



GIC HOUSING FINANCE LTD.

REQUEST FOR PROPOSAL TOWARDS IMPLEMENTATION OF WIRELESS LAN INFRASTRUCTURE, NETWORK ACCESS CONTROL SYSTEMS AND ITS MANAGED SERVICES FOR 5 YEARS PERIOD

RFP Reference Number:REF:GICHF:2024-25/07 Dt. 24-12-2024

ACTIVITY SCHEDULE		
S.NO.	ACTIVITY	DETAILS
1	Release of RFP	24th December, 2024 Tuesday
2	Address for Receipt/Submission of Bid document	GIC HOUSING FINANCE LTD National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020.
3	Bid Submission	Sealed - Technical & Commercial Bids in Hard Copy only.
4	Last Date & Time for submission	14th January, 2025 13:00 hrs
5	Bid Opening Date & Venue	15th January, 2025 (To be opened and evaluated internally at GICHFL Head Office).
6	Contact Details	<ul style="list-style-type: none"> • Shubadha Divate shubhadadivate.v@gichf.com • Premraj Avasthi, AVP-IT premraj.avasthi@gichf.com

About GIC Housing Finance Ltd:

GIC Housing Finance Ltd (GICHFL) is a company registered under Section 25 of the Companies Act, 1956 with its Registered Office at National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020 and its 72 Branch Offices across PAN India.

Our Promoters are General Insurance Corporation of India, The New India Assurance Company Ltd, United India Insurance Company Ltd, The Oriental Insurance Company Ltd and National Insurance Company Ltd.

Objective of RFP:-

GIC Housing Finance Limited (hereinafter referred to as “GICHFL”) is issuing this Tender document (hereinafter referred to as “the Tender Document” which expression shall include all attachments and annexures hereto as well as all amendments, addendums, modifications, and alteration hereto) to service providers, (hereinafter referred to as “the Bidder”) to enable them to participate in the competitive bidding for “WLAN Infrastructure Implementation with Support”. The Selected Bidder must provide, manage, and maintain all necessary infrastructure components and services that would be necessary as per the defined requirements of the Bid Document. The Selected Bidder must ensure that all desired objectives of GICHFL are fulfilled.

GICHFL invites proposals for “Wireless Local Area Network (WLAN) Infrastructure Implementation with Support” at all its PAN India Branch offices (As per Scope of Work) from interested Bidders who have proven experience in similar field. GICHFL is seeking a high-performance WLAN system with Network Access Controls enabled to support access to the internet and intranet within and across GICHFL premises. The proposed WLAN system must be implemented with state-of-the-art, proven technology, and must be flexible enough to accommodate the rapid evolution of wireless technologies and business applications without a major overhaul or upgrade.

MINIMUM ELIGIBILITY CRITERIA FOR BIDDER TO PARTICIPATE IN THE TENDER

Sr. No	Specific Requirement	Documents Required	Bidder's Response along with details of supporting documents
1.	The bidder must be a Company/LLP/Partnership Firm incorporated in India and registered under the Companies Act 2013 or Limited Liability Partnership Act 2008 or Partnership Act 1932 as applicable and must have a registered office in India for at least 5 years.	Copy of Certificate of Incorporation/Registration	
2.	Firm should have all necessary licenses, permissions, consents, No Objections, approvals as required under law for carrying out its business. Bidder should have valid GST and other applicable taxes registration certificates /PAN etc.	An undertaking to be submitted along with copy of PAN card and GST Registration certificate	
3.	The Bidder should have been in the business of supplying/ supporting Networking equipment and WLAN Services for a period of at least 3 years as on 31.03.2023.	<p>Any one of the following documents:</p> <p>a) Work/ Purchase Orders confirming year and area of activity with Self-certification from bidder that supplies/projects against orders have been executed.</p> <p>b) Execution certificate by client with order value.</p> <p>c) Any other document in support of order execution like Third Party Inspection release note, etc.</p> <p>In case any bidder is seeking exemption from Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer.</p>	
4.	The Bidder should have had an average annual turnover of Rs. 9 Crores in the last three Financial Years i.e., 2020-21, 2021-22 & 2022-23.	<p>Copy of Audited Balance sheet for the financial years i.e., 2020-21, 2021-22 & 2022- 23 must be submitted.</p> <p>In case any bidder is seeking exemption from Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer</p>	

5	The Bidder should have earned profit in at least 2 of the last 3 audited financial years. (2020-21, 2021-22 & 2022-23).	Audited annual account or auditor certificate must be submitted. In case any bidder is seeking exemption from Turnover Criteria, the supporting documents to prove his eligibility for exemption must be uploaded for evaluation by the buyer.	
6	OEM Authorization (MAF)	Manufacturers Authorization letter from OEM in favour of Bidder must be enclosed	
7	Presence: The Bidder should have branch/ service centres/ franchises in Mumbai with at least 10 Support Engineers	Self-Declaration from competent authority	
8	The Bidder must not have been blacklisted by any department or institution or undertaking of the Government of India and the Government of Maharashtra.	Declaration in this regard by the authorized signatory on behalf of the bidder on the company letter head.	
9	The bidder should not be under liquidation, court receivership or similar proceedings, should not be bankrupt.	The bidder should upload self-declaration regarding the same on the official letterhead of the company.	

Declaration:

- 1) All the information provided by me/ us herein above is correct.
- 2) I/ We have no objection if enquiries are made about the work listed by me/ us in the accompanying sheets/ annexure.
- 3) I/ We have read all the terms and conditions of bid and the instructions, and these are acceptable to me/ us.

Signature:

Name & Designation of the Authorized Signatory:

Official Seal:

Date:

Place:

Please provide supporting documents for all the pre-qualification criteria listed above. Bids which do not pre-qualify based on the above criteria will be summarily rejected. To qualify for bid, bidder should satisfy following eligibility criteria.

SCOPE OF WORK :-**Broad Requirement:-**

The purpose of this tender document is to invite bids for:

1. Supply, Installation, Implementation, Integration, and maintenance of Wireless LAN (Local Area Network) Infrastructure, hereinafter referred to as WLAN Infrastructure, at all GICHFL domestic locations as per Annexure I.
2. Implementation of Network Access Control mechanism for all approved devices within Wired or Wireless LAN Infrastructure of all PAN India Branch Offices.
3. Buyback existing LAN equipment – A tentative list of Buy-back devices are attached as Annexure -IV. Before pickup of those old assets, the list of items like D-Link/Tp-link unmanaged switches, Cisco Routers, etc are to be noted and sent to HO for approval with Branch Manager's recommendation
4. The estimated number of access points and Access switches required are given in Annexure I and Annexure II. Bidders are to quote for these quantities, and these quotes will be used to identify the selected bidder. The selected bidder will then do a survey to identify the exact number of each equipment that will be required. The rates quoted in the bid will be used for extra items, if any are required. The number of items may also decrease as a result of the survey. All bidders must also quote for all the items given in Annexure II.

The Selected bidder will carry out the following:

1. Network Assessment:
 - a. Identify the actual number of Access Points and Access Switches required based on a survey of offices. The list of offices is provided in Annexure-I.
 - b. Finalize the Bill of Material (BOM) including the removal of existing D-Link or TP-Link Switches as Buy-back.
 - c. Identify any potential interference sources that may affect the wireless signal quality and share a Quality/ Risk Management Plan.
2. Network Design:
 - a. Based on the network assessment, design a wireless LAN setup that meets the requirements of GICHFL. This will include wired LAN networks for connecting Access Points to Access switches.
 - b. Provide equipment which satisfies all Technical Specifications mentioned in Annexure III of Bid Evaluation Document. The equipment must be able to support the entire network load of all users at each location and provide reliable and high-speed connectivity.

- c. Design the network topology that includes Access switch, Smart Racks, Wireless Controllers, Network Access Control (NAC), etc. (please specify others).
3. Network Implementation:
 - a. Install the hardware devices and configure them according to the network design.
 - b. Configure the wireless controllers to manage the access points and ensure seamless roaming between them.
 - c. Integrate the wireless LAN network with the existing Software Defined Wide Area Network (SD-WAN) setup of GICHFL.
 - d. Configure the NAC to provide network security by enforcing access policies and detecting any unauthorized devices.
 - e. Test the network connectivity and ensure that it meets the performance standards.
 4. Network Support:
 - a. Provide ongoing support and maintenance for the wireless LAN setup.
 - b. Monitor the network traffic and performance to detect any issues and take corrective action promptly.
 - c. Upgrade the network devices and firmware as needed to ensure optimal performance and security.

Detailed Scope of Work:-

The Selected Bidder must carry out comprehensive Network Assessment as detailed above, propose final Solution Architecture Diagram with detailed BOM, prepare Network Architecture Low Level Diagram (LLD) for all locations, Implement the Wireless LAN Infrastructure, provide equipment & software/ licenses on CAPEX Model and provide support for the contract period.

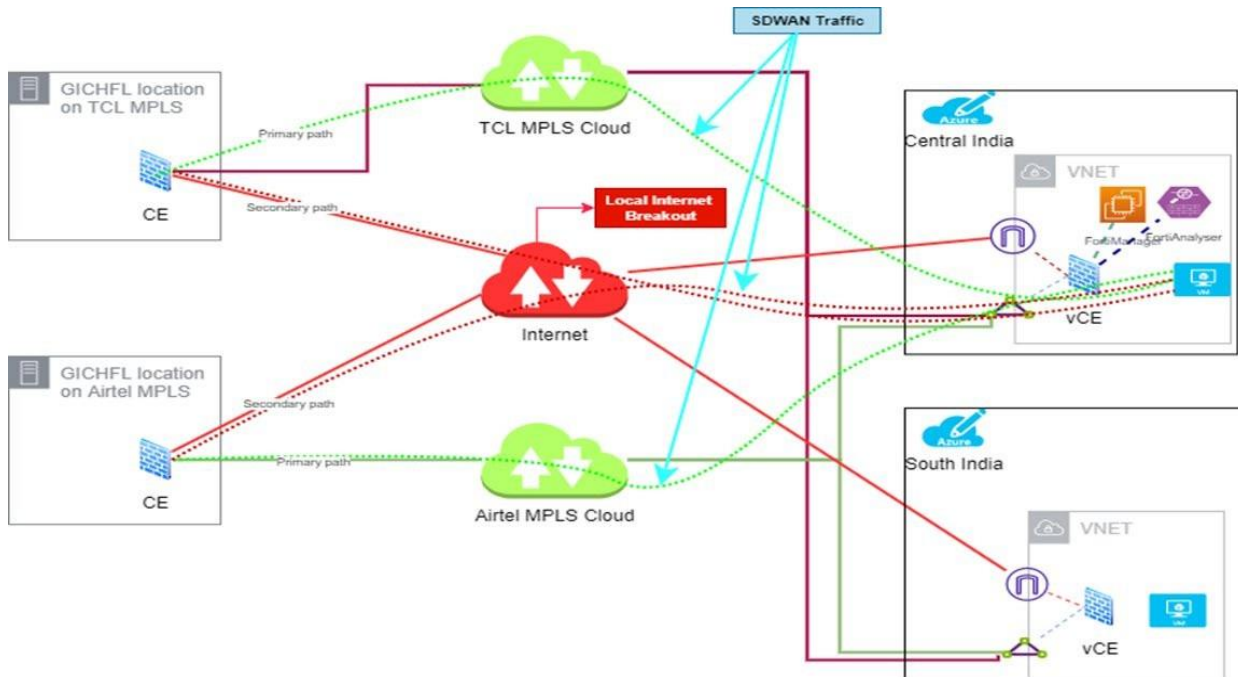
The proposed CAPEX Models Conditions must comprise of the components below (but not limited to):

- a. Ownership of all the hardware & software components and its corresponding licenses will be of GICHFL from day 1 of Contract Period.
- b. Any upgrade or updates of the software and replacement of faulty hardware must be included in the Commercial Bid for the Contract Period.
- c. At the end of Contract Period knowledge transfer/ training must be provided by the Selected Bidder and management of all software and hardware equipment provided, installed and present at GICHFL, during the contract period to any of GICHFL's designated System Integrator.
- d. All equipment necessary for the functioning (to the satisfaction of GICHFL) of WLAN Infrastructure will be property of GICHFL. Any hardware/ software/ licenses required to enable the functionality must be included in the Bid and provided from Day 1.
- e. Maintenance, replacement and warranty of all hardware and software equipment must be included by the successful bidder for the period of the contract.

Part A: Supply, Installation, Implementation, Integration and maintenance of Network Devices and Wireless LAN Infrastructure.**I. Existing Setup:**

1. All GICHFL branches are now functioning over wired LAN connection for all users with Internet and application access.
2. All GICHFL branch offices including head office (addresses can be found here: <https://gichfindia.com/Branch%20Locator.php>), are connected through SD-WAN with MPLS and ILL (local break-out). The SD-WAN is established by Firewall at each location. The DC is with Central India, Azure and DR is with South India, Azure.
3. There are few branches connected through site-to-site VPN in the same Hub and Spoke model. The Selected Bidder must ensure that VLANs from GICHFL HO are able to communicate to VLANs of all branches during VAPT audits, which are conducted by 3rd party auditors from GICHFL HO.
4. The Selected Bidder must integrate and configure the wireless LAN with the existing SD-WAN and manage the LAN, up to the firewalls, at all locations as part of this project. All necessary assistance needed from CSP will be provided.
5. The Selected Bidder must ensure that the proposed solution is able to work with third party networking components such as SD-WAN.
6. The proposed solution must support all the existing network and application requirements of GICHFL and any other application which GICHFL implements in future.
7. The proposed solution must be scalable (bandwidth, network devices, etc.) to meet future requirements on demand.
8. Further the SD-WAN architecture will be shared with Selected Bidder post signing NDA.

Existing Network Architecture for all Branches in Azure Cloud with Fortinet Firewalls



- Each Branch location is having one Fortinet firewall (1 Qty-40F) and HO Site is with Fortigate FG-200E (HA) setup.
- At DC (Azure Central India) , FG-VM04 Virtual firewall in HA is already deployed. SDWAN Fetaure is enabled on this Virtual firewall
- AT DR (Azure South India) , FG-VM02 Virtual firewall in standalone mode is already deployed. SDWAN Fetaure is enabled on this Virtual firewall
- Topology will be hub & spoke, Hub will be azure DC (Central India) & DR (South India)
- Regarding Internet access, all the traffic will be breakout via local internet and incase local internet is not available then traffic will flow via MPLS underlay and will breakout from Mumbai HO/Azure DC
- All the devices are being centrally managed by FortiManager, which is deployed in the Azure DC.
- Centralised Monitoring & management of Remote SDWAN devices are happening through Forti-manager & Forti-analyser. These compoents are deployed in DC (Azure Central India)

II. Proposed Setup:

Branch & HO Setup:-

- The Bidder shall be able to identify the exact number of Access Points and Access switches based on site surveys of the Branches, details of which, including the Carpet Area (in Sq. Ft) are provided in Annexure-I. 3.
- The Bidder must remove the existing D-Link or TP-link or any unmanaged Network switches replacing against the Managed Network Switches as specified in the BOM with exact LAN points provisioned at each Branch.

