GIC HOUSING FINANCE LTD.

REQUEST FOR PROPOSAL

FOR

IMPLEMENTATION OF MICROSOFT O365 / M365 LICENSES

ENTERPRISE FEATURES AND MANAGED SERVICES

FOR 5 YEARS PERIOD

RFP Reference Number:REF:GICHF:2024-25/06

Dt. 15-05-2024

ACTIVITY SCHEDULE

S.NO.	ACTIVITY	DETAILS
1	Release of RFP	**15th May, 2024**
2	Address for Receipt/Submission of Bid document	GIC HOUSING FINANCE LTD National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020.
3	Bid Submission	Sealed - Technical & Commercial Bids in Hard Copy only.
4	Last Date & Time for submission	**23nd May, 2024** **13:00 hrs**
5	Bid Opening Date & Venue	**24rd May, 2024** (To be opened and evaluated internally at GICHFL Head Office).
6	Contact Details	• **B Ramanathan** Group Executive Ph:9892313811 • **Manish Abhishek** Executive | IT Ph:7739215866
7	E-mail ID's	ram@gichf.com manish.abhishek@gichf.com

About GIC Housing Finance Ltd:

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

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

Objective of RFP:-

GICHFL has lately upgraded to Microsoft O365 E1 PLUS & M365 E3 LICENSES from O365 EOP2, E1 and E3 licenses. We were earlier limited to only mailing solutions and had implementation of only rudimentary configurations and policies. Warrying to the rabid spreading of Phishing, Scams, fraud malpractices etc. have propelled us to take a hop and get accustomed set of rules and policies which will give us an edge and enable GICHFL compliant and less susceptible to ongoing fraudulent pursuits overlaid in every strata of online campaigns in modern workforce. The foremost idea to deploy EDR, MDM/MAM/Patch/Asset management is to enhance cybersecurity posture by stationing advanced threat detection and response system across our endpoints, thereby mitigating risks and safeguarding sensitive data and assets.

MINIMUM ELIGIBILITY CRITERIA FOR BIDDER TO PARTICIPATE IN THE TENDER

- In order to qualify for bid, bidder should satisfy following eligibility criteria. Following format to be filled by the bidder and must submit in Envelope A in its order along with relevant documentary proof.

Sr. No	Specific Requirement	Documents Required	Bidder's Response along with details of supportingdocuments
1.	The bidder must be a Company/LLP/Partnership Firm incorporated in India and registered under the Companies Act 2013 or LimitedLiability Partnership Act 2008 or Partnership Act 1932 as applicable and must have a registered office in India for atleast 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 taxesregistration certificates /PAN etc.	An undertaking to be submitted along with copy ofPan card and GST Registration certificate	
3.	The bidder should be ISO27001:2013/2022 certified.	Copy of a valid certificate should be attached	
4.	The Bidder should have experience in implementing and managing EDR & MDM Solution in at least two Financial Institution / NBFC / Public Sector Bank /Government Organization / Large Corporates in India not older than 3 years.	An undertaking from the vendor on the company letter head or a document certifying the same is to be produced with clients list attached.	

1. MICROSOFT O365 LICENSE IMPLEMENTATION & MANAGED SERVICES.

➢ SCOPE OF WORK :-

- **Business Scenario**

The understanding of the current environment is summarized as follows:

- Around 925 users in the organization
- Using O365 E1+, M365 E3, MDO P1 and MDE P2 licenses
- Devices are Active Directory domain joined (On-Premise model hosted with Azure)
- When a user is created in On-premise model AD, simultaneously same user should be created in M365 and license to be assigned. UPN ID and Email ID are same
- AD identities are not synced to cloud identities
- Using ADFS to authenticate against apps hosted on Azure

➢ Business Needs and Proposed Solution

- GICHF requires Single Sign On (SSO) solution to M365 resources and manage user identities in Active Directory Implementing features and capabilities of O365 E1+, M365 E3, MDO P1 and MDE P2 licenses and Co-Pilot Add-on for the users.

➢ Service Deliverables

The key service deliverables will be as follows:

- Service delivery as per scope provided.
- Installation Guide / Manual.
- Knowledge transfer Support along with document throughout the engagement

- Active issues and risks must be monitored and reassessed on a weekly basis. Mutually agreed upon issue escalation and risk management processes will be defined at the outset of the project.

➢ M365 E1 Plus and E3 Features, with Defender for Office 365 Plan 1 & Defender for Endpoint Plan2

- **Technical Scope of Work and Effort estimate**

- **Environment Analysis**
  - Study of current Network Infrastructure
  - Requirement Study – Software and Hardware
  - Study of IS policy implementation.
  - Study of dependencies with respect to domains
  - Risk Analysis
- **Implementation Phase**
  - Identification of business requirement based.
  - Implement identity and access management
  - Implementation of Conditional Access Policies
  - Implementation of Intune

- Implementation of Information Protection
- Implementation of Data Loss Prevention
- Implementation of Defender for Endpoint Plan 2
- Implementation of Defender for Office 365 Plan 1

- **Analyzing current setup of GICHFL**
  - Study of present M365 tenant
  - Verifying and adding necessary DNS records in the public DNS
  - Assigning required license for the users.

➢ **Protecting your Identities**

- **Configuration of Entra ID (Azure AD)**
  - Setting up automatic enrollment for Windows devices
  - Configure Hybrid Entra ID join for Active Directory domain-joined device
  - Configuring self-service password reset for end users.
  - Configure company branding to provide a consistent look-and-feel on your orgs sign-in pages

➢ **Configuration of Microsoft Entra ID Connect to sync existing AD user identities to Microsoft Entra ID (Azure AD)**

- **Pilot Phase:**
  - Create and update user attributes in on - premise to match the user attributes in Entra ID.
  - Prepare environment to install Entra Connect on one of the member Windows Server which meets the prerequisites.
  - Configure Entra Connect as per best practise.
  - Configure latest version password hash synchronization / Pass Through highly secured Authentication.
  - Validation of user sign-ins in hybrid setup.
  - Test SSO functionality.
  - End users must be able to sign in with synchronized password.

