and each success or failure, complete with output, queue view, source control updates or cloud inventory refresh.	
12	The software should be able to log activities securely and the same should be viewable later on. The same should support export facility also via API connects.	
13	It should support audit trail of all changes made to automation tool itself -job creation, inventory changes, and credential storage, all securely tracked.	
14	The same notifications should be able to SMS, email, and more -or post notifications to a custom webhook to trigger other tools in your infrastructure.	
15	It should help to manage entire infrastructure and able to pull inventory from public/private MeITY empanelled cloud providers such as Amazon Web Services, Microsoft Azure etc.	
16	It should have inbuilt portal mode and survey features to delegate automation job runs to users across the organization -synchronized directly from corporate directories such as LDAP, Active Directory or delegated SAML authentication.	
17	The software should verify whether machines are in compliance based on certain standards	
18	It should help to discover how a machine has changed over time with respect to baseline configurations or compare machines in running cluster to see how they are different.	
19	It should support REST API and CLI for integration with other tools	
20	The offered automation software should support containerized deployment to scale at runtime as needed	
21	The offered automation tool should provide mapping of organizations and teams from SAML attribute, configuration of two-factor authentication with SAML, use for multiple LDAP servers within the software	
22	The offered software should work as OAuth2 consumer, allowing easier integration with third party applications for automation	
23	Offered software should be able to cache isolated node facts	
24	Proposed solution should come in Highly Available deployable configuration to Automate logical endpoints like FW, LB, Linux, Windows, Storage, Servers etc	
25	Proposed Automation solution should be able to perform hardening on either servers, storage devices or networking devices based on the compliance policy shared.	
26	Capable to do automation of virtual infrastructure (vSphere, RHV, etc) and public cloud platforms (Azure/AWS etc)	
27	Capable to do automation of network and security equipment (NW Switches / Firewalls etc)	
28	Capable to do automation of storage appliance	

29	Capable to do automation using monitoring tools as triggers	
30	Pull and sync automation job playbooks (script) from source version control systems	
31	Provide capability to define workflow for multiple automation jobs	
32	Proposed solution should have a partner driven network to provide joint certified collections (plugins) /reusable content to speed up reliable automation.	
33	The platform should be capable to integrate with generative AI based tools which can assist in creation of automation tasks	
34	The proposed automation platform should have the capability to implement event-driven automation within and across multiple IT use cases like issue remediation, user administration tasks and operational logic.	

16. Annexures

Annex 1 – Declaration-Cum-Undertaking Regarding Blacklisting/ Non-Blacklisting

<To be submitted on the letter head of the Bidder>

I/ We, Proprietor/ Partner(s)/ Director(s) of [Company Name] hereby declare that the firm/company namely M/s. , as on the date of bid submission, has not been blacklisted or debarred in the last three years and is not under blacklisting period/active debarred list by NIC/NICSI or any of the Central or State Government organization/ Public Sector Undertaking/ Autonomous Body etc.

OR

I/ We Proprietor/ Partner(s)/ Director(s) of M/S hereby declare that the firm/company namely M/S in the last three years, was blacklisted or debarred by NIC/NICSI, or any other Central or State Government organization/ Public Sector Undertaking/ Autonomous Body etc. for a period of months/years w.e.f. The period is over on and, as on the date of bid submission the firm /company is not in active blacklisting period and now entitled to take part in Government tenders.

In case the above information found false I/We are fully aware that the tender/ contract will be rejected/cancelled by NIC/NICSI and execution of Bid Securing Declaration. In addition to the above NIC/NICSI will not be responsible to pay the bills for any completed/ partially completed work if Tender was allotted.

(Signature of Bidder with Seal)

Name:

Capacity in which as signed:

Name & address of the Company/ Firm:

Date & Place:

Annex 2 – Instructions to fill the Bill of Material

a) Bidder shall provide all prices as per the prescribed format under this Annexure. Bidder shall not leave any field blank. In case the field is not applicable, Bidder shall indicate "0" (Zero) in all such fields. Quoting of zero (0) as rate for a specific item shall imply that there shall be no charges on any level of usage of that particular item during the Contract Period including the extension. However, quoting of NIL value/no/dash (-) for any item, as listed in the detailed financial Bid shall imply that the Bidder has quoted zero (0) as rate for a specific item. Purchaser in such case reserves the right to seek clarification/ undertaking from the Bidder. If the Bidder fails to agree or provide undertaking for the clarification, Purchaser reserves the right to consider rejecting the Bid of the Bidder.

b) All the prices (even for taxes) are to be entered in Indian Rupees ONLY (%age values are not allowed)

c) It is mandatory to provide breakup of all Taxes, US Dollar component, Duties and Levies wherever applicable and/or payable while submitting the financial Bid (refer **Annex 5**— Bill of Material).

d) The rate revision due to dollar fluctuation shall be considered when the average monthly fluctuation is ±10% of the above reference value. The revised rate shall become the reference value for any further rate revision and so on. If the fluctuation is upwards/downwards, Purchaser shall automatically initiate the process for increasing or reducing the rate by following the same procedure.

e) Purchaser reserves the right to ask the Bidder to submit proof of payment against any of the taxes, duties, levies indicated.

