NOTICE INVITING TENDER

The Finance Department invites sealed bids through an open tender process from eligible, experienced, and reputed vendors/system integrators for the design, supply, installation, commissioning, and maintenance of a Micro Data Centre to support the operations of the State Integrated Financial Management System (SIFMS2.0) "Pranali" application.

1. Scope of Work:

The successful bidder will be responsible for the end-to-end setup of a Micro Data Centre, including but not limited to:

- Design and deployment of a secure, scalable, and modular Micro Data Centre infrastructure.
- Provisioning of servers, storage, networking, cooling, fire suppression, UPS, and related systems from the Indian Manufacturers having the machinery parts and accessories built in India.
- Integration with existing IT infrastructure of the Finance Department.
- Ensuring high availability and disaster recovery capabilities.
- Support and maintenance for a defined contract period with complete warranty of the equipment.
- Supply, Installation, Testing, Commissioning and maintenance for one year, including Warranty and onsite Support for the period of 5 years from the date of commissioning. The broad Technical specifications are provided below.

S.No.	A-Major Description of Items	Qty.
1	2U Rack Server	4
2	Smart Rack Solution including, Servers Racks, Cooling System, UPS system, Battery Banks, Access Control System, iBMS, Fire Safety & Suppression, CCTV, Water Leakage Detect System, Rodent Repellent, Alarm etc.	1
3	Silent DG with AMF Panel	1
4	32TB Usable NAS/SAN	1
5	24 Port Network Switch(2) and SAN Switch(1)	3
6	Next Gen Firewall	2
7	VMware/ Proxmox VE	1
8	Windows Server 2022 or above(Data centre edition)	24
9	SQL Server 2022 STD or above version	24
11	Antivirus	24
12	LAN Cables (OFC & Cat6)	1
13	Manpower (System Admin)dedicated full-time resource for project and warranty	1

Sl.No.	B-DETAILED ITEM DESCRIPTIONSUNDER (A) FRO SERVERS VMWARES/Proxmox VE OPERATING SYSTEMS STORAGE ETC	Qty.

1	Server Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM 2x Processor Intel Xeon Gold 6442Y 2.6G, 24C/48T, 16GT/s, 60M Cache, 1024 GB RDIMM, 4800MT/s Dual Rank 4, RAID Controller SAS Front 1 3 x Hard Drives 480GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 2 x Power Supply Dual, Hot-plug, Power Supply Redundant (1+1), Mixed Mode, NAF 1, iDRAC9/iLO, Enterprise 16G 1, 1 x OCP 3.0 Network Adapters Broadcom 57454 Quad Port 10GbE Base-T Adapter, OCP NIC 3.0 1, 1 x Fibre Channel Adapters Emulex LPe35002 Dual Port FC32 Fibre Channel HBA, 5 yrs. Warranty or Latest Model with higher or similar configuration having security and health system.	4
2	VMware including vSphere & vCentre for total 192 Core of processor (core based, bulk License) or Proxmox VE (as per requirement)	192
3	NextGen Firewall - Hardware Plus 24x7 UTM Bundle for 5 years (Minimum steps, given in technical Bid) (DETAILS ON SEPARATE TABLE BELOW)	2
4	Storage with 30 tb usable SSD, Components Base Array-1 Controller Cards 32Gb FC Type-B 8 Port Dual Controller 1, 16G/SFP and 32G/SFP+ FC Optics 2X SFP, FC16, 16GB -1, Multi-Mode FC LC-LC Cables Networking Cable, OM4 LC/LC Fiber Cable, (Optics required), 8X2 Meter, Hard Drives-5, Hard Drive Blank Filler 3.5, 5X Hard Drive 3.84TB SSD SAS ISE, Read Intensive, up to 24Gbps 512e 2.5in with 4 X 3.5in HYB CARR, AG Drive	1
5	Windows Server 2022 or latest for 24 vm	24
6	SQL Server 2022 STD for 24vm	24
8	Antivirus for VM Server	24
9	Cisco Gigabit Network Managed Switch(2)and SAN Switch (1)	3
10	LAN Cables (OFC & Cat6)	1