3. The Bidder must provide detailed network assessment report, detailed floor plans, all diagrams, cable route plans, and perform laying of cables, rack, nodes, AP locations/placement, etc. in consultation with GICHFL, to ensure precise device placement and interference analysis.
4. The Selected Bidder may modify the quantities in the BOM provided in Annexure II based on the survey of sites.
5. The Selected Bidder must perform manual channel plans in dense areas and include drawings of each floor, if any with device placement and cable management. Final Network diagram and detailed Floor plans must be submitted after the survey.
6. The number of sites/ locations mentioned in this tender document may increase/ decrease during the Contract Period. For future scaling, the Selected Bidder must supply equipment of same make and model or better (compatible) from the proposed/ original OEM complying with the technical specifications of the tender at the quoted prices only.
7. Selected Bidder must provide Smart Racks / Network Racks, if there is no extra space available at the existing Rack to fit the Managed Switches, if required. A separate Approval must be obtained from IT Dept. for the additional Rack deployment.
8. Selected Bidder must provide, maintain, and support high speed uninterrupted Wireless Local Area Network (WLAN) across all GICHFL locations (Annexure I), for a period of 5 years from the date of GO-LIVE of this project. The proposed solution must be scalable to meet future requirements as and when required by GICHFL.
9. The proposed solution should also cover seamless integration with SIEM, SOAR solutions for threat analysis and Audit monitoring perspective at no further additional cost for the entire contract period.

Part-B: Solution Design and Implementation

1. The Selected Bidder must design, implement, and maintain a high-performance Wireless Local Area Network (WLAN) at all GICHFL locations (Annexure I) with specifications as detailed in this tender document.
2. The Selected Bidder must propose a detailed design architecture for all locations including all network/ other equipment. The Selected Bidder will be evaluated based on the most efficient use of equipment in the proposed Solution design.
3. CAPEX Model of offering must include the following (but not limited to):
 - a. GICHFL taking complete ownership of all equipment proposed at various locations including compliance with various licensing and usage regulations, etc. from day 1.
 - b. Full warranty and support for the Contract Period.
 - c. Flexibility to scale the solution.
 - d. Role-based access control to allow all types of users and devices to securely connect through the controller.
 - e. Next-generation security against malware and other cyber security threats.

- f. Integrated security for IoT.
 - g. PCI compliance.
 - h. Network monitoring, quality and performance testing and reporting.
 - i. Guest management: custom splash pages with options for Wi-Fi, and social media integration with a configurable option.
 - j. Managed Wi-Fi network support from wireless and security certified network engineers.
4. The proposed Wireless LAN Solution must carry all network and application traffic seamlessly and integrate with the SD-WAN devices at every location.
 5. The proposed Wireless LAN Solution must contain all LAN components like Midspan Injector devices for Non-PoE Access switches, Access switch smart racks, network racks, cabling, all other network equipment, etc., for seamless network and application traffic flow at all locations mentioned in Annexure I and to and from the DC-DR sites as well.
 6. If the BOM (Annexure II) specified in this tender document is missing any equipment/ component necessary for the Solution to function properly, the Bidders must highlight the same and seek clarification/ provide justification as part of their pre-bid queries via E-mail.
 7. The proposed solution and scope of work includes major civil work, physical installation, smart racks, and tools for diagnostics of all components that are to be installed at all locations. Bidders must cover all aspects of the scope of work in their bid.
 8. The Bidders must provide functionalities of all the components like WLAN Controller (centralized Software-based), NAC, AAA (Authentication, Authorization and Accounting), RADIUS, SMS Gateway, Captive Portal, customization, and branding of services, etc. in the solution design document. All specifications relevant for Software/ Cloud controller shall be applicable. Hardware/ Physical controller specification shall not be considered.
 9. The Bidders must provide centralized software WLAN controller with a fixed no. of licenses. The Controllers must be configured (in HA) on VMs running in GICHFL's cloud environment at both DC & DR.
 10. The proposed solution must include compatible specifications for WLAN controller, management software, NAC solution, etc., as it needs to be hosted at GICHFL's Azure Cloud environment.
 11. The bidders must provide the pre-requisite VM requirement for the software controller. Based on that GICHFL will provide the environment at its Azure Cloud environment. The cost of this is not part of this RFP.
 12. The proposed solution must integrate seamlessly with GICHFL's SD-WAN Setup which consists of firewalls with MPLS & ILL links. GICHFL will only declare GO-LIVE after complete verification of this integration.

13. The solution must have an integrated security capability such as content filtering, blocking malicious attacks, etc. to provide security to the overall network infrastructure.
14. The Bidders must quote the products strictly as per the BOM given in Annexure II and also specify missing components, if any, which will be discussed as part of their pre-bid queries.
15. The Bidders must quote products that satisfy the specifications given in Annexure I of Bid Evaluation Document (or better), mentioning model number, make and exact specifications.
16. The Selected Bidder must perform physical installation and powering (with existing UPS) of all supplied components as per approved layout.
17. The scope of work includes complete design, configuration, and integration of all the components of the Local Area network for all locations to the satisfaction of GICHFL.
18. Any structure, permanent or temporary, dismantled or destroyed during the execution of the work shall be refilled or remade or restored to its previous condition by the Selected Bidder at their own cost. If there is any unavoidable dismantling or structural change required for the proposed solution, Selected Bidder must mention the same in the proposed solution as part of bid document for technical evaluation. GICHFL is open to dictating a solution to the Selected Bidder to overcome unavoidable structural modifications.
19. The Selected Bidder must supply, install, commission, and integrate the switches, smart rack, network rack, access points, UPS, and all required accessories / components as part of this project.
20. The proposed equipment must not be on the list of end-of-support or end of life declarations by OEMs for at least 5 years after the end of Contract Period.
21. The Bidders should provide Compliance and Remarks as per Technical Scope of Work attached as Annexure- III.
22. The Bidders must submit all documents as mentioned under Annexures.
23. The Selected Bidder must perform successful User Acceptance Testing of the entire setup including the Active and Passive equipment before issuance of go-live / signoff from GICHFL.
24. The Selected Bidder must conduct VAPT audit (via Third Party auditors) of the implemented solution. GICHFL will declare GO-LIVE only after satisfactory report of this audit.
25. The proposed solution must be strong/ robust enough to prevent any unauthorized access.
26. The Selected Bidder must include cost of installation and commission and provide operation and configuration training to GICHFL's identified technology staff.
27. The Selected Bidder must cover all intended coverage areas with wireless AP for high-rate data applications. The APs must be configured with auto-failover.

28. The Selected Bidder must deploy all components in HA mode to ensure 100% uptime.
29. Selected Bidder must provide end-to-end solution including (but not limited to) hardware, software, licenses, etc., for setting up Wi-Fi network at GICHFL and its Offices (Annexure I).
30. The proposed solution must involve cable connectivity for each workstation at all locations as a backup connectivity option for exigencies. In addition to cabins, the solution must also provide 5-7 extra ethernet / IO ports connectivity in a distributed manner from the Access / Floor Switches. Any Civil Work necessary for this must be included in the bid submission.
31. The Selected Bidder must implement IP Sec AES 256 or similar encryption for every location as per existing setup of GICHFL, wherever suitable. DTLS encryption is acceptable and IPsec AES 256 requirement is necessary only wherever applicable.
32. The Selected Bidder must arrange for all equipment and tools required for civil work, installation, testing, maintenance etc. at their own cost.
33. Selected Bidder must provide State of the art, reliable, scalable, Wi-Fi internet setup with single/ multiple SSIDs. The end users must be granted internet access based on OTP/ MAC/ password.
34. Selected Bidder must be responsible for end-to-end process and operations of Wi-Fi services including SMS for OTP and other associated services.
35. The submitted bid proposal must include copies of certifications and resumes for all engineers who will be responsible for installation and ongoing support of entire scope during the contract period. If there is any change in personnel working on the project other than those declared in the technical bid, approval from GICHFL must be taken for the same.
36. Respective OEM (s) must review the implementation after completion and if there are any changes suggested by the OEM, they must be done by the Selected Bidder in conjunction with qualified personnel from OEM at no additional cost.
37. The Selected Bidder must integrate GICHFL's existing SD-WAN infrastructure setup (Network and application traffic flow to and from DC & DR sites to the various locations i.e., GICHFL Offices including H.O.) with the new WLAN Network.
38. The Selected Bidder must submit the detailed BOM of the equipment offered duly verified and certified by the respective OEM. If the BOM varies from the one provided in this tender document, the Selected Bidder must justify/ clarify the same as part of their pre-bid queries.
39. The Selected Bidder must assign project manager and associate support personnel for this project.
40. All the technical literature for the products offered by the Bidders must be uploaded with the technical bid. Incomplete bids are liable to be rejected.
41. Guest/ un-identified users: Any endpoint or user who is not having their credentials defined in the (Authentication, Authorization and Accounting) AAA server, when they try to connect to the network, they shall be redirected to a Guest (Virtual LAN)

VLAN with no access to request for temporary password. These users shall be redirected to a captive portal for Guest user authentication. If such a user has been assigned a temporary password by the network admin, then he/ she may get authenticated using these temporary credentials with dual factor authentication, whose validity must be time bound (the passwords configured to expire automatically after certain time period). The Selected Bidder must configure separate SSID for guest users. Such temporary/ guest users shall be assigned a guest role and only be allowed limited access to the Internet.

42. The Proposed Solution must maintain all logs for all users and devices (including guests) for security and audit purposes live for at least 6 months and thereafter archive the logs in external storage. The Selected Bidder must review all logs and submit monthly report of observations/ recommendations based on the review.
43. Guest users must be registered using mobile numbers. The Proposed Solution must support instantaneous User creation (with separate User ID and password). The facility for integration with GICHFL's guest registration process must be there so that users are created automatically once registered. Facility for defining validity period for each user must be there. The users must be deactivated automatically after the validity period. No user will be deleted from the database (audit purposes).
44. The proposed solution must have the capability of defining, restricting, or enhancing internet bandwidth for guest access or any specific user for specified period.
45. The proposed solution must provide a portal to manage access for all user types. The portal must be secure and managed by the Selected Bidder.
46. Configured SSIDs must be the same and enable seamless connectivity with endpoints and other devices across the Organization including people roaming to other branches of GICHFL.
47. GICHFL has a Windows Server OS based Domain Controller (AD) which is used to authenticate all employees as necessary. This AD can be used as a backend authentication system for the AAA server of the WLAN system. If a separate authentication server is required, or a separate AAA server is required or both, beyond the WLAN controllers and Access Points, then the hardware and software for these functions must be included within the cost quoted in the commercial bid. The Prospective Bidders must size and specify the details as part of the Technical Bid submission.
48. The Selected Bidder must ensure seamless integration of its AAA platform with the supplied network equipment and Access points. User Authentication must be done through dual factor authentication using user's mobile number via SMS and/ or email.
49. The Selected Bidder must configure, troubleshoot, and support Wi-Fi Access for all Wireless enabled devices like Laptops, Mobiles, printers, scanners and MFDs (Multi-Functional Devices).
50. Network Bandwidth requirement:
 - i. The Selected Bidder must understand the existing network setup and co-ordinate with the data center service provider for designing/ sizing the network architecture/ bandwidth requirement per user.

- ii. The proposed solution must be compatible and integrated with SD-WAN solution that is implemented at GICHFL.
- iii. Primary internet traffic for all GICHFL branches will flow through ILLs terminating in SD-WAN CPEs.

Part-C: Software Solution for WLAN Management

1. The proposed solution must allow GICHFL to have the user management and monitoring rights for the Wi-Fi setup proposed under this tender document.
2. The access to the User Management/ Monitoring Module for GICHFL or its authorized Network Integrator must be given as a part of the solution and must support features such as Dashboard, SLA Monitoring, user activity logs, troubleshooting, error logs analysis, MIS Reports, User authentication through OTP (One Time Password) on mobile no. and email etc.
3. The proposed solution must be capable of generating various MIS reports on a dashboard in graphical/pictorial representation such as:
 - i. No. of Users with details: IP details, MAC ID, Access Point, and Channel Wise etc.
 - ii. Internet Usage: User wise/ Access Point/ Location wise etc.
 - iii. Total Bandwidth Available on each AP/Hotspot and its Usage
 - iv. All reports related to SLA & project monitoring.
 - v. Change management reports: Configuration, firmware, patches, upgrades etc.
 - vi. Data usage
 - vii. User activity logs
 - viii. Error Logs
 - ix. Any other reports that may be required from time to time.
4. The Selected Bidder must review all such logs and submit monthly report of observations / recommendations based on the review.
5. The Selected Bidder must ensure that the solution supports all the existing applications of GICHFL and is compatible with the technologies for at least the next 10 years. The Selected Bidder must provide support to integrate any future applications or equipment which GICHFL implements during the contract period.
6. The Solution must facilitate the administrators for policy level blocking, monitoring, and filtering of data flow i.e., initial policies for example must be to block pornography, torrents, pirated, poker/casino-related websites and contents.
7. The solution must have the capability to restrict network access based on devices. GICHFL may provide different rights/ restrictions for personal devices and for official devices. If this feature is to be achieved using different SSIDs, the solution must have the capability to restrict certain devices to access specific SSID(s).
8. The Solution must provide the administrator with the capability to hide SSIDs or make them public.
9. Wi-Fi usage log: Selected Bidder shall be responsible for keeping log of Wi-Fi usages/ services to be utilized by the end users such as endpoint/ User Authentication, login success/ failure events, Mobile number MAC & IP addresses, access time,

duration, data consumed, etc. to meet the compliance with all Regulatory and Legal guidelines issued by Department of Telecommunications (DOT)/ TRAI from time to time. These logs must be maintained for at least 1 month on real time basis and forever/ infinitely on external storage and must be provided to GICHFL in readable format on demand. The Selected Bidder must review all logs and submit monthly report of observations/ recommendations based on the review.