Annex 3 – Abridged Financial Bid

Abridged Financial Bid for Submission of Grand Total Value
Prices shall be quoted in Indian Rupees (inclusive of all taxes) and indicated both in figures and words. **Price in words shall be considered for evaluation, in the event of any mismatch**.

Table-1: Grand Total Value

Grand Total Value (GTV) i.e., value of **Annex – 4** (Detailed Financial Bid, in figures)	
(Rupees_____) in words	

Note: The Bidder shall ensure that the Grand Total Value given in **Annex 3** (Grand Total Value) must match the Grand Total Value given in **Annex 4** (Detailed Financial Bid).

Annex 4- Detailed Financial Bid

Bidder Name: .....

Prices in the Financial Bid (inclusive of all taxes) shall be quoted in the following format. All prices shall be quoted in Indian Rupees and indicated both in figures and words. Figures in words shall prevail.

Grand Total Value (GTV)

The grand total value shall be derived as below:

Grand Total Value (GTV) = shall be the sum total of the following components inclusive of taxes:

Table-1: Grand Total Value

S. No.	COMPONENT (A)	AMOUNT (Including taxes) (B)
1	Total cost of Financial Computation for Procurement, AMC Cost **(Annex 5(A) (TP1) + Annex 5(B) (TP2))** **(TP = TP1+TP2)**	To be filled by the Bidder
	GTV = (TP)	To be filled by the Bidder

In Words:

In case of discrepancy, amount in words will prevail.

Place:
Date:

Authorised Signatory Name:

Annex 5 – Bill of Materials (BoM)

Bidder Name: .....

Instructions to fill the Bill of Materials

a) The Bidder has to quote the price of each and every component having financial impact in the proposed solution.

b) The bill of material in the table below shall include all the components required for installation and commissioning of platforms specified in paragraph 14.1 for achieving the scope of work as defined in the RFP.

c) The hardware quoted in bill of material to support the requirements/solution products shall be with one-year warranty.

d) AMC value per/every year should be in rupees as numerical value calculated in % of unit cost of item/ sub item. The AMC value quoted should be minimum 6% of item unit. If quoted less than 6%, NIC/NICSI through FEC reserves the right to distribute maintenance charges as deemed appropriate.

e) The software licenses shall be delivered with the initial one-year cost and annual renewal cost for subsequent years to be included in the BOM for each year. All software subscription license costs unless justified shall be equal annually during the contract period. In case the Purchaser feels that the price quoted is unjustified, the total quoted cost for the line item shall be divided into equal instalments.

f) The warranty of the platform and components shall be effective from the date of Go-Live, for a period of one year. 2nd year AMC shall start after completion of warranty i.e. after completion of one year from the date of Go-Live.

5(A) Table for Procurement

S. No.	Item Description per technical specs	Supply unit costs (in INR)	GST on product	Total procurement cost (All-inclusive of taxes)	Total Qty	Total cost (A)	AMC for 2nd Year (Inclusive of Tax)* (B)	Product HSN Code
	1	2	3	4=2+3	5	6 = 4*5	7	12
1								
2								
3								
4								
5.								
6								

Total						**A**	**B**	
Grand Total in INR (TP1 = A+B)					**A+B (to be filled by the Bidder)**			

Note:

(a) Extension beyond two years would be done on the 2nd year price itself.

