गृहे सौख्यम् विराजते

GIC HOUSING FINANCE LTD.

Request for Proposal of

Consolidated and Comprehensive Security Framework Implementation

RFP Reference Number: REF: GICHFL-IT: SYS: 2025-26/ S109

Dt. 29-12-2025

GIC Housing Finance Ltd
14, 6th Floor, J. Tata Road,
Churchgate, Mumbai -400020
Tel:22-22831578
Email: itadmin@gichf.com

1. Table of Contents

1. Introduction

1.1 About the Company

GIC Housing Finance Ltd (GICHFL) herein after called as the Company, one of the leading Housing Finance Company, has a network of 84 offices spread throughout the country as on date. GICHFL is a company registered under Section 25 of the Companies Act, 2013 with its Registered Office at National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020.

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.

1.2 Invitation for Tender offers

GIC Housing Finance Limited (GICHFL) invites sealed tender offers (Technical bid and Commercial bid) from eligible, reputed Original Equipment Manufacturers (OEM) for Procurement, Design, Implementation and Support Maintenance of Consolidated and Comprehensive Security Framework at GICHFL. In this Request for Proposal (RFP), the term bidder / prospective bidder refers to the primary bidder participating for delivering services mentioned in various sections of Scope of Work. The service partner and OEM participating in the RFP are responsible for submitting correct and optimal response. Multiple service partners can submit RFP responses for more than 1 OEMs to ensure appropriate BOM/BOQ with optimal cost proposal is finalized post Security Gap Assessment exercise is conducted, it is the first activity that the selected service partner shall execute before a particular OEM, cost and feature implementation list is finalized. The finalized feature implementation list may have mix of OEMs who would be selected to provide selected specific security requirements. The OEMs shall provide rate per units for devices / licenses and Service partners shall provide the managed service quotations.

The RFP is available through Company website for certain days. The Company reserves the right to reject any or all offers without assigning any reason.

Technical Specifications, Bill of Material documents, Terms and Conditions and various formats and pro forma for submitting the tender offer are described in this document, Annexures and Appendices.

1.3 Information Provided

This document contains statements derived from information believed to be reliable at the date obtained but does not purport to provide all the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with the Company in relation to the solutions. Neither the Company nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

1.4 For Respondents Only

The document is intended solely for the information of the party to whom it is issued herein after called as “Recipient” or “Respondent” or “Bidder”.

1.5 Confidentiality

The invitation document and the information contained in this RFP are strictly confidential. The Recipient (Bidder) shall not disclose, reproduce, transmit, or make the invitation document available to any other person or party not involved in responding to the RFP, nor to other potential Bidders. By receiving this RFP, the Bidder agrees to maintain the confidentiality of the document and all information provided by the Company. The Company may or may not update or revise the document or any part of it, and the Bidder acknowledges that any such revised or amended document will be subject to the same confidentiality obligations. Furthermore, the information in the RFP, whether provided verbally or in writing, shall be subject to the terms and conditions outlined in the RFP and any additional terms under which the information is provided. The Recipient shall not disclose or discuss the contents of the document with any officer, employee, consultant, director, agent, or other person associated with the Company or its customers or suppliers without the prior written consent of the Company.

1.6 RFP disclaimer

This Request for Proposal (RFP), including Annexures and any subsequent Addenda and Corrigenda (hereinafter referred to as the RFP or Tender), has been prepared solely for the purpose of enabling the Company to select a Service Provider for the Implementation & Management of a Consolidated and Comprehensive Security Framework Implementation, including interfaces, integrations and connectivity to various services that may be exposed from third party solutions located at different locations under the scope of the specifications, terms and conditions, and SLAs defined in this RFP (hereinafter referred to as the CCSF). The Bidder is expected to be innovative, capable, and committed to extending all necessary resources and services to meet the Company's expectations in delivering the required services. This RFP document does not constitute a recommendation, offer, or invitation to enter into a contract, agreement, or any other arrangement regarding the supply and services as per the scope of the RFP. It is an invitation for Bidder responses, and no contractual obligation shall arise from the invitation process unless and until a formal Purchase Order/Work Order is signed and executed by duly authorized officials of the Company and the selected Bidder.

1.7 Important Details (Schedule of Events, contact & communication details etc.)

Particulars	Details
Tender Number	REF: GICHFL-IT: SYS: 2025-26/ S61
Tender Title	Request for proposal for Selection of vendor for Procurement, Implementation and Maintenance of Request for Proposal of Consolidated and Comprehensive Security
RFP Release Date	December 29, 2025
Last Date for submission of Bids	January 16,2026
Bid Opening Date	TBD
Bid Validity	30 Days

Contact Persons for any clarifications	22 43041920
Contact Email ID	itadmin@gichf.com
Place of Opening of Bids	GIC Housing Finance Ltd 14, 6th Floor, J. Tata Road, Churchgate, Mumbai, 400020

Subsequently, the company will evaluate the Technical Bids, and the bidders shall be suitably intimated about their technical bid after evaluation.

1.8 Costs to be borne by bidders

All costs and expenses incurred by Bidders in any way associated with the development, preparation, and submission of their responses to the RFP, including but not limited to attendance at meetings, discussions, presentations, demonstrations, etc. and providing any additional information required by the Company, will be borne entirely and exclusively by the Bidder.

1.9 Legal Relationship

No binding legal relationship will exist between any of the Bidders and the Company until execution of a contractual agreement.

1.10 Disqualification

Any form of canvassing/lobbying/influence/cartelization, etc. by the Bidder may result in disqualification of such Bidder.

1.11 Recipients' Obligation to Inform Itself

It is the Recipient's responsibility to conduct all necessary investigation and analysis regarding any information contained in the document and the meaning and impact of that information.

1.12 Evaluations of Offers

Each Recipient acknowledges and accepts that the Company may, at its sole and absolute discretion, apply whatever criteria it deems appropriate in the selection of bidder, not limited to those selection criteria set out in this document. The issuance of document is merely an invitation to offer and must not be construed as any agreement or work order or arrangement nor would it be construed as material for any investigation or review to be carried out by a Recipient. The Recipient unconditionally acknowledges by submitting its response to this document that it has not relied on any idea, information, statement, representation, or warranty given in this document.

1.13 Errors and Omissions

Each Recipient should notify the Company of any error, omission, or discrepancy found in this document. Notification should be made to the address found in proposal related details.

1.14 Acceptance of Terms

The purpose of the RFP is to provide necessary information to the potential Bidders who qualify and intend to submit their response to the RFP. Although the RFP has been prepared with sufficient care and diligence with an endeavour to provide all required information to the potential Bidders, Company acknowledges the fact that the potential Bidders may require more information than what has been provided in the RFP. Accordingly, in such cases, the potential Bidder(s) may seek additional information/clarification required from Company. Company reserves the right to provide such additional information/ clarification at its sole discretion. In order to respond to the RFP, if required, and with the prior permission of Company, each Bidder may conduct their own study and analysis, as may be necessary, at their own cost and expense ensuring they adhere to the timelines mentioned in the RFP. No additional time will be provided to Bidders to undertake any analysis or study.

Company makes no representation or warranty and shall incur no liability, whatsoever, under any law, statute, rules or regulations on any claim the potential Bidder may make in case of failure to understand the requirement and respond to the RFP.

Company may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information given in the RFP and specify additional user requirements or cancel the RFP at any time without assigning any reason thereof and without any notice.

While due care has been taken in the preparation of this document, Company will not be held responsible for any inaccuracy in the information provided herein. The recipient of the RFP must apply its judgment, care and conduct its own investigation and analysis regarding any information contained in the RFP document including but not limited to the scope of work, deliverables and timelines, etc.

It is the Bidder's responsibility to:

- Properly understand and examine the RFP.
- Examine all other information available on reasonable inquiry relevant to the risks, contingencies and circumstances affecting its response.
- Satisfy itself as to the completeness, correctness and sufficiency of its response.

A recipient will, by responding to the Company's RFP document, be deemed to have accepted the terms as stated in this RFP document.

2. Scope of Work

2.1 Project Objectives

This document outlines the scope of work is to select a Service Provider for the Implementation & Management of a Consolidated and Comprehensive Security Framework (CCSF) Implementation The objective of this RFP is to identify and engage a qualified vendor to design, supply, implement, and support a CCSF solution to secure GICHFLs Users, Devices, Applications with PAN India spread.

The proposed solution must address the following objectives:

1. Evaluate and integrate secure connectivity, identity-based access, and advanced threat protection to enhance the overall security posture of the organization.
2. Ensure secure and seamless access for GICHFL or non-GICHFL users across PAN India remote locations, branch offices, on-premises / Cloud infrastructure.
3. Provide real-time unified dashboard visibility via centralized monitoring with security operations capabilities driven by advanced analytics including behaviour analysis across network, devices, users connecting to the GICHFL corporate network and automated incident response.
4. Enforce identity and policy driven access controls preventing unauthorized or non-compliant devices connecting to GICHFL corporate network. The applicability of security policies to be applied via all GICHFL enterprise networks to all devices, users accessing GICHFL resources.
5. Ensure secure operations for integrations with regulators, regulated entities or other critical networks, meeting applicable Indian telecommunications, cybersecurity and DPDP requirements.
6. Consolidated security solution with scalability, enhanced operational efficiency, and compliance with industry regulations and best practices.

Bidders are requested to submit commercial proposal considering above projections as per Appendix 01 – Bill of Materials. The calculation will be considered for arriving at Total Cost of Ownership (TCO) for evaluation purpose; however, the payment will solely be based on actuals.

2.2 Tenure

The tenure of the contract initially would be for Five years from the date of the issuance of first purchase order by the Company. Company can further extend this at its discretion at mutually agreed terms.

2.3 Implementation Methodology

1. The selected Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly lay out the overall steps from initiation to closure of this engagement.
2. The Security Gap Report, Technical Documentation and Project Plan would be reviewed by the company, and the selected bidder is expected to remediate all gaps identified by the Company.
3. The methodology should address all stages of implementation, customization, and Facilities Management services. Each step should provide details of data involved, flow involved and related security application. The selected Bidder should further provide the deliverables and sign off process for each of the deliverables at various stages. The selected Bidder would need to deploy team for implementation (including Project Manager) onsite (as and when required) at Company’s location (Mumbai) on full time basis.
4. The selected Bidder must ensure that these resources are on the project on a full-time onsite basis during the implementation phase.

2.4 Security Gap Report

1. The selected bidder shall conduct a detailed study of GICHFLs existing security implementations at GICHFL and provide a Security Gap Report. The report shall also recommend alternatives or solutions for the identified security gap. The report shall also serve purpose to reconcile the RFP requirements and redefine the scope and cost, as mentioned in section 1.2.

2.5 Technical Documentation and Project Plan

1. The selected bidder shall prepare a detailed security gap report and provide alternatives and/or recommendations as Security requirements for implementations.
2. The selected bidder shall prepare a detailed technical document describing each security feature planned to be implemented in GICHFL.
3. Technical document shall include security architecture, impact analysis for security features, implementation designs, Threat modelling results, Standards and protocols followed in the implementation.
4. Technical document shall include the implementation impact on business processes or workflows.
5. Technical document shall include detail regarding the existing configurations and controls implemented with the recommended security implementations.
6. Technical document shall include list of software components, tools including Open-source libraries required.
7. Technical document shall include details of testing requirements needed to have identified security implemented and tested.
8. Technical document shall include details of logs capturing like scope, configurations, and criteria for logs capture. Also details of monitoring setup of the logs captured.
9. Technical document shall include detailed instructions for process of patch management.
10. Technical document shall include support and maintenance schedules and details, policy details for systems and software used in security implementation.
11. Technical document shall include details of security implementation meeting all the needed list of compliances, legal and regulatory requirements.
12. The selected bidder shall prepare a detailed Implementation Plan with assigned ownership, resources required and timelines with exhaustive testing of security measures.
13. Technical document shall include details of roles and responsibilities matrix carving clear actors and actions on any event / incident.
14. Technical document shall be marked completed when signed off from the Company.

2.6 Customization

1. The selected bidder shall undertake a detailed study of current security framework and related processes implemented at GICHFL.
2. The selected bidder shall identify the current state gaps of security and related processes followed by the Company against the standards and compliances needed by legal and regulation. The selected bidder shall document the current state assessment gaps and get the same reviewed and approved by the Company.
3. The selected bidder shall ensure all legal, statutory and regulatory audit data and reports are available for the Company. No additional costs shall be considered and paid either for gaps observed and/or gaps observed for statutory or regulatory reports as required by the Company.
4. The selected bidder is expected to provide a resolution to all security gaps observed in current GICHF security framework, conduct Product Demonstrations, prepare technical implementation document detailing solutions to be implemented and respective compliance achievements, ensure robust testing of the security implementation is conducted and signed off, and applying the signed of security implementations on Production.
5. The selected bidder must carry out all the security enhancements / customizations without any additional cost to the company unless any new software or tool procurement is required.
6. The selected bidder must provide detailed documentation for enhanced / customized security solutions, features, configurations, audit and logs details and training for the same to security admins / analysts.
7. Additional enhancements / customization beyond the RFP requirements: The Company may require the selected bidder to address additional requirements that are none of the following:
    - Bug fixes
    - Gaps found in current GICHFL security framework.
    - Gaps against the CCSF requirements mentioned in sections 2.9 to 2.12.
8. Any additional requirements over and above RFP requirements will be discussed, and respective cost and efforts phase wise role out will be based on severity and criticality of security.
9. The selected bidder will have to ensure that the software provided as part of the solution meets all the requirements described in detail in the CCSF requirements section and to carry

out all enhancements / customizations to meet mentioned RFP requirements at no additional license charge/fees/expenses.

10. The selected bidder shall provide all the dashboards and MIS reports as per the CCFS requirements mentioned in the RFP and those required as per Regulatory Audit and Compliance. It is preferable that the selected bidder provides a report generation tool and train the Company personnel to create and fetch reports for quick reference or reporting purpose.
11. The selected bidder shall document and submit to the Company all the testing activities, procedures and results. The selected bidder is required to ensure that the software / tools implemented as part of security framework, provides API interfaces to integrate with various systems in the Company, at no additional cost or fees or charges or expenses.
12. The selected bidder shall provide the Company with daily automated reports on the incidents and actions with relevant date and details for Company to learn regarding the same. Frequency and audience of such reports shall be discussed during implementation.
13. Enhancements / Customizations will be both with respect to the security software / tools and respective interfaces that the Company proposes to implement through the selected bidder.
14. Security log (Historical as well on going) shall be retained for 1 year on rotation basis. User access related data except PII shall be retained for 1 year. User PII data cannot be stored and has to be deleted after intended use. The security log data and user access related data must be available to users and administrators as per the agreed user access definition.

2.7 Gap Identification & Resolution

1. The selected bidder must provide all functionalities as mentioned in the below Requirements & provide all functionalities as mentioned in the CCFS requirements.
2. The selected bidder will provide Company with gap identification report along with the necessary solutions to overcome the gaps along with timeline to implement.
3. The selected bidder will ensure that all issues identified at the time of security gap implementations will be immediately resolved.
4. The selected bidder will ensure that gaps pointed out by the audit and inspection teams, statutory and regulatory bodies, or any other third-party agency engaged by the Company will be immediately resolved.