10. The Selected bidder must design the solution with the latest technologies i.e., hardware not older than one year.

Part -D: Scope of Cable plan Implementation includes Passive Cabling as well for existing wired LAN: -

1. The Selected Bidder must prepare the network layout, cable routing diagram, BOM per location and project delivery schedule, etc., within two weeks from the date of receiving the contract. The document must clearly indicate the site preparation requirements to be carried out by GICHFL and site clearance and permissions to be obtained from GICHFL.
2. The implementation shall commence only after approval of the network diagram and cable route by authorities of GICHFL.
3. The cabling plan must be implemented and documented as per the EIA/ TIA standards. The Selected Bidder must submit a documentation schema along with the tender document.
4. **Passive LAN Structured cabling:**
 - i. The Bidder shall be responsible for the Passive Networking at branch including the Wired and Wireless LANs along with Management of Access Points, Access Switches and NAC solution for the entire period of contract for 5 years.
 - ii. The bidder shall replace all faulty components of Passive Networking at branch with complete Supply and Installation for the entire five (5) year contract period with no extra cost to GICHFL.
 - iii. The Bidder shall arrange a Network resource of L2 level for all PAN India branches within same business day whenever issue reported before 1 pm or else by Next day (even Saturdays).
 - iv. The Selected Bidder shall provide centralized helpdesk for assistance or registration of user complaints through various medium like Voice Call/SMS/Email of ticket generation system.
 - v. The Resource should carry necessary equipment's like crimping and punching tool, RJ45 ports, etc. for the Networking activities with no additional cost to GICHFL.
 - vi. PVC case wiring must be done for the entire required passive cabling. Mounting of Access Points, Network Racks on walls are to be done by providing all required fittings. The PoE injectors are required to be provided with appropriate power connections and must be provided by Selected Bidder, including any wiring, casing, and power outlets that may be required, with wall mounting as needed with no extra cost to GICHFL.

- vii. All required cables must be tagged. The cables must be appropriately marked and labelled.
- viii. The Selected Bidder shall do the required passive cabling and necessary arrangements for cage nuts, clamps etc. to make the proposed solution working.
- ix. The Selected Bidder must ensure that the adopted methodology of conducting, cabling and installation work will cause no/minimum damage to the existing finish and no loss to the aesthetic beauty of the floors, walls, ceilings, gardens, open spaces etc. Any damage to the existing flooring / walls etc. shall be made good by the Bidder at their own cost.
- x. Fiber-optic cables must be used primarily for designing the network backbone and for floor-wise switch uplink.
- xi. Dedicated raceways/ cable-trays must be used for laying LAN.
- xii. All the cable raceways shall be grounded and fully concealed with covers.
- xiii. There must be enough space between data and power cabling and there must not be any cross wiring of the two, to avoid any interference, or corruption of data.
- xiv. It is proposed to have power and data cables in separate trays in cold aisles and hot aisles, respectively.
- xv. Maintenance of Cabling located at PAN India Location as per given Annexure-I in RFP.
- xvi. All cables and jack panels must support 1 Gbps data transmission. The cable & jack panels must be of the latest version of CAT 6.
- xvii. The jack panels to be installed at server rack must be provided by the Selected Bidder.
- xviii. Network racks must be placed if existing Rack is not enough to provide space.

Part-E: Documentation

1. All Bidders Documentation must include the following (but not limited to) documents as part of their bid. Technical marks will be provided based on the quality of contents of the documents below:
 - i. Infrastructure build document.
 - ii. Detailed Project Plan with milestones, resources, and deliverables.
 - iii. Support Personnel details and escalation matrix.
 - iv. Solution Architecture/ Design Document covering entire Scope of Work.
 - v. Detailed Timelines (Gantt Chart) for each phase of project.
 - vi. High Level Network Architecture Diagram
 - vii. Low Level Network Architecture Diagram
 - viii. Wi-Fi Feasibility Report
 - ix. Heat Map and Floor Plans for each floor at each location
 - x. Detailed Technical Specification Compliance Sheet
 - xi. All other documents as per RFP.

2. The Selected Bidder must submit the below documents within 30 days from date of acceptance of Purchase Order. All documents are necessary for the declaration of GOLIVE:
 - i. Program Evaluation & Review Technique (PERT) chart after consultation with GICHFL.
 - ii. Equipment list per Location.
 - iii. Daily progress to be advised to GICHFL till the entire project is implemented/commissioned.
 - iv. GSTIN ID of Selected Bidder must be provided from where goods will be supplied.
 - v. Inventory list containing host names, make, model, serial number, etc.
 - vi. Traffic flow document between the devices.
 - vii. Testing cases and test results documented before and after implementation.
 - viii. IP address allocations to various components.
 - ix. VAPT report of the implemented solution before GO-LIVE.
 - x. Duly signed declaration of material disposal as per e-waste disposal guidelines.
 - xi. Duly signed NDA, SLA, etc. as per tender document.
 - xii. All SOPs that are relevant to the solution.
 - xiii. Written assurance to certify that GICHFL's encrypted data transmitted within the network is not decrypted or modified.

Part F: -Support Service-Help Desk Support

1. The proposed solution must be managed and maintained, along with warranty of equipment, for a period of 5 years.
2. The helpdesk support period must start during the implementation phase of this project and continue for a period of 5 years.
3. On-site support to be provided by the Selected Bidder directly deputing one full-time skilled (CCNA certified) resource at Head Office for 6 months and proactive field support for repair & maintenance of WLAN infra network.
4. Support Resources must be made available on-demand within 1 hour, for GICHFL Head office and within 3 – 4 hours for Branch offices in case of any disruptions or exigencies. The support phase will start post implementation and GO-LIVE of the complete Scope of Work.
5. The Normal working hours of service are Monday-Friday 09:30-18:00 hrs, but for scheduled activities or other exigencies (for e.g., DR drill, server maintenance, etc.), the Selected Bidder must extend its support services beyond such normal working hours.
6. During the Support Period, any upgrade of software or replacement of faulty hardware components as part of warranty cover must be provided at no additional cost.
7. The Selected Bidder must provide centralized helpdesk for assistance or registration of user complaints through various media like Voice Call/ SMS/ Email of ticket generation system.
8. Login-IDs must be created by the Selected Bidder for GICHFL team for logging into the support portal for the support and logging/ viewing the status of calls/ TAC cases raised by/ for GICHFL.
9. The Selected Bidder must ensure minimum network uptime of 99.99%.

10. The Selected Bidder must closely coordinate with GICHFL and extend all required support in designing any new network solution, expansion of network as and when required and for the network architecture/ wireless LAN controller refresh during the contract period without any additional cost to GICHFL in a time bound manner after intimation to the Selected Bidder by GICHFL or any GICHFL designated SI. The Selected Bidder must submit the requirements along with proper justification. The report should contain the recommendation as per regulatory guidelines and best standard industry practice while considering scalability as well as provisioning of future requirements including bandwidth/ device requirement of various applications.
11. The Selected Bidder must hand over the AMS (Annual Maintenance Support) of the system to GICHFL or any new Vendor in 100% working conditions on termination or at the end of the contract. After rectifying incident/ failure/ issue, Selected Bidder is required to update the resolution/ call-closure on the centralized helpdesk/ NMS/ Ticketing Tool, to be provided by Selected Bidder, and the confirmation for the rectification shall be done on visibility in the deployed NMS. The Selected Bidder must provide and publish a troubleshooting guide and necessary training for the users.
12. The Selected Bidder must provide single helpdesk number for access dedicated to GICHFL, for assistance and support 24x7x365. The Selected Bidder must provide resources who can fulfil SLA requirements during the Contract Period and share their details with GICHFL. On-site & off-site support resources must ensure that all devices are secure & safe in all respects.
13. The Selected Bidder must remain responsible for all hardware, software, and connections between them.
14. Redundancy at the hardware level as well as at the link level must be implemented to ensure the unimpeded availability of LAN. Switching over from one link to another (in case the active link is down) must be seamless without any downtime.
15. The Selected Bidder must do the required passive cabling and necessary arrangements for cage nuts, clamps etc. to make the proposed solution work.
16. The Selected Bidder must provide all the power cords/ secondary/ tertiary equipment to complete implementation of proposed solution. These must be compatible with the existing power equipment.
17. The contract must be back lined with OEM for the complete contract period (five years from date of acceptance). The Selected Bidder must provide proof of back-lining, in writing in the form of an e-mail/ letter confirmation, from the OEM within 30 days from the date of acceptance of each site by GICHFL, before any payment whatsoever can be released by GICHFL.
18. The Selected Bidder must organize training about the proposed solution, after completion of installation and commissioning and without any additional cost, for ITMG personnel for 1 day every year at GICHFL's Head office. Selected Bidder must bear the cost of training materials including training manuals.
19. An onsite Warranty Service must be provided, and the warranty period must start from date of GO-LIVE.

20. The Selected Bidder must deliver and implement the technologies in conjunction with best practices guidelines & industry standards.
21. The Selected Bidder must ensure that during the execution of the project they do not damage or disrupt any existing service under and above the ground and their activities will not cause any disturbance to any other ongoing activity at the campus.
22. The Selected Bidder must ensure that the adopted methodology of conducting, cabling and installation work will cause no/ minimum damage to the existing finish and no loss to the aesthetic beauty of the floors, walls, ceilings, gardens, open spaces etc. Any damage to the existing flooring/ walls etc. shall be corrected by the Selected Bidder at their own cost.
23. The Selected Bidder must have highly qualified and CCNA certified technical staff to understand the technical problems and provide proper resolutions. Selected Bidder must appoint a Project Manager for this RFP for the entire duration of the contract. The Selected Bidder must provide a CV of Project Manager that demonstrates proven experience in executing projects similar in scope and complexity. GICHFL reserves the right to ask for a change in the Project Manager, depending upon qualification/ experience/ performance etc.
24. Any other miscellaneous requirements related to the scope described in the tender document or extra work required to be performed to fulfil scope of the tender document due to existing hardware/ software/ structure limitation must be provided by the Selected Bidder at no extra cost to GICHFL even if those items are not mentioned explicitly in this tender document. GICHFL will not accept any plea from the Selected Bidder later for omission of services on the pretext that the same was not explicitly mentioned in the tender document.
25. The Selected Bidder must submit an initial escalation matrix during the installation of the solution. Thereafter, the Selected Bidder must share with GICHFL the updated/ revised escalation matrix as and when there is any change in the said document.
26. The Selected Bidder must not outsource the contract to sub-contractor. However, in case of necessity for outsourcing the contract to sub-contractors, prior written approval by GICHFL must be obtained.
27. The Selected Bidder must provide support with its own resources which are on their permanent payroll or may sub-contract with prior approval from GICHFL.
28. The Selected Bidder must inform GICHFL about all release/ version changes of patches/ upgrades/ updates for hardware/ software/ OS/ middleware etc. as and when released by the OEM. It shall be the responsibility of the Selected Bidder to implement/ perform updates/ upgrades/ patches as and when necessary, after obtaining prior approval from GICHFL.
29. The Selected Bidder must also fix any security findings/ vulnerabilities identified by various security agencies hired/ consulted by GICHFL without any cost during the contract period. However, if the security observations cannot be closed and replacement is the only option to close the observations, then the Selected Bidder must replace the device(s) (with device meeting all the specifications of the tender document) at no extra cost to GICHFL.
30. Preventive maintenance: The Selected Bidder must conduct Preventive Maintenance (including but not limited to inspection, testing, satisfactory execution of all diagnostics, cleaning and removal of dust and dirt from the interior and exterior of the equipment, and necessary repair of the equipment) once within the first 15 days of the installation and thereafter once every quarter.

31. The Selected Bidder must provide replacement equipment if any equipment is out of the premises for repairs. Replacement must be arranged as per the Table provided in Penalty clause of SLA.
32. The Selected Bidder must coordinate with the existing facility management service provider for smooth migration and the setting up of new wireless LAN controller on existing network at GICHFL branches/ offices and troubleshooting of network related issues.
33. The Selected Bidder must ensure that the new solution is in sync with the existing infrastructure and thereby compatible with current network structure and with different OEM devices. If required, Selected Bidder must carry out all required changes/ configurations as per the requirement of GICHFL.
34. The Selected Bidder must extend all required support to GICHFL and existing facility management service provider and shall be responsible for all required configuration changes (e.g., to achieve active-active links scenario for branches/ offices using various technologies e.g., SDWAN, IPv6 migration) in the wireless LAN controllers and Access switches/ devices in GICHFL Head Offices/ branches whenever required at any stage during the Contract Period.
35. The Selected Bidder must arrange for a team of experts from OEM to carry out troubleshooting if required at the time of installation/integration or whenever required with GICHFL's SD-WAN infrastructure in coordination with the IT department and DC-DR Vendor.
36. Replacement of faulty equipment must be done as per timelines defined in Liquidated Damages clause of SLA. The Selected Bidder's support engineers must provide end-to-end support for any such occurrences.
37. If during the warranty period, any system as a whole or any subsystem has any failure on two or more occasions in a period of 3 months, it must be replaced by equivalent/ upgraded new equipment by the Selected Bidder at no cost to GICHFL.
38. The Selected Bidder must enter a Rate Contract with GICHFL for supply of the items mentioned in the proposed solution. The Rate Contract will be valid for the Contract Period.
39. All the support Engineers of Selected Bidder must be responsible for (but not limited to):
 - a. The OS updates, patches, and licenses for the proposed solution must be carried out in coordination with the respective OEMs.
 - b. Be the single point of contact (SPOC) and manage the entire setup/ solution.
40. User Management: User creation/ deletion /modification for Internet access, responding to queries of end users, user access policy management etc.
41. Audit Compliance: Carrying out recommendations provided by various auditors.
42. Fault Management: Detecting, isolating, and correcting problems, reporting problems of end users and managers, tracking trends related to problems.
43. Incident Management: The Helpdesk team must provide for an incident management process to seamlessly facilitate a fault/ call from, initial identification, notification, logging, and diagnosing and closure acceptance, to achieve final resolution. The Selected Bidder and their team must maintain the lifecycle and keep track of every incident pertaining to the proposed solution.

44. The Selected Bidder must perform Problem Management which includes (but not limited to):

- i. Document the appliance/ services fault to include date time, description of symptoms and track and report on problem status as required and provide root cause analysis as required by GICHFL.
- ii. Monitor and report on the progress of the problem resolution and confirm resolution of the problem. Close the call upon resolution of the problem.
- iii. Submission of monthly report.
- iv. Escalation Management: Escalation from One resolution process to the next higher level resolution process as per escalation matrix/ chart (to be submitted by Selected Bidder)
- v. Call Management: The calls will be handled at helpdesk based on severity.
- vi. Log Management: Retention of all logs (including user access logs, security logs, audit trail etc.) for entire period of contract. The logs must be handed over to GICHFL on need basis, every year and after the contract period.
- vii. Log Review: The Selected Bidder must review all logs and submit monthly reports of observations/ recommendations based on the review.

Part G:- Compliances

The proposed wireless internet solution must conform to applicable WPC (Wireless Planning Coordination) regulations for use of license-free spectrums in terms of Equivalent/ Effective Isotropic Radiated Power (EIRP). A declaration to this effect must be submitted which must be supplemented by annual compliance reports during the contract period.