sl. No.	C- Description of Smart rack, electrical system ,UPS, Cooling system, Fire Detection system, CCTV under –(A)	Qty	UOM
A)	**Racks and Accessories**		
1	TS8 Frame, 800 W x 2000 H x 1200 D, Front Glass Door with Rear Sheet Steel Double door & Accessories	2	EA
2	Vertical PDU, 32A, Single Phase, C13 Sockets - 16nos, C19 Sockets - 6nos, 32A MCB, Power cord of 6sqmm x 3core cable with pin type lugs.	4	EA
B)	**Cooling Unit with Piping and Low side works**		
1	External Condensing Unit (ODU) - 10kW	2	EA
2	Redundancy Controller with Display Unit	2	EA
	Zero U Rack based Heat Exchanging Unit (IDU)	2	EA
3	DX copper piping & installation of 25 mtr with refrigerant charge, cabling, stand and other low side accessories	2	Lot
C)	**CMC III monitoring system -for racks**		
1	CMC Monitoring System with Temperature, humidity, Leakage sensor, Access control, Signal pillar & Biometric reader	1	EA

D)	**Electrical Works**		
1	Electrical Works - 1no of wall mount Raw Power DB, 2Nos of UPS DB, Cabling, Cable Tray with accessories, Earthing Considered inside Data centre only. (**Customer has to provide the incoming cable for the Raw power DB & earthing cable till the data centr**e)	1	Lot
E)	**UPS System**		
1	120kVA Floor Mountable ONLINE UPS, Single Phase Input & Single-Phase output, SNMP Card, Slide rails, battery cabinets & Interlink cables	1	EA
2	SMF Batteries for 5Hours Battery backup on each UPS- External Mount Note: Distance between the UPS Room to DC Room 10mtr, anything extra it will Charges extra as per RMT basis		EA
F)	**Room based fire detection & suppression system**		
1	Rack based fire detection & suppression system **without VESDA** System for 2 racks solution	1	Set
2	Rodent Repellent system for Racks	1	Set
G)	**CCTV**		
1	2nos CCTV camera (for front & rear of Rack row monitoring) with 4 channel NVR with power cables, CAT 6 cable & PVC conduit.	1	Set

Sl. No.	D-Other Descriptions	Qty	UOM
	Site Preparation for the SITC of Smart Rack Solution		
A)	**Electrical Works**		
1	Smart Row DB Panel via 1C x 25 SQMM copper flexible Cable (Green Colour)	100	Mtr.
B)	**Biometric Access Control System**		
1	Biometric Access Control System	1	Set
C)	**DG Set**		
2	82.5KVA DG with AMF Panel, power cabling, MCCB and LINE termination with dedicated earthing and exhaust systemetc.	1	Set
D)	**Project Management Charges**		
1	PMC	1	Job

2. <u>Eligibility Criteria:</u>

- The bidder must be a registered legal entity.
- Must have executed similar projects for government or large enterprises in the last 15 years.
- The bidder is not blacklisted by any government department or agency.
- Must possess MAF Certificate from reputed Manufacturers to deal with Computer Hardware and peripherals (i.e. Servers, Racks, Storage, SAN, Switches, cooling devices, Software, Firewall etc)
- Vendor Empanelment Certificate with the Information Technology Department.
- Must be in the IT Solution Field for more than 15 Years
- **Valid Original Equipment Manufacturer (OEM) and Manufacturer's Authorization Form (MAF) Compliance Authorization Certificate** from the manufacturers of all major hardware and software components (e.g., Servers, Racks, Storage, SAN, Switches, Cooling Devices, Software, Firewall, etc.),

confirming the bidder's authorization for sales, support, maintenance, and on-site training."

- Compliance requirements, ensuring the authorized entity adheres to the OEM's standards and guidelines.
- OEM Training and Support(manpower) for 1 year.
- Must have executed **such projects** involving **Servers supply and installation in Micro Data Centres / Departments or PSUs and other autonomous bodies** for government or large enterprises in the last 15 years, supported by submission of corresponding **work completion certificates**.
- Preference will be given to those who have executed the Data Centre work/setup
- Company's 3 Financial Years balance sheet denoting a Minimum of 3.5Cr turnover.
- Must have office in and around Gangtok with Technical Manpower support for Hardware and software services and support calls.