5. The selected bidder shall resolve gaps by proposing a suitable temporary work around or customizing the proposed solution by way of modifications / enhancements, as necessary, to the proposed software solution.
6. The selected bidder will give adequate time to Company for reviewing the gap report.
7. The selected bidder will incorporate all suggestions made by Company to gap report.
8. The selected bidder will ensure that they have the necessary infrastructure and people in place to resolve all the gaps within the timelines agreed, for the implementation and roll out.
9. The cost of all customizations as mentioned above is required to be included in the price bid and the Company will not make any additional costs for such effort till all the Offices are live. While costing the customization effort required, the selected bidder should exclude the effort required from the Company. The selected bidder will understand the priorities/ implications and accordingly plan the gap remediation.
10. The selected bidder is expected to document all gaps observed by the Company at various stages of implementation including their solution and monitor and track the status of the same throughout the implementation.

2.8 Minimum Eligibility Criteria

Sr.	Specific Requirement	Documents Required	Response with supporting document details
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 2008or 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 a copy of PAN card and GST Registration certificate	
3.	The Bidder must have minimum 5 years of experience of Implementing Consolidated and Comprehensive Security Solutions and related support services for a period of at least 3 years as on today, for at least 3 Customers preferably Housing Finance or NBFC Domain.	Anyone of the following documents: a) Work/ Purchase Orders confirming year and area of activity with Self-certification from bidder that supplies/ projects against orders have been executed. b) Execution certificate by client with order value. c) Any other document in support of order execution like Third Party Inspection release note, etc.	
4.	The Bidder should have had an average annual turnover of Rs. 50 Crores in the last 3 Financial Years.	Copy of the Audited Balance sheet for the last 3 financial years 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	

5	The Bidder should have made profit in at least 2 of the last 3 audited financial years.	Audited annual accounts or an 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 bidder.	
6	OEM Proof / Certification:	The bidder must provide proof of being a Solution OEM. The Managed Service Partner should provide association proof (MAF or similar)	
7	Presence: The Bidder should have registered office and/or significance presence in India through franchises / branches / service centers with Support Engineers team to cater to PAN India service requests.	Self-Declaration from competent authority must be submitted by the bidder.	
8	The Bidder must not have been blacklisted by any department or institution or undertaking of the Government of India and 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.	
10	The bidder must provide certificate obtained under MTCTE (Mandatory Testing and Certification of Telecom Equipment) scheme.	Copy of certificate with Company stamp and Authorized signatory on it.	
11	The bidder must provide Common Criteria Certificate under IC3S.	Copy of certificate with Company stamp and Authorized signatory on it.	
12	The bidder should provide proof of being ISO 9001:2015 or latest or Similar compliance for Quality Management process adherence in their company.	Copy of certificate with Company stamp and Authorized signatory on it.	
13	The bidder should provide proof of BIS Registration under Compulsory Registration Scheme for Product safety and quality.	Copy of certificate with Company stamp and Authorized signatory on it.	
14	The bidder should provide WPC type approval or ETA (Equipment Type Approval) for using de-licensed frequency bands.	Copy of approval with Company stamp and Authorized signatory on it.	

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.

2.9 Consolidate and Comprehensive Security Framework Requirements

1. Current Security Landscape

GICHFLs current security infrastructure of SDWAN Firewall with Unified Threat Protection features, Secured VPN, M365 Enterprise Zero Trust Framework, Device MDM/MAM, Data Labelling and Email DLP, Endpoint security, Cloud security on Azure. More details can be shared with selected bidder.

2. Scope of Work

The selected bidder shall be responsible for delivering a CCSF framework and security solutions. Below 2 sections mention scope of expected functionalities and features which the selected bidder shall work for implementing.

a. Security Functions

The expected scope of security functions for selected bidder shall include, but not be limited to, the following**:**

The selected bidder,

Scope	Yes / No	Comments
Evaluation and Roadmap		
Shall conduct a detailed assessment of the GICHFLs existing Infrastructure, network and security framework, and access management framework.		
Shall design an end-to-end security framework to secure GICHFLs network, users, devices and applications which aligns with GICHFL’s consolidated and comprehensive security requirements and industry best practices.		
Shall prepare a detailed implementation roadmap, including timelines, dependencies, and resource requirements.		
Security Framework Implementation		
Shall be responsible for supplying, configuring, and implementing the hardware, software and licenses required for proposed consolidated comprehensive security solutions to secure GICHFL / non-GICHFL network connectivity, identity-based access, and centralized policy enforcement.		
Shall provide with an effective migration plan with zero disruptions to the existing business operations.		
Shall install and configure all components across all specified		

GICHFL sites, including data centers, branch offices, with on premise and/or remote networks, devices and users.		
Shall integrate with GICHFLs existing network and security infrastructure which may include current Identity and Access management implementation as well.		
Shall integrate the security solution with GICHFLs current security infrastructure.		
Shall ensure that the implemented solution is extendable and compatible with all the off-the-shelf SIEM solutions available in India, to integrate for on-premises, cloud, and hybrid environments.		
Shall ensure extensive testing of the implementation and commissioning of the new security framework.		
Security and Access Controls		
Shall implement centrally managed policies for network, devices and user access authentication, authorization, and compliance validations.		
Shall implement centrally controlled restrictions enforcing mechanisms to identify unauthorized, unmanaged, or non-compliant devices and users.		
Shall configure provisioning of secure access for remote, mobile, and third-party users as per GICHFL organizational requirements.		
Shall ensure solutions have advanced analytics-based anomaly detection and proactive threat identification.		
Shall ensure capabilities of threat detection, triage, investigation, automated response following approved play book driven actions complying local compliance for data residency, high availability, scalability.		
Shall configure and implement Case Management, IOC enrichment, threat actor profiling, feed ingestion, log normalization, correlation, MITRE Attack mapping Or CVE mapping, detection of privilege misuse, dynamic risk scoring.		
Visibility, Monitoring, and Reporting		
Shall provide centralized dashboards for real-time monitoring of GICHFL devices, users, and network activities by collecting native logs of all GICHFL IT resources.		
Shall provide implementations with advanced analytics including behavior analysis and automated incident response capabilities, with compatibility of integration with GICHFL network logs, application logs, IT infrastructure (Cloud, On premise), EDR, Threat Intelligence, telemetry and key infrastructure.		
Shall ensure comprehensive logging and audit trails for compliance and governance requirements.		
Shall ensure Governance by providing visibility of regulatory controls, operational metrics and detection trends.		

Training and Knowledge Transfer		
Shall provide with detailed training programs for implemented features, configurations, monitoring and controlling capabilities along with respective detailed technical documentation for GICHFL Administrators and Security teams.		
Shall ensure effective knowledge transfer to GICHFL personnel for independent management of the solution post-implementation.		
Shall provide documentations materials for the knowledge transfer conducted.		
Support and Maintenance		
Shall align appropriate and agreed SLA based technical support, including incident response, troubleshooting, and resolution for the contracted tenure.		
Shall be responsible for supply and timely updates, execution of security patches, and feature upgrades.		
Shall ensure agreed SLAs are met for system availability, reliability, and performance, and provide for regular service review meeting and reports.		

Table 1 (Scope of Functions)

b. Security Features

Below is list of security features for expected security requirements implementations at GICHFL over current understanding of the GICHFL IT & IS Team. The selected bidder shall perform GAP Assessment of current security landscape and propose for implementations that may be considered from any or all amongst the below list of features. The selected bidder must have extensive experience of all aspects of the implementation technicalities and support services of features as mentioned in below Table 2.

Sr.	Category	Requirement	Yes / No / Partial	Comments
1.	SASE	Zero Trust Network Access (ZTNA)		
2.	SASE	Secure Web Gateway (SWG)		
3.	SASE	Cloud Access Security Broker (CASB)		
4.	SASE	Web Application Firewall (WAF)		
5.	SASE	Data Loss Prevention (DLP on User device, Cloud and Network)		
6.	SASE	Identity and Control Mechanism (IAM, PIM, PAM)		
7.	SASE	Firewall as a Service (FWaaS)		
8.	SASE	Secured Scalability for Cloud and On-		

		premises both		
9.	NAC	Identity and Role-based device posture assessment and authentication (corporate & BYOD, laptops and hand-held devices)		
10.	NAC	Endpoint compliance checks (OS patch, AV, encryption)		
11.	NAC	Guest user access management		
12.	NAC	Device visibility (IoT, endpoints, BYOD, laptops and hand-held devices)		
13.	NAC	Integration with AD / Identity Providers		
14.	NAC	Policy enforcement with automated remediation		
15.	SIEM	Security Information and Event Management with Security Orchestration Automation and Response capabilities		
15.	Services	Solution design, deployment & configuration		
16.	Services	Integrations with GICHFLs current infrastructure and security implementations		
17.	Services	Training & knowledge transfer for GICHFL IT & IS team		

Table 2 (Scope of Features)

2.10 Functional Requirements

Below is list of expected functional security requirements that selected bidder shall implement to close the possible security gaps once identified. The list is expected functionality to be implemented and may require revision to meet the actual security gaps identified by the selected bidder. Likewise, the cost and timeline also may require revision once the actual security functional requirements are evaluated after the security gap assessment exercise.

Sr.	Requirements	Yes / No / Partial	Comments
1	Ability to configure ‘No Access’ by default for GICHFL users or external third-party vendor users. Any user or device access must be verified before giving access to GICHFL network and resources.		
2	Ability for segmentation of resource/application		

	specific access for any user or device and restricting access to whole corporate network and resources.		
3	GICHFL currently uses VPN to provide access to its network, data and resources when users or devices are connecting via non-corporate network. Ability to provide seamless, scalable, better performing and secure access provisioning is available.		
4	Ability to configure least access rights for all the internal/external users to enable permitted actions on the resources/applications assigned.		
5	Ability of continuous identity and device posture assessment to check compliance and security of GICHFLs IT landscape.		
6	Any user or device is continuously validated and granted access to only resources configured for it.		
7	Ability to extend the security policies to provide secure and least access grants to corporate resources/applications for user requests from non-corporate networks.		
8	Ability to apply consistent as well as variable security policies across GICHFL infrastructure like Cloud, On-premises, hybrid, or even containerized in future.		
9	Ability to configure various authentication / authorization methods for controlling various levels of access rights requested for corporate network, data, storage, applications or any other resources.		
10	Ability to prevent threats from malware, ransomware attack by minimizing the surface area by applying stringent security policies.		
11	Ability to provide tools for configuring user authentication/authorization, resources access and rights and maintain and provide audit logs for the same.		
12	Ability to configure capabilities for identifying excess permissions or conflicting permissions for preventing fraudulent user activities.		
13	Ability to configure and provide capabilities of centralized authentication and authorization mechanism for ensuring single trusted identity provisioning and simplification of user administration.		
14	Ability to log all activities happening on GICHFL network and resources and raise alerts for security threats.		
15	Real-time scanning of URL reputation, web traffic and downloads for detection and blocking of malicious attacks.		
16	Ability to apply security policies on managed and unmanaged devices and networks for protecting corporate devices, data network and infrastructure.		
17	Ability to analyse threats and attacks in a secluded and		

	safe environment to guard GICHFL network against any unidentified threats whether GICHFL managed and unmanaged network.		
18	Ability to prioritize web traffic to certain sites that are business critical ensuring maximum productive usage of GICHFL network.		
19	Ability to apply web access and usage policies to restrict site access to improve traffic and bandwidth productivity.		
20	Ability to configure and enforce web security policies on all devices including unmanaged devices.		
21	Ability to scan, classify, inspect and prevent PII data, Accounts related data and sensitive data, either at rest or in motion, from leakages through accidental or malicious exfiltration or unauthorized sharing, even if it is happening through allowed corporate web applications or mobile applications, web sites or thick clients.		
22	Ability to scan, monitor and control data transfers from corporate devices to data storage devices like USB drives, Hard disk drives etc. and block sensitive data transfers.		
23	Ability to scan and control data transfers from unmanaged devices (BYOD, laptops and hand-held devices) and block sensitive data downloads, printouts or uploads to unknown sites or cloud storage on the same.		
24	Ability to scan and detect uncommon user activities like uploading, downloading or printing sensitive data or large volume data to unknown site or source.		
25	Ability to configure data template matching techniques like data patterns or keywords or fingerprinting to identify sensitive data in the content being transferred and block the same.		
26	Ability of configuration and granting application specific and action specific accesses on application to users.		
27	Ability to highlight security risks on use of ‘not allowed’/ ‘unapproved’ web sites/applications for proactively identifying potential security risks and blocking the same.		
28	Ability to decrypt the encrypted web traffics to identify potential security risks.		
29	Ability to provide audit logs for configurations updates at administrative level and activity logs at each user, device level.		
30	Ability to provide reports and analytics on access, traffic and activity based productive details.		
31	Alignment with Indian government regulations and		

	compliance requirements such as GDPR, CCPA, PCI-DSS, DPDP and likewise.		
33	Ability to mitigate DoS and DDoS attacks on GICHFLs allowed / approved web sites/applications/mobile apps.		
34	Ability of analysing traffic patterns to distinguish between legitimate users and malicious bots.		
35	Ability of seamless working integrations with network firewalls, intrusion prevention system and SIEM system (if any in future).		
38	Ability to perform continuous posture assessments for continuously changing GICHFL Cloud services and resources utilized.		
39	Ability to configure and implement granular securities for Cloud services and resources.		
40	Ability to provide a centralized capability to collect all cloud resources logs, view, analyse, raise alerts and provide remediations for the security threats / gaps identified from the logs of all the GICHFL cloud resources and services.		
41	Ability to auto-apply encryption to all the GICHFL data at rest and in-transit in and out of GICHFL Cloud environment / network.		
42	Ability to integrate user identity-based authentication and authorization tool with GICHFLs endpoint management system.		
43	Ability to provide centralized solution for network access lifecycle management for unmanaged devices connecting to GICHFL non-corporate network segment.		
44	Ability to perform security posture assessment of the unmanaged devices connecting to GICHFL network segment and prohibit threat access into GICHFL non-corporate network segment.		
45	Ability of centralized solution for visibility and monitoring of all GICHFLs managed resources over GICHFL's managed or unmanaged network and unmanaged resources over GICHFLs managed network.		
46	Ability of integrating with GICHFLs AD and Cloud AD capabilities.		
47	Policy enforcement with automated remediation – Ability of automated posture assessment and policy enforcement on managed and unmanaged devices in GICHFL managed network.		
48	Ability of automated remediation of security threats identified in the posture assessment of managed and unmanaged devices in GICHFL managed network.		
51	Shall perform security and policy assessments to identify and perform requirements reconciliation as stated in this SOW. Purpose is to identify existing		

	security implementations, their adequacy and opportunity of new security features implementation, also to identify opportunities to optimize implementation cost.		
52	Shall design and deliver security solution architecture as identified in Sr No. 51, for improving security landscape with optimized cost.		
53	Shall provide a timeline project plan for configuration and deliveries for completing the Pilot implementation at few GICHF sites and then expand across PAN India in phased manner.		
54	Shall perform seem-less integration with existing GICHFL infrastructure and security features (like firewalls, VPN, AD, Cloud, on-premises servers)		
55	Shall provide complete training to GICHFL Admins and Infosec team regarding the configurations and centralized management capabilities.		
56	Shall provide and maintain complete documentation of the implementation, configurations and centralized capabilities delivered for monitoring and managing the Consolidated Security Framework Solution at GICHFL.		
57	Shall provide 1 L2 support person stationed at GICHFL site starting from implementation stage and for AMC tenure of 5 years.		
58	Experienced in implementation of above-mentioned security features in at least 3 Indian NBFCs. Provide references.		