5(B) Table for Implementation

S. No	Description	Total Cost (including taxes)
1	One time Installation and commissioning cost	Y1 (To be filled by the Bidder)
2	Any additional one-time charges before Go-Live (ex: insurance, freight etc.)	Y2 (To be filled by the Bidder)
Total	**TP2=Y**	**Y=Y1+Y2**

Total cost of Financial Computation for Product (TP= TP1 + TP2 + TP3) is to be filled by the Bidder as per 5(A), and 5(B)

5(C) Table for Import (US Dollar) Component Percentage for H/W & S/W

S. No.	Item	OEM	Model/Version	% Import (US Dollar) Component in Basic Cost	% Import (US Dollar) Component in AMC

Annex 6 – Proforma for Bank Guarantee for Security Deposit/ Contract Performance (PBG)

Ref: _____ **Date: _____**

BG Number: _____ **Bid Number: _____**

To,

Tender Processing Section
National Informatics Centre
A Block, CGO Complex, Lodhi Road, New Delhi – 110 003

1. Against contract vide Advance Acceptance of the Tender- No._____ dated _____Covering (hereinafter called the said "Contract") entered into between the NIC (hereinafter called "the Purchaser") and _____ (hereinafter called the "Bidder") this is to certify that at the request of the Bidder, we _____Bank Ltd., are holding intrust in favour of the Purchaser, the amount of _____(Write the sum here in words) to indemnify and keep indemnified the Purchaser against any loss or damage that may be caused to or suffered by the Purchaser by reason of any breach by the Bidder of any of the terms and conditions of the said contract and/or in the performance thereof. We agree that the decision of the Purchaser, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by the Purchaser shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to the Purchaser.
2. We _____Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfilment in all respects of the said contract by the Bidder i.e. till_____hereinafter called the said date and that if any claim accrues or arises against us, _____Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us_____ Bank Ltd, notwithstanding the fact that the same is enforced within six months after the said date, provided that notice of any such claim has been given to us, _____Bank Ltd, by the Purchaser before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from the Purchaser.
3. It is fully understood that this guarantee is effective from the date of the said contract and that we _____Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of the Purchaser.
4. We undertake to pay to the Purchaser any money so demanded notwithstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond being absolute and unequivocal.

The payment so made by us under this bond shall be a valid discharge of our liability for payment there under

and the Bidder shall have no claim against us for making such payment.

5. We _____Bank Ltd, further agree that the Purchaser shall have the fullest liberty, without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the Tendered from time to time or to postpone for any time of from time to time any of the powers exercisable by the Purchaser against the said Bidder and to forebear or enforce any of the terms and conditions relating to the said contract and we, _____Bank Ltd, shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Bidder or for any forbearance by the Purchaser to the said Bidder or for any forbearance and or omission on the part of the Purchaser or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.
6. This guarantee shall not be discharged due to the change in the constitution of the Bank or the Bidder.

Date _____

Place _____ Signature _____

Witness_____ Printed name_____

(Bank's common seal)

Annex 7 – No Deviation Certificate

<To be submitted on the letter head of the Bidder>

Note: The following Declaration to be submitted on the Bidder's Letter Head, duly signed & stamped and to be attached along with your technical bid of the tender.

We, M/s. [Company Name], have read and clearly understood all the terms and conditions in the Tender Schedule of [Tender Name], and accordingly, accept the same without any deviation whatsoever.

I/We unconditionally agree to all the tender conditions, and no new conditions are imposed by us in the technical/price bid. I understand that, in the event of imposing any condition in the technical/price bid, such condition would be ignored by NIC, and only the prices will be considered for the purpose of evaluation.

In case of any deviation (technical or commercial), the same is mentioned below. (Bidders, please note that deviations mentioned elsewhere would not be considered, and such deviations would be null and void)

S. No.	Document reference	NIC Specification	Firms Alternative offer
1	Nil	Nil	Nil

i. I/We confirm that none of our group concern or affiliates, etc., appears on the list of banned firms/companies by NIC, nor any of the Directors/Partners/Proprietors of the Bidder/such group concern or affiliate, etc., are involved with such company.

ii. I/We also declare that we have not been suspended or blacklisted or issued with a Show Cause Notice by NIC or any other government organization.

iii. I/We confirm that, other than us, none of our group concerns or affiliates, etc., are participating in the tender either directly or indirectly through any other agency under the same proprietor/common director(s)/common partner(s).

iv. I/We confirm that if any of the above statements/information furnished by us in this tender is found to be false/fake at any stage of tender evaluation or during the execution of the contract, NIC will have the right to initiate appropriate action, including legal proceedings/termination of contract, recovery of damages, penalties, etc., as deemed fit.