- **Production Phase:**
  - Create and update user attributes in on-premise AD to match the user attributes in Entra ID
  - Validation of user sign-ins in hybrid setup.
  - End users must be able to sign in with synchronized password.
  - Test SSO functionality.

➢ **Configuration of Entra ID Conditional access (CA) policies**

- Configure CA policy to challenge for Multi Factor Authentication (MFA) while accessing Office 365 services with no limitations.
- Configure CA policy to allow only Intune approved clients from mobile devices to connect M365 services with no limitations.
- Configure CA policy to block legacy authentication clients to access Microsoft services with no limitations.
- Configure access to Office 365 services only from devices that are Intune Compliant.

- **Threat Management**

- **Configuration of Microsoft Defender for Office 365 (Plan 1) and Exchange Online Protection as per best practices**

  - Configuring antimalware, anti-spyware, phishing, threat hunting policies, etc.
  - Configuring inbound and outbound spam filters
  - Configuring Safe Attachment Policies with size limitations, etc.
  - Configuring Sate Link Policies
  - Configuring Safe Attachments for SharePoint, OneDrive, and Teams for both internal and external users.
  - Configuring advanced anti-phishing protection
  - Overview on real-time detections
  - Monitoring and Reporting with the Weekly progressive updates on the Defender for Office 365 Services.

- **Govern and protect GICHFL data**

  Configuration of Sensitivity labels

  - Activate and configure GICHFL tenant for Unified Labelling
  - Create sensitivity labels and policies
  - Monitor activities on shared data

- **Configuration of Data Loss Prevention (for Exchange Online)**

  - Understand the sensitive information types to be protected from leakage
  - Create and test the DLP policy based on the sensitive information type (SIT) available.
  - Configure, test and fine tune the rules based on the auditing results with no limitations in count of policies.
  - Deploy the DLP policies to the pilot users
  - Test and validate the above DLP policies configured

- **CoPilot Configuration and Implementation:**

- Configuration of Microsoft 365 Co-Pilot

- **Promote Co-Pilot Features to Users.**

- Develop a communication plan to inform and aware users about Co-Pilot and its benefits.

- **Assign License to GICHFL Users.**

- Selected users who will be using Co-Pilot and assigning licenses to them.
- Verify that each user has the correct level of access and permissions aligned with their role and requirements for Co-Pilot usage.

- **Support Service Deliverables:**

- 24/7 Alert monitoring and Investigation

- Remote Support for incidents
- Proactive Protection
- Email & Telephone support.
- Reactive support for incidents with Microsoft Premier support
- Monthly Review with SOC Analyst
- Weekly/Monthly health check Report
- Review and analyze alerts, incidents, and threats using the Microsoft Security Portal.
- Minimize the impact of adverse events and expedite remediation configuration.
- Achieve situational awareness of current threats and compliance statutes and automate monitoring and enforcement of security controls.
- Continually measure and improve the processes ensure to investigate the posture of cloud workloads and recommend best practices.
- Reactive support for incidents and leverages Microsoft premier support wherever required.
- Bidder will regularly share cyber advisories and implement them on the Microsoft platform in real-time.
- Managed service for MDM is to be provided for all end users at GICHFL.
- Reporting: Service Provider will provide periodic and on-demand reports of Server assets under management as part of account review sessions or as requested by Client. This reporting capability includes detailed hardware and software asset information, hardware warranty reports, performance monitoring data, and software licensing details. Service Provider can also accommodate specific custom reporting of available data as requested by Client.
- Reporting on latest features / upgrades of the Microsoft Products for further improvisation.

➢ **Service Level Definitions**

The following general responsibilities under this Agreement:

- The SOC Engineer should monitor incidents and all information obtained from the customer that is required to establish a Service Request, including contact information, problem description, and documentation of the Customer’s environment (as applicable).
- The SOC Engineer should attempt to resolve incidents when received from the support.
- The SOC Engineer/Tech Support Engineer must escalate a Support Request to the next level creating the incidents with Microsoft Premier support upon approach of established resolution targets.
- The SOC Engineer will notify the Customer upon completion of a Service Request and shall allow the Customer to submit questions or concerns related to the Service Request before the Service Request is deemed fulfilled and closed.

1.1 MOBILE DEVICE MANAGEMENT (MDM)

- **Configuration of Intune MDM**

  - Configure MDM authority for M365 tenant.
  - Configuring Intune Mobile Application Management policies for Android and iOS devices like
  - Restrict copy/paste from corporate data to personal apps
  - Enforce encryption for data used within Managed application.
  - Allow data transfer from unmanaged Application to Managed application
  - Enforce strong authentication / Passcode when using Managed application.
  - Fingerprint to authenticate access to Managed application.
  - Restrict saving files to Local storage.
  - Allow storing files only to corporate One drive or SharePoint.
  - Restrict web transfer content only with browser
  - Disable access to Jailbroken/Rooted Devices

- **Configuration of Intune MDM for managing Windows, Mac OS devices**

Configuring Mobile Device Management MDM) authority, based on GICHFL management needs, including:

- Setting Intune as MDM authority
- Configuring tests groups to be used to validate MDM management policies.
- Setting up Intune roles (Help desk operator, admins, etc.)
- Enforce restrictions such as only Compliance devices can access the Office 365 resources.
- Enforce Minimum OS requirements to access corporate data.
- Setting up Windows Update for Business and DDM for MacOS
- Apply features and settings on GICHFL devices using device profiles
- Use the settings catalog to configure settings
- Manage endpoint security in Microsoft Intune