Table 3 (Functional Requirements)

2.11 Compliance, Governance and Integrations Requirements

The selected bidder shall provide all means, tools and support required for monitoring and managing compliance, governance and integration requirements of the CCFS (SASE and NAC) implementation. Below table lists the expected diligence, compliance and governance activities that GICHFL IT, IS, SOC / NOC, Compliance, Audit and Risk Teams should be able to use and perform their respective due diligence. This exhaustive list may have revisions while implementation based on revised guidelines and/or security gap assessment during implementation.

Note – As per the requirements below, please mark the functionality as Available (A), Customizable (C), To be Developed (D), or Not Possible (N). All the points marked as

Customizable (C) and To be Developed (D) are to be made available before Go-Live within the time frame stipulated in the RFP.

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
Regulatory and Governance Compliance			
Regulatory Alignment	Ensure all SASE and NAC policies adhere to regulations such as HIPAA, GDPR, PCI DSS, etc.		
Data Protection and Privacy	Implement and monitor consistent DLP controls and encryption measures to safeguard sensitive data on managed and unmanaged setup (network or devices).		
Identity Verification and MFA	Enforce strong, identity-based authentication mechanisms (MFA) to ensure only verified users access data.		
Documentation	Maintain detailed documentation of all security policies, procedures, and configurations for audit purposes.		
Access Control Enforcement	Provide management and verification of Role Based Access Control and micro-segmentations isolating sensitive data environments for correctness with audit capability.		
Risk Management	Continuous assessment and management of security risks associated with network access and data handling.		
Defining Ownership and Responsibility	Define users, roles, accesses, assignments and responsibilities for various aspects of the SASE and NAC environment.		
Policy Alignment	Ensure security policies align with broader business objectives and risk tolerance.		
Performance Metrics and Reporting	Establish KPIs and regular automated reporting on the security posture and compliance status to GICHFL leadership.		
Independent Auditing	Facilitate scheduled and regular, independent third-party audits to verify		

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
	and validate the efficacy of controls implemented.		
Business Continuity Management	Incorporate SASE and NAC operations into overall business continuity and disaster recovery plan of GICHFL.		
Policy Review and Updates	Periodically reviewing and updating security and access policies to align with evolving business needs, threat landscapes, and regulatory changes.		
Policy Communication	Ensures all stakeholders and users are aware of the access control policies and their responsibilities.		
Risk Assessment and Mitigation	Regularly assess network access infrastructure for vulnerabilities and potential risks; implement mitigation strategies.		
Third-Party Vendor Risk Assessment	Evaluate the security practices and compliance certifications of SASE vendors and service providers.		
Controls Mapping	Map NAC and SASE technical controls to specific regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS, SOC 2).		
Audit Trail Generation and Retention	Ensure comprehensive, tamper-proof logs are collected, retained according to regulatory mandates, and available for audit purposes.		
Internal and External Audit Support	Provide necessary documentation, reports, and evidence to facilitate internal and external audits of access controls.		
Reporting and Remediation	Develop formal reports for management and auditors detailing compliance status, exceptions, and remediation plans for identified issues.		
Configuration Management	Maintain secure baseline configurations for all NAC appliances/controllers and SASE cloud services.		
Formal Change Process	Enforce a documented change management process for all modifications to access rules, policies, and system configurations.		

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
Role-Based Access Control (RBAC) Governance	Define and manage user roles and permissions, ensuring least privilege access is consistently enforced across on-premises and cloud resources.		
Access Recertification	Periodically review and validate that all user and system access rights remain appropriate and necessary for job functions.		
Data Governance	Establish rules for threat intelligence, logs, and user data sharing between the NAC, SASE, SIEM, and other integrated systems.		
Incident Response Plan Governance	Ensure incident response plans are tested regularly and cover scenarios involving both physical network access and SASE cloud incidents.		
Training and Awareness Governance	Oversee training programs to ensure IT staff possess the necessary skills to manage and secure the combined NAC and SASE environment effectively.		
Daily Operations and Management			
Security Operations and Management	Background verified, continuously trained and skilled personnel experienced as SOC L1, L2, Threat Hunters, Technical Account Manager with well-defined escalation matrix performing regular reporting and presentations on security posture assessment, incidents and compliance.		
Continuous Monitoring and Alerting	Real-time monitoring of all network activity and device posture to detect and respond to anomalies.		
Policy Review and Updates	Regular automated / manual management of access and security policies to address new threats and operational changes.		
Automated Posture Assessment	Regular automated compliance and management of all devices to meet security benchmarks (e.g., AV updates, patch levels).		
Incident Response and Remediation	Regular and continuous IRR activities for automated isolation of		

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
	compromised devices or users in a threat incident situation and related automated first level troubleshooting alert and reporting to the respective GICHFL stakeholders.		
User and IT Staff Training	Provide ongoing security training on secure access procedures and policy adherence.		
Authentication & Authorization	Monitor daily access logs to verify authorized users and compliant devices are accessing resources based on 'Zero Trust' principles.		
Continuous Posture Assessment	Real-time validation of device health (e.g., AV status, patch levels, secure configurations) and automatic enforcement of actions (quarantine/restriction/resolution).		
Traffic and Threat Monitoring	Track network and application traffic across all SASE and NAC points of presence (PoPs) to detect and mitigate potential threats or policy violations.		
Incident Response Triage	Investigate access-related security events, such as unauthorized access attempts, policy violations, or non-compliant endpoints.		
Policy Enforcement Verification	Daily and consistent verification and enforcement of access policies (identity-centric and context-aware) across both on-premises NAC and global SASE perimeters.		
Log Review and Analysis	Regular review of aggregate logs from NAC enforcement points and SASE components (CASB, SWG, FWaaS) for anomalies, performance issues, and potential breaches.		
Guest/BYOD Lifecycle Management	Provision, monitor, and de-provision temporary guest accesses and ensure BYOD enforcement aligns with implemented access policies at GICHFL.		
System Health & Availability Checks	Ensure all NAC appliances/controllers and SASE services (cloud gateways, PoPs) are operational, highly available,		

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
	and performing within expected metrics implemented at GICHFL.		
Integrations			
Identity Providers	Enable single sign-on (SSO), sync user identities and group memberships, and enforce conditional access policies based on identity and context setup at GICHFL.		
Multi-Factor Authentication	Enforce strong authentication for all access requests (on-premises and remote), adding a critical layer of verification.		
Endpoint Protection	NAC: Perform real-time device posture checks (AV status, patch levels, installed software). SASE: Use device context to permit or deny access to cloud resources.		
Network Hardware (Switches, WAPs, Firewalls)	NAC: Dynamically assign VLANs/ACLs or quarantine non-compliant devices at the port level. SASE: Ensure firewalls are configured to accept traffic from SASE gateways.		
Security and Event Logs Monitoring	Save and provide all security and event logs for centralized dashboard visibility and actions, correlation of events, and long-term retention for compliance.		
Automated Incident Response	Provide with automated incident response workflows, such as automatic quarantine or isolation of a compromised endpoint or blocking a malicious IP address detected by SASE.		
Cloud Service Provider APIs (Azure, M365)	SASE (CASB/DLP): Monitor data at rest within sanctioned SaaS apps, detect misconfigurations, and enforce data loss prevention policies via API.		
IAM Lifecycle via HRMS (SAP)	Automate user provisioning and de-provisioning workflows (joiners/transfers/leavers) to ensure access is immediately granted or revoked.		

Activities	Description	Available (A)/Customizable (C)/To be Developed (D)/ Not Possible (N)	Remarks
ITSM / Ticketing Systems	Automatically generate incident tickets for non-compliant devices, access policy violations, or system health alerts.		
Threat Intelligence Platforms	Ingest external threat data to proactively block known malicious IPs, domains, and files across all SASE security functions.		
Configuration Management Database (CMDB)	Populate the CMDB with details of managed devices and access policies to maintain an accurate inventory and streamline change and patch management processes.		

2.12 Technical Requirements

GICHFL will award the contract to the successful Bidder who has and shall showcase proven industry experience of NAC and SASE security implementations for Housing Finance in Banks or NBFCs. Following is the technical SOW the selected bidder should service GICHFL with:

Experienced in implementation of above-mentioned security features in at least 3 Indian NBFCs. Provide references.

1. The selected bidder shall perform security and policy assessments to identify and perform requirements reconciliation as stated in the functional and technical requirements.
2. The selected bidder shall identify existing security implementations, their adequacy and opportunity of new security features implementation.
3. The selected bidder shall identify opportunities to optimize cost of security implementations and related future maintenance, operations, support and services.
4. The selected bidder shall perform thorough security gap assessment.

5. The selected bidder shall analyse current security implementations at GICHFL and recommend an implementations roadmap for identified missing security functions at GICHFL measuring applicability and cost optimizations.
6. The selected bidder shall design and deliver security solution architecture as identified in security assessment for improving security landscape with optimized cost.
7. The selected bidder shall provide a timeline project plan for configuration and deliveries for completing the Pilot implementation at few GICHF sites and then expand across PAN India in phased manner.
8. The selected bidder shall provide and perform all required security solutions / software / tools / dashboards / services / third party utilities installation, configuration, integration, providing requisite interfaces, migration (if any), implementation, testing, training, liaising with GICHFLs existing vendors, management, maintenance and support.
9. The selected bidder shall perform seem-less integration with existing current GICHFL infrastructure and security features.
10. The selected bidder shall provide and maintain complete technical documentation of the implementation, configurations and centralized capabilities delivered for monitoring and managing the CFSS at GICHFL.
11. The selected bidder shall provide complete training to GICHFL Admins and Infosec team regarding the configurations and centralized management capabilities.
12. By means of diagrammatic / pictorial representations, the selected bidder should provide complete details of the software and network architecture of the security solution implemented; including the project plan for go live. The selected bidder also provides security setup proposed in the solution and various layer of risk identification and mitigation measures.
13. The selected bidder shall provide technical security operations support and services for a period of five years (including implementation, Warranty and AMC & ATS).
14. Shall provide one L2 person stationed at GICHFL starting from implementation stage and for AMC tenure of 5 years.
15. In case of incident emergency or if necessity arises, the selected bidder should arrange required security engineers on holidays and beyond working hours as well, if required, station at GICHFL. The extension after 5 years shall be subject to mutual

agreement between the bidder and the company.

16. The selected bidder shall provide On-Site maintenance of the solutions and related products with configuration management, reports customization as desired by regulatory compliance. Performance tuning of all involved solutions, software tools and databases, necessary and adequate patches for all solutions, databases and system, upgrades, utilities, tools etc. after successful Go Live of the security solution for GICHFL, inclusive of providing support for day to day functional and technical support to GICHFL team.
17. L2 resource stationed at GICHFL shall have effective technical and communication skills to pro-actively monitor the down calls of solution and ensure that calls are closed in time and submit the monthly/quarterly down call reports to GICHFL for calculation of SLA. Ticketing system to be used to lodge and track the service calls.
18. The selected bidder shall provide the complete documentation including technical, operations, like license, user manuals, training manual, technical manual, standard operating procedure, solution architecture and design, system flow document, data dictionary and other necessary documents etc.
19. The selected bidder shall provide System Infrastructure Requirements document for the Hardware and Software (OS/Application) required for Implementation. Also, requirements of implementation on DC and DR at GICHFL, integrating the product with other systems in GICHFL DC and DR both, during first implementation and subsequent upgrades as well. This applies to any product upgrades impacting DC and DR, selected bidder shall support and ensure security solutions and its integration to be successfully up and running in both DC and DR. This activity should be covered as part of AMC.
20. The selected bidder shall provide upgrades / patches related to CERT-IN or Regulatory guidelines or any CVE providers that intimates regarding security caution alerts or directives which may also result in any additional customizations related to Regulatory compliance, must be provided as a part of AMC without any extra cost.
21. The support service shall be provided on 24x7x365 basis for ensuring proper upkeep and maintenance of the solution.
22. The Solution should be implemented in higher security standards like Virtualization, Segregation of Servers, and compartmentalization. Secured Coding

Practices, OWASP etc. to ensure 100% security of the Solutions implemented. The selected bidder shall provide Security Certificate for the products implemented to comply with RBI/IRDA/NHB security directions and guidelines.

23. The selected bidder shall provide at least once a year VA-PT certificate, security certificate, code review certificate for the security solutions or products with no open observations critical to the security of GICHFL data and IT environment.
24. Any version changes / upgradation of the software's involved should be implemented by the selected bidder for the GICHFL free of cost during contract AMC period.
25. Validation of models, processes and maintenance of application software, system software, database, any other related interfaces and as required by the GICHFL (existing or proposed) etc.
26. The selected bidder shall train designated GICHFL officials on the administration, configuration, operations / functionalities, maintenance, support & administration for involved software, Databases, OS / Middleware, application architecture and components, installation, troubleshooting processes of the proposed solution.
27. The selected bidder shall provide all-hands onsite support for current security implementations events and logs collection and data migration to its dashboard tools. The selected bidder shall provide and execute the validation checklist to ensure that migration of such data is successful for end-to-end security systems functioning at GICHFL.
28. The selected bidder shall provide post Implementation support.
29. Post Go-Live, GICHFL and selected bidder shall execute an Escrow agreement for the security solutions software source code with the purpose of maintaining and ensuring the Configuration version sanctity of the source that is deployed at GICHFL and remains untouched unless specific modifications are requested and approved by GICHFL. Every upgrade on GICHFL version of the solutions will be secured with the Escrow provider.
30. The solution / software involved if any, developed or customized should follow a standard development process to ensure that it meets functional, security, performance, scalability & regulatory requirements of GICHFL.

Please respond to below list of Requirements with a Y (Yes), if you agree of and shall perform expected responsibility of the stated requirement ELSE with a N (No) if you are not in Agreement, with remarks.

S. No.	Requirements	Agree (Y/N)	Remarks
1	The selected vendor should implement and host the proposed security solution at GICHFLs on-cloud (GICHFL) / on-premises in High Availability mode, along with DR and a minimum uptime time of 99.50 %.		
2	Architecture should have the ability to increase the number of concurrent instances to keep the proposed security solutions, involved servers and databases server utilization parameters such as CPU/GPU, RAM, Virtual Memory / Paging, Storage space occupied, well below 70% of total allocation based on request load and scalability settings.		
3	Before deploying proposed security solutions, selected bidder shall ensure that the underlying GICHFL network supports advanced access control mechanisms.		
4	The selected bidder shall define network segments (VLANs, VRFs) for different trust levels (e.g., Corp, Guest, IoT, Quarantine) as may be discussed and confirmed after conducting assessment of GICHFLs current security landscape.		
5	The selected bidder shall ensure that proposed security solutions work with all GICHFL access layer switches and wireless access points (WAPs), supports 802.1X and can integrate with Authentication Authorization and Accounting (AAA) servers and related protocols at GICHFL to enforce port/user-level access control.		
6	The selected bidder shall ensure that proposed security solutions are compatible with 802.1X.		
7	The proposed security solution must integrate with Authentication Authorization and Accounting (AAA) servers and related protocols at GICHFL to enforce port/user-level access control.		
8	The proposed security solution must maintain accurate IP address management to profile and track devices effectively as they connect.		
9	The proposed security solution must verify the internet uplinks at all GICHFL locations and can handle the shift of traffic inspection to cloud-based SASE services without degradation.		