3. <u>Bidding Process</u>:-There shall be two bid process in this tender, viz;

A. Technical Bid:- Comprising of the following broad parameters with the design, architecture, Hardware, Specifications and the justifications supporting the chosen product and manufacturer in terms of quality and grade of the hardware, supported with relevant documents, data and statistics as per the minimum requirement given above in A,B,C,D. This is not inclusive list of the technical bid specifications but only represents the broad parameters under it.

a. Data Centre Core Infrastructure (Smart Rack Solution)
b. Core IT Hardware
c. Network & Security Equipment
d. Software/Hardware Licenses
e. Firewall system and specifications.
f. Cabling, Circuits, Networking
g. Power & Electrical Infrastructure
h. Technical Human Resources with technical qualifications, Experience and Skills in handling the data center projects.
i. Project Management policy/Strategy
j. Project timeline
k. Warranty period, Support, Maintenance, with time line .
    - **i.** Availability of strong technical support and professional services for seamless operations**.**
    - ii. Location and Infrastructure for support and maintenance: Proximity to data centers and the availability of robust infrastructure .
    - iii. Warranty with extended period within the project cost.

l. **Server and other hardware specifications with ISO compliance as per the details given above under A,B,C, D.**
m. Justifications for the technical architecture and the quality of hardware chosen with its details as under:-
    - i. Chosen servers based on performance, reliability, and scalability to meet the specific needs.
    - ii. **Cost-Effectiveness:** including initial purchase, maintenance, and energy consumption ratings as well life period under normal circumstances.
    - iii. **Justifications** for choosing the manufacturer of the hardware indicated in the technical bid**.**
n. **Firewall and Antivirus, Warranty other details .**

B. <u>Financial Bid</u>:-Financial bid indication item-wise price for the items mentioned in the technical bid. The Financial bid of the bidders qualifying the technical bid shall only be opened.

<u>Next Generation Firewall</u>(Items Details)

Minimum specification
Make & model *((Please specify make & unique model name))*
Next Generation Firewall – Architecture
The solution should provide Next Generation Firewall capabilities.
Appliance based Security platforms should provide Threat Prevention functionality in a single appliance.
Appliance hardware should be a multicore CPU Architecture with a hardened 64-bit operating system for faster processing.
Solution should be able to support Firewall, IPS, Application Control, URL Filtering, AV, BOT features, Geo-Protection and cloud sandboxing.
The Solution should support integrated ZTNA capabilities to enable employees and third parties to access on-premises applications and infrastructure from anywhere and IPSEC VPN/SSL VPN with Client Software.
Performance & Operational Requirement
The proposed solution should be supplied with Primary & HA appliance that should be same model & features of primary device.
The Firewall shall support failovers in case of primary hardware failure without session loss and manual intervention to a standby unit.
The Firewall shall support a minimum of 3 Gbps of Threat Prevention throughput with multiple security modules implemented and running.
The Firewall shall support a minimum of 3.3 Gbps of IPS throughput.
The Firewall shall support a minimum of 750 Mbps of TLS Inspection Throughput from day one for scanning the SSL encrypted traffic.
The Firewall shall support a minimum of 120,000 SSL Inspection connections from day.
The Firewall shall support a minimum of 2 Gbps of IPSec VPN throughput.
Hardware & Interface Requirement
Minimum 16 Numbers of 1G Ethernet ports and Min. 2 x 10G SFP+ ports per firewall. The solution should be provided with 2x10SFP+ multimode module alongwith firewall.
Should support both Console port and USB Ports.
Should have integrated redundant power supply on both primary & HA firewalls.
Should have min 16GB or 32GB+ RAM in both primary & HA firewalls.
Should have a minimum and much larger SSD storage (256GB or 500GB+) of Internal SSD Storage for keeping the logs & firmware backup etc in both the firewall.
Security Operational Requirement
The solution must have the ability to inspect all network traffic through security scanning to protect against threats including vulnerability exploits, viruses, spyware and data leakage.
The solution should support the ability to work in Transparent/Bridge mode.
The proposed Solution should support automatic ISP failover as well as ISP load sharing or load balancing for outbound traffic.