• The Selected Bidder must:

1. Configure the solution as per IS policy of GICHFL and preserve/ record the same.
2. Configure the new devices as per GICHFL's existing setup as GICHFL is replacing existing devices by new devices, the syntax/ policies/ access rules/ routes/ NAT/ Object group etc. of existing devices needs to be checked properly and converted as per the new device's configuration format.
3. Provide/ install Software/ Firmware/ OS/ Signature updates and upgrades to fix/ mitigate security vulnerabilities, define actions on signatures, firewall rule review, etc., at no cost to GICHFL as and when required, during the validity of the Contract Period.
4. Mitigate various audit points, Compliance and Mitigation of VAPT points at no cost to GICHFL within one week as and when required during the validity of the Contract Period.
5. Take prompt action on the advisories shared by GICHFL at any point of time during the validity of the Contract Period.
6. Be in full Compliance with GICHFL's IS Security policy, which includes (but not limited to):
 - i. Be responsible for data and application privacy and confidentiality.
 - ii. Be Responsible for system and software access control and administration.

- iii. Custodial responsibilities for data, software, hardware, and other assets of GICHFL being managed by or assigned to the Selected Bidder.
- iv. Physical Security of the facilities
- v. Physical and logical separation from other customers of the Selected Bidder.
- vi. Incident response and reporting procedures
- vii. Password Policy of GICHFL.
- viii. Data Encryption/ Protection requirement of GICHFL. (Must support 256 bit & upcoming algorithms in future).

ANNEXURE I**LOCATION DETAILS:-**

The Selected Bidder shall deploy WLAN solution across all GICHFL's work locations (as mentioned in table below):

SR NO	BRANCH	LOCATION	AREA	ADDRESS	Emp Count (Nos)	ACCESS POINT (EST. COUNT)	CORE SWITCH	PORT
1	AHMEDABAD	AHMEDABAD	753sq.ft super builtup	Shrangrila Arcade, 2nd floor, 100 feet road, 210, near Shyamal Crossing, Prahalad Nagar, Satellite area, Ahmedabad- 380015	3	1	1	24
2	BANGALORE	BANGLORE	2700sq.ft. super built up	Leo Shopping Centre, 6TH floor, 44/45, Residency Cross Road, Bangalore-560025	20	3	2	24
3	BARASAT	KOLKATA	720 sq.ft. Carpet Area	Second floor, Kailas Bhavan, 7 4/37 Jessore road Sisir Kunja . SBI Bank Barasat Kolkata 700127	5	1	1	24
4	Bhubaneshwar	BHUBANESHWAR	1170 sq.ft carpet	Narula Market, 2nd floor, Plot no 501, Unit 3, Near Sriya Talkies Square, Janapath, Kharvel nagar, bhubaneshwar- 751001. Odisha	4	1	1	24
5	BOISAR	PALGHAR	840 sq.ft Carpet	Harmony plaza, 2nd floor, 235, Opposite State Bank of India, Tarapur road, boisar (w), Palghar- 401501	2	1	1	24
6	Borivali	MUMBAI	1123 SQ. FT. CARPET	401, 4th Floor, Soni Shopping Centre Above Om Jewellers, L.T. Road, Borivali west -400092	5	1	1	24
7	CHANDANAGAR	HYDERABAD	1500 sq.ft. super built up	No. 4-113 , 2nd Floor, Chandanagar Main Raod, Chandanagar Village, Mumbai Highway Near oriental Bank Of Commerce -500050	4	1	1	24
8	CHANDIGARH	CHANDIGARH	1089 sq.ft	SCO No 44, Sector 31-D, Chandigarh-160031.	6	1	1	24

9	Chennai	CHENNAI	1834 sq.ft built up	Khivraj complex-2,480, Anna salai, Opp. To Nandanam Arts College, Nandanam, Chennai-600035	8	2	1	24
10	CHINCHWAD	PUNE	2200 sq.ft. built up area	Off. Nos. 202 & 203, Second Floor, Premier Plaza II, G - Wing, Next to Premier Ltd, Pune-Mumbai Highway, Chinchwad, Pimpri, Pune --- 411019	7	2	1	24
11	COIMBATORE	COIMBATORE	1450 sq.ft. built up	Jaya Complex, 100 feet road, 2nd floor, shop no 383, Opp. to Ganga Yamuna Theatre, Above Jayashri Electronics, Gandhipuram, Coimbatore-641012	4	1	1	24
12	CORPORATE OFFICE - 4TH FLOOR	MUMBAI	2266 SQ.FT.	4th floor National Insurance building, 14 Jamesdji Tata, Churchgate, Mumbai 400020	59	NOT REQUIRED	2	48
13	CORPORATE OFFICE - 6TH FLOOR	MUMBAI	7920 sq.ft.	6th floor National Insurance building, 14 Jamesdji Tata, Churchgate, Mumbai 400020	100	NOT REQUIRED	4	48
14	DEHRADUN NEW	DEHRADUN	806 sq.ft Carpet Area	Plot No.2/2A, First Floor, Near Kishan Nagar Chowk, Ballupur Road, Dehradun-248001, Uttarakhand.	3	1	1	24
15	DELHI	DELHI	1260 sq.ft Carpet Area	UGF – 10A-E, Kanchanjunga building, 18 Barakhamba Road, Opp. to Metro station, Connaught place, New Delhi-110001	12	2	1	24
16	DURGAPUR	DURGAPUR	1600 sq.ft. Carpet Area	Plot no MNAV-20, ground floor, North Avenue, Bengal Ambuja, P.S. durgapur--713216	3	1	1	24
17	DWARKA	DELHI NCR	1000sq.ft Carpet Area	Bhagwati Plaza, F-102 & F-103, First Floor, Plot No.12, Sector 5, Dwarka, Delhi – 110075.	3	1	1	24
18	ELECTRONIC CITY	BANGALORE	1500 sq.ft	96/1, GOBIND TOWERS, 2nd Floor, Hosur Road, Singasandra, above sbi bank, Bangalore- 560 068.	2	1	1	24
19	GARIA	KOLKATA	800SQ. FT.	21, AnandaAbasan, Garia station road, hoilding no:186 near saktibodh math kolkata - 700084.	6	1	1	24
20	Gaziabad	Gaziabad	631 sq.ft. Carpet	Shop no 3, 1stfloor, In Astoria Boulevard, RDC, Rajnagar, Ghaziabad-201002	9	1	1	24

21	Greater Noida	GREATER NOIDA	903 sq.ft Super Area	Office no 303, 3rd floor, Tradex tower-1.Alpha Commercial belt, sector alpha -1,Near Pari chowk, Greater noida UP-201307	4	1	1	24
22	GURGAON (NEW PREMISES) unit 301	DELHI NCR	1051 sq.ft super	Unit No.3001/3002,3rd Floor,MGF Metropolis,M.G.Raod,Gurgaon- 122001.	15	2	1	24
	GURGAON (NEW PREMISES) unit 302	DELHI NCR	1011sq.ft super	Unit No.3001/3002,3rd Floor,MGF Metropolis,M.G.Raod,Gurgaon- 122001.				
23	GUWAHATI	GUWAHATI	1248 sq.ft. Carpet	House no.34, Ulubari, Dr. B. Baruah bye lane, Guwahati-781001. Assam	2	1	1	24
24	HADAPSAR	PUNE	558sq.ft. built up	Office No.212, 2nd Floor, Jaymala Business Court, E-Wing, Mauje Manjri BK, Pune-Solapur Road, Taluka Haveli, District Pune – 412307	4	1	1	24
25	HINJEWADI	PUNE	740 sq.ft. Carpet Area	Office no 104, 1st floor, Pushpak Business Hub S No 130/4 4b+5, Bhumkar Chowk,Next to my car showroom & Royal Enfield showroom Pune- Mumbai highway Wakad Pune 411057	3	1	1	24
26	HYDERABAD	HYDERABAD	2850 sq.ft. carpet	4 TH Floor, 3-6-438/4, Naspur House Himayatnagar- 500029	23	3	2	24
27	INDORE	INDORE	1197 sq.ft Super Built up	Apt No 309, 3rd floor, Commerce House, 7 Race Course Road, Indore, MP-452001	3	1	1	24
28	JAIPUR	JAIPUR	1532sq.ft super	Office no 403 and 404A Ganapati Plaza, 4th floor,, M.I road, Near Govt hostel, Jaipur- 302001	7	2	1	24
29	JODHPUR	JODHPUR	1080sq.ft carpet	Prem Tower, Ground floor, P.NO 947, 10th D road, Sardarpura, Jodhpur-342003	5	1	1	24
30	KALYAN	KALYAN	795 sq.ft Built up	Ved Mantra Building, 3rd floor, B-301, Agra road, Near Dakshin Mukhi Hanuman Mandir, Kalyan (w), Dist Thane- 421301	4	1	1	24
31	KENGERI	BANGALORE	900 sq.ft super built up	1104, 1st Main Road, 1st Floor, Kengeri Satellite town bangalore- 560060	2	1	1	24

32	KOCHI	KOCHI	1500 sq.ft Area	Elias Chamber, 1ST floor, Door no XL / 5396, Next to Sarita Theatre, Banerjee road, Kochi- 682018	5	1	1	24
33	KOLHAPUR	KOLHAPUR	480 sq.ft Carpet Area	Royal Plaza, 1st floor, C / 12, Dabholkar Corner, Kolhapur-416001	5	1	1	24
34	KOLKATA	KOLKATA	1777 sq.ft Area	National Insurance building, Ground floor, Opposite to GPO 5, Netaji Subhas road, Near the Mayor's bungalow, Kolkatta- 700001	12	2	1	24
35	KOZHIKODE	KOZHIKODE	480 sq.ft carpet	Shop No. 5/3282 J, Bldg. No. V/3282-A, 4th Floor, Holiday City Center, Opp. Kurisupally, Kozhikode - 673001	3	1	1	24
36	LB NAGAR	HYDERABAD	550 sq.ft	H NO-3-13-124, 2nd floor, Rajiv Gandhi Nagar , L B Nagar Hyderabad-500060	2	1	1	24
37	LUCKNOW	LUCKNOW	2011 sq.ft super built up	Centre Court Building, 3rd floor, 3c, 5 Park road, Thapar house, Lucknow- 266001	4	2	1	24
38	LUDHIANA	CHANDIGARH	500 sq.ft super builtup	501, 5th Floor, San Plaza Building, Sco 15 Feroze Gandhi Market Ludhiana-141001	2	1	1	24
39	MADURAI	MADURAI	900 sq.ft Carpet	Shanmuga Towers, 38/2, Krishnanagar Tank Road, Madurai main, Madurai, Poondhotam, Tamil Nadu-625001.	4	1	1	24
40	Mangalore Branch Office	MANGALORE	715sq.ft. built up	Shop no 109, 1st floor, Inland Ornate, Navabharath Circle, Opp. Ocean Pearl hotel, Mangalore-575003	4	1	1	24
41	MARGAO	GOA	653sq.ft.	L & L Correia's Pride, Office No. AS15, 2nd Floor, Above KFC Adjacent to MATHANY SALDANHA Administrative Complex Salcete Goa- 403601	4	1	1	24
42	MEERUT	MEERUT	1100 sq.ft Carpet area	Darshan Plaza, 2nd floor, Samrat Enclave, Garh road, Meerut, UP- 250004	4	1	1	24
43	Mumbai	Mumbai	1687 sq.ft	4th FLOOR, CHOKSEY MANSION, OFFICE NO.303, SHAHID BHAGATSINGH ROAD, OPP. BLUE DART COURIER, LANDMARK -	10	2	1	24

				NEXT TO CAFE UNIVERSAL				
44	NAGPUR	NAGPUR	418 Sq. ft. Carpet	OFFICE 1-A, THIRD FLOOR, POONAM CHAMBER WING A,CHINDWARA ROAD, BYRAMJI TOWN, SADAR, NAGPUR- 440013	3	1	1	24
45	NASHIK	NASHIK	275 sq.ft Built Up Area	Niwas Plaza, Ground floor, 3-B, Sharanpur, Trimbak Link road, Opposite Tibetan Market, Nashik- 422005	4	1	1	24
46	NAVI MUMBAI BRANCH	NAVI MUMBAI	890 SQ.FT / 1100 Built up area	B-410, BSEL Tech ParkOpp Vashi Railway Station,Sector 30A, Vashi,Nav Mumbai - 400 705.	13	2	1	24
47	Navi Mumbai HUB	Navi Mumbai	1266 sq.ft. Carpet	SATRA PLAZA, 211,2ND FLOOR,PLOT NO.19,20, SECTOR NO.19 DPALM BEACH ROAD, VASHINAVI MUMBAI- 400703.	20	3	2	24
48	NELLORE BRANCH	NELLOR E	1020 sq.ft. built up	Door No.26-15- 27/4,2nd Floor,Sridhar,Towers,Annam aiah Circle,Mini Bypass Road,Nellore-524003	1	1	1	24
49	NERE PANVEL	Panvel	400 SQ FT	Mahalaxmi nagar, Panvel - Matheran road, Nere, Raigad dist- 410206	3	1	1	24
50	NOIDA	NOIDA	536 sq.ft. carpet	Vishal Chambers, B-104, Sector 18, Noida UP- 201301	6	1	1	24
	NOIDA ADDITIONAL	NOIDA	720sq.ft. carpet	Vishal Chambers, B-104, Sector 18, Noida UP- 201301				
51	Panvel (New Premises)	PANVEL	2073sq.f t	SHOP NO 2-6, SURYAKIRAN CHS LTD, PLOT NO: 05, SEC NO :05 BEHIND D'MART, OPP NEEL VARDHAMAN, NEW PANVEL (EAST) RAIGAD DISTRICT- 410 206.	8	2	1	24
52	PANAJI	Panaji	746 sq ft carpet area	Akash Bhavan, B-202, 2nd floor, Opposite Mathias Plaza, 18th June road, Panaji- 403001	4	1	1	24
53	PATIALA	CHANDI GARH	510 sq.ft.	S-42, DLF Colony, Sirhand road, Near HDFC Bank, Patiala-147001	4	1	1	24