S. No.	Requirements	Agree (Y/N)	Remarks
10	The selected bidder shall focus on NAC deployment to have granular control and visibility at the physical network edge.		
11	The proposed security solution shall provide capabilities of automatic device discovery.		
12	The selected bidder should ensure that proposed and implemented security solutions must classify all connected devices like laptops, printers, CCTV cameras, biometrics, UPS with SNMPs, or any other device connecting to GICHFL network, based on various attributes such as MAC OUI, NMAP scans, DHCP fingerprints.		
13	The selected bidder shall configure AAA services on the NAC to handle authentication requests from managed or unmanaged networks trying to connect to GICHFL resources.		
14	The proposed security solution shall integrate with the GICHFLs primary Identity Provider (IdP) using protocols like LDAP, Secure LDAP or SAML to verify user identities and roles.		
15	The proposed security solution implementation takes care of deploying the endpoint agents (if agent-based NAC) or use agentless methods to evaluate the security posture and health of connecting devices like OS version, patch level, running antivirus, local firewall status, etc.		
16	The proposed security solution shall provide to configure dynamic access control lists (ACLs) or VLAN steering to grant appropriate access based on compliance status.		
17	The proposed security solution shall provide to implement an automated quarantine mechanism that places non-compliant devices into a restricted network segment and provides clear remediations through its L2 resource stationed at GICHFL.		
18	The proposed security solution shall provide to configure ZTNA connectors or agents on endpoints to establish secure, encrypted micro-tunnels only to specific, authorized applications, not the entire internal network.		
19	The proposed security solution shall provide to define access policies based on identity, device posture, location, and application sensitivity ("never trust, always verify").		
20	The proposed security solution shall provide routing to all internet-bound traffic through the SASE PoPs for inspection.		
21	The proposed security solution shall provide configuration of URL filtering.		

S. No.	Requirements	Agree (Y/N)	Remarks
22	The proposed security solution shall provide content inspection.		
23	The proposed security solution shall provide SSL decryption (with proper certificate management).		
24	The proposed security solution should provide threat prevention (IPS/IDS).		
25	The proposed security solution shall provide configuring and managing application control policies.		
26	The proposed security solution shall provide to integrate the CASB via APIs with sanctioned SaaS applications (e.g., M365 and others at GICHFL) to monitor data at rest and detect security configuration drift.		
27	The proposed security solution shall provide to implement unified DLP rules that apply consistently across all traffic channels (web, email, SaaS applications).		
28	The proposed security solution shall provide to manage synergy between NAC and SASE consolidated an comprehensive security posture management.		
29	The proposed security solution shall provide establishing a central management console to manage consolidated and comprehensive policies across both on-premises access (NAC) and cloud access (SASE), ensuring consistency.		
30	The proposed security solution shall provide leveraging SAML / SCIM protocols for synchronizing identity and group data from the GICHFLs IdP across both solutions.		
31	The proposed security solution shall provide to ensure that the NAC shares device posture and compliance status with the SASE controller, and vice versa, so that a compromised device detected by one system is instantly restricted by the other.		
32	The proposed security solution shall provide configuring comprehensive logs forwarding (Syslog, CEF, etc.) from all NAC appliances and SASE cloud components to the implemented dashboarding tool for monitoring, analysis, and automated response capabilities.		
33	The proposed security solution shall support SSO (Single Sign On) with Microsoft AD Authentication. The product should integrate with the core business systems (LMS-LCS, LOS, SAP FICO Accounts, Datawarehouse / data lake / MIS) and able to pull/push data from/to the interfaces.		

S. No.	Requirements	Agree (Y/N)	Remarks
34	The proposed security solution should be platform agnostic and responsive – not dependent on a particular hardware or OS setup.		
35	The proposed security solution should be capable of, and be offered in, a manner that includes installation package, either as a single instance or multi-instance, depending on GICHFLs requirements.		
36	The proposed security solution shall support real time DC to DR setup and sync and Rollover from DR to DC.		
37	The proposed security solution should support database and OS level clustering.		
38	The proposed security solutions client / dashboard views should be thin and light weight, easily accessible with low bandwidth availability.		
39	The selected vendor shall deploy the proposed security solutions in Production, DR, Training and/or Development / UAT environments, all environments that are applicable.		
40	The proposed security solution shall cater to jurisdictions as per the Local Regulations as well as Client needs, based on GICHFs Office location.		
41	The proposed security solution should offer maximum flexibility in Administration and management for all the modules while making available all the required user control tools at the hands of the GICHFL users. The solution should support super administration for GICHFL business as well as local administrators and user controls at Head/ Regional / branch level.		
42	The selected bidder should provide necessary changes to logs / dashboards for meeting the regulatory / statutory guidelines / requirement as part of AMC.		
43	The selected bidder shall execute proactive monitoring and capacity planning well in advance at regular intervals and advise GICHFL on software/hardware upgrades.		
44	The selected bidder shall plan and provide with adequate staging procedures for supporting staging and availability of proposed software systems 24*7*365 for SIT, UAT and data migration.		
45	The selected bidder shall maintain integrity of GICHFL data 100% of time during the engagement tenure.		

S. No.	Requirements	Agree (Y/N)	Remarks
46	The proposed security solution, software, and system should adhere to DPDP law to protect PII data at rest and in transit. Any API communications must be on secure encrypted channel.		
47	The proposed security solution, software, and system shall comply with the IT Security Policy, Cyber Security Policy and IT Policy of GICHFL.		
48	The selected bidder shall create adequate controls ensuring that, when exceptional or abnormal conditions occur, do not allow users to bypass security checks or obtain access to any network / system. The solution shall have robust exception management and logging for RCA analysis.		
49	The proposed security solution, software, and system must provide comprehensive audit trail and audit logs features that should also be available on the dashboarding tool monitoring activity of all users / programs / functions / processes / data files etc. and as per GICHFLs Policy and / or requirements. Audit logs should contain logs for all users including admin users.		
50	The proposed security solution, software, and system must provide enabling of segregation of duties (e.g. segregated function between system and application administration). Multi-level administrators, i.e. system, functional, etc with modular approach of every kind.		
51	The proposed security solution, software, and system should have the ability to define or use groups so that access can be categorized.		
52	The proposed security solution, software, and system are required to be fully integrated and responsive for device agnostic usability.		
53	The proposed security solution, system and software should provide support to standard messaging protocols for interfacing.		
54	The proposed security solution, software, and system interface should be able to handle exceptions (e.g. should be able to output to log files, retries) when unsuccessful. System should be able to handle continual processing or gracefully terminate.		
55	The selected bidder shall provide performance / load threshold testing evidence / reports.		

S. No.	Requirements	Agree (Y/N)	Remarks
56	The proposed security solution, software, and system shall provide the store-and-forward mechanism in case of a communication breakdown.		
57	The proposed security solution, software, and system shall log all the events and activities and report the same on the dashboard tool.		
58	The proposed security solution, software, and system to provide session log files. These logs shall be utilized for information needed to process forensic analysis, incident response, anomaly checks, runtime detection and quarantine, and so on.		
59	The proposed security solution, software, and system to provide tracking of the client's IP & Network Interface address.		
60	The proposed security solution, software, and system to provide for integration with MIS systems for generating reports additional to Standard and regulatory reports.		
61	The proposed security solution, software, and system should be Platform independent with respect to OS, third party tools etc.		
62	The proposed security solution, software, and system should be able Incident Management system, Risk Management System, SMS and Email System, or any other systems of GICHFL required for security implementation. The select bidder shall have the required APIs for the desired interfacing.		
63	The proposed security solution, software, and system architecture must be scalable and shall support increasing number of users and concurrent processing		
64	The proposed security solution, software, system and required hardware for supporting the required present/future volume to be mentioned as part of the Software's System Infrastructure Requirement. Vendor shall assume, current concurrency of users and annual increase of up to 5-10% for next 5 years. Actual numbers can be confirmed during agreement signing. Sizing storage should be computed accordingly, which can be sustained for the entire contract period.		
65	The proposed security solution, software, and system should provide separate Admin Modules for System and User Admin functionalities.		
66	The proposed security solution, software, and system administration and configurations modules must appropriately		

S. No.	Requirements	Agree (Y/N)	Remarks
	validate data during user entry and capture audit details on save and update operations.		
67	The proposed security solution, software, and system should provide facility to upload and attach documents, images in compressed and encrypted form for audits, forensic purpose and should be available for use by users with different workflows or access rights.		
68	All integrations should be in STP mode with/without minimum intervention from user and leveraging existing platform		
69	The proposed security solution, software, and system should work satisfactorily with low bandwidth (32 kbps VSAT/64 Kbps lease line)		
70	The proposed security solution, software, and system should be compatible with any Web Browser like, Internet Explorer 8.0 and above/ Mozilla Fire Fox/ Google Chrome etc.		
71	The selected bidder should present and prepare security solutions, software, and system implementation plan, report the status of implementation to relevant stakeholders regularly.		
72	The selected bidder shall participate in regular Steer-co meetings with Seniors at both ends, for project status and actions on critical requirements or road-blockers.		
73	The selected bidder shall annually provide Security Audit / Information Security Audit Reports for the solution with no open observations.		
74	The selected bidder vendor shall annually provide source code (if applicable) audit / review report of the solution.		
75	The selected bidder shall perform initial configurations for workflows, business rule engine, parameters, etc. while implementing the solution.		
76	Post Go-Live, Vendor shall provide onsite hands-on support personnel for supporting as well as training GICHF admins for managing Change Requests for workflows, business rule engines, parameters, etc. This activity should be free of cost covered in post-production support warranty and period of this support can be decided during the agreement signing.		
77	AMC contract shall include details and T&Cs referencing from Section 2.16 and Section 3.		
78	SIEM Dashboard should have the tool/facility to create / customize / configure / modify any reports, by the team of GICHFL itself without depending on the vendor.		

S. No.	Requirements	Agree (Y/N)	Remarks
79	DOCUMENTATION The following minimum documentation (hard copy and soft copy) on the proposed software components must be made available in English: 1. Security Assessment Report 2. Requirements Definition Document 3. Requirements Traceability Matrix 4. Network Diagram 5. Detailed Project Plan 6. Design Document (High Level Design & Low Level Design) 7. Installation documentation 8. Configuration documentation 9. Secure Configuration Document 10. Integration Traceability Matrix 11. Configured Compliance Dashboard 12. Configured Audit Documentations 13. Acceptance Criteria and Test Plan 14. Standard Operational Procedures 15. Roles and Responsibilities Matrix 16. Incident Playbook 17. Incident Response Procedure Document 18. BCP Guide 19. Training Materials and User Manuals 20. Licenses, SLA, Warranty and Support Manual 21. Final Project Report		
80	The selected bidder shall provide root cause analysis for all incidents, performance, availability, technical or functional issues reported on Production. Formal root cause analysis to be delivered within 5 days of problem occurrence, including- 1. Explanation of the root cause 2. Actions taken to resolve the problem 3. Action plan to prevent recurrence, with project plan/tasks required and timing for each major milestone of the correction effort, and identification of GICHFLs responsibilities in the correction process.		

S. No.	Requirements	Agree (Y/N)	Remarks
81	Undertake and assist GICHFL official in the following server administrator activities (indicative): 1. Solution software Re-installation in the event of system crash/failures 2. Configuring file systems, volumes and apportioning disk space. 3. Ensure proper configuration of server parameters. 4. Periodic system performance tuning. 5. Addition, deletion, re-configuration of devices, additional users etc. 6. Implementing security patches on servers at all levels. 7. Security management - Configuring account policy, access rights, password control as per GICHFL's security policy. 8. Ensure all critical services are running properly on the servers. Schedule and optimize these services. 9. Maintain lists of all system files, root directories and volumes. 10. Performance tuning of servers, databases, or any other dependent environment. 11. Monitoring access logs and application logs 12. Purging of temporary Files, logs in accordance with GICHFLs policies 13. Data backup and restoration. 14. Applying service packs, hot fixes and security rollouts. 15. Troubleshooting Problems etc. 16. Regular submission of various reports for all activities undertaken at periodicities, formats and activities etc. as decided by and at the discretion of GICHFL.		
82	Undertake with and assist the GICHFL official in the following server administrator activities (indicative): 1. Configure Backup for automatic backup of Application and Data. 2. Recovery of Data in case of necessity etc. 3. Regular submission of various reports for all activities undertaken at periodicities, formats and activities etc. as decided by and at the discretion of GICHFL.		

S. No.	Requirements	Agree (Y/N)	Remarks
83	Monitoring and confirming the DR replication and performing DR Drill: 1. Ensuring that the application maintains the RPO and RTO as per GICHFLs requirements. 2. Performing switchover and switchback operations for DR drills as per GICHFLs requirements. 3. Coordinating with GICHFL for creating infrastructure for Disaster Recovery and Business Continuity Management as per GICHFLs policies.		
84	All professional services of the selected bidder required for installation, commissioning and maintenance of the solution shall be included in the scope of work.		
85	The solution shall integrate with the GICHFLs existing network and security solutions.		
86	The Vendor will be responsible for notification of new versions / releases of the solution and supervise their implementation in mutually agreed deadlines.		
87	The software service must be conducted in a manner not compromising the security and integrity of GICHFLs data and not compromising the quality of operation of branches and administrative offices, particularly the services rendered to customers.		

2.13 Testing

i. The Company proposes to conduct “User Acceptance Testing” (“UAT”) and Pilot Testing of the solution, system and software, for the purpose of ensuring that all the functionalities requested for by the Company are available and are functioning accurately. The selected bidder should test and provide QA and SIT sign off along with release notes for initiating UAT. Also, detailed test cases along with test data and test results shall be provided by the selected bidder and approved by the Company. The Company may also add test cases if it identifies any gaps. During UAT all necessary support needs to be provided by the selected bidder for timely fixing UAT issues.

ii. The selected bidder will convey to the Company that all the customizations that are required for “Go Live”, as agreed upon and signed off by the Company are completed and the solution is ready for final testing.

iii. The Company expects the test environment to always be available to the Company, for the purpose of testing.

iv. The Bidder is expected to provide access for the company employees to its test infrastructure. The Company plans to use the testing environment throughout the period of the contract.

v. The Bidder will assist the Company in conducting all the tests and analysing/comparing the results. Bidder shall provide adequate full-time resources conversant in respective business areas, for troubleshooting and resolving defects during the entire UAT process.

vi. Any deviations/discrepancies/errors observed during the testing phase will be formally reported to the selected Bidder and the selected bidder will have to resolve them immediately or within the UAT approach and guidelines formulated between the Bidder and the Company. The resolution timelines will be completely aligned to the committed project timeline by the bidder in the response of this RFP.

vii. The selected bidder will be responsible for maintaining appropriate program change control and version control for all the modifications/enhancements carried out during the implementation/testing phase.

viii. The selected bidder will be responsible for providing and updating system & user documentation as per the modifications.

2.14 Training

2.14.1 End User Training

Vendor shall provide training plan in detail covering the following.

i. The training is to be provided to all Administrators (IT Admin / Security Admin / System Admin) of GICHFL.

ii. Training should include training aids such as online tutorials, manuals, etc.

iii. Provide detailed training plan for this purpose as part of the deliverables.

iv. Provide training material for an on-line training course which can be undertaken by employees as an e-learning program.