(Contractor Signature with Seal)

Contractor Signature

Contractor Seal

Annex 8 – Manufacturing Authorization Form (MAF)

1. A copy of the MAF should be uploaded on GeM portal as part of the technical bid. The Purchaser may choose to reject the bid in case the MAF is not submitted.
2. The Bidder must ensure that the MAF should be dated between the tender release date and bid submission date including date of release of tender and bid submission date. Any deviation may lead to rejection of bid.
3. It may be noted that validity of MAF will be till the finalization of the tender and contract period.
4. The Bidder should comply with the below mentioned points:
   - 4.1 The letter should be submitted on the letter head of the manufacturer / OEM and should be duly signed by the authorized signatory.
   - 4.2 The letter must be addressed to National Informatics Centre , Block, CGO Complex, Lodhi Road, New Delhi
   - 4.3 The tender name and bid number must be mentioned in the MAF.
   - 4.4 The MAF must ensure the following:
     - 4.4.1 The OEM provides support for 5 years from the date of supply of the equipment as per tender terms.
     - 4.4.2 The MAF should state the Bidder address same as quoted by the Bidder in the submitted bid documents.
     - 4.4.3 Proof has been provided by the Bidder in case of any deviation in the OEM name and name of the company of OEM.
     - 4.4.4 The MAF should be signed and stamped by Bidder as well.

Annex 9 – Covering Letter

<To be submitted on the letter head of the Bidder>

<Place>
<Date>

To
Tender Processing Section
National Informatics Centre
A Block, CGO Complex
Lodhi Road, New Delhi – 110003

Subject: **Submission of Bid for _____Tender Name_____ (Tender ID: _____)**

Dear Madam/Sir,

This is to notify that our company is submitting technical Bid in response to Tender No Purchaser/…for _____tender name____

Primary & Secondary contact for our company are as follows:

<M/s Company Name>	**Primary Contact**	**Secondary Contact**
Name		
Title		
Address		
Phone		
Mobile		
Fax		
E-mail		

We are responsible for communicating to the Purchaser in case of any change in the Primary or/and Secondary contact information specified above. We shall not hold Purchaser responsible for any non-receipt of Bid process communication in case such change of information is not communicated and confirmed with NIC on time.
We are submitting our Bid for _____tender name_____ as per the scope and requirements of the tender document:

By submitting the proposal, we acknowledge that we have carefully read all the sections of this tender document including all forms, scheduled and appendices hereto, and are fully informed to all existing conditions and limitations. We also acknowledge that the company is in agreement with terms and conditions of the tender and the procedure for bidding and evaluation.

We have enclosed the earnest money deposit as per the tender Conditions. It is liable to be forfeited in accordance with the provisions of tender document.

Deviations:
We declare that all the services shall be performed strictly in compliance with the Tender Document. Further, we agree additional conditions, if any, found in the Bid documents, other than those stated in the tender document, shall not be given effect to.

Bid Pricing:
We do hereby confirm that our Bid prices exclusive all taxes, as applicable on the last date of submission of Bid. We further declare that the prices stated in our proposal are in accordance with your terms & conditions in the bidding document.

Qualifying Data:
We confirm having submitted in qualifying data as required by you in your tender document. In case you require any further information/documentary proof in this regard before evaluation of Bid, we agree to furnish the same in time to your satisfaction.

We confirm that information contained in this response or any part thereof, including documents and instruments delivered or to be delivered to Purchaser are true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part misled Purchaser in its evaluation process.

We fully understand and agree that on verification, if any of the information provided here is found to be misleading the evaluation process or result in unduly favours to our company in evaluation process, we are liable to be dismissed from the selection process or termination of the contract during the contract with Purchaser.

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

Itis hereby confirmed that I/We are entitled to act on behalf of our corporation/ company/firm/organisation and empowered to sign this document as well as such other documents, which may be required in this connection.
Yours sincerely,
On behalf of [Bidder's name]
Authorised Signature [In full and initials]:
Name & Title of signatory:

Name of Firm:
Address:

Seal/Stamp of Bidder:

Place:
Date:

Annex 10 - Format for Bid Security Declaration Form

<On Company's Letter Head>

Date: _____ Tender No. _____

To (*insert complete name and address of the Purchaser*)
I/We. The undersigned, declare that:
I/We understand that, according to your conditions, bids must be supported by a Bid Securing Declaration.
I/We accept that I/We may be disqualified from bidding for any contract with NIC-NICSI for a period of five years from the date of notification if:

a) I am/We are in a breach of any obligation under the terms and conditions of this tender; or
b) Have withdrawn/modified/amended, impair or derogate from this tender, my/our Bid during the period of bid validity specified in the form of Bid; or
c) Having been notified of the acceptance of our Bid by the Purchaser during the period of bid validity; and
   (i) failed to execute the contract, or
   (ii) failed to furnish the Performance Bank Guarantee and Security deposit, in accordance with the tender terms and conditions.
d) Any act of any representative of the company through any communication platform(online/offline) that invokes the bid securing declaration as per any clause in the tender.