54	PATNA	PATNA	420 SQ.FT.	MaSharde Complex, 1st floor, East Boring Canal road,Above SBI Bank, Patna-800001	4	1	1	24
55	PITAMPURA (DELHI)	DELHI NCR	1972 sq.ft. carpet	511,5th floor, PP TOWER, Netaji Subhash Place, Delhi - 110034	6	2	1	24
56	Porur (Chennai)	CHENNAI	410 sq.ft Area	163/215, 1st floor, Mount Poonumallee, High road, near Iyyappanthangal bus depot Opp.Bharat Petrol Bunk ,Iyyappanthangal,Chennai, Porur chennai-600056	4	1	1	24
57	PUNE	Shivaji Nagar	1100 sq ft carpet area/1400 build up	Neelkanth, C.T.S No 1018, F.P.No 870, Deep Bungalow Chowk, Near Model Colony, Shivaji Nagar, Bhamburda, Pune-411016	9	2	1	24
58	RAIPUR	RAIPUR	500 sq.ft Built Up	Unit no.217,2nd floor, B wing,Crystal Arcade, Nr. Awanti Bai Chowk,Shankar nagar Raipur- 492007	2	1	1	24
59	SILIGURI	SILIGURI	551 sq.ft Carpet Area	H.NO.43/138/117, Word No.XI of SMC,3rd floor, Hill Cart Road,Siliguri,West Bengal- 734001.	3	1	1	24
60	SUCHITRA CIRCLE	HYDERABAD	1100 sq.ft built up	plot no.64, 1st floor, Raghavendra Nagar opp: Godavari Homes kaman ,Quthbullapur , Suchitra,Secunderabad - 500055	2	1	1	24
61	SURAT	SURAT	404 sq.ft carpet	111, SNS Business Park, University Road, Vesu,Surat - 395 007	2	1	1	24
62	TAMBARAM (Chennai)	CHENNAI	270sq.ft.	Solomon Street, No 2C, Adhi Nagar, East Tambaram, Chennai-600059	5	1	1	24
63	Thane Office	THANE	1632 sq.ft. Carpet	Horizon Tower, 1st floor, Hariniwas Circle, Opp to Monalisa Building, Bhakti Mandir Rd,Thane (w)- 400602	11	2	1	24
64	THRISSUR BRANCH	THRISSUR	900 sq.ft Carpet Area	Door No. 25/500, 3rd floor, Maheshwari Building, M.G. Road, Thrissur, Kerala - 680001	3	1	1	24
65	TRICHY	TRICHY	1150sq.ft. built up	Sri Krishna Enclave, NO 75, E / 3, 3rd floor, Thillai Nagar, trichy-620018	4	1	1	24

66	TRIVANDRUM	TRIVANDRUM	980 sq.ft Super built up	P.T.C. Tower, 1st floor, S.S. Kovil road, Thampanoor, Thiruvananthapuram-695001	4	1	1	24
67	VADODARA	VADODARA	640 sq.ft. Carpet	S. F 211, Panorama Complex, 2nd floor, R.C Dutta road, Above Kala Niketan Store, Alkapuri, Vadodara-390005	2	1	1	24
68	VARANASI	VARANASI	1564 sq.ft. carpet	Prem Complex, 4th Floor, Plot no.C-33/2, Chandua Siga, Infront of Bharat Mandri. Varanasi- 221010.	2	1	1	24
69	VASAI	VASAI-VIRAR	850 sq.ft Carpet Area	B/101. 1st floor, Kini Arcade, Near stella petrol pump, banampur Vasai (w) Dist-Palghar-401202	3	1	1	24
70	Vijayawada	VIJAYAWADA	500 sq.ft.	1st floor, D NO 59A-13-2, old P&T colony, Nirmala convent road, Near NTR circle, Vijayawada-520010	3	1	1	24
71	VIRAR	VIRAR	3440 sq.ft. carpet	Sandeep house, 3rd floor, near Vijay vallabh hospital, Tirupati nagar, Phase-1 Virar (w), Thane dist- 401303.	8	2	1	24
72	Vizag	Vizag	1455 sq ft carpet/1 699.64 buildup	Sai shopping centre, 3rd floor, Room no 306 & 307, 47 – 14- 1, Dwarka Nagar, Vizag 530016.	3	1	1	24
73	WHITE FIELD	BANGALORE	600 sq.ft carpet	No.1, 2nd floor, Thimmaiah Complex, Immadihalli road, Whitefield, Bangalore- 560066	5	1	1	24
74	YELAHANKA	BANGLORE	1000 sq.ft. carpet	Unit no 792, MIG II STAGE, M.D.Road, Yelahanka, Bangalore- 560064	4	1	1	24
Grand Total					551	92	81	

*In case of any addition/ reduction in the number of locations, the Selected Bidder must provide/ adjust the equipment as per rate card provided in Commercial Bid of this Tender Document.

ANNEXURE II**BILL OF MATERIAL (BOM)**

S.NO.	Particulars	Qty	Unit Price (Rs.)	Total Cost (Rs.)
1	WIFI 6 Access Point and its accessories with 5 years OEM NBD Support	92 Access Points in 73 locations *		
2	TPM Secured 24 ports Managed switch with robust DRAM and buffer along with accessories and 5 years OEM NBD Support	75 Access switches in 72 locations* of 24 10/100/1000 BASE-T ports and 4 1G SFP ports and one 1G SFP transceiver		
3	TPM Secured 48 ports Managed switch with robust DRAM and buffer along with accessories and 5 years OEM NBD Support	6 Access Switches for HO with 48x ports 10/100/1000BASE-T Ports 4x 10G SFP+ ports and two 10G SFP+ transceivers		
4	NAC solution (Software & hardware) for 2000 endpoints including 100 BYOD devices along with 5 years OEM NBD Support	At Datacenter & DR Site.		
5	Midspan Injector devices Smart Rate 802.3at 30W along with Power Cords	As per count of Access Points		
6	Network Racks 9U *	15		
7	Network Racks 12U *	15		
8	Network Racks 24U *	5		
9	One Time Implementation			
10	Recurring cost for Managed Services for 5 years period (Payable in Quarterly arrear basis)			
11	Recurring cost for Passive LAN Networking complete Management for 5 year period of Contract (Payable in Quarterly arrear basis)			
12	Buy-back amount of existing D-link/ Tp-link switches / Racks etc. with branch specific list in Annexure – IV.			
13	Net Amount after deducting Buy-back amount			

* Estimated Quantities. The selected bidder will then do a site survey , network assessment, network design to arrive at the actual BOM.

ANNEXURE- III:-**1. Central Management: -**

Sr. No	Specifications	Compliance Yes / No	Remarks
1	The NMS tool should provide a complete view of the devices that are monitored and managed by tool. It also allows end-end provisioning, management, monitoring, and maintenance operations for the devices. NMS tool should simplify network operations by providing zero-touch setup, centralized management of networks, historical data reporting, and troubleshooting for networks located around city or around the state.		
2	NMS tool should have Guest management, flexible captive portal templates, captive portal customization, custom welcome text and terms/conditions, guest self-registration, sponsored access, social logins for Wi-Fi.		
3	Proposed solution should Streamlined Network Operations and eliminates the inefficiency of using disjointed, domain-specific network management tools and should have network health summary dashboard that provides quick insights to analyse and improve the network-of wireless LAN performance across the WAN.		
4	Tool should have Single dashboard for IT operators for readily assess the state of the network with views into global and site-level details. Selecting a site changes the interface to only show network devices and connected clients specific to that location. IT operators can swiftly identify potential problems, as well as zero-in on specific locations that require their immediate attention.		
5	NMS tool should simplify Onboarding and Provisioning of network infrastructure. Tool should accelerate this process with an easy setup wizard, flexible configuration options, and zero touch provisioning, and provide an intuitive mobile installer app.		
6	NMS tool should provide simplify network device configurations with templates and a user interface option with guided, step-by-step workflows. For devices with common configuration requirements, network admins can use groups to instantly apply or modify settings across large sets of devices.		
7	NMS tool should provide Zero touch provisioning, intuitive workflow for setting up network devices without onsite IT involvement. Configuration parameters can be defined within monitoring and management tool based on network- or site-specific requirements. To get started,		

	<p>simply plug in and power on a device. As the device boots up, it connects to centralised cloud-based tool and automatically receives its running configuration from the cloud. Customer a possibility to run any software of your choice from the available releases and will support each of them. NMS toll should allow administrator to test a software version in pilots and deploy them reliably at a larger scale. Administrator should be able to choose and stay on a firmware and tool should not have forced firmware upgrade policy.</p>		
8	<p>Monitoring tool should have Detailed health and analytics dashboards, broad visibility into network-wide performance, and drill-in to specific sites with summaries of device utilization, configuration compliance, and other statistics. Monitor application health across the network, ensuring critical services receive priority traffic while tracking and enforcing acceptable usage by site, device, or location.</p> <p>Delivers a multitude of details on devices connected to the network, including insights into client performance, connectivity status, physical location, and the data path. Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more. IT operators gain visibility into the health and utilization of switches. This includes port status, PoE consumption, VLAN assignments, device and neighbour connections, power status, and more-with built-in alerts and events that accelerate wired network troubleshooting. NMS tool should have Installer app for easy ZTP Role based admin access</p>		
9	<p>NMS Tool should have Built-in troubleshooting capabilities include live events, packet capture, logs, and rich command line tools. Tool should have Diagnostic checks such as ping tests and traceroutes and device-level performance tests. NMS tool should have debug capability from day one.</p>		
10	<p>Solution Should support URL Categorization and Same AP can work with controller & controller-less</p>		
11	<p>NMS tool should have CLI Configuration, Cloud Remote Console, Backup CLI config and Template Automation</p>		
12	<p>NMS tool should have Firewall Session Visibility</p>		
13	<p>NMS tool should have Artificial Intelligence to do Site Comparisons, Auto Baselines, Closed Loop Insights.</p>		
14	<p>NMS tool should have AI-powered Search, Dynamic PCAP & Crash Logs, AI-powered RF Mgmt., Network Insights, Broadcast Multicast Traffic Control, Configurable to Move Sticky Clients and WiFi6 Resource Management.</p>		

15	NMS tool should have AI-powered Client Profiling and Client Insights and should have Firmware Flexibility for firmware compliance		
16	NMS tool should support Live AP Events to give Immediate Responses, Unified Client List with 30 Second Updates, WLAN Connectivity Analysis, Wi-Fi Connectivity and WPA Handshake failures		
17	Management tool should provide reporting features Reports should cover device connectivity, network health, capacity planning, and the ability to baseline and compare user experience across various sites in the network. A reporting wizard is also provided to generate scheduled and on-demand reports that highlight network and application health, throughput and usage data, device and client inventory, activity auditing, and much more. Toll should have minimum 30 days of statistic and 90 days of reporting data.		
18	Management tool should have GUI-based workflow to upgrade firmware on deployed network devices. This includes the ability to complete live upgrades to reduce maintenance windows and ensure continuous operations. Upgrades can be completed at the site level and can also be scheduled during non-peak hours of operation. Management tool should support rules governing firmware compliance for all managed devices. NMS tool should have flexibility to deploy in On-Premises as well in cloud without changing the network devices. The Tool should have golden firmware option like Test one firmware & deploy and support rollback.		
19	NMS tool should support Customizable Severity and CPU / Memory alerts		
20	Management tool should support deep packet inspection capability with minimum 500+ apps with URL categorization.		
21	Management tool should support CLI access for Access point to Config Backup, Granular Overrides per site via CLI templates		
22	Management tool should have Firewall Session Visibility		
23	Management tool should support peer baseline and support AI insight.		
24	Management toll should support below Monitoring dashboard. - Access Request Dashboard - Auth Failure Charts - Client AAA Details - Reports		
25	NMS tool should also manage can configure the switch		

26	NMS tool must be configured for all Switches and access points supplied as part of this tender from day one		
----	---	--	--

2. Access Point:-

Sr. No	Specifications	Compliance (Yes/No)	Remarks
	Technical Specification		
1	Access Point radio should be minimum 2x2 MIMO on 2.4Ghz and minimum 4x4 MIMO on 5ghz . The AP should have Dual Radio 802.11ax access point with OFDMA.		
2	Access Point should be 802.11ax ready from day one and support WPA3 and Enhanced Open security from day one		
3	AP should have one Smart Rate port (RJ-45, maximum negotiated speed 2.5Gbps) Auto-sensing link speed (100/1000/2500BASE-T) and one 10/100/1000 Mbps speed LAN port		
4	Access point should support Built-in technology that resolves sticky client issues for Wi-Fi 6 and Wi-Fi 5 devices		
5	Access point should support OFDMA and MU-MIMO for enhanced multi-user efficiency		
6	Access point should IoT-ready Bluetooth 5 and Zigbee support		
7	Minimum aggregate data rate of 2.6 Gbps (HE80/HE40)		
8	Access Point can have integrated internal antenna		
9	The Max transit power of the AP + Antenna should be as per WPC norms for indoor Access Points. OEM to give an undertaking letter stating that the AP will be configured as per WPC guidelines for indoor AP and also submit the WPC certificate showing approval.		
10	Access point should have Interna/External Bluetooth Low energy beacon to support advance location-based services for Mobile engagement solutions and Applications.		
11	Should support 16x BSSID per AP radio.		
12	The access point should be capable of performing security scanning and serving clients on the same radio. It should be also capable of performing spectrum analysis and security scanning using same radio.		
13	Should support BPSK, QPSK, 16-QAM, 64-QAM, 256 QAM modulation types		
14	Access point should support 802.3af/at/bt POE standard and Midspan Injector for connecting with non-POE switch		

15	Intelligent Power Monitoring (IPM) to continuously monitor and report hardware energy consumption. AP can also be configured to enable or disable capabilities based on available PoE power – ideal when wired switches have exhausted their power budget.		
16	Access point should have option of external power adaptor as well.		
17	Access point should have console port.		
18	Must operate as a sensor for wireless IPS		
19	AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention service		
20	The Access Point should have the technology to improve downlink performance to all mobile devices.		
21	Access point must incorporate radio resource management for power, channel, coverage hole detection and performance optimization		
22	AP mounting kit should be with locking mechanism so that AP cannot be removed without using special tools.		
23	AP should have Kensington security slot		
24	AP should support standalone mode/ Inbuilt Virtual controller mode for specific requirements.		
25	The AP should support Advanced Cellular Coexistence (ACC) to minimizes interference from 3G/4G cellular networks, distributed antenna systems and commercial small cell/femtocell equipment		
26	The AP should support Supports priority handling and policy enforcement for unified communication apps, including MS Teams, Skype for Business with encrypted videoconferencing, voice, chat and desktop sharing		
27	The AP should support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories		
28	Pass point Wi-Fi (Hotspot 2.0) offers seamless cellular-to-Wi-Fi carryover for guests		
29	The Access point should support maximum ratio combining (MRC) for improved receiver performance		
30	The Access point should support cyclic delay/shift diversity (CDD/CSD) for improved downlink RF performance		
31	The Access point should support Space-time block coding (STBC) for increased range and improved reception		
32	The Access point should support Low-density parity check (LDPC) for high-efficiency error correction and increased throughput		

33	The Access point should support Transmit beamforming (TxBF) for increased signal reliability and range		
34	The Access point should support 802.11ax Target Wait Time (TWT) to support low-power client devices		
35	AP should be UL 2043 certified.		
36	Regulatory Compliance FCC/ISED CE Marked RED Directive 2014/53/EU EMC Directive 2014/30/EU Low Voltage Directive 2014/35/EU UL/IEC/EN 62368-1 EN 60601-1-1, EN60601-1-2		
37	Certifications UL2043 plenum rating Wi-Fi Alliance: - Wi-Fi CERTIFIED a, b, g, n, ac - Wi-Fi CERTIFIED ax - WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, W-Fi Agile Multiband - Wi-Fi certified Location - Passpoint (release 2) -Bluetooth SIG		
38	Proposed access points must be of Enterprise grade and supplied with OEM NBD response remote TAC support		