2.14.2 Technical and Operations Training

The selected bidder shall provide training plan in detail covering the following,

i. Provide training to personnel identified by the GICHFL from Technical and administrative aspects of the implemented CCSF security solution.
ii. The training must be conducted by the instructors from the OEM.
iii. The Supplier should provide the following trainings:
iv. Solution Administration Training
v. Security Administration Training
vi. Parameter Configuration Training
vii. New Configuration Training, etc.
viii. Training should include training aids such as online tutorials, manuals, etc. for the IT personnel of GICHFL.
ix. Provide detailed training plan for this purpose as part of the deliverables
x. Provide training material for an on-line training course which can be undertaken by employees as an e-learning program.
xi. Training in usage and development of customized controls / configurations / rules / engines to be given separately to all officers as part of the training.

Note: - Further, the overview of the application provided during the UAT / Pilot phase will not form part of the training.

2.15 Facility Management Services

The selected bidder shall deploy one FM support at GICHFL at Head Office, to support the CCSF security implementation 24/7. However, the bidder shall provide and maintain requisite skilled resources at their end as and when support required by GICHFL.

The brief scope for the FM resources is as below:

i. Responsible for maintaining the Solution, System and Software up time of implemented CCFS system as specified by GICHFL.
ii. The selected bidder should have knowledge of security domains like NAC and SASE and related Operations required for managing the security solution up

time of the solution.

iii. Co-ordinate with GICHFLs IT Team or other teams identified by GICHFL, Field staff and for resolving the infrastructure related issues.

iv. Performing the Backup/restoration/patch/updates/upgrades of related activities pertaining to the OS/APP/DB/WEB/Middleware/ Servers, related peripherals and configurations.

v. FM personnel will be responsible for Log shipment, Backup, DC DR cutover drill, Restore-implementation of disaster recovery plan, if required as advised by GICHFL.

vi. User Management /Maintenance of implemented CCFS system.

vii. Maintenance of Key Management of implemented CCFS system.

viii. Follow the Incident reporting / ticketing system of GICHFL and update the same.

ix. Log ticket with helpdesk for support related issues through any of the following modes: Telephonic, Email, Ticketing Tool.

x. Maintain log of all down calls for MIS purpose and provide required MIS/reports etc. to GICHFL as per requirement.

xi. Provide daily, weekly, monthly, quarterly reports to GICHFL in formats finalized during operations.

xii. Prepare necessary documentation for CCFS systems.

xiii. Work as per Standard Operating Processes defined by GICHFL.

xiv. Escalate issues internally or to GICHFLs team for quick resolution of issues.

xv. Extend necessary support for special activities like Quarterly Disaster Recovery Drills, Information Security Audits or any other activities pertaining to RFP scope of work.

xvi. Follow and implement change management process as per GICHFLs guidelines/policies.

xvii. Vendor shall act as single point contact and carry out necessary coordination (call lodge, follow-ups etc.) with all stake holders for smooth functioning of the solution deployed within stipulated time frame.

xviii. Regular Patch Management of implemented security solutions, servers, systems.

2.16 Warranty and AMC/ATS for Software and Licenses

i. The selected vendor should provide comprehensive warranty for proposed solution for a period of three months from the date of Go-Live, including other software, associated modules and services required to meet the requirements in the RFP. Support and services for the remaining tenure will be covered under AMC+ATS.

ii. The vendor shall be responsible for updates, patches, bug fixes, version upgrades.

iii. The vendor shall provide AMC+ATS services for software provided as part of the solution.

iv. During ATS, the vendor shall be responsible for the following:

- Overall maintenance and working of the CCFS system being implemented
- Defects/Bugs and relevant rectifications wherever necessary and deliver patches/ version changes effected. Provision should be available for version control and restoring the old versions in case of need by GICHFL.
- Bug fixing, enhancement, modifications, customization, patches, upgrades due to statutory, regulatory, industry, Organization specific changes (including installation of new upgrades.)
- Configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, replacement / support, technical support for application and data maintenance, recovery, query generation and management etc. of all software supplied under this RFP.
- Undertake immediate bug fix actions in the event of software failure causing an interruption of operation of the CCFS system as per the response / resolution times defined by GICHFL.
- Notify all the detected software errors and correct them as per the agreed timelines.
- Support GICHFL in integrating CCFS system with any new applications (web / mobile / exe), tools, dashboard, etc.
- Routing the transactions through the backup system in case the primary system fails Switching to the DR site in case of system failure.
- No visiting costs, out of pocket expenses will be provided by GICHFL
- If selected bidder fails to resolve or does not attend the issue in mentioned time frame, penalty will be charged proportionately

2.17 Inspections and Tests

GICHFL or its representative(s) shall have the right to and may visit and /or inspect any of the selected Bidder's premises to ensure that data provided by GICHFL is not misused. GICHFL shall notify the bidder in writing, in a timely manner, of the identity of any representatives for these purposes.

GICHFL will not bear any charges payable to the bidder's representative for such regulatory compliance inspections.

Should any inspected or tested Goods/software fail to conform to the Specifications, GICHFL may reject the Goods/software, and the bidder shall make alterations necessary to meet specification requirements at no additional cost to GICHFL.

GICHFL's right to inspect, test and, where necessary, reject the software after the software delivery shall in no way be limited or waived because of the software having previously been inspected, tested and passed by GICHFL.

2.18 Change Orders

GICHFL may at any time, by a written order given to the selected bidder make changes within the general scope of the signed Contract in any one or more of the following:

i. the place of implementation; and / or
ii. the Services to be provided by the selected bidder

2.19 Delays in The Supplier's Performance

Delivery of the Goods and performance of Services shall be made by the bidder in accordance with the project plan timeline provided by the bidder in RFP response.

If at any time during performance of the Contract, the bidder should encounter conditions impeding timely delivery of the Goods and performance of Services, the bidder shall promptly notify GICHFL in writing of the fact of the delay, its likely duration and its cause(s). As soon as GICHFL is notified, GICHFL shall evaluate the situation and may at its discretion extend the bidder's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of the Contract.

2.20 Sub-Contracting

The selected OEM vendor will not subcontract or delegate or permit anyone other than their on-roll personnel to perform any of the work, service or other performance required under the signed agreement without the prior written consent of GICHFL.

2.21 Warranty/Post-Warranty Services

The selected bidder must support and maintain the security solution implemented (including supporting software and hardware) under the contract for the Solution under the warranty support till 3 months from go-live and AMC+ATS for remaining tenure post warranty.

The selected bidder shall submit a detailed plan including the manpower to be deployed during the post-implementation support of the solution. Manpower can be changed only with personnel with similar experienced substitute, after giving an advance notice of two weeks and taking approval from GICHFL.

The selected bidder should provide Resume/Curriculum Vitae and Background Verification of the personnel/ engineer assigned at GICHFL to be part of the Implementation/Onsite support for security solution. Also, the personnel/engineer will be interviewed by GICHFL. GICHFL reserves the right to disqualify any personnel/ engineer if the personnel do not match GICHFLs requirements.

2.22 Software performance

Performance, Load balancing, Autoscaling shall be responsibility of the selected vendor and delays / failures in resolution of any issues shall be liable to SLAs under agreement as defined by GICHFL.

2.23 Backup and Archiving

The selected bidder shall suggest a suitable backup and archiving solution for all the data collected for past 5 years, Documents and Data, setup and periodically validate the same during the contract period. For 5 years after Production period, the bidder shall provide support to GICHFL for retrieval/access of data, documents from the backup/archival as part of AMC+ATS without any additional cost.

2.24 Disaster Recovery and Business Continuity Plan

The selected bidder shall provide a security software / system / solution which is compatible and supports Business Continuity and Disaster Recovery plan as per GICHFLs policies. The selected bidder should highlight the provisions for disaster recovery and show that the application facilitates disaster recovery.

2.25 Preventive Maintenance

The selected bidder shall provide onsite preventive maintenance on quarterly basis. Providing all deliverables, including warranty services etc., shall be the sole responsibility of the bidder. GICHFL will not be responsible for any delays/violation from third party vendors, if such services are availed from the bidder as part of agreement.

2.26 Mean Time Between Failures (MTBF)

The selected bidder shall agree that if during the warranty period, the Software or any of the related/dependent components fail on four or more occasions in a quarter, it shall be replaced by equivalent / superior / part by the vendor at no additional cost to GICHFL.

2.27 Clarification of Offers

To assist in the scrutiny, evaluation and comparison of offers / bids, GICHFL may, at its sole discretion, ask some or all bidders for clarification of their offer / bid. The request for such clarifications and the response will necessarily be in writing and no change in the price or substance of the bid shall be sought, offered or permitted. Any decision of GICHFL in this regard shall be final, conclusive and binding on the bidder.

3. Service Levels

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:

i. The selected bidder will get 100% of the Quarterly payment if the baseline performance metrics are complied with.
ii. The selected bidder will get quarterly payment after deducting penalty at the rates specified below in case of performance not meeting the SLA terms.

3.1 Security Uptime:

i. Maintaining Quarterly 99.999% uptime and availability of security features, devices, network and infrastructure where CCSF security is implemented.
ii.
iii. Failure of Quarterly Security Availability Uptime of 99.999% will result in monetary penalty being calculated and recovered against Quarterly Recurring Charges as per signed AMS + ATS.
iv.
v. Any security lapses leading to regulatory or compliance penalties will result in GICHFL recovering the actual amount from selected bidder as levied by the regulators or compliance / audit / consumer authorities.

3.2 Security Incident Response and Resolution (IRR):

i. For Security Incidents Response and Resolution, selected bidder must follow the below metrics and penalties clauses for maintaining satisfactory performance. The metrics to measure poor performance are based on timeline defined for identification of incident, intimation and acknowledgement of the same, first line of response and resolution of security incident impact. Incidents related to all and any security in GICHFL devices, network and infrastructure are considered that can lead to device failures, network outage, firewall outages or failures, performance issues in GICHFL managed devices, network or infrastructure due to security incident, any performance issues or failures on GICHFL Cloud attributed to security incident, any unplanned GICHFL managed devices, network, Cloud, infrastructure or software downtimes attributable to security incident. Below is the table of SLA categorization based on critical of security incident impact:

Impact	Severity
Any GICHFL site outage for more than 8 hours attributed to any security lapse. Outage can be either of GICHFL managed network, devices, infrastructure, cloud, software outage. OR Impacts 10% or more of users using GICHFL managed infrastructure, device, cloud, network or software are affected by security incident.	Critical
Any GICHFL site outage for more than 4 hours and less than 8 hours attributed to any security lapse. Outage can be either of GICHFL managed network, devices, infrastructure, cloud, software outage. OR Impacts 10% or less of users using GICHFL managed infrastructure, device, cloud, network or software are affected by security incident.	Medium. (If the outage time > 8 hours OR Users impacted crosses > 10%, severity is Critical)

Any GICHFL site outage for more than 2 hours and less than 4 hours attributed to any security lapse. Outage can be either of GICHFL managed network, devices, infrastructure, cloud, software outage. OR Impacts 5% or less of users using GICHFL managed infrastructure, device, cloud, network or software are affected by security incident.	Low (If the outage time > 4 hours OR Users impacted > 5%, severity is Medium)

ii. Unless there is a planned downtime / outage approved by GICHFL, as Security is seem-less and non-stop service without any holidays or leave and is of paramount criticality, every day is a working day. 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.

iii. The outage will be calculated in hours.

iv. The selected bidder shall 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).

v. At the end of a Month, selected bidder shall calculate the total amount of outage time due to attributed security IRR lapse or non-performance when a fault/ incident of "Critical" Severity Level occurs Or 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 outage is restored. This will be referred to as the "Security Outage Time" and will be used in the calculation of "Availability Uptime".

vi. "**Availability Uptime**" will be calculated monthly and must always be 99.999%. This will be calculated as below:

Availability Uptime =

(1 – {(Security Outage Time / Net Working Time) in hours} *100%.

vii. Penalty will be calculated as a % of QRC against sliding % of Availability Uptime as per below table:

Availability Uptime %	% of QRC
>=99.999	0
>=99.5 & <=99.999	1
>=99.3 & <=99.5	2
>=98.95 & <=99.3	3
>=98.6 & <=98.95	5
>=97.9 & <=98.6	7
>=97.2 & <=97.9	9
>=96.67 & <=97.2	10
<96.67	10

viii. The selected bidder shall provide GICHFL with a prompt online dashboard of the security service lapses, unavailability, downtime, timeline of identification, acknowledgement, response and resolution, view of impacts of GICHFL site or users due to security incident.

ix. The Penalty will be calculated monthly and then added up for a quarter and deducted from Quarterly Recurring Charges (QRC) of the ATS+AMS Cost to the selected bidder. The selected bidder shall adhere to all requirements laid out in the Tender Document and this Agreement.

x. The penalty calculated for IRs is exclusive of SLAs and penalties for Service Requests (SRs).

xi. The selected bidder must share a detailed Incident Closure Report with RCA for each Incidents.

3.3 Service Requests SLA

The Company expects selected bidder to adhere to the following minimum Service Levels:

i. Any fault/ issue/ defect failure intimated by Company through any mode of communication like call/e-mail/fax etc. are to be acted upon, to adhere to the service levels. Business/ Service Downtime and Deterioration shall be the key considerations for determining "Penalties" that would be levied on the selected bidder.

ii. The selected bidder should have 24X7 monitoring, escalation and resolution infrastructure.

iii. Time bound problem addressing team (onsite/offsite) for the complete contract period.

iv. The selected bidder to arrange and provide for updates required in the system to meet the changes suggested by regulatory authorities towards compliance as part of ATS at no extra cost to Company for the entire contract period. Any delay in meeting the timelines would result in penalty.

v. The selected bidder will have to guarantee a minimum uptime of 99.5%, calculated monthly. Application (As a whole / any module of the application) availability, will be 99.5% on 24x7x365. The penalty will be calculated on basis of unplanned downtimes attributable to software issues, as per the details given below.

vi. **Uptime percentage**: 100% less Downtime Percentage

vii. **Downtime percentage**: Unavailable Time divided by Total Available Time, calculated monthly.

viii. **Total Available Time**: 24 hours per day for seven days a week excluding software, infrastructure and network planned downtimes.

ix. **Unavailable Time**: Time is involved while the solution is inoperative or operates inconsistently or erratically.

Uptime Percentage (A)	Penalty Details
A >= 99.5%	No Penalty
A >= 99% and A < 99.5%	5% of AMC+ATS Cost
A >= 98.5 % and A < 99%	10% of AMC+ATS Cost
A < 98.5%	20% of AMC+ATS Cost

x. The uptime percentage would be calculated on monthly basis, and the calculated amount would be adjusted from every monthly payment. If Vendor materially fails to meet an uptime of 99.50% for three (3) consecutive months, the Company may have the right to terminate the contract. In case there are no pending invoices to be paid by the Company to the vendor, the vendor shall submit a pay order or cheque, payable at Mumbai and in favor of GICHFL, for the penalty amount within 30 days from the notice period issued by the Company.