I/We understand this Bid Securing Declaration shall cease to be valid after thirty days of expiration of the validity of my/our Bid.

Authorized signatory*

Name: (*insert complete name of person signing the Bid Securing Declaration***)**

Dated on _____ day of _____ (insert date of signing)
Corporate Seal (where appropriate)

****The letter of authorization in favour of the signatory, signed by the board to be enclosed as a part of the bid.***
(Note: In case of a Joint Venture, the Bid Securing Declaration must be in the name of all partners to the Joint Venture that submits the bid)

Annex 11 - Format for Integrity Pact

INTEGRITY PACT

(*To be executed on plain paper and to be signed by the Bidder and Purchaser*)

National Informatics Centre (Purchaser) here in after referred to as "The Procuring Agency".

AND

M/s…….. hereinafter referred to as

"The Bidder/Bidder"

PREAMBLE

The Procuring Agency intends to award, underlaid down organisational procedures, contract/s for……. The Procuring Agency value full compliance with all relevant laws of the land, rules, regulations, economic use of and of fairness/transparency in its relations with its Bidder (s) and/or Bidder(s). In order to achieve these goals, the Procuring Agency shall appoint an Independent External Monitor (IEM), who shall monitor the tender process and the execution of the contract for compliance with the principles specified above.

SECTION 1 – COMMITMENTS OF 'THE PROCURING AGENCY'.

1. The Procuring Agency commits itself to take all measures necessary to prevent corruption and to observe the following principles: -
   a. No employee of the Procuring Agency, personally or through family members, shall in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the personal is not legally entitled.
   b. The Procuring Agency shall during the tender process treat all Bidder(s)/Bidder(s) with equity and reason. The Procuring Agency shall in particular, before and during the tender process, provide to all Bidder(s)/Bidder(s) the same information and shall not provide to any Bidder(s)/Bidder(s) confidential/additional information through which the Bidder(s)/Bidder(s) could obtain an advantage in relation to the process or the contract execution.
   c. The Procuring Agency shall exclude from the process all known prejudiced persons.
2. If the Procuring Agency obtains information on the conduct of any of its Employees which are a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Procuring Agency shall inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

SECTION 2 – COMMITMENTS OF 'THE Bidder(s)/Bidder(s)'

1. The Bidder/Bidder commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.
   a. The Bidder(s)/Bidder(s) shall not, directly or through any other persons or firm, offer promise or give to any of the Procuring Agency's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage or during the execution of the contract.
   b. The Bidder(s)/Bidder(s) shall not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications,

certifications, subsidiary contracts, submission or non-submission of Bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

c. The Bidder(s)/Bidder(s) shall not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/Bidder(s) shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information or documents provided by the Procuring Agency as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

d. The Bidder(s)/Bidder(s) of foreign origin shall disclose the name and address of the Agents/representatives in India, if any. Similarly, the Bidder(s)/Bidder(s) of Indian Nationality shall furnish the name and address of the foreign Procuring Agency, if any. All the payments made to the India agent/representative have to be in Indian Rupees only.

e. The Bidder(s)/Bidder(s) shall, when presenting his Bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

f. The Bidder(s)/Bidder(s) who have signed the Integrity Pact shall not approach the courts while representing the matter to IEMs and shall wait for their decision on the matter.

2. The Bidder(s)/Bidder(s)shall not instigate third persons to commit offences outlined above or be an accessory to such offences.

SECTION 3: DISQUALIFICATION FROM TENDER PROCESS AND EXCLUSION FROM FUTURE CONTRACT

If the Bidder(s)/Bidder(s), before award or during execution has committed a transgression through a violation of Section2 above or in any other form such as to put his reliability or credibility in question, the Procuring Agency is entitled to disqualify the Bidder(s)/Bidder(s) from the tender process or to terminate the contract, if already signed, for such reasons.

SECTION 4: COMPENSATION FOR DAMAGES

1. If the Procuring Agency has disqualified the Bidder(s)/Bidder(s) from the tender process prior to the award according to Section 3, the Procuring Agency is entitled to demand and recover the damages equivalent to Bid Security or execution of Bid Securing declaration form, whichever is applicable.
2. If the Procuring Agency has terminated the contract according to Section3, or if the Procuring Agency is entitled to terminate the contract according to Section3, The Procuring Agency shall be entitled to demand and recover from the Bidder liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

SECTION 5: PREVIOUS TRANSGRESSION

1. The Bidder declares that no previous transgressions occurred in the last three years with any other company in any country conforming to the anti-corruption approach or with any other public sector enterprise in India that could justify his exclusion from the tender process.
2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process and appropriate action can be taken including termination of the contract, if already awarded, for such reason.