Solution should Support 6 to 4 NAT, or 6 to 4 tunnels.
The IPS should scan all parts of the data packet in both directions by default and should not buffer traffic before scanning for IPS.
Solution should have the functionality of Geo Protection to Block the traffic country wise in incoming direction, outgoing direction or both.
IPS should be able to detect and prevent embedded threats within SSL traffic.
The solution should have featured Deep Packet Inspection SSL scanning, block files-based on extensions & should not buffer traffic before scanning for virus.
The solution must be capable of inspecting TLS/SSL and SSH encrypted connections regardless of port or protocol & the proposed system shall support for TLS cipher suites up to TLS 1.3.
The solution should have the capability to protect against Denial of Service (DoS) and DDoS attacks and should have flexibility to configure threshold values to prevent DOS and DDOS attacks.
The solution should have protection against Flood attacks (UDP/TCP-syn/ICMP floods), Smurf attacks, LAND (Local Area Network Denial) attacks , Spank Protection and other denial of service attacks.
The solution should have URL categorization, reputation-based URLs protection for checking, providing additional security against attempts to bypass the rating system.
It should be able to block Instant Messaging like Yahoo, MSN, ICQ, Skype etc.
It should enable blocking of Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC etc.
The solution should provide a mechanism to limit application usage based on bandwidth consumption or BMW.
Vendor must have an integrated Anti-Bot and Anti-Virus protection capabilities on the next generation firewall.
The firewall should have signature-based detection engine to protect internal server from known attacks SQL Injections, man-in-the-middle or Session Hijacking, URL Tampering, Cookie Poisoning etc.
Solution should support detection & prevention of cryptojacking & ransomware. Anti-bot applications must be able to detect and stop suspicious abnormal network behavior/attack.
SAML Single Sign-On for User identification, Firewall administration, and Remote Access VPN (SSLVPN).
The proposed firewalls shall support Zero Trust Network Access (ZTNA) capabilities to ensure that user and device trust are repeatedly verified before granting access to specific applications, regardless of location and endpoint type to private apps hosted behind firewall. The solution must include 5 (Five) ZTNA licenses from day one.
Solution must support data integrity with md5, sha1 SHA-256, SHA-384 and AES-XCBC
Should support both Static and all major Dynamic routing protocols.
The proposed firewall must be able to integrate with SIEM, NAC or Microsoft Azure Sentinel for security information event management (SIEM) and security orchestration automated response (SOAR) solution.

The proposed firewall solution supports a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic.
NGFW should be capable to couple with endpoint protection to block, viruses entering network through servers, laptop and other unprotected systems.
Next-generation antivirus must use a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state on windows servers.
The solution must ensure every server accessing the network has the appropriate EDR software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Solution should have Automated deployment and installation option of EDR in clients across the network to minimize administrative overhead.
NGFW solution should have the option to integrate with EDR solution and both solutions should be same OEM.
Anti-Malware & Advanced Persistent Threat
The solution shall support cloud based and On Prem based advanced threat protection technology for preventing zero-day threats. OEM must have the own advanced threat protection technology for cloud based and On Prem based Sandboxing.
NGFW should have cloud advanced threat protection functionality to protect organization from Advance Persistence Threats. In case any additional license is required, bidder must include it in proposal from day one.
The cloud advanced threat protection functionality block file download until a verdict is returned, that ensures no packets get through until the file is completely analyzed. The file is held until the last packet is analyzed. If the file has malware, the last packet is dropped, and the file is blocked. The threat report provides information necessary to respond to a threat or infection.
The cloud advanced threat protection should support Executables, PDF,doc , xls ,docx , xlsx , Archives (.jar, .apk, .rar, .gz, and .zip).
The cloud advanced threat protection displays a list of all the files that have been scanned and analyzed. User can filter results, search, search for specific strings to show scans from the last month, last week, last 24 hours, and in the last hour.
The cloud advanced threat protection should have submitted a sample option allows user to browse for supported files, submit, and scan them for analysis. Supported files include .EXE, .MSI, .ZIP, .APK, and .PE files with a file size of 5MB or more.
Administrator can view file-analysis status details including file submission time, source /destination IP, File size, File type, Suspicious Act etc.
Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis.
High Availability
The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component.
The NGFW shall support stateful session synchronization in the event of a fail-over to a standby unit.