3.4 Availability Service Level Default

i. Availability Service Level will be measured on a monthly basis.

ii. A Service Level Default will occur when the vendor fails to meet Minimum uptime (99.5%), as measured monthly.

iii. Bidder shall determine the severity levels based on the criteria mentioned below:

Severity Level	**Number of users impacted**	**Effective Downtime**
Severity 1	Any problem where > 20% of the users of the application are affected	100%
Severity 2	Any problem <= 20% of the users and > 10% of the users of the application are affected	90%
Severity 3	Any problem where <= 10% of the users of the applications are affected	80%

iv. **Service SLA Penalty Calculation:**

E.g.: There is an incident which occurs under the Severity Level 2 for which the downtime is for 5 hours in a month.

Therefore, the effective downtime for the month would be: **5 hours x 90% = 4.5 hours**

Therefore, the downtime of 4.5 hours would be considered due to this incident while computing the availability of the application.

3.5 Non-Compliance of SLAs

The vendor must take note that the Max limits of penalties are of upper tolerance and GICHFL reserves the right to terminate the contract at any point in time for breach of SLAs without reaching the Max limit of penalties.

4. RFP Response Instructions

4.1 RFP Process

The Request for Proposal (RFP) documents shall be published on GICHFL Corporate website. Responses from interested parties shall be accepted within the state timeframe after which no vendor response entries shall be accepted. The responses shall be evaluated on Quality and Cost Based Scoring (QCBS) methodology to identify T1-L1. Following this evaluation process, the Company shall exercise its discretion to identify and select vendors deemed capable of meeting the majority of the project's functional and technical requirements. This RFP is being conducted as a closed and limited procurement process; accordingly, only those vendors shortlisted through this internal evaluation shall be eligible to receive the RFP documents and participate further in the solicitation process.

4.2 Late bids

Any bid received after the last date and time for submission of bids as prescribed in this RFP will be rejected and returned unopened to the Bidder.

4.3 Formation of Bid

The bid must be made in an organized and structured manner. The Bid should be properly sealed and marked as "Request for Proposal of Consolidated and Comprehensive Security Framework Implementation", RFP Reference Number, Bidder's name and address. The RFP response shall contain the following documents with bidder's seal and signature: -

S.No.	List of Documents
1	Tender Covering Letter
2	The response to the Functional and Technical requirements in PDF format, as per Sections 2.9 and 2.10, along with the additional documents requested in Section 5 for the evaluation of bids
3	Sealed Envelope containing commercial Bid price as per Appendix 1 duly labeled as 'Commercial Bid price and RFP Reference No., Name of the Bidder'.

4	Any other document indicating the feature of the product.

4.4 Performance Bank Guarantee

The successful bidder has to submit the Performance Bank Guarantee equivalent to 10% of Contract Value for the due performance of the contract, valid for 60 months including 3 months claim period. It is to be submitted centrally at HO IT Department level within 10 days from the letter of selection.

In case vendor(s) fails to perform the Contract or fails to pay the due penalty, if any, as demanded by GICHFL, GICHFL shall invoke the Bank Performance Guarantee to recover penalty/damages.

4.5 Erasures or Alterations

The Bid should contain no alterations, erasures or overwriting except as necessary to correct errors made by the Bidder, in which case corrections should be duly stamped and initialled / authenticated by the person/(s) signing the Bid. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents or submission of bid not substantially/conclusively responsive to the bidding documents in every respect will be at the Bidders risk and may result in rejection of the bid.

4.6 Others

i. Responses to this RFP by the Bidders shall not constitute an obligation on the part of the Company to award a contract for any services or combination of services. Failure of the Company to select a Bidder shall not result in any claim whatsoever against the Company and the Company reserves the right to reject any or all bids in part or in full, without assigning any reason whatsoever.

ii. By submitting a proposal, the Bidder agrees to promptly contract with Company for any work awarded to the Bidder, if any. Failure on the part of the selected Bidder to execute a valid contract with Company within 45 calendar days from the date of Purchase order herein will relieve Company of any obligation to the Bidder, and a different Bidder may be selected based on the selection process of Company.

iii. The terms and conditions as specified in the RFP, addenda and corrigenda issued by the Company thereafter are final and binding on the Bidders. In the event the Bidder is not willing to accept the terms and conditions of Company, the Bidder may, in sole discretion of Company, be disqualified.

iv. The Bidder must strictly adhere to the delivery dates or lead times identified in their proposal including the project timeline. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Company, may constitute a material breach of the selected Bidder's performance. In the event that the Company is forced to cancel an awarded contract (related to this RFP) due to the Bidder's inability to meet the established delivery dates that bidder will be responsible for any re-procurement costs suffered by the Company. The liability of re-procurement costs in such an event could be limited to the amount actually spent by Company for procuring similar deliverables and services. The re-procurement cost would be established post a reasonable due – diligence of the re-procurement cost to be incurred.

v. By submitting the bid, the Bidder represents and acknowledges to the Company that it possesses necessary experience, expertise and ability to undertake and fulfil its obligations, under all phases involved in the performance of the provisions of this RFP. The Bidder represents that all services supplied in response to this RFP shall meet the proposed Solution requirements of the Company. The Bidder shall be required to independently arrive at a Solution, which is suitable for the Company, after taking into consideration the effort estimated for implementation of the same. If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or services and are required for proper performance or provision of the deliverables or services in accordance with this RFP, they shall be deemed to be included within the scope of the deliverables or services, as if such services, functions or responsibilities were specifically required and described in this RFP and shall be provided by the Bidder at no additional cost to Company, unless bidder is able to explicitly justify the noninclusion of such deliverables or services in the scope. The Bidder also acknowledges that Company relies on this statement of fact, therefore neither accepting responsibility for, nor relieving the Bidder of responsibility for the performance of all provisions and terms and conditions of this RFP, Company expects the Bidder to fulfil all the terms and conditions of this RFP. The modifications, which are accepted by the Company in writing, shall form a part of the final contract.

vi. The Bidder shall represent that the proposed software solution and its documentation and/or use of the same by Company shall not violate or infringe the rights of any third party or the laws or regulations under any governmental or judicial authority. The Bidder further represents that the documentation to be provided to Company shall contain a complete and accurate description of the software, hardware and other materials and services (as applicable), and shall be prepared and maintained in accordance with the highest Industry standards. The Bidder represents and agrees to obtain and maintain validity throughout the Contract, of all appropriate registrations, permissions and approvals, which are statutorily required to be obtained by the selected Bidder for performance of the obligations of the selected Bidder. The Bidder further agrees to inform and assist the Company for procuring any registrations, permissions or approvals, which may at any time during the contract period be statutorily required to be obtained by the Company for availing services from the selected Bidder.

vii. All terms and conditions, payments schedules, time frame for implementation, expected service levels as per this RFP will remain unchanged unless explicitly communicated by Company in writing to the Bidders. The Bidder shall at no point be entitled to excuse themselves from any claims by Company whatsoever for their deviations in conforming to the terms and conditions, payments schedules, expected service levels, time frame for implementation etc. as mentioned in this RFP.

viii. The Bidder covenants and represents to Company, the following:

a. It is duly incorporated, validly existing and in good standing under as per the laws of the jurisdiction of its incorporation.

b. It has the corporate power and authority to perform its obligations hereunder and to execute appropriate contracts in terms of this RFP. The performance of terms and conditions under the RFP by it and the performance of its obligations hereunder are duly authorized and approved by all necessary action.

c. The execution, delivery and performance under an Agreement by such Party:

d. Will not violate or contravene any provision of its documents of incorporation.

e. Will not violate or contravene any law, statute, rule, regulation, licensing requirement, order, writ, injunction or decree of any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority by which it is bound or by which any of its properties or assets are bound.

f. Except to the extent that the same have been duly and properly completed or obtained, will not require any filing with, or permit, consent or approval of or license from, or the giving of any notice to, any court, governmental instrumentality or other regulatory, governmental or public body, agency or authority, joint venture party, or any other entity or person whatsoever.

g. To the best of its knowledge, after reasonable investigation, no representation or warranty by such party in this tender and subsequent agreement, and no document furnished or to be furnished to the other party to this RFP and subsequent agreement, or in connection herewith or with the transactions contemplated hereby, contains or will contain any untrue or misleading statement or omits or will omit any fact necessary to make the statements contained herein or therein, in light of the circumstances under which made, not misleading. There have been no events or transactions, or facts or information which has come to, or upon reasonable diligence, should have come to the attention of such party and which have not been disclosed herein or in a schedule hereto, having a direct impact on the transactions contemplated hereunder.

h. The selected Bidder shall undertake to provide appropriate manpower as well as other resources required, to execute the various tasks assigned as part of the project, from time to time. The Company has the right to interview all of the resources deputed by the selected bidder and only upon satisfaction will allow the resource to work on the project.

i. All RFP response documents would become the property of the Company, and the Company also would not return the bid documents to the Bidders.

j. Company will not bear any costs incurred by the Bidder for any discussion, presentation, demonstrations etc. on proposals or proposed contract or for any work performed in connection therewith.

k. Company reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.

5. Evaluation Methodology

The evaluation will be a three-stage process. The stages are:

- Functional and Technical Bid Evaluation
- Commercial Bid Evaluation
- Weighted evaluation

The Functional & technical evaluation and the commercial evaluation shall have the weightage of 70% and 30% respectively. This weightage shall be considered for arriving at the successful bidder. The evaluation methodology vis-à-vis the weightages is as under:

5.1 Technical Bid Evaluation

S.No.	Proposed Bid Evaluation	Scores
1	Standing of the Company & Credential Strengths	10
2	Technical requirements evaluation	60
3	Functional requirements evaluation	30
Maximum Proposal Bid Evaluation Score		**100**

The technical evaluation would involve the following major areas:

i. Standing of the Bidder and Credential strengths of the Bidder

Each Bidder having Credential strengths will get marks according to their financial strength, No. of clients, Certifications & accreditations, Regulatory compliances, No. of full-time resources. The bidder must submit an undertaking confirming these details, including the number of clients, Full-Time Equivalent (FTE) count, and copies of certifications and accreditations.

The bidder should provide the Certificate of Incorporation & Commencement of Business (applicable for Public Ltd./ Private Ltd Companies). A certified copy of the same are required to be submitted with the Bid.

ii. Techno-Functional features evaluation and Demonstration

- The bidder is required to respond to each line item on the tables provided in Sections 2.9 and 2.10, as per the instructions outlined in those sections. The responses should be included along with the RFP submission. The company may request the bidder to demonstrate the product and will provide advance notice if a full or partial demonstration of any line item is required.
- The demonstration shall be carried out in Company's premises in Mumbai Head office.
- This will also enable the Company to understand the solution's features and fit with the proposed architecture and identify the level of customization required.
- The Company will communicate a date, time and location to the bidders any time after the last date for submission of proposals.

During the Product Demonstration, the Company will assess the Bidder based on the functionalities of the proposed solution, using Sections 2.9 and 2.10 as the basis.

The proposed solution offered, however, should have at least 70% of the requirements as a part of the standard product. The remaining shall be customized before Go Live at no extra cost to the GICHFL.

The total marks obtained against the total number of functional and technical specifications will be proportionately modified to a maximum of 50 for the sake of evaluation.

iii. Experience in Information Security Domain

The Bidder should provide information on their experience in the domain of Information Security and related implementations of security features that bidder is submitting the response for. Experience specifically within HFCs / NBFCs / Banks is preferable. The Bidder's past experience shall be evaluated, and the score obtained by the Bidder shall be considered for evaluation.

The Bidder should provide details of implementations in HFCs / NBFCs / Banks including details of Scope of Project, security features implemented, number of sites involved with breakup of the roles-responsibilities and Proof of Implementations. The bidder is required to provide detailed and verifiable references for these implementations, including the name of the organization, the reference contact person, and their contact details.

iv. Bidder presentations and Project Plan Timelines

The company will require bidders to submit presentations covering various aspects of the proposed solutions. These presentations will be scored on the following key areas.

#	Evaluation of the Bidder Presentation
1	Project Execution Methodology
2	Solution Architecture and Design – Key Features and Functionalities
3	Operational Ease
4	Adherence to Project Timelines
5	Execution Competency (Solution Accelerators, Functional & Technical Competency)

The company may also invite bidders to make presentation on a case-by-case basis at the company's head office in Mumbai. This process will allow the company to seek clarifications on any issues arising from the bidders' responses to the RFP.

5.2 Commercial Bid Evaluation

The commercial bid evaluation will be carried out through sealed envelope containing "commercial bid Price". Based on the commercial bid values obtained, the bidder with the lowest commercial proposal will be designated as L1 Bidder.

i. Weighted Evaluation:

Based on the combined weighted score for technical and commercial evaluation, the bidders shall be ranked in terms of the total score obtained. The proposal obtaining the highest total combined score in evaluation of quality and cost will be ranked as H-1 followed by the proposals securing lesser marks as H-2, H-3 etc. The proposal securing the highest combined marks and ranked H-1 shall be recommended for award of contract.

As an example, the following procedure can be followed:

A score (S) will be calculated for all qualified bidders using the following formula: Clow/C X100 +T (1-X)

C stands for discounted rate arrived basis of commercial evaluation; Clow stands for the lowest rate arrived basis of commercial evaluation. T stands for technical evaluation score and X is equal to 0.30.

#	**Bidder**	**Technical Evaluation Marks (T)**	**Discounted Rate (C)**	**T * 0.70 (A)**	**[(Clow / C) * 100] * 0.30 (B)**	**Score (S = A +B)**
1	AAA	75	120	52.50	25.00	77.50
2	BBB	80	100	56.00	30.00	86.00
3	CCC	90	110	63.00	27.27	90.27

In the above example, Clow is 100. CCC, with the highest score, becomes the successful bidder (H1).

In case of more than one vendor with equal highest score (S) up to three decimals, then number of decimals will be increased.

The Company may in its absolute discretion, engage in discussion or negotiation with H1 bidder. The decision of the Company shall be final and binding on all the vendors to this document. The Company reserves the right to accept or reject an offer without assigning any reason whatsoever.

6. Payment Terms

The bidder must accept the payment terms proposed by the Company. The commercial bid submitted by the bidder must be in conformity with the payment terms proposed by the Company. Any deviation from the proposed payment terms would not be accepted. The Company shall have the right to withhold or deduct (in event of SLA breach) any payment due to the selected bidder, in case of delays or defaults on the part of the selected bidder. Such withholding of payment shall not amount to a default on the part of the Company. If any of the items / activities as mentioned in the price bid is not taken up by the Company during the course of the assignment, the Company will not pay the professional fees quoted by the vendor in the price bid against such activity / item.

6.1 Payout Structure

The payment will be released as follows:

Phase	Percentage of Payment	Milestone
Phase 1	10%	On project kick-off with final project report acceptable to GICHFL duly supported / substantiated by documentary support/evidence etc.
Phase 2	20%	On successful implementation of software in UAT environment and verified by GICHFL. UAT user group training to be completed
Phase 3	20%	On successful UAT Signoff, implementation of software in production, Pilot user training and Go-live completion at Pilot Branches.
Phase 4	30%	Roll out across all remaining locations and go live with Successful completion of all user training.
Phase 5	20%	After three months of successful and stable functioning of the complete system. (warranty support period)

6.2 Pricing

Upon completion and signoff of the project milestones mentioned in section 6.1 bidder will be eligible to raise the invoices to GICHFL. The Company will pay invoices within a period of 45 days from the date of receipt of undisputed invoices. Any dispute regarding the invoice will be communicated to the selected bidder within 15 days from the date of receipt of the invoice. After the dispute is resolved, Company shall make payment within 30 days from the date the dispute stands resolved.