- **Qualification for the L1 Support staff for Managed Services of MDM**

Sr. No.	**Category**	**Qualification**
1.	**Education**	1. A bachelor's degree in computer science, information technology, or a related field can provide a good foundation for support staff.
2.	**Microsoft Certifications**	• Microsoft Certified: Modern Desktop Administrator Associate • Microsoft Certified: Security, Compliance, and Identity Fundamentals • Microsoft Certified: Enterprise Administrator Expert (relevant for broader Microsoft 365 services, including MDM)
3.	**Experience**	• Should have experience working with Microsoft MDM solutions, such as Microsoft Intune and Microsoft Endpoint Manager. • Experience in deploying and managing MDM policies, device enrollment, application management, and security features is highly beneficial.

Managed Services for Microsoft MDM might include but not limited to:

i. **Deployment and Configuration**: Assistance with initial setup, configuration, and deployment of Microsoft MDM solutions tailored to the organization's needs and requirements.

ii. **Policy Management**: Developing and implementing device management policies, including security policies, compliance rules, and application management policies, to ensure devices adhere to organizational standards and regulatory requirements.

iii. **Device Enrollment**: Managing the enrollment process for devices, which may involve on-boarding new devices, provisioning user accounts, and configuring device settings for seamless integration with the organization's infrastructure.

iv. **Monitoring and Maintenance**: Continuous monitoring of devices and MDM infrastructure to detect and address issues promptly. This includes monitoring device health, security compliance, and performance metrics.

v. **Patch Management and Updates**: Ensuring that devices receive timely patches, updates, and security fixes to mitigate vulnerabilities and protect against emerging threats.

vi. **User Support**: Providing end-user support for device management-related issues, such as troubleshooting connectivity problems, resolving configuration issues, and assisting with device setup and usage.

vii. **Reporting and Analytics**: Generating reports and analyzing data on device usage, compliance status, security incidents, and other relevant metrics to assess the effectiveness of MDM policies and identify areas for improvement.

viii. **Security and Compliance**: Implementing security best practices and compliance measures to safeguard sensitive data, prevent unauthorized access, and maintain regulatory compliance.

ix. **Training and Documentation**: Offering training sessions and creating documentation to educate administrators and end-users on MDM best practices, security guidelines, and proper device usage policies.

2. ENDPOINT DETECTION AND RESPONSE (EDR) SOLUTION

i. SCOPE OF WORK:

Scope of work for management and implementation of proposed EDR solution includes but is not limited to:

a. Planning and Deployment:

- Plan and execute the deployment of the proposed EDR solution across all endpoints on all locations covering GICHFLs Headquarter (HO), branches and hubs (approx. 78 locations) following industry best practices and OEM recommendations. Onsite resource will be required in GICHFLs HO for planning, co-ordinating and deployment of EDR solution. Resource can plan and deploy the agents in GICHFL branches and hubs from GICHFL HO.
- Configure and optimize the EDR solution to maximize threat detection capabilities while minimizing false positives, including but not limited to:
  - Fine-tuning detection rules and policies.
  - Customizing alert thresholds and escalation levels.
  - Implementing behavioural analysis and machine learning models.
- Conduct thorough testing and validation to ensure the stability, reliability, and performance of the deployed solution.
- Provide documentation and knowledge transfer on the deployed solution's architecture, configuration, and operation.

b. Ongoing Support and Maintenance:

- Monitor alerts, anomalies and security events generated by the EDR solution.
- Investigation and analysis of security incidents identified by the EDR solution. Incident response and remediation actions.
- Offer comprehensive technical support and maintenance services to ensure the continued operation and effectiveness of the EDR solution.
- Provide timely assistance and troubleshooting for issues and inquiries related to the EDR solution.
- Define procedures for handling alerts, investigating incidents and containing threats.
- Integrate the EDR system with security tools (SIEM, firewalls, etc.) and O365 / M365 plans.
- Fine-tune policies on timely basis.
- Oversee regular software updates, patches and bug fixes to address security vulnerabilities and performance improvements.
- Monitor the health and performance of the EDR solution, proactively identifying and addressing potential issues.

c. Documentation and Reporting:

- Maintain comprehensive documentation of all aspects of the EDR solution, including:
  - Architecture diagrams, deployment plans, SOPs etc.
  - Configuration settings and policies.
  - Incident response procedures and playbooks.

- Generate regular reports on the performance, efficacy, and findings of the EDR solution, including:
  - Incident trends and analysis.
  - Provide executive summaries for management review.
  - Compliance status and adherence to regulatory requirements.
  - Recommendations for enhancements and improvements.

d. Vendor Relationship Management:

- Serve as the primary point of contact for interactions with the EDR solution OEM.
- Coordinate OEM support, maintenance, and escalation of technical issues or enhancement requests.
- Stay informed about product roadmaps, updates, and new releases, providing guidance and recommendations to the GICHFL on potential opportunities for innovation and improvement.

ii. IMPLEMENTATION OF EDR SOLUTION:

Bidder should provide an on-site resource for successful planning and deployment of the proposed solution across all endpoints on all locations, following industry best practices and OEM recommendations. He would be responsible for:

- Co-ordination with internal stakeholders and OEM for deployment.
- Configure and optimize the EDR solution to maximize threat detection capabilities while minimizing false positives, including but not limited to:
  - Fine-tuning detection rules and policies.
  - Customizing alert thresholds and escalation levels.
  - Implementing behavioural analysis and machine learning models.
- Conduct thorough testing and validation to ensure the stability, reliability, and performance of the deployed solution.
- Provide documentation and knowledge transfer on the deployed solution's architecture, configuration, and operation.