The NGFW must support Active-Active/ Active-Passive stateful High Availability options.
The HA solutions should support silent firmware upgrade process that ensures minimum downtime.
The NGFW shall support interface link monitoring failover.
Centralized Management
Should support both CLI and GUI configuration management.
Management solutions should be able to do Log analysis and Reporting in same appliance or different appliance. Vendor must propose own solution. The management & reporting platform shall be hardware or virtual appliance or cloud based solution.
Management Solution must include the option to search inside the list of events, drill down into details for research and forensics
Management Solution must include predefined OnDemand, daily, weekly or monthly reports. Including at least Top events, Top sources, Top destinations, Top services etc.
The solution should store analytics data at a minimum of 7 days and 60 days log retention depends on disk utilization. Bidder can offer individual solution based on OEM architecture to meet the requirements.
The proposed solution must support Packet Monitor, Ping, Traceroute Diagnostics tools for troubleshooting.
The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
The management solution must allow the report to be exported into other formats such as PDF, CSV etc and support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis
Centralized Management of Firewalls shall create templates and perform commits at the "All Tenants" . This streamlines updates across all tenants, ensuring consistency, efficiency, and faster deployments.
Centralized Management of firewall cloud backups and change firewall time within templates.
Admins can view out-of-date firmware information on the Management inventory page. They can also group by firmware version to view firewall versions running on their firewalls in Inventory.
Admins can generate attack report of devices. Attack reports provide visibility into potential security incidents, allow admins to investigate, respond, and enhance network security measures to prevent future breaches.
Admins can generate Web Activity Schedule PDF report to analyze websites visited by the users
Warranty and Support for Firewall system
All Required features of firewall, management & reporting software should be done by OEM.
License for NGFW high availability with next generation firewall security applications, including intrusion protection, application control, URL filtering, Anti-Bot, Anti-Virus, DNS protection, advanced threat protection etc,
The License for Management, Reporting and any other license required to meet the above features should be provided from day 1 for min. period 3 (three) years.

The proposed solution including Firewall, Transceivers, Sandboxing, ZTNA, Management & Reporting must be from same OEM for better correlation.
5 years comprehensive warranty and support for hardware, software updates and patches shall be offered directly from the OEM
OEM should have AI-Driven Open XDR SIEM to provide proactive threat analytics and automatic remediation for your firewall, servers and other devices through 24/7 Socas in future.
OEM must have own managed service solution along with 24x7 monitoring, health check etc. Customer may avail the solution for proposed Firewall as and when required in future as an addon service. OEM may propose this solution along with required license.
OEM should have TAC and R&D centre in INDIA. Proposed solution should support 24x7 remote technical support by OEM through chat/email / remote access.
Industry Standard/Certification
Proposed Firewall manufacturer should be placed in Gartner Magic Quadrant of Enterprise/Network firewall for last three years.
The Firewall, Antivirus & Advanced Threat Defence module should have ICSA or other equivalent Certification.
OEM should have scored a minimum of 97% in Exploit Block rate and 93% in Security Effectiveness in the last NSS Lab report for NGFW (2019).
The firewall should have FIPS 140-2 Level 2 (with Suite B) , IPv6/USGv6 and Common Criteria/EAL4+ certified certifications from day one.