Upon the system going live across all branches and end of warranty period, the initiation of the Annual Maintenance Contract (AMC), payments shall be made monthly, following the end of each calendar month, against the submission of the original invoice from the company. The agreed prices shall remain fixed and shall not be subject to escalation once finalized and accepted by the Company and the selected bidder. Payments will be made by the Company in accordance with the above payment terms, contingent upon the submission of all relevant documentation.

7. Terms & Conditions

7.1 Special Terms and Conditions

- The Bidders shall abide by the Special Terms and Conditions (STC) listed in this RFP document.
- 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.
- 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.
- 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.
- No binding legal relationship shall exist between any of the Bidders and GICHFL until the execution of SLA.
- 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, appropriate penalties may be levied.
- 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.

- 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.
- 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.
- Any quotation or billing linked to GICHFL's Assets and/ or Revenue will disqualify the Bidder.
- If at any point in time the services of the selected bidder are found to be non-satisfactory, the contract will be terminated as per the termination provisions of the SLA.
- 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. The selected bidder shall sign the Reciprocal Non-Disclosure Agreement (NDA) agreement with GICHFL to maintain and protect the confidentiality of Data and Information.
- All supporting documentation submitted by the selected bidder as part of this proposal shall become the property of GICHFL.
- 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.
- 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.

- GICHFL reserves the right to take appropriate action against the selected 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.
- GICHFL reserves the right to:
  a. Accept/ reject any or all the bids submitted by any Bidder, without assigning any reasons thereof.
  b. Add, modify, relax, or waive off any condition(s) stipulated in the bid whenever deemed necessary.
- It is construed that the Bidder has read all the terms and conditions before submitting the bid.
- GICHFL authority will not be held responsible for any technical snag or network failure during on-line bidding.
- 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.
- 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.
- 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.
- 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.
- 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 into the gap report.

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

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

7.2 General

- The Company expects the vendor to adhere to the terms of this RFP document and will not accept any deviations to the same.
- The company expects that the vendor appointed under this RFP Document shall have the single point responsibility for fulfilling all obligations and providing all deliverables and services required by Company.
- Unless agreed to specifically by the Company in writing for any changes to the RFP document issued the vendor responses would not be incorporated automatically in the RFP document.
- Unless expressly overridden by the specific agreement to be entered into between the Company and the vendor, the RFP document shall be the governing document for arrangement between the Company and the selected vendor.

7.3 Indemnity

The Selected Vendor shall indemnify the company, and shall always keep indemnified and hold the Company, its employees, personnel, officers, directors, (hereinafter collectively referred to as "Personnel") harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Company as a result of:

- Company’s authorized / bona fide use of the Deliverables and /or the Services provided by selected Vendor under this RFP; and/or
- any act of commission or omission, fraud, negligence, breach on the part the selected Vendor and/or its employees, agents, sub-contractors in performance of the obligations under this RFP; and/or any act of omission of statutory requirement and/or
- claims made by employees or subcontractors or subcontractors’ employees, who are deployed by the selected Vendor, against the company; and/or
-
- claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the selected Vendor to its employees, its agents, contractors and sub-contractors.
- breach of any of the term of this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty of the selected Vendor under this RFP/subsequent agreement; and/or
- any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or
- breach of confidentiality obligations of the selected Vendor contained in this RFP; and/or
- The acts, errors, representations, misrepresentations, willful misconduct or negligence or gross misconduct attributable to the selected Vendor or its employees or sub-contractors under this RFP/subsequent agreement.
- Loss of data due to selected vendor provided facility or
- Any deficiency in the services of selected Bidder.
- Any transaction contemplated under this RFP/subsequent agreement.
- The provisions of this Clause shall survive the termination of RFP and subsequent Agreement made thereafter.

The selected Vendor shall at its own cost and expenses defend or settle at all point of time any claim against the Company that the Deliverables and Services delivered or provided under this RFP infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in the country where the Deliverables and Services are used, sold or received, provided the Company:

- notifies the selected Vendor in writing as soon as practicable when the Company becomes aware of the claim; and
- Cooperates with the selected Vendor in the defense and settlement of the claims.

However, (i) the selected Vendor shall take sole control of the defense and all related settlement negotiations (ii) the company provides will the selected Vendor with the assistance, information and authority reasonably necessary to perform the above and (iii) the Company does not make any statements or comments or representations about the claim without the prior written consent of the selected Vendor, except where the Company is required by any authority/regulator to make a comment/statement/representation.

If use of deliverables is prevented by injunction or court order because of any such claim or deliverables is likely to become subject of any such claim then the selected Vendor, after due inspection and testing and at no additional cost to the Company, shall forthwith either 1) replace or modify the software / equipment with software / equipment which is functionally equivalent and without affecting the functionality in any manner so as to avoid the infringement; or 2) obtain a license for the Company to continue the use of the software / equipment, as required by the Company as per the terms and conditions of this RFP and subsequent agreement and to meet the service levels; or 3) refund to the Company the amount paid for the infringing software / equipment and bear the incremental costs of procuring a functionally equivalent software / equipment from a third party, provided the option under the sub clause (3) shall be exercised by the Company in the event of the failure of the selected Vendor to provide effective remedy under options (1) to (2) within a reasonable period which would not affect the normal functioning of the Company.

The selected Vendor shall not be liable for defects or non-conformance resulting from:

- Software, hardware, interfacing, or supplies for the solution not approved by selected Vendor; or
- any change, not made by or on behalf of the selected Vendor, to some or all of the

software/deliverables supplied by the selected Vendor or modification thereof, provided the infringement is solely on account of that change.

7.4 No liability

- All employees engaged by the Service Provider shall be in sole employment of the Service Provider and the Service Provider shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall company be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the Service Provider.
- Company shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third-party software or modules supplied by the Service Provider as part of this Agreement.
- Under no circumstances Company shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project, even if Company has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business.

7.5 Extension of Contract Post Expiry

- The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safeguard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.
- The Company expects the benefits from any unanticipated decrease in technology infrastructure costs, over the term of the contract due to reduction of prices, efficient use of IT infrastructure/reduction of statutory charges, etc. and operations management methods that yield more efficient operations, to be passed on through re-negotiation. No conflict between the Selected Bidder and

the Company will cause cessation of services.

7.6 Termination of Contract

- Company shall have the option to terminate any subsequent agreement and / or any particular order, in whole or in part by giving Vendor at least 90 days prior notice in writing. It is clarified that the Vendor shall not terminate the subsequent Agreement for convenience.
- However the Company will be entitled to terminate subsequent agreement, if Vendor breaches any of its obligations set forth in this RFP and any subsequent agreement and Such breach is not cured within thirty (30) Working Days after the Company gives written notice; or if such breach is not of the type that could be cured within thirty (30) Working Days, failure by Vendor to provide the Company, within thirty (30) Working Days, with a reasonable plan to cure such breach, which is acceptable to the Company.
- Nonconformity of the Deliverables or Services with the terms and Specifications of the RFP as observed during post-delivery audit or otherwise; or serious discrepancy in the quality of service/hardware/software expected during the implementation, rollout and subsequent maintenance process.
- This Tender and subsequent Agreement shall be deemed to have been terminated by either Party one day prior to the happening of the following events of default:
- The other Party becomes unable to pay its debt as they fall due or otherwise enters into any composition or arrangement with or for the benefit of its creditors or any class thereof; A liquidator or a receiver is appointed over all or a substantial part of the undertaking, assets or revenues of the other Party and such appointment continues for a period of twenty-one (21) days.
- The other Party is subject of an effective resolution for its winding up other than a voluntary winding up for the purpose of reconstruction or amalgamation upon terms previously approved in writing by the other Party; or the other Party becomes the subject of a court order for its winding up.
- In the event of a termination of the Contract by the Company, the Bidder shall do all such acts or deeds as may be required to fully compensate the Company

for all expenditure incurred by the Company in executing or obtaining the execution of the Project, till such time of termination and for any removal and/or relocation that may be required by the Company following such termination. The Company shall not bear any liability in this regard. The company shall recover all the cost of replacing vendor and or the company shall impose liquidated damages. In the event of the Company communicating its intention to terminate the Contract, selected bidder shall continue to render such Services as it is required to under this RFP/bid and subsequent Contract, including but not limited to Facilities Management, support and maintenance for the Deliverables for a period up to 6 months following notice of intention to termination, until such time that the Company indicates that it has been able to make alternative arrangements for the provision of such Services, in accordance with the terms, including those pertaining to payment, contained herein.

- In the event of the Company communicating its intention to terminate the Contract due to change in its policy or Business Practice or any other reason which may arise due to unforeseen circumstances, selected bidder shall continue to render such Services as it is required to under this RFP/bid and subsequent Contract, including but not limited to Facilities Management, support and maintenance for the Deliverables for a period up to 6 months following notice of intention to termination, until such time that the Company indicates that it has been able to make alternative arrangements for the provision of such Services, in accordance with the terms, including those pertaining to payment, contained herein.
- Any other reason.

7.5.1 Other Rights or Remedies

Termination of the contract in whole or part is without prejudice to any other rights or remedies that either Party may have under the contract including the invocation of the performance guarantee by the Company and does not affect any accrued rights or liabilities of either Party at the date of termination.

7.5.2 Effects of Termination

Notwithstanding termination of the contract in whole or in respect of any part of the Services for any reason, the contract continues in force to the extent necessary to give effect to those of its provisions which expressly or implicitly have effect after termination; and Where Company terminates any Part of the Project, the parties shall continue to perform their respective obligations under the contract in connection with that portion of the Project in respect of which there has been no termination.

7.5.3 Consequence of Termination

If Company terminates the contract in whole or in respect of any part of the Project in accordance with its terms, it will incur no liability to the selected bidder as a result of such termination, other than:

- the charges or any other amounts due to selected bidder up to the date of termination.
- amounts payable for any Services already performed at the date of the termination.
- amounts payable for Services yet to be performed but which the parties agree not to terminate after performance of those services; and

The selected bidder understands the scale, tenure and criticality of this Project and that it would require tremendous commitment of financial and technical resources for the same from the selected bidder for the tenure of this tender and subsequent Agreement/Contract. The parties therefore agree and undertake that an exit at any point in time resulting due to expiry or termination of RFP and subsequent Agreement/Contract for any reason whatsoever would be a slow process over a period of six (6) months, after the completion of the notice period of three (3) months, and only after completion of the selected bidder's obligations under a reverse transition mechanism. During this period of Reverse Transition, the selected bidder shall continue to provide the Deliverables and the Services in accordance with this RFP and subsequent Agreement/Contract and shall maintain the agreed Service levels.

Upon Company's request, with respect to (i) any agreements for maintenance, disaster recovery services or other third-party applications/solutions, and any Deliverables not owned by the selected Bidder, being used by the selected Bidder to provide the Services and (ii) the assignable agreements, selected Bidder shall, use its reasonable commercial endeavours to transfer or assign such agreements and selected Bidder's equipment to Company and its designee(s) on commercially reasonable terms mutually acceptable to both parties.

Upon Company's request in writing, selected bidder shall be under an obligation to transfer to Company or its designee(s) the Deliverables being used by the selected bidder to perform the Services free and clear of all liens, security interests, or other encumbrances at a value calculated as stated.

As part of the reverse transition services, Company shall have the right, and selected bidder shall not object to or interfere with such right, to contract directly with any selected bidder's subcontractor.

Procedure for transition and migrating to the new appointed Bidder is as follows:

- Time frame for parallel run
- Skill transfer mechanism
- Requirement
- Reverse Transition Plan

Reverse Transition Services are the services provided by selected bidder to Company during the reverse transition period which will start after completion of the three (3) months' notice period to facilitate an orderly transfer of the Services to Company or to an alternative third partly service provider nominated by Company. Where Company elects to transfer responsibility for service delivery to multiple Bidders, Company will nominate a services provider who will be responsible for all dealings with such Bidders regarding the delivery of Reverse Transition Services.

The Reverse Transition Services, to be provided by the selected bidder to the Company shall include the following:

7.5.4 Data Migration

The selected Bidder will assist the company in migration exercise without any cost to the company.

7.5.5 Knowledge Transfer

The selected bidder shall provide such necessary information, documentation to the Company or its assignee, for the effective management and maintenance of the deliverables under this RFP. Selected bidder shall provide documentation (in English) in electronic form of all existing procedures, policies and programs required to support the services. Such documentation will be subject to the limitations imposed by selected bidder's Intellectual Property Rights of this RFP and shall include:

- Operational work instructions
- Listing of all events being monitored and the monitoring frequency
- Listing of all third (3rd) party vendors those have been directly related to the provision of the Services and that may be the subject of a request by Company or the replacement service provider for assignment, cancellation or renovation

All trainings that the Company feels are necessary to be imparted to the Company or its designees' personnel, the same shall be scoped and reasonably charged additionally.

7.5.6 Warranties

- All the warranties held by or in the name of the selected bidder shall be assigned or transferred "As Is" in the name of the Company. The selected bidder shall execute any and all such documents as may be necessary in this regard.
- The parties shall return confidential information and will sign-off and acknowledge the return of such confidential information.
- Selected bidder shall provide all other services as may be agreed to by the parties in connection with the reverse transition services. However, in case any other services, in addition to the above are needed, the same shall be scoped and reasonably priced. Reverse transition services shall be charged based on selected bidder's then current time and materials rates.
- The selected bidder recognizes that considering the enormity of the assignment, the transition services listed herein are only indicative in nature and the selected bidder agrees to provide all assistance and services required for fully and effectively transitioning the services provided by the selected bidder under this tender and subsequent agreement, upon termination or expiration thereof, for any reason whatsoever.

7.7 Compliance with Laws

- Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify the Company about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Company and its employees / officers / staff / personnel / representatives / agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.
- Compliance in obtaining approvals/permissions/licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Company and its employees/officers/staff/personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Company will give notice of any such claim or demand of liability within reasonable time to the Bidder.
- The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would cover damages, loss or liabilities suffered by the Company arising out of claims made by its customers and/or regulatory authorities.

7.8Assignment

- The selected bidder agrees that the selected bidder shall not be entitled to assign any or all of its rights and/or obligations under this tender and subsequent agreement to any entity including selected Bidder's affiliate without the prior written consent of the Company.

- If the Company undergoes a merger, amalgamation, takeover, consolidation, reconstruction, change of ownership, etc., this RFP/contract shall be considered to be assigned to the new entity and such an act shall not affect the rights of the Company and the Bidder under this RFP.

7.9 Transportation and Insurance

All the costs should include cost, insurance and freight (c.i.f). However, the selected bidder has the option to use transportation and insurance cover from any eligible source.

7.10 Inspection of Records

All records of bidder with respect to any matters covered by this RFP shall be made available to the Company or its designees at any time during normal business hours, as often as the Company deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. Company would execute confidentiality agreement with the Bidder, provided that the auditors would be permitted to submit their findings to the Company, which would be used by the Company. The cost of the audit will be borne by the Company. The scope of such audit would be limited to Service Levels being covered under this RFP and subsequent contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities. The Bidder's records and sites managed for the Company shall also be subject to Regulator/Company inspection.