iii. MANAGEMENT OF EDR SOLUTION:

- The selected bidder shall provide remote support on shared resource model to manage the proposed solution with all components and related infrastructure on 24x7x365 basis for all the activities including but not limited to device management, alert and incident management, incident response, threat hunting, solution hardware and software administration, patching, update / upgrade, configuration management, monitoring, integration, fine-tuning and other technical support as required by the GICHFL for EDR solution.
- L2 resource to be provided in General Shift i.e. 9:30 AM to 6:30 PM Monday to Saturday. L1 resource to be provided in other shifts.
- L2 resource should be on payroll of bidder.
- Successful Bidder is expected to assign clearly defined Roles & Responsibilities among deployed resources.
- Bidder must do first level of checking / examine / interview / verification and then recommend the suitability of the resources to GICHFL. GICHFL reserves the right to interview all the professionals to be deployed in the project and reject, if not found suitable. At a later stage also, if any of the professional found unsuitable or incapable or violates any of the GICHFL guidelines GICHFL may ask to remove all such professionals at a short notice.
- Escalation process should be in place for unresolved issues.
- The bidder has to maintain educational qualification and experience requirements of the resources in the project. Any deviation in the educational/qualification of the resources is only under GICHFL discretion.
- The Bidder shall ensure reduction in the overall incidents and false positives thereby improving the cyber security posture of the GICHFL.
- Any incidents shall be notified to the designated stakeholders and resolution of such incidents shall be resolved without any delay.

Following are qualifications and indicative Roles & responsibilities. Roles and Responsibilities including but not limited to the following shall be reviewed from time to time as per the requirement of the GICHFL.

Resource Category	Qualifications	Indicative Roles & Responsibilities
L1	Graduate Engineer in CS or IT or EC/ MCA with minimum 1 year of Experience in XDR / NDR / EDR / Incident Response / Threat Hunting / Forensics solutions. OR	1. Validation of all support cases to ensure technical issues. 2. Manage installation and configuration assistance. 3. Details / Log Information, basic level troubleshooting. 4. To know issues through OEM knowledge base articles.
	BCA / B.Sc.-IT / B.Sc. Computers / Diploma in computer science or Information Technology with minimum 2 years of Experience in XDR / NDR / EDR / Incident Response / Threat Hunting / Forensics solutions. • Trained on Help Desk Operations management. **Desirable -** Certified as XDR / NDR / EDR / Incident Response / Threat Hunting / Forensics solution handling technician.	5. Monitoring the solution and checking the system health on daily basis. 6. Preparation of reports (as per GICHFL's requirement) and submission to concerned officials / department at defined frequency (daily, weekly, fortnightly, monthly, etc.) 7. Handling EDR related calls from end users and trouble shooting. 8. Performing installation and trouble-shooting related tasks for EDR solution and its components. 9. Case logging and problem identification and Level 2 escalation. 10. Overall application availability, health and performance monitoring will be part of the responsibility. Onsite team shall be responsible for application and database administration, daily technical housekeeping activities, patching, update/upgrade, configuration management, monitoring, integration, fine tuning.

L2	Graduate Engineer in CS or IT / MCA with minimum 3 years of Experience in XDR / NDR / EDR / Incident Response / Threat Hunting / Forensics solutions. OR BCA / B.Sc.-IT / B.Sc. Computers / Diploma in computer science or Information Technology with minimum 5 years of Experience in XDR / NDR / EDR / Incident Response / Threat Hunting / Forensics solutions. • Good Knowledge on Linux & Windows operating systems, Databases, Network Management Software and IT technologies. • Having L2 certificate of any reputed XDR / NDR / EDR / Threat Hunting / Forensics product features known as certified security expert.	**1.** Advance or complex installation and configuration. **2.** Follow up of service tickets opened on OEM. Knowledge transfer to Level 1 Engineers. 4. Fault isolation, case diagnosis and troubleshooting, updating operational knowledge base. 5. Any cyber threat / incidents reported from branches/offices should be attended and a suitable solution should be provided and implemented to resolve the issue. 6. All the EDR solution infrastructure (hardware, software, network) are to be kept in up and running condition. 7. Overall application availability, health and performance monitoring will be part of the responsibility. Responsible for daily technical housekeeping activities, patching, update/upgrade, configuration management, integration with other IT/Security solutions, monitoring, integration and fine tuning. 8. Conducting threat hunting activities and proactive remediation / removal of threats to ensure GICHFL's IT infrastructure is protected at all times. 9. Incident Analysis, Investigation including Root cause analysis of alerts / incidents and submission of recommendations / remediation steps.

SERVICE LEVELS:

- SLA for Solution Availability:

Bidder must ensure that solution meets the agreed business requirement. In case of solution failure, Bidder may be liable for penalties and GICHFL may also be entitled to terminate the contract without any liability or obligation.

Sr. No.	**Uptime % calculated on Quarterly basis for each solution**	**Penalty Item wise (% of Quarterly respective Line-item Cost)**
1	**99.999% and above**	**0%**
2	**99.8% to 99.998%**	**7%**
3	**99.7% to 99.8%**	**10%**
4	**99.6% to 99.7%**	**15%**
5	**Below 99.6%**	**20%**

Availability is defined as (%) = (Operation Hours – Notified Planned Downtime) * 100% / (Operation hours)

- Root Cause Analysis (RCA) of any outage incidents should be communicated to GICHFL within 24 hours from the time of occurrence of the incident/issue.