3. Access switch: -

S.No	Specification	Compliance Yes/No	Remarks
	Architecture		
1	Shall be 19" Rack Mountable		
2	The switch should have dedicated Console Port		
3	At least 4GB SDRAM and 16GB flash		
4	The Switch should support 8000 MAC address		
5	The switch should have minimum 512 Ipv4 Unicast Routes and 512 Ipv6 Unicast Routes 512 Icmp Groups ,512 Mld Groups		
6	At Branch, The switch should have 24 10/100/1000 BASE-T ports and 4 1G SFP ports and one 1G SFP transceiver.		
	At Head Offices, the switch should have 48x ports 10/100/1000BASE-T Ports 4x 10G SFP+ ports and two 10G SFP+ transceivers		
7	The Access switch for Branch should have at least 56 Gbps of Switching Capacity and 41 Mpps Throughput		

	Capacity and for HO location, the 48 port switch should have at least 176 Gbps of switching capacity and up to 98.6 Mpps Throughput.		
	IPv6 feature		
8	Switch should support IPv6 host enables switches to be managed in an IPv6 network		
9	Switch should support Dual stack (IPv4 and IPv6) transitions from IPv4 to IPv6, supporting connectivity for both protocols		
10	Switch should support MLD snooping forwards IPv6 multicast traffic to the appropriate interface		
11	Switch should support IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic		
12	Switch should support IPv6 Static routing		
13	Switch should support RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping		
	High Availability and Resiliency		
14	The Switch should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni directional traffic is detected, preventing loops in STP-based networks.		
15	The Switch should support IEEE 802.3ad LACP supports up to 8 LAGs and support for static or dynamic groups and a user-selectable hashing algorithm		
16	The Switch should support IEEE 802.1s Multiple Spanning Tree provides high link availability in VLAN environments where multiple spanning trees are required and legacy support for IEEE 802.1d and IEEE 802.1w		
17	The switch should support Strict priority (SP) queuing, Traffic prioritization (IEEE 802.1p), Class of Service (CoS), IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ, Rate limiting, per-queue minimums Large buffers for graceful congestion management		
	Management		
18	The Switch should support Built-in programmable and easy to use REST API interface		
19	The Switch should support On-premises and cloud- based management		
20	The Switch should have Scalable ASIC-based wire speed network monitoring and accounting using s Flow (RFC 3176) with no impact on network performance.		
21	The Switch should support Industry-standard CLI with a hierarchical structure		

22	The Switch should support Management security restricts access to critical configuration commands, provides multiple privilege levels with password protection, and local and remote syslog capabilities allow logging of all access		
23	The Switch should support SNMP v2c/v3 provides SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions.		
24	The Switch should support Remote monitoring (RMON) with standard SNMP to monitor essential network functions. Switch should support events, alarms, history, and statistics groups as well as a private alarm extension group.		
25	The Switch should support TFTP and SFTP support offers different mechanisms for configuration updates.		
26	The Switch should support Debug and sampler utility support ping and traceroute for IPv4 and IPv6		
27	The Switch should support Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients.		
28	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network to facilitate easy mapping by network management applications		
29	The Switch should support Dual flash images provides independent primary and secondary operating system files for backup while upgrading. Switch should support Multiple configuration files which can be stored to a flash image		
	Multicast		
30	The Switch should support IGMP Snooping to allow multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN		
31	The Switch should support Multicast Listener Discovery (MLD) enables discovery of IPv6 multicast listeners; supports MLD v1 and v2		
32	The Switch should support Internet Group Management Protocol (IGMP) and supports IGMPv1, v2, and v3		
	Layer 2 Switching		
33	The Switch should support 4094 VLAN IDs and 512 VLANs simultaneously		
34	The Switch should support Jumbo packet to improves the performance of large data transfers and support frame size of up to 9198 bytes		

35	The Switch should support Rapid Per-VLAN Spanning Tree (RPVST+) to allow each VLAN to build a separate spanning tree to improve link bandwidth usage.		
36	The Switch should support MVRP to allow automatic learning and dynamic assignment of VLANs		
37	The Switch should support Bridge Protocol Data Unit (BPDU) tunnelling to Transmits STP BPDUs transparently		
38	The Switch should support Port mirroring duplicates port traffic (ingress and egress) to a monitoring port and support minimum 4 mirroring groups		
39	The Switch should support STP supports standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
40	The Switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network		
	Layer 3 Routing		
41	The Switch should support Static IP routing.		
42	The Switch should support Dual stack static IPv4 and IPv6 routing to provide simple manually configured IPv4 and IPv6 routes		
43	The Switch should support Dual IP stack to maintain separate stacks for IPv4 and IPv6 to ease the transition from an IPv4-only network to an IPv6-only network design		
	Convergence		
44	The Switch should support LLDP-MED (Media Endpoint Discovery) to define a standard extension of LLDP that stores values for parameters such as QoS and VLAN to automatically configure network devices such as IP phones		
45	The Switch should support Auto VLAN configuration for voice RADIUS VLAN and use standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones		
	Security		
46	The Switch should support integrated trusted platform module (TPM) for platform integrity. This ensures the boot process started from a trusted combination of switches.		
47	The Switch should support Access control list (ACL) support for both IPv4 and IPv6 to allow for filtering traffic to prevent unauthorized users from accessing the network, or for controlling network traffic to save resources. rules can either deny or permit traffic to be		

	forwarded. rules can be based on a Layer 2 header or a Layer 3 protocol header		
48	The Switch should support ACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis		
49	The switch should support Remote Authentication Dial-In User Service (RADIUS) and minimal Access Controller Access-Control System (TACACS+)		
50	The Switch should support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks		
51	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards		
52	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port and accepts up to 32 Concurrent sessions of IEEE 802.1X, Web, and MAC authentications		
53	The Switch should support Secure management access delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3		
54	The Switch should support CPU protection to provide automatic protection against malicious network traffic trying to shut down the switch.		
55	The Switch should support ICMP throttling.		
56	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user		
57	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs and prevent forged BPDU attacks		
58	The Switch should support Dynamic IP lockdown to block traffic from unauthorized hosts, preventing IP source address spoofing		
59	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes		
60	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator		

61	The Switch should support MAC address lockout to prevent particular configured MAC addresses from connecting to the network		
62	The Switch should support Source-port filtering to allow only specified ports to communicate with each other		
63	The Switch should support Secure shell to encrypt all transmitted data for secure remote CLI access over IP networks		
64	The Switch should support Secure Sockets Layer (SSL) to encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch		
65	The Switch should support Critical Authentication Role to ensure that important infrastructure devices such as IP phones are allowed network access even in the absence of a RADIUS server		
66	The Switch should support MAC Pinning to allows non-chatty legacy devices to stay authenticated by pinning client MAC addresses to the port until the clients logoff or get disconnected		
67	The Switch should support Security banner displays a customized security policy when users log in to the switch		
68	The switch should support 256 Access control entry		
	Certification		
69	The Switch should support Green initiative for RoHS (EN 50581:2012) and WEEE regulations		
70	IEC / EN 62368-1: 2014 IEC / EN 62368-1: 2018 UL 62368-1: 2014, 2nd Ed., CSA C22.2 No. 62368-1:14, 2nd Ed		
71	Proposed Switches must be of Enterprise grade and supplied with OEM NBD response remote TAC support		

4. Network Access Control:-

SL No.	Specifications	Compliance Yes/No	Remarks
1	The proposed solution shall meet the below specifications. Any hardware/software/licenses required to enable the functionality shall be provided from Day 1		
2	Device Profiling and Visibility		
3	Provide automatic detection and categorization of endpoints for security and audit demands, regardless of device type, using contextual data and use this data for optimizing access policies		
4	Stored profiling data should identify device profile changes and dynamically modify authorization privileges. For example, if a printer appears as a Windows laptop, the system can automatically deny access. Should support Load balancing for profile scans and Scheduled Subnet scans		
5	Support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI and TCP SYN-ACK handshakes		
6	Support active device profiling methods such as SNMP, Subnet Scan, SSH, Sflow, WMI and NMAP Scan. NAC solution should support profile Load balancing for profile scans, IPFIX support.		
7	Internal device fingerprint dictionaries that provide a way to automatically or manually update periodically. Capable to define custom fingerprints for wired and wireless devices		
8	Offer a comprehensive dashboard to see the total number of endpoints, and the number by category, family and device type.		
9	Authentication, Authorization and Accounting (AAA)		
10	Integrated scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as user's role, device type, location, time of day etc.		
11	User and device authentication based on 802.1X, and Web Portal access methods across multi-vendor wired networks, wireless networks, and VPNs		
12	Usage of multiple authentication protocols concurrently, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public		
13	Must support RADSEC protocol to support RADIUS datagrams over TCP and TLS		
14	Must be supplied with fine-grained control using attributes from multiple identity stores, such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database,		

	token servers, and internal databases across domains within a single policy from day one		
15	Non-802.1X devices (such as printers, IP phones, IP cameras and IOT devices) can be identified as known, based on the presence of their MAC addresses in database, or unknown upon connecting to the network.		
16	Integrated TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels from day one. It should keep a track of the changes made by the logged-in user.		
17	NAC solution should support reporting with manual or scheduled reports in PDF/CSV/xls formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through email		
18	HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management		
19	Mobile Device Management Integration to fetch information such as device manufacturer, model, OS Version, Jail-broken, presence of any black-listed application, MDM Agent installation status etc. and use this information in access policies		
20	API Integration with helpdesk software allowing dynamic creation of problem tickets of any network triggered policy breaches		
21	Inbuilt utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network		
22	Process inbound threat-related events (which are Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.		
23	Must have Multi domain AD support		
24	All the user machines must be evaluated before allowed on the network and thus must only deploy with a secured IEEE 802.1X architecture . NAC solution must support deny access policy first.		
25	NAC solution should support Multivendor. Should have third party integration from day one. Should support automatic HA failover and Auto Upgrade tools NAC solution should use 802.1x authentication using native client of operating system		

26	NAC solution should support Per policy-based Certificate, Multifactor Authentication using MFA tool.		
27	Endpoint Posture Checking		
28	Perform advanced endpoint posture assessments to ensure organization's compliance is met before devices connect		
29	Support the following operating systems and versions: Microsoft Windows 11 and above, Apple macOS 10.10 and above		
30	Users of unhealthy endpoints that do not meet compliance requirements, should receive a message about the endpoint status and instructions on how to achieve compliance		
31	Endpoint posture and health checks should include Installed Applications, single Antivirus and multiple AV, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines, USB Devices etc		
32	Provide persistent agent for operating system to provide nonstop monitoring of the end point with automatic remediation and control		
33	Offer web-based dissolvable agent for endpoint compliance check of personal and non-IT-issued devices		
34	Must be able to detect multiple network interfaces and control it		
35	Must be able to detect USB, disable it and remove it		
36	Posture policy should support Configuration of time period for which posture Agent should ignore missing patches. Administration can be able to specify the grace period in hours, days, weeks, or months.		
37	NAC solution should update file check hash, health state for policy purposes, grace period in all health categories, client log uploads to remote server, Dashboard for posture request stats and MAC address randomization tracking/reporting		
38	Guest Access Management		
39	Easy-to-use guest management solution for visitors, contractors, partners, Auditors etc. on wireless and wired networks using any type of device.		
40	Guest access through captive portal with extensive branding and customization including company logos, visual imagery and optional advertisements with multimedia content to extend organization's messaging		
41	Captive portal should have mobile device awareness to automatically size for smart phones, tablets and laptops		
42	Guest self-registration through the web portal, delivering username and password directly to the visitor's Web browser, or sent via email or SMS.		

43	Sponsor-based approval workflow to enable an internal employee to approve guest account before guest is allowed to access the network		
44	Customize guest access privileges to enforce bandwidth limits, access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days		
45	Guest portal shall have an option to accept social logins using Facebook, Twitter, Slack and other social media credentials.		
46	Third-party integration providing customizable workflows using rest-based API's for delivering streamlined registration and payment system integration		
47	Personal Device (BYOD) Management		
48	Automatically configure and provision mobile devices such as Windows, macOS, iOS, Android, Chromebook, and Ubuntu, enabling them to securely connect to enterprise network. Number of users would be 100 nos.		
49	Offer built-in certificate authority (CA) to secure device onboarding without requiring the implementation of an external CA or make changes to an internal public key infrastructure (PKI). In case for some reason any OEM unable to provide inbuilt CA then can provide it externally, however from day one. should work as a Root or Intermediate CA and support Self-help portal for certificate management		
50	Support the distribution of in-built CA generated certificates to third-party applications using SCEP and EST (RFC 7030) protocols.		
51	Ensure rapid revocation and deletion of certificates for specific mobile devices if a user leaves the organization or the mobile device is lost or stolen.		
52	Support Online Certificate Status Protocol (OCSP)		
53	Capable to define the number of devices that can be on-boarded per user and validity of their certificates		
54	Automatic device certificate provisioning/installation with sponsor approval required option for onboarding		
55	Certificate Provisioning must work even after failover of its nodes		
56	Must support Oauth and SAML 2.0 Identity Provider, which allows seamless single sign-on (SSO) to the cloud or on-premises applications.		
57	Should support Secure certificate based onboarding and Automatic device certificate provisioning / installation		
58	Management and Reporting		
59	Predefined templates for reporting must be available		

60	A reporting option must be available to provide a method for delivering validated templates to unique requirements in a timely manner.		
61	Understanding trends, compliance and forensic analysis requires the ability to generate reports on data from selectable time frames in the past as well as on current data i.e Specific date and time range		
62	The reporting systems must provide robust filtering options in order to provide the information needed to make decisions and minimize data overload,		
63	Must have support for notifications via email		
64	Web-based user interface that simplifies policy configuration, monitoring and troubleshooting		
65	Requirement Summary		
66	Virtual Appliance (Automatic HA failover) with 1:1 redundancy for Azure. In Virtual Appliance, it shall offer with OEM recommended Hardware/VM Hypervisor for Azure		
67	Licenses supporting minimum 2000 concurrent sessions for AAA, Endpoint posture check, on Day 1		
68	5-Year 24x7 Hardware and Software Warranty with perpetual licenses. If it is not possible to offer perpetual licenses, the solution must include at least 10 years of licensing subscription upfront		
69	OEM and Product Eligibility/Compliance		
70	OEM shall have R&D facility in India; if required site visit shall be arranged		
71	OEM shall be capable of providing direct onsite warranty service for the products procured. The warranty service datasheet shall be attached with the proposal		