7.11 Publicity

The Bidder shall not make any press releases or statements of any kind including advertising using the name or any service marks or trademarks of the Company regarding the contract or the transactions contemplated hereunder without the explicit written permission of the Company. The Bidder shall not, use the Company's name as a reference, without the express written permission of the Company first being obtained, and then only strictly in accordance with any limitations imposed in connection with providing such consent. The Company agrees not to use the Bidder's trade or service marks without the Bidder's prior written consent.

7.12 Solicitation of Employees

During the term of the Contract and for a period of two years after any expiration of the contract period/termination or cancellation of the Contract, both the parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and two year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and two years thereafter, neither party will cause nor permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party.

The above restriction would not apply to either party for hiring such key personnel who

- initiate discussions regarding such employment without any direct or indirect solicitation by the other party; or
- respond to any public advertisement placed by either party or its affiliates in a publication of general circulation

7.13 Visitorial Rights

The Company and its authorized representatives, including any regulator shall have the right to visit any of the vendor's premises without prior Request for Proposal - Selection of notice to ensure that data provided by the Company is not misused. The selected bidder shall cooperate with the authorized representative/s of the Company and shall provide all information/ documents required by the Company.

7.14 Monitoring and Audit

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 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.

7.15 Guarantees

- Bidder shall guarantee that the software and allied components used to service the Company are licensed and legal. All hardware and software must be supplied with their original and complete printed documentation.
- The Bidder also undertakes to keep all the licenses in force till the expiry of the contract period by renewing them as and when necessary.

7.16 Force Majeure

- The Selected Bidder 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.
- For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Selected Bidder and not involving the Selected Bidder's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.

- Unless otherwise directed by the Company in writing, the Selected Bidder shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
- 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 delay continues beyond a period of three months, the Company and the Selected Bidder shall hold consultations in an endeavour to find a solution to the problem.
- Notwithstanding above, the decision of the Company shall be final and binding on the Selected Bidder.

7.17 Resolution of Disputes

- The Company and the selected bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project managers of the Company and the selected bidder, any disagreement or dispute arising between them under or in connection with the contract.
- If the Company project manager and Empanelled bidder's project manager are unable to resolve the dispute after thirty days from the commencement of such informal negotiations, they shall immediately escalate the dispute to the senior authorized personnel designated by the selected bidder and Company respectively.
- If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the selected bidder and Company, the Company and the selected bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration.

7.18 Arbitration

- Any dispute, controversy or claims arising out of or relating to this RFP, its validity, breach or termination thereof, shall be settled by arbitration in accordance with the provisions of the Indian Arbitration and Conciliation Act, 1996.

- All questions, claims, disputes or differences arising under and out of, or in connection with the RFP/ subsequent contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the RFP/ subsequent contract shall be referred to arbitration by a sole Arbitrator to be appointed by the Company.
- The place of arbitration shall be at Mumbai.
- The arbitral procedure shall be conducted in the English, and any award or awards shall be rendered in English. The procedural law of the arbitration shall be the Indian law.
- The award of the arbitrator shall be final and conclusive and binding upon the Parties, and the Parties shall be entitled (but not obliged) to enter judgment thereon in any one or more of the highest courts having jurisdiction. The Parties further agree that such enforcement shall be subject to the provisions of the Indian Arbitration and Conciliation Act, 1996 and neither Party shall seek to resist the enforcement of any award in India on the basis that award is not subject to such provisions.
- The rights and obligations of the Parties under or pursuant to this Clause, including the arbitration clause in this RFP, shall be under the exclusive jurisdiction of the courts located at Mumbai only.
- If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be first transmitted by facsimile transmission by postage prepaid registered post with acknowledgement due or by a reputed courier service, in the manner as elected by the Party giving such notice. All notices shall be deemed to have been validly given on (i) the business date immediately after the date of transmission with confirmed answer back, if transmitted by facsimile transmission, or (ii) the expiry of five days after posting if sent by registered post with A.D., or (iii) the business date of receipt, if sent by courier.

7.19 Governing Law and Jurisdiction

This RFP and subsequent agreement with the Selected Bidders shall be governed and construed in accordance with the laws of India and courts in Mumbai will have the exclusive jurisdiction to determine the issues arising out of this RFP.

7.20 Corrupt and Fraudulent practice

- As per Central Vigilance Commission (CVC) directives, it is required that Bidders observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of this policy.
- “Corrupt Practice” means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
- “Fraudulent Practice” means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Company and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Company of the benefits of free and open competition.
- The Company reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
- The Company reserves the right to declare a Bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract.
- The successful bidder will be required to enter into an integrity pact with the Company as per the CVC guidelines. The integrity pact is available on the CVC website.

7.21 Waiver

No failure or delay on the part of either party relating to the exercise of any right, power, privilege or remedy provided under this RFP or subsequent agreement/contract with the other party shall operate as a waiver of such right, power, privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right, power, privilege or remedy preclude any other or further exercise of such or any other right, power, privilege or remedy provided in this RFP all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

7.22 Violation of Terms

The Company clarifies that the Company shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the bidders from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Company may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

7.23 Addition/Deletion of Qualified Offerings

- Both parties agree that the intent of this RFP is to establish an initial set of service offerings. The Company recognizes that, as the use of these services expands, it is possible that additional services and/or service categories will be needed. In addition, the Company recognizes that from time to time, hardware and software products that are provided as part of selected bidder’s services will be upgraded or replaced as technology evolve. Replacement and/or supplemental hardware and software products that meet or exceed the minimum proposal requirements may be added with the prior approval of the Company. For this purpose, a Change Order Procedure will be followed. Company may request a change order in the event of actual or anticipated change(s) to the agreed scope of work, services, deliverables and schedules. The selected bidder shall prepare a change order reflecting the actual or anticipated change(s) including the impact on deliverables schedule. The selected bidder shall carry out such services as required by the Company. The terms of the contract would apply to such incremental deliverables and services.
- The selected bidder shall agree that the price for incremental offering cannot exceed the original proposed cost, and the Company reserves the right to re-negotiate the price. At the unit rates provided for TCO calculations, the

Company has the right to order as much as it wants at those rates. However, this excludes the hardware to be provided by the Bidder at their cost due to under sizing.

- The Company is under no obligation to honour such requests to add service categories or amend this contract.
- As a method for reviewing selected bidder's services and Company requirements, the Company will sponsor regular reviews to allow an exchange of requirements and opportunities.
- All quantities mentioned in this RFP are indicative. The quantities of components to be procured as part of this RFP can be varied by the Company. This also includes the right to modify the number of source systems, targets, reports & statements, dash boards, score cards, concurrent users etc.

7.24 Master Service Agreement and Non-Disclosure Agreement

The selected vendor shall execute:

- Master Service Agreement (MSA), which must include all the services and terms and conditions of the services (SLA) to be extended as detailed herein, and as may be prescribed or recommended by the Company
- Non-Disclosure Agreement (NDA), the selected vendor shall execute the NDA within two months the date of acceptance of letter of appointment or as intimated by the Company.
- The stamp duty or any other associated charges to execute the above-mentioned document shall be borne by the successful bidder.

7.25 Liquidated Damages

- Company expects that the selected bidder completes the scope of the project as mentioned in section 2.9 and 2.10 – within Project timeline committed by the bidder. Inability of the selected bidder to either provide the requirements as per the scope or to meet the committed timelines would be treated as breach of contract and would invoke the penalty clause. The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. Company at its discretion may apply this rule to any major nondelivery, non-adherence, non-conformity, non-submission of agreed or mandatory documents as part of the Project.

- Thereafter, at the discretion of the Company, the contract may be cancelled. Company also has the right to invoke the Performance Guarantee, Penalty Clause on delay which is not attributable to Company and is attributable to the selected Bidder.
- Inability of the selected bidder to provide services at the service levels defined would result in breach of contract and would invoke the clause.
- Notwithstanding anything contained above, no such penalty will be chargeable on the selected bidder for the inability occasioned, if such inability is due to reasons entirely attributable to Company.

7.26 Set Off

Without prejudice to other rights and remedies available to the company it shall be entitled to earmark, set off or adjust any amounts due to the company, under any clause of the RFP, from the selected bidder Provider against payments due and payable by the company to the selected bidder/Service Provider for the services rendered.

The provisions of this Clause shall override all other clauses and shall survive the termination of this Agreement.

7.27 Information Ownership

All information processed, stored, or transmitted by equipment belongs to the Company. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

ISMS Framework (latest): The selected bidder and the team shall abide by the ISMS framework of the Company which includes Incident Management, Change Management, Capacity Management, Configuration Management etc.

7.28 Sensitive Information

Any information considered sensitive must be protected by the selected bidder from unauthorized disclosure, modification or access.

Types of sensitive information that will be found on Company's systems the selected bidder may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

7.29 Privacy and Security Safeguards

The selected bidder shall not publish or disclose in any manner, without the Company's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Company location. The selected bidder shall develop procedures, and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all Company data and sensitive application software& data. The selected bidder shall also ensure that all sub-contractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Company's prior written consent, the details of any security safeguards designed, developed, or implemented by the selected bidder under this contract or existing at any Company location.

7.30 Confidentiality

- "Confidential Information" means any and all information that is or has been received by the selected bidder ("Receiving Party") from the Company ("Disclosing Party") and that relates to the Disclosing Party; and is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.
- Without limiting the generality of the foregoing, Confidential Information shall

mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials relating to the licensed software, the modules, the program documentation, the source codes, the object codes and all enhancements and updates, services, systems processes, ideas, concepts, formulas, methods, know how, trade secrets, designs, research, inventions , techniques, processes, algorithms, schematics, testing procedures, software design and architecture, computer code, internal documentation, design and function specifications, product requirements, problem reports, analysis and performance information, business affairs, projects, technology, finances (including revenue projections, cost summaries, pricing formula), clientele, markets, marketing and sales programs, client and customer data, appraisal mechanisms, planning processes, etc. or any existing or future plans, forecasts or strategies in respect thereof.

- "Confidential Materials" shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes, whether machine or user readable. Information disclosed pursuant to this clause will be subject to confidentiality forever.
- Nothing contained in this clause shall limit the selected bidder from providing similar services to any third parties or reusing the skills, know-how and experience gained by the employees in providing the services contemplated under this clause, provided further that the selected bidder shall at no point use the Company's confidential information or Intellectual property.
- The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not use the Company's confidential information or IPR, without obtaining the written consent of the Company.

7.31 Disclosing Party

The Disclosing Party shall disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, company or any other entity other than its directors, partners, advisers, agents or employees, sub-contractors and contractors who need to know the same for the purposes of maintaining and supporting the solution provided as a part of the RFP/ Contract. The Receiving Party shall be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees, sub-contractors and contractors is in accordance with the terms and conditions and requirements of this RFP; or

- Unless otherwise agreed herein, use of any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.
- In maintaining confidentiality hereunder, the Receiving Party on receiving the Confidential Information and materials agrees and warrants that it shall:

a. Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure

b. Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party

c. Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub- contractors and contractors so involved to protect the Confidential Information and materials in the manner prescribed in this document.

d. Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such information and materials, in whatsoever form, including any and all copies thereof

- The Receiving Party who receives the Confidential Information and Materials agrees that on receipt of a written demand from the Disclosing Party, immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control
- To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party
- So far as it is practicable to do so, immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control
- To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries, the requirements of this paragraph have been fully complied with
- The rights in and to the data/information residing at the Company's premises, even in the event of disputes shall at all times solely vest with the Company
- The Bidder represents and agrees that during the term of this RFP and subsequent contract, the Company shall not be responsible for any loss/damage (including malfunctioning or non-functioning of Deliverables) caused to the Deliverables for any reason, unless such loss/damage (including malfunctioning or non-functioning of Deliverables) is caused due to the wilful act or gross wilful misconduct of the Company or any of its personnel as certified jointly by the Company and Selected bidder. In such an event, the selected bidder shall promptly repair and/or replace the non-performing Deliverable with a suitable replacement, if required, without affecting the service level standards in this RFP.
- The restrictions in the preceding clause shall not apply to:

a. Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same

b. Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

- The Confidential Information and Materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document or subsequent agreement
- Confidential Information is any and all proprietary information disclosed by one party to the other. Confidential Information does not include information that is or becomes available to the recipient prior to the party providing such information or is public information in accordance with the applicable laws. Software in human-readable form (e.g. source code) and the Company’s data values stored in computers will be considered Confidential Information whether or not marked as such.
- The selected bidder shall also undertake to keep confidential all information (written or oral) concerning all facts of the business of the Company, which has been obtained or understood during the course of the assignment.
- The confidentiality obligations shall survive the expiry or termination of the agreement/contract between the Selected Bidder and the Company.

7.32 Technological Advancements

The selected bidder shall take reasonable and suitable action, taking into account economic circumstances, at mutually agreed increase/decrease in charges, and the Service Levels, to provide the Services to the Company at a technological level that will enable the Company to take advantage of technological advancement in the industry from time to time.

7.33 Intellectual Property Rights

- The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables upon the terms and conditions contained in this RFP. The Company agrees and acknowledges that except as expressly provided in this RFP, all Intellectual Property Rights in relation to the Software and Documentation and any adaptations, translations and derivative works thereof whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the Bidder during, in connection with or in relation to fulfilling its obligations under this RFP belong to and shall remain a property of the Bidder.
- During the term of this project and, if applicable, during the Reverse Transition Period, Company grants selected bidder a right to use at no cost or charge the Software licensed to the Company, solely for the purpose of providing the Services.
- The selected bidder shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Software used by the selected bidder in performing its obligations under this project. The selected bidder shall also be responsible for renewal of all such licenses from time to time during the contract period. The Bidder shall quote for all such renewals in the commercial bid and in case the Bidder fails to quote for renewal of any licenses in the bid, the selected bidder shall renew such licenses at their cost, and the Company shall not pay for other than the commercials mentioned in the price bid.
- The selected bidder shall under no circumstances, allow any associated license to expire and allow any associated software to be out of support during the contract period. If a third party's claim endangers or disrupts the Company’s use

of the Software, the Bidder shall at no further expense, charge, fees or costs to the Company, (i) obtain a license so that the Company may continue use of the Software in accordance with the terms of this tender and subsequent Agreement and the license agreement; or (ii) modify the Software without affecting the functionality of the solution in any manner so as to avoid the infringement; or (iii) replace the solution with a compatible, functionally equivalent and non-infringing product.

7.34 Grievance Redressal

Any vendor who claims to have a grievance against a decision or action with regards to the provisions of this RFP may file a request to IT department at itadmin@gichf.com. It may please be noted that the grievance can be filed by only that vendor who has participated in Procurement proceedings in accordance with the provisions of this RFP.

8. Appendix 1

Bill of Materials

S.No	**Items**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Amount**	**Total Cost Excluding Taxes (INR)**
a.	Perpetual Corporate License, unlimited Users	**X**	**X**	**X**	**X**	**X**		
b.	One time cost of gap analysis, customization, implementation, deployment, testing to achieve RFP requirements	X	X	X	X	X		
c.	AMC + ATS costs							
d.	Other costs (please specify)							
e.	Cost of for Change Requests of 50-man days each year (Statutory / Regulatory changes will be at no extra cost)							
	TOTAL COST OF OWNERSHIP (TCO)							

Note: 50-man days per year for change requests on software / security solutions has been given to compare prices. Payment will be made at actuals at the rates per man day as per the quotes under item e above.