- **Turnaround Time (TAT) for resolution of security Incidents/ Issues:**

Successful bidder should stick to the following turnaround time:

S.No.	Severity	Severity Level	Initial Response	Mitigation / resolution time	Submission of RCA
1	Critical	P1	15 Minutes	2 Hours	48 Hours
2	High	P2	30 Minutes	4 Hours	3 days
3	Medium	P3	60 Minutes	8 Hours	5 days
4	Low	P4	120 minutes	24 hours	1 week

- **The Severity Levels are categorized as below:**

Critical	Critical Impact/System Down. Complete system outage.
High	Significant Impact/Severe downgrade of services.
Medium	Minor impact/Most of the system is functioning properly.
Low	Low Impact/Informational.

Note:

- Start time of the incident/issue will be considered as the time of intimation/ logging of incident/ issue reported by GICHFL or SOC Service Provider or recorded in EDR solution.
- The mitigation time will start after Initial Response Time period only.

SLA Penalty for Non Resolution of security incidents:

		Incident/ issue Restoration SLA **Mitigation time (T)**	**Non-Performance Charges (NPC)**
Sr. No.	**Severity of Incident/ issue**		
1.	**Critical**	>2 Hours and ≤ 4Hours 4% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 10% of total Annual Resource cost. >4 Hours 5% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 15% of total Annual Resource cost	4% 5%
2.	**High**	>4 Hours and ≤ 8Hours 4% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 10% of total Annual Resource cost >8 Hours 5% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 15% of total Annual Resource cost	4% 5%
3.	**Medium**	>8 Hours and ≤ 16 Hours 4% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 10% of total Annual Resource cost >16 Hours 5% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 15% of total Annual Resource cost	4% 5%
4.	**Low**	>24 Hours and ≤ 48 Hours 4% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 10% of total Annual Resource cost >48 Hours 5% of Quarterly charges payable for ResourceCost for respective solution for every incident/issue, Up to 15% of total Annual Resource cost	4% 5%

3. Scope of Work on Patch Management

Scope of Services:

- The selected vendor shall be responsible for delivering a comprehensive range of services, encompassing both the implementation of the patch management solution and the ongoing managed services for its operation. The scope of services includes, but is not limited to, the following:

A. Implementation Phase:

I. Assessment and Planning:

- Conduct a detailed assessment of the Client's existing patch management processes, infrastructure, and security posture.
- Collaborate with key stakeholders to define objectives, requirements, and success criteria for the patch management solution.
- Develop a comprehensive implementation plan, including timelines, milestones, resource requirements, and risk mitigation strategies.

II. Solution Design and Configuration:

- Design a robust and scalable patch management solution tailored to the Client's specific needs, environment, and compliance requirements.
- Configure patch management tools, systems, and workflows to align with industry best practices and organizational policies.
- Implement integration with existing IT systems, security controls, and monitoring platforms to ensure seamless operation and visibility.

III. Testing and Validation:

- Establish a dedicated testing environment to validate the functionality, performance, and security of the patch management solution.
- Conduct thorough testing of patch deployment processes, rollback mechanisms, and failover procedures to ensure reliability and resilience.
- Collaborate with internal IT teams to conduct user acceptance testing (UAT) and address any identified issues or concerns.

IV. Training and Knowledge Transfer:

- Provide comprehensive training sessions and workshops for internal IT staff to familiarize them with the patch management solution's features, capabilities, and best practices.
- Develop user guides, documentation, and knowledge base materials to support ongoing usage, troubleshooting, and optimization.
- Facilitate knowledge transfer sessions to empower IT personnel with the skills and expertise required to effectively manage and maintain the patch management solution.

B. Managed Services Phase for Patch Management

I. Patch Identification and Prioritization:

- Utilize advanced scanning and vulnerability assessment tools to identify missing patches, security vulnerabilities, and compliance gaps across all relevant systems and applications.
- Prioritize patches based on severity, criticality, and potential impact on business operations, security posture, and regulatory compliance.
- Maintain a comprehensive inventory of software and hardware assets to facilitate accurate patch

identification and prioritization.

II. Patch Deployment and Configurations:

- Implement the deployment of approved patches across servers, workstations, and endpoints using the configured patch management solution.
- Implement scheduling, dependency management, and rollback mechanisms to minimize risks and optimize efficiency.
- Ensure seamless integration with existing change management processes and tools to facilitate controlled and auditable patch deployments.
- The bidder shall design Patching Calendar for every year in accordance with the GICHFL Holiday calendar.

III. Monitoring and Alerting:

- Continuously monitor patching activities, system health, and performance indicators to proactively identify issues and anomalies.
- Configure real-time alerts and notifications for critical events, such as failed patch deployments, compliance violations, and security breaches.
- Implement proactive remediation measures and automated workflows to address common issues and prevent service disruptions.

IV. Vulnerability Management:

- Conduct regular vulnerability scans and assessments to identify emerging threats, zero-day vulnerabilities, and configuration weaknesses.
- Analyze scan results and prioritize remediation actions based on risk severity, exploitability, and business impact.
- Collaborate with internal security teams to develop and implement effective mitigation strategies, including patching, configuration changes, and compensating controls.

V. Compliance Management:

- Ensure adherence to regulatory requirements, industry standards, and internal policies governing patch management, cybersecurity, and data protection.
- Conduct periodic compliance assessments and audits to validate patching practices, documentation, and reporting capabilities.
- Generate compliance reports and attestations for stakeholders, auditors, and regulatory authorities as needed.

VI. Performance Optimization:

- Continuously monitor and optimize the performance of the patch management solution, including server resources, database queries, and network bandwidth.
- Implement tuning and optimization strategies to improve patch deployment speed, reliability, and scalability.
  Conduct regular reviews and capacity planning exercises to accommodate growth, seasonal fluctuations, and evolving business needs.