ANNEXURE – IV: -**BRANCH WISE LIST OF TENTATIVE BUY-BACK ITEMS**

Branch Name	DLINK	UNWANTED DEVICE
Ahmedabad	8 PORT SWITCH	digisol and one airtel xstream fiber, Cisco 892
Borivali	24 PORT DLINK	CISCO-800, AIRTEL XSTREAM FIBER
Bhubaneshwar	16 PORT DLINK	Digisol
Bangalore	24 PORT DLINK	CISCO892
Boisar	24 PORT DLINK	CISCO892
Barasat	24 Port Dlink switch	CISCO892
Chinchwad	24 PORT DLINK	MULTIVIEW AND CISCO BINATONE, 777VR1
Chandanagar	8 PORT + 8 PORT DLINK	CISCO892
Chennai	24 PORT DLINK	CISCO
Coimbatore	16 PORT DLINK	DIGISOL, BINATONE
Chandigarh	16 PORT DLINK	CISCO892
Delhi	16 PORT DLINK	CISCO892
Dehradun	8 PORT SWITCH	CISCO892
Durgapur	16 PORT DLINK	CISCO
Dwarka	24 PORT DLINK	NA
Electronic city	2 8 PORT DLINK SWITCH	CISCO
Gurgaon	24 + 24 PORT DLINK SWITCH	CISCO892
Ghaziabad	8 PORT	CISCO, BINATONE AND HUAWEI ROUTER
Greater Noida	24 PORT SWITCH	CISCO AND ONE MORE DEVICE
Guwahati	24 PORT HP SWITCH	HUAWEI ROUTER
Garia	24 PORT DLINK	CISCO892
Hyderabad	24 PORT DLINK	CISCO892
Hadapsar	24 PORT DLINK	NA
Hinjewadi	24 port switch	1 device is present need to confirm
Indore	24 PORT DLINK	CISCO892
Jaipur	16 + 16 + 8 + 4 PORT DLINK	CISCO ROUTER, 777VR1 ROUTER
Jodhpur	8 PORT DLINK SWITCH	CISCO892
Kolhapur	8 PORT SWITCH	TPLINK, CISCO892
Kalyan	24 PORT DLINK	CISCO892
Kochi	8 PORT SWITCH	CISCO 800
Kolkata	24 PORT SWITCH	CISCO892
Kengeri	16 Port dlink	CISCO892
Kozhikode	24 PORT DLINK	NA
L.B. nagar	8 + 8 PORT DLINK	CISCO892
Lucknow	16 PORT DLINK	CISCO892
Ludhiana	8 PORT DLINK	AIRTEL XSTREAM FIBER

Madurai	16 PORT DLINK	CISCO892
Mangalore	24 Port switch	digisol
Meerut	8 PORT SWITCH	JIO (2 AIRTEL DEVICES ARE ALSO THERE NEED TO CONFIRM THEIR CONN)
Margaon	8 PORT DLINK + 16 port	CISCO 892
Mumbai	24 PORT DLINK	NA
Nagpur	24 PORT DLINK	8 PORT DLINK
Nashik	16 PORT DLINK	CISCO892
Nere Panvel	8 PORT SWITCH	NA
Noida	16 PORT DLINK	CISCO892
Navi mumbai	24 PORT DLINK	NA
Nellore	16 PORT DLINK	NA
Panaji	16 PORT DLINK	CISCO892
Panvel	24 PORT DLINK	CISCO892
Patiala	8 PORT SWITCH	CISCO892
Patna	8 PORT DLINK	CISCO892
Pitampura	16 + 16 PORT DLINK	
Porur	8 PORT DLINK	AIRTEL XSTREAM FIBER
Pune	24 PORT DLINK	CISCO892, SANSCORD
Raipur	16 PORT SWITCH	AIRTEL XSTREAM FIBER
Siliguri	16 PORT SWITCH	AIRTEL XSTREAM FIBER
Suchitra	8 PORT SWITCH	POE ADAPTER
Surat	24 PORT DLINK	TPLINK(BRANCH PERSON IS SAYING THAT IT IS ALSO USING IN CONNECTION)
Tambaram	8 PORT SWITCH	NA
Thane	24 + 24 PORT DLINK SWITCH	CISCO892
Thrissur	16 PORT DLINK	CISCO892
Trichy	8 PORT SWITCH	CISCO892
Trivandrum	8 PORT SWITCH	CISCO892
Vadodara	8 PORT SWITCH	DIGISOL, CISCO892
Varanasi	8 PORT SWITCH	NA
Vasai	24 PORT DLINK	NA
Vijayawada	8 PORT SWITCH	CISCO892
Virar	16 PORT DLINK	CISCO892
Vizag	16 PORT DLINK	CISCO892
Whitefield	16 PORT DLINK	
Yelahanka	8 PORT DLINK	
Head office – 6 th Floor	3 units of HP 2530 Switch & D-link or TP-Link switches	HP 2530; Cisco 892, Cyberoam; Netgear
Head Office 4 th floor	3 Units of Dlink – 24 port switch	Cyberoam

1. SPECIAL TERMS AND CONDITIONS

1. The Bidders shall abide by the Special Terms and Conditions (STC) listed in this RFP document.
2. The Bidders are advised to submit the Bids strictly based on the terms and conditions and specifications contained in the RFP tender document including amendments, if any, issued by GICHFL prior to the date of submission of the Bids. The formats prescribed in this tender document should be scrupulously followed by the Bidders. Bids that do not comply with the terms and conditions hereof or are incomplete are liable for rejection. The Bidders must take due care and caution in this regard.
3. The contract shall be in force for the Contract Period, i.e., total period including implementation phase plus 5 years from the date of Go-Live declared by GICHFL. However, the contract can be extended further if mutually decided by GICHFL and the Selected Bidder.
4. The Selected Bidder shall enter into a detailed Service Level Agreement (SLA), a Non-Disclosure Agreement (NDA), a Deed of Indemnity with GICHFL (as per draft attached with tender document) within 30 days from the receipt of notification of the award of the contract. However, GICHFL reserves the right to alter/ vary/ amend/ modify all or any of the terms set out in the said draft Agreements before the same are signed.
5. No binding legal relationship shall exist between any of the Bidders and GICHFL until the execution of SLA.
6. In addition to the grounds prescribed under STC, if the Selected Bidder fails to furnish the Service Level Agreement, Reciprocal Non-Disclosure Agreement, Integrity Pact, Deed of Indemnity in accordance with provisions, terms, and conditions of the tender, the EMD shall be forfeited.
7. The Selected Bidder shall follow the Information Security Policy of GICHFL, which will be shared after submission of NDA. In case the Selected Bidder is found to be in violation of the said policy, GICHFL reserves the right to terminate the contract in addition to any other remedies for breach, injunctive relief, and indemnity as per the contract and the applicable laws.
8. During evaluation and comparison of bids, GICHFL may, at his discretion, ask the Bidder for clarifications on the bid and/or shortfall information/ documents. The request shall be given as per RFP rules, asking the Bidder to respond by a specified date, and mentioning therein that, if the Bidder does not comply or respond by the date, his bid will be liable to be rejected. Depending on the outcome, such bids will be rejected or considered further. It is, however, clarified that no post-bid clarification at the initiative of the Bidder shall be entertained.
9. Correct technical information must be filled in. Filling up of the information using terms such as “OK”, “Accepted”, “Noted”, “As given in Brochure/ Manual” “negotiable”, “to be discussed” is not acceptable. GICHFL may treat such bids as not adhering to the guidelines and as unacceptable.
10. Any quotation or billing linked to GICHFL’s Assets and/ or Revenue will disqualify the Bidder.

11. If at any point in time the services of Selected Bidder are found to be non-satisfactory, the contract will be terminated as per the termination provisions of the SLA.
12. The Selected Bidder will treat all confidential data and information about GICHFL, obtained in the execution of this tender including any business, technical or financial information, in strict confidence and will not reveal such information to any other party. Successful Bidder shall sign the Reciprocal Non-Disclosure Agreement (NDA) agreement with GICHFL to maintain and protect the confidentiality of Data and Information.
13. All supporting documentation submitted by the Selected Bidder as part of this proposal shall become the property of GICHFL.
14. Amendments/ Corrigendum to the tender document, if any, would be hosted on GICHFL Website as per rules. 15. Any effort made by the Bidder to influence GICHFL in the evaluation/ contract award decision, may result in the rejection of the bid. It is GICHFL's intent to select the bid that is most advantageous to GICHFL, and each bid will be evaluated using the criteria and process outlined.
15. GICHFL reserves the right to conduct an audit of the Selected Bidder to determine whether the activities are being performed as required by the Scope and as agreed in the contract.
16. GICHFL reserves the right to take appropriate action against Bidder in case of breach of GTC including cancellation of contract, treating the contract as null and void and rejecting the Services, without any cost or consequence to GICHFL.
17. GICHFL reserves the right to:
 - a. Accept/ reject any or all the bids submitted by a Bidder, without assigning any reasons thereof.
 - b. Add, modify, relax, or waive off any condition(s) stipulated in the bid whenever deemed necessary.
18. It is construed that the Bidder has read all the terms and conditions before submitting the bid.
19. GICHFL authority will not be held responsible for any technical snag or network failure during on-line bidding.
20. The Selected Bidder shall adhere and comply with all the applicable laws of land and rules, regulations and guidelines prescribed by various regulatory, statutory and Government authorities of India.
21. A Bidder shall submit only one proposal/ bid, either individually or as a joint venture in another proposal/ bid. If a Bidder including a joint venture partner submits or participates in another proposal/ bid, all such proposals/ bids shall be disqualified.
22. All information provided by GICHFL in this tender is offered in good faith. Individual items are subject to change at any time. GICHFL makes no certification that any item is without error. GICHFL is not responsible or liable for any use of the information or for any resulting claims.
23. Any publicity by the Selected Bidder in which the name of GICHFL is to be used must be done only with the explicit written permission of GICHFL.
24. The Selected Bidder will be responsible for gap identification and resolution to:

- a. Provide all functionalities mentioned in the scope of work.
- b. The Selected Bidder will provide GICHFL with the gap identification report along with the necessary solutions to overcome the gaps and the time frames.
- c. The Selected Bidder will ensure that gaps identified at the time of testing will be immediately resolved within the timelines agreed.
- d. The Selected Bidder shall resolve gaps by customizing the proposed solution by way of modifications / enhancements, as necessary.
- e. The Selected Bidder will give adequate time to GICHFL for reviewing the gap report.
- f. The Selected Bidder will incorporate all the suggestions made by GICHFL to the gap report.

25. In case of any queries, kindly contact us at: -

GIC HOUSING FINANCE LTD
IT DEPARTMENT
NATIONAL INSURANCE BUILDING
6TH FLOOR, 14, J.TATA ROAD,
CHURCHGATE, MUMBAI – 400020.
TEL.NO. 022-43041920

2. SERVICE LEVELS:

a. MEASUREMENT OF SERVICE LEVEL AND LIQUIDATED DAMAGES

In the event of poor performance or delay as per the requirements of the SLA and Tender Document, the Selected Bidder is solely responsible for the Penalty which shall be calculated as below.

Quarterly Recurring Charges (QRC) will be calculated from the AMS (Annual Maintenance Support) cost component provided in the Commercial Bid. The QRC used below refers to QRC applicable for the quarter in which the Service or Incident Request was created.

Payments will be adjusted for breach of SLA conditions against Quarterly Recurring Charges or QRC.

The Penalty Calculation depends on two levels of performance, namely:

- a. The Selected Bidder will get 100% of the Quarterly payment if the baseline performance metrics are complied with.
- b. The Selected Bidder will get quarterly payment after deducting penalty at the rates specified below in case of performance not meeting the SLA terms.

Penalty will be calculated based on the parameters below:

a) Service Request (SR) Management:

- i. Service Requests (SR) will consist of requests for changes to the existing network, audit recommendations, VAPT activities, custom reports generation, log reviews, other requests not explicitly mentioned in Scope of Work, etc.

- ii. The Selected Bidder shall make an estimate of the time required for carrying out the requested service/ task and this will be mutually agreed upon by the selected Bidder and GICHFL. Thereafter, the penalty cost for missed deadlines of each SR will result in a penalty of 1% of QRC per SR up to a maximum of 10% of QRC.
- iii. The monitoring/ support tool provided by Selected Bidder must capture such time frames for SRs and subsequent penalty calculations.

b) Incident Request (IR) Management:

- i. Incidents will consist of any event that disrupts the functioning of the infrastructure, like network device failure, DC component failure, network outage, network performance issues, unplanned downtimes, etc. The penalty for Incidents will be calculated based on the Network Uptime and the severity of the Incident. Incidents will be categorized as below:

Impact	Severity
<ul style="list-style-type: none"> • WLAN Services are down/ offline for an entire Branch/ HO. • When more than 20% of users are affected by WLAN issues in any floor of HO/ branch. • Smart Rack not functioning as desired/ issues with DC Infrastructure. 	Critical
More than 10% of users are affected by WLAN issues in any floor of HO/ branch. Medium	Medium
More than 5% of users are affected by WLAN issues in any floor of HO/ branch.	Low

- ii. Selected Bidder shall maintain the Wireless Network and in-house DC in Proper Operational Condition.
- iii. Network & Services will be considered unavailable if the fault/ incident reported to the Selected Bidder by GICHFL or identified by Selected Bidder himself is of Severity Level “Critical” and will be referred to as “Network & Service Unavailability”.
- iv. The Selected Bidder shall calculate, monthly, the “Network & Service Unavailability Time” experienced by GICHFL, in hours. A month shall be deemed to begin at 12:00AM Indian Standard Time (“IST”) on the first day of a calendar month (“Month”) and end 12:00AM IST on the first day of the next calendar month.
- v. The Selected Bidder shall also calculate “Net Working Time” in hours based on the number of calendar days in that month (e.g., January will have $31 * 24 = 744$ hours of Net Working Time).
- vi. At the end of a Month, Selected Bidder shall calculate the total amount of time the Network & Services were unavailable measured from the time when a fault/ incident of “Critical” Severity Level was reported to the Selected Bidder or is identified by Selected Bidder, whichever first occurs, until the time the fault/ incident is repaired/ resolved, and the Network & Services restored. This will be referred to as the “Network & Service Unavailability Time” and will be used in the calculation of “Network Uptime”.

vii. For “Medium” & “Low” category incidents, penalty will be calculated as below:

For Severity Level “Medium”: -

S.No.	Duration of Service Unavailability	Penalty
1	0 – 12 hours	No Penalty
2	After 12 hours	Severity level to be set to “Critical” and to be treated as “Network & Service Unavailability Time”

For Severity Level “Low”: -

S.No.	Duration of Service Unavailability	Penalty
1	0 – 12 hours	No Penalty
2	After 12 hours	Severity level to be set to “Critical” and to be treated as “Network & Service Unavailability Time”

viii. “Network Uptime” will be calculated monthly and must always be 99.99% or above as mentioned in SOW.

This will be calculated as below:

Network Uptime = $(1 - \{(\text{Network \& Service Unavailability Time} / \text{Net Working time}) \text{ in hours}\}) * 100\%$.