4. **Submission of Earnest Money Deposit:**

The bidder has to submit an interest-free Bid Security/ Earnest Money Deposit(EMD)of**₹7,50,000/-***(Rupees seven lakhs fifty thousand)* in the form of a Cheque /Demand Draft drawn on a Nationalized Bank in favour of the Secretary**, Finance Department, Government of Sikkim** payable at Gangtok at the time of submission of bids.

a) The EMD of the Bidder failing to qualify the tender shall be refunded back
b) The Bid Security of the successful bidder shall be returned, without any interest, only after the submission of their acceptance against the issued award of contract within the stipulated time period and furnishing of the Performance Bank Guarantee @5 % of the total order value.

5. Bid Price:-

The Bidders would have to quote the prices in Rupees only, for the total scope of work including Supply, Installation, Testing and maintenance of Servers and other hardware as mentioned above. No separate itemized bids will be accepted. The Bidders are advised not to indicate discount

separately. Discount, if any, should be mentioned in the quoted prices. The Price quoted should be inclusive of GST and all other applicable Taxes/Duties.

6. **Licensing Requirements: -**

a. All system software, licenses, etc. have to be procured in the name of the Secretary, Finance Department of Sikkim.

b. The system software licenses mentioned in the Bill of Materials shall be genuine, perpetual, full use and should provide upgrades, patches, fixes, security patches and updates directly from the OEM.

c. A comprehensive warranty that covers all components shall be issued after the completion of the work by the successful bidder. The warranty should cover all materials, licenses, services, and support for all the related software, patches upgrades. The warranties shall be with serial number and warranty period.

7. **Installation Process:**

a. During installation at site, if any item is found to be defective or broken, it will be replaced with new one by the vendor at its own cost and risk immediately.

b. Consolidated Installation Report, based on the successful installations of the individual items, shall be submitted to the Finance Department of Sikkim along with the bills.

8. **Right to Accept and Reject the Bid:**

Notwithstanding anything contained in this document, the Competent Authority of the Finance Department, Government of Sikkim, reserves the right to accept or reject any bids including the proposal of the lowest bidder.

9. **Site Visit by interested eligible bidders:** If required the bidder may visit the installation site i.e. Finance Department, Government of Sikkim on prior intimation to the IT Section of the Finance Department and obtain information at its own responsibility and risk. The costs of visiting the office shall be at the bidder's own expense. However, failure of a bidder to visit the site will not be a cause for its disqualification.

10. Payment terms:

a. No advance payment will be made.

b. Payment can be made against the work progress.

c. The final payment shall be made after completion of the work.

d. 5% Security deposits shall be deducted from the gross payment.

11. Super scripting quotation Proposal Envelope:

The Bidders shall submit their Bids in three separate sealed envelopes in the following format:

a. COVER- A containing Earnest Money Deposit should be sealed in a separate envelope subscribing " **EMD**";

b. COVER B containing **TECHNICAL BID** should be sealed in a separate envelope subscribing **"Technical Bid"**.

c. COVER C containing **FINANCIAL BID** should be sealed in a separate envelope subscribing "**Financial Bid**".

All the above mentioned three envelopes together should be enclosed and submitted in a properly sealed separate envelope mentioning the name of the quotation as "**MICRO DATA CENTRE BIDS**" along with the Quotation Reference. No. If any Bidder deviates from submitting its Bid other than the prescribed format, the Bid shall be summarily rejected and shall not be taken into consideration for evaluation.

12. Submission of Documents:

The following documents are also to be submitted by the Bidders in the envelope '**COVER-B'** along with the Technical Bid:

a. Bidder's Profile.

b. Documents in proof of GST Registration, TIN No and PAN No.;

c. Last three years Income-tax Clearance Certificate, if applicable;

d. Audited Balance sheets of last three years;

e. The bidder's annual financial turn over during last five Financial Years.

f. Self-declaration on a duly Notarized Affidavit in a Stamp Paper of Rs.200/- that the Bidder has not been blacklisted by any Government Departments of the Country/Central/ State Government/ Public Sector Undertaking/ Autonomous Bodies under Central and State Governments in India.

g. Proof of office address at Gangtok.

h. Original Equipment Manufacturer (OEM) and Manufacturer's

Authorization Form (MAF) Compliance authorization certificate

i. Technical proposal indicating Make, Model and manufacturing year of items offered with detailed specifications.