VII. Risk Management and Incident Response:

- Assess patch-related risks and vulnerabilities across the IT environment, including third-party software, cloud services, and IoT devices.
- Develop and maintain a risk register to track identified risks, their likelihood, potential impact, and mitigation strategies.
- Establish incident response procedures and playbooks to guide the timely detection, containment, investigation, and resolution of patch-related incidents.

VIII. Continuous Improvement:

- Facilitate regular service reviews and performance evaluations to assess the effectiveness of patch management activities and service delivery.
- Solicit feedback from stakeholders, end-users, and IT personnel to identify opportunities for improvement, innovation, and service enhancement.
- Implement a formalized process for capturing lessons learned, best practices, and success stories to inform future initiatives and decision-making.

IX. Knowledge Management and Training:

- Develop and maintain a centralized knowledge base containing articles, FAQs, troubleshooting guides, and best practices related to patch management.
- Conduct training sessions, workshops, and webinars for IT staff, system administrators, and end-users to increase awareness and proficiency in patching processes and tools.
- Foster a culture of continuous learning and skill development by providing access to relevant training resources, certification programs, and professional development opportunities.

X. Documentation and Reporting:

- Maintain accurate documentation of patch management processes, procedures, configurations, and operational workflows.
- Generate comprehensive reports and dashboards to provide stakeholders with visibility into patching activities, compliance status, performance metrics, and key performance indicators (KPIs).
- Customize reporting formats and frequency based on stakeholder preferences and requirements, ensuring timely and actionable insights are available to support decision-making.

C. Educational Qualification required for L2 Support staff for Patch Management

Sr. No	Category	
1.	**Educational Background**	• A bachelor's degree in computer science, information technology, or a related field is preferred. • Relevant coursework or certifications in cybersecurity, network administration, or systems management can be beneficial.
2.	**Certifications**:	• Microsoft Certified: Modern Desktop Administrator Associate (relevant for managing Microsoft patch management solutions) • CompTIA Security+ (provides a foundational understanding of cybersecurity concepts) • Other certifications such as CompTIA Network+, Microsoft Certified: Azure Administrator Associate, or Certified Information Systems Security

		Professional (CISSP) may also be advantageous.
3.	**Experience**(**3-5 years**)	• Hands-on experience with Microsoft patch management solutions such as Windows Server Update Services (WSUS), Microsoft Endpoint Configuration Manager (formerly SCCM), or Microsoft Intune. • Experience in planning, deploying, and managing software updates and patches across enterprise environments. • Familiarity with patch management best practices, including patch testing, deployment scheduling, and rollback procedures. • Understanding of common vulnerabilities and exposure (CVE) identifiers and the National Vulnerability Database (NVD).
4.	**Technical Skills**	• Proficiency in using patch management tools and software, including Microsoft's suite of patch management solutions. • Strong understanding of Microsoft Windows operating systems and related technologies. • Knowledge of networking concepts, Active Directory, and Group Policy management.
5.	**Analytical Skills**	• Analytical mindset to assess the impact of software vulnerabilities, prioritize patch deployments, and troubleshoot patch-related issues. • Ability to interpret patch management reports, analyze patch compliance data, and identify areas for improvement.
6.	**Communication Skills**	• Effective communication skills, both verbal and written, for interacting with clients, documenting processes, and conveying

		technical information. - Ability to collaborate with cross-functional teams, including system administrators, network engineers, and security professionals.
7.	**Continuing Education**:	- Willingness to stay updated with the latest developments in patch management practices, Microsoft technologies, security threats, and industry trends. - Participation in relevant training programs, webinars, and conferences to enhance skills and knowledge.

- **Project Timelines**

Sr. No	Activity	Timelines
1	Installation , configuration & Commissioning of entire Solution	Within 2-4 weeks. On Critical Patches, the implementation should be completed within 2 to 5 days max.
2	Training and documentation	

4. Scope of Work on Asset Management

a. Implementation Phase:

i. Assessment and Planning:

- Conduct a thorough assessment of the Client's current asset management processes, tools, and data sources.
- Engage stakeholders to gather requirements, objectives, and success criteria for the implementation.
- Develop a detailed project plan outlining key milestones, deliverables, and resource requirements.
- Define roles and responsibilities for project team members and stakeholders.

ii. Solution Design and Customization:

- Design the architecture and configuration of the Microsoft Asset Management Solution based on the assessment findings and client requirements.
- Customize the solution to align with the Client's specific asset management workflows, data fields, and reporting requirements.
- Configure user roles, permissions, and access controls to ensure appropriate security and data privacy.

iii. Implementation and Integration:

- Install and configure the Microsoft Asset Management Solution according to the approved design specifications.
- Integrate the solution with existing IT systems, databases, and third-party tools, such as IT service management (ITSM) platforms, procurement systems, and financial management software.
- Develop and execute data migration strategies to transfer existing asset data into the new system while ensuring data integrity and accuracy.
- Design should cater identification of Network devices too.

iv. User Training and Change Management:

- Develop customized training materials, user guides, and documentation tailored to different user roles and proficiency levels.
- Conduct training sessions, workshops, and webinars to familiarize users with the functionality, navigation, and best practices of the asset management solution.
- Provide ongoing support and assistance to address user questions, issues, and feedback during the transition period.

b. Managed Service Phase for Asset Management:

i. System Administration and Configuration:

- Provide ongoing administration and maintenance of the Microsoft Asset Management Solution, including user provisioning, configuration changes, and system upgrades.
- Monitor system health, performance metrics, and usage trends to identify optimization opportunities and ensure scalability.
- Implement configuration management processes to track and manage changes to system settings, workflows, and integrations.

ii. Data Management and Governance:

- Establish data governance policies and procedures to ensure the accuracy, completeness, and consistency of asset data within the system.
- Conduct regular data quality checks, audits, and reconciliation processes to identify and address discrepancies, duplicates, and outdated records.
- Implement data retention and archiving policies in compliance with regulatory requirements and organizational policies.

iii. User Support and Training:

- Provide ongoing user support through helpdesk services, ticketing systems, and knowledge base resources.
- Offer advanced training sessions and workshops for users to enhance their proficiency in utilizing the asset management solution effectively.
- Develop and deliver targeted communications and awareness campaigns to promote user adoption and engagement.

iv. System Monitoring and Reporting:

- Monitor system performance, availability, and security events through proactive monitoring tools and dashboards.
- Configure alerts and notifications for critical incidents, system errors, and performance anomalies.
- Generate regular reports and analytics on asset utilization, lifecycle management, compliance status, and cost optimization opportunities.

v. Continuous Improvement and Innovation:

- Facilitate regular service reviews and performance evaluations with stakeholders to assess the effectiveness of the asset management solution and managed services.
- Solicit feedback from users and stakeholders to identify improvement opportunities, feature requests, and innovation initiatives.
- Collaborate with Microsoft and other technology partners to stay informed about product updates, best practices, and emerging trends in asset management.

vi. Compliance and Security Management:

- Ensure compliance with relevant industry standards, regulations, and best practices governing asset management, data privacy, and information security.
- Conduct periodic security assessments and vulnerability scans to identify and remediate potential risks and vulnerabilities.
- Implement access controls, encryption, and audit trails to protect sensitive asset data and maintain data integrity.

vii. Change and Release Management:

- Establish change management processes to manage and control changes to the asset management solution, including configuration changes, patches, and updates.
- Conduct impact assessments, risk analyses, and testing procedures to minimize the risk of service disruptions and maintain system stability.
- Coordinate release schedules and communication plans with stakeholders to ensure seamless deployment and adoption of new features and enhancements.

viii. Vendor Management and Collaboration:

- Serve as the primary point of contact for Microsoft and other technology vendors involved in the asset management solution ecosystem.
- Coordinate vendor relationships, contracts, and service level agreements (SLAs) to ensure alignment with client requirements and expectations.
- Facilitate collaboration and knowledge sharing among vendors, partners, and stakeholders to drive innovation and value creation.

ix. Documentation and Knowledge Management:

- Maintain comprehensive documentation of system configurations, workflows, procedures, and support materials.
- Develop a centralized knowledge base containing articles, FAQs, troubleshooting guides, and best practices for reference and training purposes.
- Ensure documentation is kept up-to-date and accessible to users, administrators, and other stakeholders as needed.

- **Educational Qualification required for L1 Support staff for Asset Management**

Sr. No.	Category	
1.	**Educational**	Bachelor's Degree: A bachelor's degree in a relevant field is required. It may include: • Computer Science • Information Technology • Business Administration • Management Information Systems (MIS) • Accounting (for understanding financial aspects of asset management)
2.	**Certifications**	• CompTIA IT Asset Management (ITAM) Certification • Certified Software Asset Manager (CSAM) • Microsoft Certified: Modern Desktop Administrator Associate (relevant for managing Microsoft assets) • ITIL Foundation (for understanding IT service management practices) • Support staff should be willing to stay updated with the latest developments in asset management tools, software, regulations, and industry trends.

- **Project Timelines**

Sr. No	Activity	Timelines
1	**Installation,Configuration & Commissioning of entire Solution**	**Within 1-2 weeks** from the date of PO
2	**Training and documentation**	**Within 2 weeks** from the date of PO

Non-Compliance of SLAs

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

  Note: SLA will be calculated quarterly.

AUDIT REQUIREMENTS:

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

RIGHT TO 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 auditsmay 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. Theselected bidder must provide the Company access to various monitoring and performance measurement systems (bothmanual 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.

KNOWLEDGE TRANSFER:

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

- **Knowledge Transfer Obligations: -**

  From Outgoing Provider: The Outgoing Provider agrees to:

- Provide complete and accurate documentation related to the services being transitioned. This includes, but isnot limited to, system architecture, process flows, incident reports, configuration details, and user guides.
- Offer detailed briefings and hands-on training sessions to the Incoming Provider's designated personnel on all aspects of the service operations, including the handling of any proprietary tools or specialized software.
- Facilitate a series of shadowing opportunities for the Incoming Provider's team to observe daily operations, incident response procedures, and maintenance routines.
- Make available subject matter expert (SME) to answer queries and provide advice to ensure a smooth handoverand continuity of services.
- Ensure the transfer of all relevant digital assets, credentials, and access permissions to the Incoming Providerin a secure manner.