- c. Penalty will be calculated as a % of QRC against sliding % of Network Uptime as per below table:

Network Uptime %	% of QRC
≥ 99.99	0
$\geq 99.5 \& \leq 99.9$	1
$\geq 99.3 \& \leq 99.5$	2
$\geq 98.95 \& \leq 99.3$	3
$\geq 98.6 \& \leq 98.95$	5
$\geq 97.9 \& \leq 98.6$	7
$\geq 97.2 \& \leq 97.9$	9
$\geq 96.67 \& \leq 97.2$	10
< 96.67	10

- i. The Selected Bidder shall provide GICHFL with a prompt online report of the service unavailability & downtime.
- ii. The Penalty will be calculated monthly and then added up for a quarter and deducted from Quarterly Recurring Charges (QRC) of the AMS Cost to the Selected Bidder. The Selected Bidder shall adhere to all requirements laid out in the Tender Document and this Agreement.
- iii. The penalty calculated against SRs & IRs will be mutually exclusive.

- iv. The Selected Bidder must share detailed RCA report after closure of each such Incidents

d) Replacement of Faulty hardware: Delays in replacement of faulty hardware will be treated as Incidents and assigned severities as below if the timelines are not met by Selected Bidder.

Equipment	Replacement Timelines	Incident Severity
Access Points	2 days	Low
Access/ Access switch	24 Hours	Critical
Rack/ Rack Component	5 days	Critical
NAC Appliance/ Server	3 days	Medium
Cat6/ fiber Cables, I/O Ports, RJ45, all other equipment	2 days	Low

Non-Compliance of SLAs

- a. The vendor must take note that the Max limits of penalties are upper tolerance and GICHFL reserves the right to terminate the contract at any point of time for breach of SLAs without reaching the Max limit of penalties.
- b. **Note:** SLA will be calculated quarterly.

3. AUDIT REQUIREMENTS:

- a. GICHFL is subjected to various audits [internal / statutory / RBI etc.]. In the event of any observation by the audit regarding security, access etc., the same will be intimated to the Bidder. The Vendor to carry out the changes for enabling GICHFL to comply on the same, if required. No additional cost would be paid by GICHFL.

4. RIGHT TO AUDIT:

- a. Compliance with security best practices may be monitored by various periodic security audits performed by or on behalf of the Company. The periodicity of these audits will be decided at the discretion of the Company. These audits may include, but are not limited to, a review of access and authorization procedures, physical security controls, backup and recovery procedures, security controls and program change controls. To the extent that the Company deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the selected bidder shall afford the Company's representatives access to the selected bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The selected bidder must provide the Company with access to various monitoring and performance measurement systems (both manual and automated). The Company has the right to get the monitoring and performance measurement systems (both manual and automated) audited without prior approval/notice to the selected bidder.

5. KNOWLEDGE TRANSFER:

- a. This section outlines the obligations and procedures for a comprehensive knowledge transfer from the incumbent service provider ("Outgoing Provider") to the newly selected service provider ("Incoming Provider") in the event of a change in service provision. The objective is to ensure a seamless transition with minimal impact on the client's operations, maintain service quality, and secure the continuity of critical functions.

6. Knowledge Transfer Obligations: -

From Outgoing Provider: The Outgoing Provider agrees to:

- a. Provide complete and accurate documentation related to the services being transitioned. This includes, but is not limited to, system architecture, process flows, incident reports, configuration details, and user guides.
- b. Offer detailed briefings and hands-on training sessions to the Incoming Provider's designated personnel on all aspects of the service operations, including the handling of any proprietary tools or specialized software.
- c. Facilitate a series of shadowing opportunities for the Incoming Provider's team to observe daily operations, incident response procedures, and maintenance routines.
- d. Make available subject matter experts (SME) to answer queries and provide advice to ensure a smooth handover and continuity of services.
- e. Ensure the transfer of all relevant digital assets, credentials, and access permissions to the Incoming Provider in a secure manner.

7. Submission of Proposals/ Guidelines for Bidders & Other related Terms & Conditions:

- a. The Bidders should ensure that all assumptions/clarifications required are clarified beforehand. Any bids with words/phrases such as (but not limited to) "assumption", "it is understood that", "conditional offer" may be subjected to rejection at any stage of evaluation.
- b. Bidders should submit their responses as per the formats given in this RFP in the following manner:
- c. Technical Proposal and Eligibility Criteria in first envelope – Sealed Envelope 1 (Hard Copy).
- d. Commercial Proposal in second envelope – Sealed Envelope 2 (Hard Copy).
- e. Please note that prices should not be indicated in the technical proposal but should only be indicated in the Commercial proposal. However, a masked bill of material masking the price information be provided along with the technical proposal.
- f. The two sealed envelope containing copies of technical Proposal and commercial Proposal, clearly marked "Response to RFP towards Wireless LAN Infrastructure and Network Access Control (NAC)" for GICHFL.
- g. The outer envelope thus prepared should also indicate clearly the name, address, telephone number and E-mail ID of the Bidder to enable the Bid to be returned unopened in case it is found to be received after the time and date of Proposal submission prescribed herein
- h. All the pages of the Proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bidder's Proposal.
- i. The original Proposal shall be prepared in indelible ink. It shall contain no interlineations or

- overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initiated by the authorized signatory of the Bidder.
- j. All pages of the bid shall be initialed and stamped by the authorized signatory of the Bidder.
 - k. The Bidder must submit a certificate of undertaking on its official letterhead duly signed by its authorized signatory confirming the acceptance of all the terms & conditions contained in and spread throughout this Bid Document.
 - l. The Bidder should provide supportive documents regarding the proof of being an authorized LSP of OEM. Failing which will lead to the disqualification of such Bidder.
 - m. Decision as to any arithmetical error, manifest or otherwise in the response to Bid Document shall be decided at the sole discretion of GICHFL and shall be binding on the Bidder. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder. Bidder should be a legal entity and financially solvent. Bidder must warrant that no legal action is pending against them in any legal jurisdiction which affects its ability to deliver the RFP requirements.
 - n. GICHFL reserves the right to re-issue/re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder.
 - o. GICHFL reserves the right to modify its requirement for each product/service at any stage of the process.
 - p. Modification to the RFP, if any, will be made available as an addendum on GICHFL website/will be emailed to bidder.

8. Managed Security Service:

- a. The bidder shall raise the invoice on arrear basis for the quarter along with a credit note for penalty for that quarter. The net of same will be released.
- b. Payment for any quarter will be made after deducting TDS/other taxes and applicable penalty/LD pertaining to the quarter.
- c. On receipt of payment advice from the company, the bidder has to acknowledge the same and submit payment receipt/ confirmation.
- d. Payment for subsequent quarters will be made subject to satisfactory performance during the serviced period.
- e. The company has the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the company.
- f. All payments will be made within 1 month of receiving the undisputed invoice along with credit note/invoice, if applicable.
- g. The Bidder must accept the payment terms proposed by the company. The financial bid submitted by the Bidder must be in conformity with the payment terms proposed by the company.

9. Notification of Award/Purchase Order:

- a. After selection of the T1 L1 bidder and obtaining internal approvals and prior to expiration of the period of Bid validity, GICHFL will send Notification of Award/Purchase Order to the selected Bidder.

10. Signing of Purchase Order:

- a. Within 2 days of receipt of the Purchase order the successful Bidder shall accept and acknowledge the Purchase Order.
- b. Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

11. Termination of Contract with selected bidder:

- a. There will be 2 months' prior notice that will be given by GICHFL to selected Bidder in case GICHFL wishes to discontinue the contract, be it any reason as inability to provide standard service/ due negligence in any part and so on during the contract period or as GICHFL may deem fit. If the selected Bidder wishes to discontinue the contract, then the Bidder must give a minimum of 6 months of prior notice.

12. Confidentiality Agreement

- a. Everyone to maintain confidentiality and shall disclose anything related to bid only to those employees involved in preparing the requested responses. The information contained in the RFP may not be reproduced in whole or in part without the express permission of the institution/org. (in this case GICHFL).

13. Payment in case of Termination of contract:

- a. Subject to the terms of the RFP, in case the contract is terminated, payment towards services will be made on a pro rata basis, for the period services have been delivered, after deducting applicable penalty and TDS/other applicable taxes.

14. Force Majeure

- a. The Vendor shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.
- b. For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Vendor and not involving the Vendor's fault or negligence and not foreseeable. Such events may include Acts of God or of public enemy, acts of Government of India in their sovereign capacity and acts of war.
- c. If a Force Majeure situation arises, the Vendor shall promptly notify the company in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the company in writing, the Vendor shall continue to fulfil Vendors obligations under the Contract as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- d. In such a case the time for performance shall be extended by a period (s) not less than duration of such delay. If the duration of the delay continues beyond a period of three

months, the company and the Vendor should hold consultations in an endeavor to find a solution to the problem.

15. Governing Law & Disputes

- a. All disputes or differences whatsoever arising between the parties out of or in relation to the construction, meaning and operation or effect of these Tender Documents or breach thereof shall be settled amicably. If however, the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. The Arbitrator/Arbitrators shall give a reasoned award. Any appeal will be subject to the exclusive jurisdiction of the courts at Mumbai, Maharashtra.
- b. During the arbitration proceedings the Vendor shall continue to work under the Contract unless otherwise directed in writing by GICHFL or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or the umpire, as the case may be, is obtained.

16. KEY INSTRUCTIONS FOR THE BIDDERS:

1. Right to Terminate the Process

- a. GICHFL may terminate the RFP process at any time without assigning any reason. GICHFL makes no commitments, expresses or implies that this process will result in a business transaction with anyone.
- b. This RFP does not constitute an offer by GICHFL. The Bidder's participation in this process may result in GICHFL selecting the Bidder to engage towards execution of the subsequent contract.

2. SUBMISSION INSTRUCTIONS:

1. Two sealed Envelopes in Hard Copy to be submitted:

Envelope 'A'

- a. The envelope shall be sealed and marked as "Envelope A-Tender to RFP towards Wireless LAN Infrastructure and Network Access Control (NAC) For GICHFL." in the top left-hand corner. The envelope shall be dated with the current date in the top right-hand corner.

It should contain the following:

- I. Minimum Eligibility Criteria table for Bidder and its supporting documents as specified in the RFP above.
- II. Technical Requirements table with their compliance status as specified in the RFP above.

Envelope ‘B’

- a. The envelope shall be sealed and marked as “Envelope B-Tender Envelope A-Tender to RFP towards Wireless LAN Infrastructure and Network Access Control (NAC) For GICHFL” in the top left-hand corner. The envelope shall be dated with the current date in the top right-hand corner.
- b. Please note that no other information other than the commercials should be furnished in this envelope. **Format for commercial bid is attached to Annexure II.**

It should contain the following:

- a. Cost for licenses for year-on-year basis. (It should cover separate costs for Year 1, Year 2 and so on).
- b. One-time implementation cost.
- c. Detailed description of cost for Managed service for One Time Implementation and Managed Services for the contract period.

17. Service Level Agreement

- a. SLAs define the quality and timeliness of service delivery during the agreement/contract period as mutually agreed upon. They help GICHFL sustain the planned business outcomes from the solution deployed on a continued basis over a sustained period.
- b. The Bidder needs to execute a Service Level Agreement with GICHFL covering all terms and conditions of this tender. Bidders need to strictly adhere to Service Level Agreements (SLA). GICHFL shall, without prejudice to its other rights and remedies under and in accordance with the GICHFL terms, levy liquidated damages in case of breach of SLA by the bidder. Services delivered by bidder should comply with the SLA. Service Levels will include Availability measurements and Performance parameters.
- c. Performance measurements would be assessed through audits or reports, as appropriate to be provided by the Bidder e.g. utilization reports, response time measurement reports, etc. and will be monitored by using existing GICHFL.
- d. Scheduled operation time means the scheduled operating hours of the System for the month. All planned downtime (for system maintenance) on the system would be deducted from the total operation time for the month to give the scheduled operation time.
- e. Commencement of SLA: The SLA shall commence immediately after contract is awarded. The liquidated damages will be deducted from the next payment milestone after the SLA holiday period.
- f. GICHFL business hours are typically between 9 am to 7 pm (Monday to Saturday) and the SLA will be applicable according to the technological operations window i.e. 24*7*365.

18. Taxes and Duties:

- a. All taxes deductible at source, if any, at the time of release of payments, shall be deducted at source as per the prevailing rate while making any payment.
- b. Commercial Bid should be specific and inclusive of GST, duties, charges and levies of State or Central Governments as applicable, VAT/Sales Tax, insurance, service taxes, Octroi etc.

- c. The benefits realized by the bidder due to lower rates of taxes, duties, charges and levies shall be passed on by the bidder to GICHFL.

19. Compliance Terms: -

Sr. No.	Terms to be agreed upon	Compliance (Yes / No)
1	The price quote should be in INR only.	
2	The aforesaid Scope of Work points are agreed by us for the period of 5 years or until the contract exists. If there are any discrepancies, Bidder should provide detailed update on SoW non-deliverables else, entire aforesaid SoW is considered to be agreed.	
3	The price quoted by the bidder should be valid for the period of 5 years by signing an SLA Agreement and NDA with GICHFL.	
4	The bidder should be responsible in providing the Implementation Support and Maintenance including technical support in coordination with OEMs during the contract period.	
5	The Bidder shall abide by all the Terms & Conditions as stated by GICHFL in the aforesaid RFP.	

20. PAYMENT TERMS:

1. The Contract price shall be equal to the amount specified in the Commercial Bid. Payments will be released only on satisfactory acceptance of the deliverables for each task as per the following schedule:
 - a. The Selected Bidder shall complete the implementation of Wireless LAN infrastructure and Network Access Control within 12 weeks of acceptance of the Purchase Order (PO). The new infrastructure must be end-user ready and fully live/ functioning within the above timelines.
 - b. One-Time Charges, which include WLAN Implementation, as per the Commercial Bid would be paid for completion of activities as per Scope of work and sign-off from GICHFL.
 - c. Recurring charges, for Annual Maintenance Support, would be paid at the end of each quarter, on arrear basis, on receipt of invoice, thereafter for the duration of the Contract Period.
2. All Payments shall be made in Indian Rupees Only and will be subject to provisions of the Penalty or any other recoverable due from Selected Bidder to GICHFL.
3. GICHFL shall be entitled to make recoveries from the Selected Bidder's bill/ invoice or from any other amount due to the Selected Bidder, of the equivalent value of any payment

made to it due to inadvertence, error, collusion, misconstruction, misstatement, or mistake.

4. Selected Bidder shall be deemed to have considered all the costs required for successful implementation of the Scope of Work as per Tender Document and this Agreement while submitting the Commercial bid. GICHFL will not be liable to pay any extra cost, charges or out-of-pocket expenses.
5. Payment for the implementation of the Scope of Work as per the Tender Document and this Agreement will be released after signing off for successful completion of the Scope of Work.
6. The Selected Bidder shall not, in any case whatsoever, link its billing to GICHFL's assets and/or revenue base.

-----END OF RFP DOCUMENT-----