SECTION 6: EQUAL TREATMENT OF ALL BidderS / VENDORS / SUB- CONTRACTORS.

1. In case of sub –contracting, the Procuring Agency Bidder shall take the responsibility of adoption of Integrity Pact by the Sub – Contractor.

2. The Procuring Agency shall enter into agreements with the identical conditions as this one with all Bidders and Vendors.
3. The Procuring Agency shall disqualify from the tender process all Bidders who do not sign this Pact or violate its provisions.

SECTION 7: CRIMINAL CHARGES AGAINST VIOLATION Bidder(S)/ Bidder(S) / Bidder(S).

If the Procuring Agency obtains knowledge of conduct of a Bidder(s)/Bidder(s) which constitutes corruption, or if the Procuring Agency has substantive suspicion in this regard, the Procuring Agency shall inform the same to the Chief Vigilance Officer.

SECTION 8: INDEPENDENT EXTERNAL MONITOR/MONITORS

1. The Procuring Agency appoints competent and credible Independent External Monitor for this Pact after approval of Central Vigilance Commission. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.
2. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. The Monitor shall have access to all contract documents, whenever required. It shall be obligatory for him to treat the information and documents of Bidders /Vendors as confidential. He reports to the Managing Director, Purchaser.
3. The Bidder(s)/Bidder(s) accepts that the Monitor has the right to access without restriction to all project documentation of the Procuring Agency including that provided by the Bidder/Bidder. The Bidder shall also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors.
4. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/Bidder(s) with confidentiality. The Monitor has also signed declarations on "Non – Disclosure of Confidential Information" and of "Absence of Conflict of Interest" In case of any conflict of interest arising at a later date, the IEM shall inform Managing Director, Purchaser and recuse himself/herself from the case.
5. The Procuring Agency shall provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Procuring Agency and the Bidder. The parties offer to the Monitor the option to participate in such meetings.
6. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he shall so inform the Management of the Procuring Agency and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
7. The Monitor shall submit a written report to the Managing Director, Purchaser within 8 to 10 weeks from the date of reference or intimation to him by the Procuring Agency and, should the occasion arise, submit proposals for correcting problematic situations.
8. If the Monitor has reported to the Managing Director, Purchaser, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Managing Director, Purchaser has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.
9. The word "Monitor" word includes both singular and plural.

SECTION 9: PACT DURATION

This pact begins when both parties have legally signed it. It expires for the Bidder 12 months after the last payment under the contract, and for all other vendors 6 (six) months after the contract has been awarded. Any violation of the same would entail disqualification of Bidders and exclusion from future business dealings. If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by DG, Purchaser.

SECTION 10: OTHER PROVISIONS

1. This agreement is subject to Indian Law. Place of performance and jurisdiction is the registered office of the Procuring Agency i.e., New Delhi.
2. Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.
3. If the Bidder is a partnership, this agreement must be signed by all partners.
4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties shall strive to come to an agreement to their original intentions.
5. Issues like Warranty/Guarantee etc. shall be outside the purview of the IEMs.
6. In the event of any contradiction between the Integrity Pact and its Annexure, the clause in the Integrity Pact shall prevail.

(For & on behalf of the Procuring Agency) (For & on behalf of Bidder/Bidder)

(Office Seal) (Office Seal)

(Authorised Signatory of the Bidder)

Place:
Date:

Witness 1: …….
Witness 2: …….

Annex 12 – Non-Disclosure Agreement

THIS AGREEMENT FOR NON-DISCLOSURE OF CONFIDENTIAL INFORMATION is entered into on this _____ day of _____ ***2024*** by and between:

1. National Informatics Centre (NIC), having its registered office at A**-Block, Lodhi Road, CGO Complex, Pragati Vihar, New Delhi, Delhi 110003** hereinafter referred to as [the Discloser] and

2. _____, having its registered office or based in [insert the Legal Address of the Entity] hereinafter referred to as [the Recipient]

WHEREAS:

The Recipient hereto desire to collaborate/work under, the Discloser, for _____, and to further aid and contribute to the overall success and enhancement of the _____.

Throughout the aforementioned discussions, the Discloser may share proprietary information or Confidential Information with the Recipient subject to the terms and conditions set forth below.

NOW IT IS AGREED AS FOLLOWS:

1. Confidential Information

1.1 For the purposes of this Agreement, Confidential Information means any data or information shared by the Discloser that is not generally known to the public or has not yet been revealed, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to:

(i) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology, or method.