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

- The Bidders should ensure that all assumptions/clarifications required are clarified beforehand. Any bids with words/phrases such as (but not limited to) "assumption", "it is understood that", "conditional offer" may be subjected to rejection at any stage of evaluation.
- Bidders should submit their responses as per the formats given in this RFP in the following manner:
- Technical Proposal and Eligibility Criteria in first envelope – Sealed Envelope 1 (Hard Copy).
- Commercial Proposal in second envelope – Sealed Envelope 2 (Hard Copy).
- Please note that prices should not be indicated in the Technical proposal but should only be indicated in the Commercial proposal. However, a masked bill of material masking the price information be provided along with the technical proposal.
- The two sealed envelope containing copies of technical Proposal and commercial Proposal, clearly marked "Response to RFP for IMPLEMENTATION OF MICROSOFT O365 / M365 LICENSES ENTERPRISE FEATURES AND MANAGED SERVICES For GICHFL.
- The outer envelope thus prepared should also indicate clearly the name, address, telephone number and E-mail ID of the Bidder to enable the Bid to be returned unopened in case it is found to be received after the time and date of Proposal submission prescribed herein
- All the pages of the Proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bidder's Proposal.
- The original Proposal shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialed by the authorized signatory of the Bidder.
- All pages of the bid shall be initialed and stamped by the authorized signatory of the Bidder.
- The Bidder must submit a certificate of undertaking on its official letter-head duly signed by its authorized signatory confirming the acceptance of all the terms & conditions contained in and spread throughout this Bid Document.
- The Bidder should provide supportive documents in regards to the proof of being an authorized LSP of Microsoft. Failing which, will lead to the disqualification of such Bidder.
- Decision as to any arithmetical error, manifest or otherwise in the response to Bid Document shall be decided at the sole discretion of GICHFL and shall be binding on the Bidder. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder. Bidder should be a legal entity and financially solvent. Bidder must warrant that no legal action is pending against them in any legal jurisdiction which affects its ability to deliver the RFP requirements.
- GICHFL reserves the right to re-issue/re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder.
- GICHFL reserves the right to modify its requirement for each product/service at any stage of the process.
- Modification to the RFP, if any, will be made available as an addendum on GICHFL website/will be emailed to bidder.

➢ Managed Security Service:

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

- **Notification of Award/Purchase Order:**

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

- **Signing of Purchase Order:**

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

- **Termination of Contract with selected bidder:**

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

- **Confidentiality Agreement**

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

- **Payment in case of Termination of contract:**

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

- **Force Majeure**

- The Vendor shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.

- For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Vendor and not involving the Vendor's fault or negligence and not foreseeable. Such events may include, Acts of God or of public enemy, acts of Government of India in their sovereign capacity and acts of war.

- If a Force Majeure situation arises, the Vendor shall promptly notify the Bank in writing of such conditions and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the Vendor shall continue to perform Vendors 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 Bank and the Vendor shall hold consultations in an endeavour to find a solution to the problem.

- **Governing Law & Disputes**

- All disputes or differences whatsoever arising between the parties out of or in relation to the construction, meaning and operation or effect of these Tender Documents or breach thereof shall be settled amicably. If however the parties are not able to solve them amicably, the same shall be settled by arbitration in accordance with the applicable Indian Laws, and the award made in pursuance thereof shall be binding on the parties. The Arbitrator/Arbitrators shall give a reasoned award. Any appeal will be subject to the exclusive jurisdiction of the courts at Mumbai, Maharashtra.

- During the arbitration proceedings the Vendor shall continue to work under the Contract unless otherwise directed in writing by GICHFL or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator or the umpire, as the case may be, is obtained.

- **KEY INSTRUCTIONS FOR THE BIDDERS:**

  Right to Terminate the Process

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

- **SUBMISSION INSTRUCTIONS:**

- **Two sealed Envelops in Hard Copy to be submitted:**

Envelope 'A'

- The envelope shall be sealed and marked as "Envelope A-Tender *to RFP for IMPLEMENTATION OF MICROSOFT O365 / M365 LICENSES ENTERPRISE FEATURES AND MANAGED SERVICES For GICHFL.*" in the top left hand corner. The envelope shall be dated with the current date in the top right hand corner.

It should contain following:

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

Envelope 'B'

- The envelope shall be sealed and marked as "Envelope B-Tender Envelope A-Tender *to RFP for IMPLEMENTATION OF MICROSOFT O365 / M365 LICENSES ENTERPRISE FEATURES AND MANAGED SERVICES For GICHFL*" in the top left hand corner. The envelope shall be dated with the current date in the top right hand corner.
- Please note that no other information other than the commercials should be furnished in this envelope. **Format for commercial bid is attached in Annexure A.**

It should contain following:

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

- **Service Level Agreement**

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

- **Taxes and Duties:**

- All taxes deductible at source, if any, at the time of release of payments, shall be deducted at source as per then prevailing rate while making any payment.
- Commercial Bid should be specific and inclusive of GST, duties, charges and levies of State or Central Governments as applicable, VAT/Sales Tax, insurance, service taxes, Octroi etc.
- The benefits realized by bidder due to lower rates of taxes, duties, charges and levies shall be passed on by the bidder to GICHFL.

- **Compliance Terms: -**

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

➢ 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. 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.

- Payment will be made annually based on signing the SLA WITH GICHFL.

- Payment mode will be made thru RTGS/NEFT transfer in 30 days after receipt of invoices

Payment terms are as follows:

- MS O365 plans Implementation and One-time EDR Implementation (Covering Implementation, Migration, Testing, Go-Live & Training):
- 20% on advance along with PO & terms.
- 20% on completion of overall Pilot / UAT testing.
- 60% on post completion of implementation on all Endpoints, Licensed Users and Sign-off from GICHFL team.

➢ Commercial BID Format:

Implementation & Managed Services Cost.

Sr. No.	**Particulars/ Service Model(s)**	**One time Implementation Cost (₹)**	**Price for 1st year (₹)**	**Price for 2nd year (₹)**	**Price for 3rd year (₹)**	**Price for 4th year (₹)**	**Price for 5th year (₹)**	**GST (₹)**	**Total Price for 5 years (₹)**
1.	**One time Implementation Cost(O365 license implementation & services, EDR,MDM etc.)**								
2.	**Managed Services and Technical Support (O365 incidents, Asset, Patch, EDR, MDM etc.)**								
	Total (Incl. GST) (₹)								

***Other service models can also be explored once the L1 bidder is identified.**

Note:

- The commercial bid format specified as PART-A has to be provided in the prescribed format only. No other format, except the given one, will be accepted.
- The Grand total should be written in figures and words. In case of any discrepancy in the figure and words, the amount in words will prevail.
- Lowest Grand Total price (inclusive of taxes) will be considered as L1 Price to award the contract.

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