13. <u>On-site Warranty & Maintenance:</u>

a. The onsite comprehensive warranty for the same shall be for minimum of **05(Five) years**. Same to be calculated from the date of installation.

b. All cost of repairs/replace such as additional spare parts, patches, labour, transportation cost and any software updates/upgrades required to run the aforementioned hardware items shall be included in the warranty of the product at **<u>no extra cost</u>**.

c. Preventive Maintenance Service: Free onsite quarterly preventive maintenance service shall be provided by Seller during the period of warranty.

14. <u>Service & Support:</u>

a. The bidder must be able to provide service and support within 24 hours of reporting of a fault in the devices so that no any delay is caused in restoring the fault. Also, a Company Authorized Service Centre at Gangtok must be available.

b. In case of non-availability of service centre at Gangtok (Capital City),the selected bidder shall empanel or authorize such service centres at Gangtok for maintenance and support.

c. Bidder has to complete the required Service / Rectification within 24 hours or a maximum extension of seven days' time which may be considered by the Finance Department Government of Sikkim in its discretion. If the successful bid- der/awardee of the work fails to complete service / rectification with de- fined time limit, a penalty of 0.5% of Project cost be charged as penalty for each week of delay from the seller during the warranty period. No extra charges viz. hardware installation, maintenance, TA/DA will be paid.

15. <u>Delivery & Installation:</u>

a. Delivery and installation will have to be done within 30 days from the date of issuance of work order.

b. The successful bidder has to do all the installation including laying of electrical cabling inside the MDC, network cable, etc whichever would be required for installation and commissioning.

c. All aspects of safe transportation of Goods and Material at installation site shall be the exclusive responsibility of the successful bidder.

d. The successful bidder should install and make his own arrangement for loading and unloading the goods at specified site without any additional charge.

e. Any deviation found in the specifications of the delivered goods from the tender specification, will lead to cancellation of the work order and the investments made in the project shall also be borne by the successful bidder receiving the work order.

16. <u>Terms and Conditions:</u>

a. Bidders are advised to study all technical and commercial aspects, instructions, forms, terms and specifications carefully in the tender document. Failure to furnish all information required in the Tender Document or submission of a bid not substantially responsive to the tender document in every respect will be at the Bidder's risk and may result in the rejection of the bid. It will be imperative on each bidder to fully acquaint himself with all the local condition sand factors, which would have any effect on the performance of the contract.

b. This tender document is not transferable. Consortium, Outsourcing and Sub-contracting is not allowed at any stage of the project.

c. No Hardware/Software will be provided by the Finance Department. The successful Bidder is required to set-up all the necessary hardware/software at its own cost at the specified locations.

d. The Finance Department may terminate the agreement, if the work done is not satisfactory without assigning any reasons.

e. The bidders while bidding are expressly required to mention all the terms and condition of this tender document or sign each and every page of this tender document and all the Annexures, which shall be considered as acceptance of all the terms of this tender document.

17. Tender Document & Submission:

- Detailed tender documents can be downloaded from www.sikkimfred.gov.in.
- The Tender Application cost is Rs.20000/- (Non-refundable). A Bank receipt under the receipt head. 0070-00-800-04-00-00 need to be submitted along with the Tender Documents.
- The last date for submission of bids is 10-09-2025 **up to 4:00PM**.
- Bids must be submitted in accordance with the terms and conditions specified in the tender document.

18. Contact for Queries:

For any clarifications or queries, please contact:

(1) Joint Director, IT Cell
Finance Department
Email:sairaj19.chettri@gmail.com/dydiritcell.2020@sikkim.gov.in

(2) Deputy Director, IT Cell
Finance Department
Email: prasant.pao@gmail.com/aopranali.2020@sikkim.gov.in

The Finance Department reserves the right to accept or reject any or all bids without assigning any reason.

-sd-
Secretary Cum Controller of Accounts
Finance Department,
Government of Sikkim.