(ii) any concepts, samples, algorithms, reports, data, know-how, works-in-progress, designs, drawings, photographs, development tools, specifications, software programs, source code, object code, flow charts, and databases.

(iii) any marketing strategies, plans, financial information, or projections, operations, sales estimates, business plans and performance results relating to the Discloser's past, present or future business activities, or those of its affiliates, subsidiaries, and affiliated companies.

(iv) trade secrets; plans for products or services, and customer or user lists.

(v) any other information that should reasonably be recognized as Confidential Information by the Discloser.

1.2 The Discloser and the Recipient agree hereby that Confidential Information needs not to be novel, unique, patentable, copyrightable or constitutes a trade secret in order to be designated Confidential Information and therefore protected.

1.3 The Recipient hereby acknowledge that the Information shared by the Discloser is the sole property of the Discloser and it has been obtained through great efforts and shall be regarded and kept as Confidential Information.

1.4 Notwithstanding the aforementioned Confidential Information shall exclude information that is already in the public domain at the time of disclosure by the Discloser to the Recipient or thereafter enters the public domain without any breach of the terms of this Agreement.

2. Purpose of the Disclosure of Confidential Information

The purpose of the disclosure of confidential information to the Recipient is for carrying out Research activities, which could further aid in the enhancement of _____and thereby improve the Service delivery through the App.

3. Undertakings of the Recipient

3.1 In the context of research activity, discussions, preparations or any other activity related to the _____ Application, the Discloser may disclose Confidential Information to the Recipient. The Recipient agrees to use the Confidential Information solely in connection with purposes contemplated in this Agreement and not to use it for any other purpose or without the prior written consent of the Discloser.

3.2 The Recipient will not disclose and will keep confidential the information received, except to its employees, representatives, students, research scholars or contractual staffs who need to have access to the Confidential Information for the purpose of carrying out their duties in connection with the permitted purposes specified in clause 2. The Recipient will inform them about the confidential quality of the information provided and will ensure that their agreement is obtained to keep it confidential on the same terms as set forth in this Agreement. Hence the Recipient will be responsible for ensuring that the obligations of confidentiality and non-use contained herein will be strictly observed and will assume full liability for the acts or omissions made for its personnel, representatives, students, research scholars or contractual staffs.

3.3 The Recipient will use the Confidential Information exclusively for the permitted purpose stated in clause 2 and not use the information for their own purposes or benefit.

3.4 The Recipient will not disclose any Confidential Information received to any third parties, except as otherwise provided for herein.

3.5 The Recipient shall treat all Confidential Information with the same degree of care as it accords to its own Confidential Information.

3.6 The Discloser shall undertake every possible effort to provide anonymized data/information to the Recipient for the purpose as mentioned in Clause No.2. However, in case if any data/information shared with the Recipient does contain any Personally Identifiable Information or any other information which may reveal an individual's identity or if the recipient found a way to de-anonymize the data, then the Recipient shall promptly inform the Discloser regarding this and shall undertake to voluntarily delete all such Personally Identifiable/De-anonymized information.

3.7 The Recipient shall regularly share with the Discloser the outcomes of the Research and its derivates, which were arrived at using the confidential information.

3.8 The Recipient shall also undertake to transfer to the Discloser, any knowledge or expertise or skill or Intellectual Property or technology or software or research material, which was gained or generated using the confidential information shared by the Discloser.

3.9 All Confidential Information disclosed under this Agreement shall be and remain under the property of the Discloser and nothing contained in this Agreement shall be construed as granting or conferring any rights to such Confidential Information on the Recipient. Principally, nothing in this Agreement shall be deemed to grant to the Recipient a licence expressly or by implication under any patent, copyright or other intellectual property right. The Recipient hereby acknowledges and confirms that all the existing and future intellectual property rights related to the Confidential Information are exclusive titles of the Discloser. For the sake of clarity based in good faith, the Recipient will not apply for or obtain any intellectual property protection in respect of the Confidential Information received. Likewise, any modifications and improvements thereof by the Recipient shall be the sole property of the Discloser.

3.10 The Recipient shall promptly return or destroy all copies (in whatever form reproduced or stored), including all notes and derivatives of the Confidential Information disclosed under this Agreement, upon the earlier of (i) the completion or termination of the dealings contemplated in this Agreement; (ii) or the termination of this Agreement; (iii) or at the time the Discloser may request it to the Recipient.

3.11 In the event that the Recipient is asked to communicate the Confidential Information to any judicial, administrative, regulatory authority or similar or obliged to reveal such information by mandatory law, it shall notify promptly the Discloser of the terms of such disclosure and will collaborate to the extent practicable with the Discloser to comply with the order and preserve the confidentiality of the Confidential Information.

3.12 The Recipient agrees that the Discloser will suffer irreparable damage if its Confidential Information is made public, released to a third party, or otherwise disclosed in breach of this Agreement and that the Discloser shall be entitled to obtain injunctive relief against a threatened breach or continuation of any such a breach and, in the event of such breach, an award of actual and exemplary damages from any court of competent jurisdiction.

3.13 The Recipient shall immediately notify upon becoming aware of any breach of confidence by anybody to whom it has disclosed the Confidential Information and give all necessary assistance in connection with any steps which the Discloser may wish to take prevent, stop or obtain compensation for such a breach or threatened breach.

3.14 The Confidential Information subject to this Agreement is made available "as such" and no warranties of any kind are granted or implied with respect to the quality of such information including but not limited to, its applicability for any purpose, noninfringement of third-party rights, accuracy, completeness, or correctness. Further, the Discloser shall not have any liability to the Recipient resulting from any use of the Confidential Information.

3.15 The Recipient shall not disclose any information shared by the Discloser to anyone who is either a citizen or a resident of a foreign country. The Recipient shall also undertake that they shall not involve any citizen or resident of a foreign country in the research activities involving the information disclosed by the Discloser.

3.16 The Discloser is not under any obligation under this Agreement to disclose any Confidential Information it chooses not to disclose.

3.17 Nothing in this Agreement shall be construed to constitute a partnership, joint venture, or other similar relationship between the Discloser and Recipient.

3.18 The recipient must ensure to provide the signed NDA in case of change in antecedents, delegates and the sub-contractors from time-to- time. The recipient will notify the discloser promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Contract or with the authority of the Discloser.

S. No.	Name of the Resource	Designation/ Position	Signature
1			
2			

4. Miscellaneous

4.1 Duration and Termination

4.1.1 This Agreement shall remain in effect for a term of 5 Years. Notwithstanding the foregoing, the Recipient's duty to hold in confidence Confidential Information that was disclosed during the term shall remain in effect indefinitely, save otherwise agreed.

4.1.2 At any point of time, the Discloser may direct the Recipient to return all the confidential information shared by the Discloser and its derivatives. Upon receiving such request, the Recipient shall duly comply with the direction and return the confidential information and destroy all copies of the information (if any). The Recipient shall submit a signed undertaking that they have returned the Confidential information and destroyed all copies of the information and its derivates.

4.2 Applicable Law and Jurisdiction
This Agreement shall be construed and interpreted by the laws of India. The High Court of Delhi shall have jurisdiction on any matters related to this agreement.

IN WITNESS WHEREOF, the Parties hereto have caused this Non-Disclosure Agreement to be executed as of the date stated above.

FOR [*insert name of* Corporation/Company/Firm]

[insert name of authorized representative]
[*insert title*]

Done at [*place*]on [*date*]

Annex 13 – Make In India Certificate

To Whom So Ever It May Concern

Date:

Sub:- Make in India Certificate in respect of << Bidder's Name>> for the Bid No …… for "Selection of Bidder for supplying and maintaining ICT components for log management analytics "

This is to certify that M/s ……<>>…….. having its Registered Address at --------- ---------- complies with Letter no P45021/2/2017- (BE-II) dated 15.06.2017 Public Procurement (Preference to Make in India) Order 2017" (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised and amended time to time and also clarifications, guidines and FAQ issued by DPIIT in this respect from time to time.

Accordingly, we Statutory Auditor/ Cost Auditor of M/s ……<>…….. (A "Class-…. Local Supplier) hereby certify that the Local content as defined under the PPP-MII, in the Goods/Equiment(s)/Service(s)/Works to be supplied by the "Class-…. Local Supplier" for "Selection of Bidder for supplying and maintaining ICT components for log management analytics " is more than …..%.

The definition and calculation of local content is in accordance with Letter no P45021/2/2017- (BE-II) dated 15.06.2017 Public Procurement (Preference to Make in India) Order 2017" (MII) of Department for Promotion of Industry and Internal Trade, (DPIIT - Public Procurement Section) as revised and amended time to time and also clarifications, guidines and FAQ issued by DPIIT in this respect from time to time.

Seal and signature of the Statutory Auditor/ Cost Auditor

(Name of the Statutory Auditor/ Cost Auditor)

Place:

Membership No Date:
Firm Registration No
UDIN: