सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

CBHFL/2425/RFP/IT/002 09-12-2024

Request for Proposal (RFP) for procurement/subscription of Cloud based Endpoint Security Solutions

The Company intends to acquire an off-the-shelf End point Security solution/product as perthe scope of work mentioned in Annexure – C of this RFP.

2. The details of annexures are as below,

Annexure	Annexure Details
A	Terms and conditions
B	Technical proposal covering letters (Format I, II & III)
C	Scope of the activities
D	Eligibility and Scoring criteria (Format I and II)
E	Commercial Proposal Covering letter and Bid Format
F	Non-Disclosure Agreement
G	Service Level Agreement

3. Interested parties are requested to submit their technical and commercialproposals in a big envelop (with separate envelops for technical and commercial proposals) addressing to Pankaj Kumar as per the schedule of events of this RFP.

   On the top of the envelop should be : "RFP response for Endpoint Security Solutions"

4. Technical proposal should consist of all Annexures (except Annexure E) and other supporting documents required for bid evaluation.

   Commercial bid should consist of Annexure E.

Yours faithfully

Pankaj Kumar

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

Schedule of Events

S. No.	Particulars	Remarks
1.	Contact details of issuing department (Name, Designation, Mobile No., Email, and office address for sending any kind of correspondence regarding this RFP)	CTO Email ID: pankaj.kumar@cbhfl.com Contact Address: CBHFL 6th floor, Central Bank of India, Mumbai Main Office Building, MG Road, Fort, Flora Fountain, Hutatma Chowk, Mumbai – 400 023. Contact Number: 022-69519323 Point of Contact 1) Lalit Kumar Rout,CISO Contact Number: 022-69519323 Mobile no.:- 7024155316 email: lalit.rout@cbhfl.com 2) Pankaj Kumar,CTO Mobile no.:- 9810663466 email: - pankaj.kumar@cbhfl.com
2.	Last date for requesting clarification	Up to 17.00 Hrs on 20/12/2024 All communications regarding points / queries requiring clarifications are required to be sent by e-mail to lalit.rout@cbhfl.com
3.	Pre - bid Meeting.	From 16.00 Hrs to 17.00 Hrs on21/12/2024 through onlinemeeting
4.	Last date and time for Bid submission	on 24/12/2024
5.	Date and Time of opening of Eligibility and Technical Bids	11.00 AM on 26/11/2024
6.	Opening of Commercial Bids	Commercial Bid of technically qualified eligible bidders only will be opened on 27/12/2024
7	Bank Guarantee – 5% of the total Project cost	Performance Security in form of BG should be valid for 05 (five) year(s) and 03 (three) month

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

ANNEXURE A - TERMS AND CONDITIONS

1. **Definitions**:

   a. "The Company" means the CBHFL (including branches)
   b. "Applicant/Bidder" means an eligible entity/firm submitting the Bid in response to this RFP.
   c. "Bid" means the written reply or submission of response to this RFP.
   d. "Vendor/Service Provider" is the successful Bidder found eligible as per eligibility criteria set out in this RFP and selected as per the selection criteria set out in the RFP and to whom notification of award has been given by the Company.
   e. "Solution/Product" means the software(s) and its components including licenses and documentation, which a Bidder is required to supply to the Company under the Contract.
   f. "Services" means all services, scope of work and deliverables to be provided by a Bidder as described in the RFP and include provision of technical assistance, training, certifications, auditing, and other obligation of Service Provider covered under this RFP.
   g. "The Contract" means the agreement entered between the Company and Service Provider, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

2. Service Providers are advised to study the RFP document carefully. Submission of proposal shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications. The response to this RFP should be full and complete in all respects. The Service Provider must quote for all the items asked for in this RFP. The SERVICE PROVIDER shall bear all Prices associated with the preparation and submission of the proposal, including Price of presentation for the purposes of clarification of the proposal, if so desired by CBHFL. CBHFL will in no case be responsible or liable for thosePrices, regardless of the conduct or outcome of the selection process.

3. **Disclaimer** :

3.1 Subject to any law to the contrary, and to the maximum extent permitted by law, CBHFL and its Directors, officers, employees, contractors, agents, and advisors disclaimall liability from any loss or damage suffered by any person acting or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the loss or damage arises in connection with any omission, default, lack of care or misrepresentation on the part of CBHFL or any of its officers, employees, contractors, agents or advisors.

3.2 This RFP is not an offer by CBHFL, but an invitation to receive responses from the eligible Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of CBHFL with the selected Bidder.

3.3 The purpose of this RFP is to provide the Bidder(s) with information to assist preparation of their Bid proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information contained in this RFP and where necessary obtain independent advices/clarifications. Company may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

3.4 CBHFL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, Price or expense which may arise from or be incurred orsuffered on account of anything contained in this RFP or otherwise, including the accuracy,adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process.

3.5 CBHFL also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

3.6 The issue of this RFP does not imply that the CBHFL is bound to select a Bidderor to appoint the Selected Bidder, as the case may be, for the Project and the Company reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

3.7 The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder's risk and may result in rejection of the Bid.

3.8 Proposed solution must be as per the detailed Technical Specifications and the Vendor should adhere to Scope of Work mentioned in this RFP.

3.9 Failure to open bids on account of submission of improper details of technical & commercial during the bid opening process, will result in disqualification of bidder. Keep separate envelop for each technical & commercial documents.

3.10 A print-out of the decrypted bid shall be kept on record and treated as the original bid for all official purposes.

3.11 No modification in the Bid shall be allowed, after the deadline for submission of Bids.

4. Bid Integrity:

Willful misrepresentation of any fact within the Bid will lead to the cancellation of the Contract without prejudice to other actions that the Company may take. All the submissions, including any accompanying documents, will become property of the Company. The Bidders shall be deemed to license, and grant all rights to the Company, to reproduce the whole or any portion of their Bid document for the purpose of evaluation and to disclose the contents of submission for regulatory and legal requirements.

5. Contract Period: 5 years

The contract period will be for a period of 3 years from the date of signing of the agreement which can be extended further on mutual terms and conditions for the period as decided by the Company. The performance of the successful Bidder shall be reviewed every quarter. Any offer falling short of the contract validity period is liable for rejection.

6. Evaluation of Bid and Contract:

CBHFL shall evaluate bids based on techno-commercial aspects. Techno-commercial evaluation shall include minimum eligibility criteria and commercial evaluation based on L1 bid.CBHFL reserves the right to further negotiate the contract price/terms with the selected vendor.

Contract will be awarded to final selected vendor on fixed cost basis, for the mentioned activities as per scope.

7. Contacting the Company:

No Bidder shall contact the Company on any matter relating to its Bid, from the time of opening of commercial Bid to the time, the Contract is awarded.

8. Any effort by a Bidder to influence the Company in its decisions on Bid evaluation, Bid comparison or contract award may result in the rejection of the Bid. CBHFL will reserve the rights to issue a **full or partial purchase** order on a selected vendor. In case of inability from vendor to execute the order or failed to execute the Service Level Agreement or Non-Disclosure Agreement in the Company's standard format or any othersuch failure, CBHFL will reserve rights to place an order with another bidder of its choice. **CBHFL is not bound to accept the lowest or any bid it may receive and will reserve the rights to scrap the entire vendor selection process initiated through this RFP, without assigning any reasons whatsoever.**

9. Payment :

a) **One time implementation cost**: 100 % payment upon 100% completion of one-time implementation as per the timeline of this RFP.

b) **Penalties for Delayed Implementation** – CBHFL will charge a penalty of 1%of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

c) **Annual Subscription Cost**: shall be paid quarterly subject to applicable penalties as mentioned in Annexure – C : Scope of work.

10. Miscellaneous :

I. The vendor and its employees will strictly undertake not to communicate or allow to be communicated to any person or divulge in any way any information relating to the ideas, know-how, technique, data, facts, figures and any information whatsoever concerning or relating to the CBHFL and its affairs to which they said employees have access in the course of the performance of the contract. Such employees shall also execute letters of fidelity and secrecy in such form as may be prescribed by the CBHFL.

II. All disputes and differences of any kind whatever arising out of or in connection with the purchase order shall be referred to arbitration. The arbitrator may be appointed by both the parties or in case of disagreement, each party may appoint an arbitrator and the decision of the arbitrator(s) shall be final. Such arbitration is to be governed by the provisions of the Indian Arbitration Act.

III. The vendor shall explicitly absolve CBHFL of any responsibility and liabilityfor use of the solution / software's delivered /used along with the equipment (i.e. thevendor shall absolve CBHFL in all cases of possible litigation / claims arisingout of any copyright / license violation for sourced items either form third parties or from themselves).

IV. CBHFL shall be under no obligation to accept the lowest bid or any other response to this tender notice including incomplete tenders/responses without assigning any reason whatsoever. CBHFL reserve the right to modify / alterthe full or partial terms and conditions of the tender/RFP/process and reissue fresh, ifconsidered necessary.

V. Vendor has to sign Non-Disclosure-Agreement to CBHFL before commencement of the activities and Service Level Agreement within 10 days from the date of issue of letter of intent / purchase order.

VI. Patent Rights: For any licensed software used by the Vendor for performing services or developing software for the company, the Vendor should have right as well right to license for the outsourced services. Any license or IPR violation on the part of Vendor should not put the CBHFL at risk. The CBHFL should reserve the right to audit the license usage of the Vendor. The Vendor shall, at their own expenses, defend and indemnify the CBHFL against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial designrights arising from use of the products or any part thereof in India or abroad. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design, the vendor shall after due inspection and testing get the solution redesigned for CBHFL at no extra cost. The vendor shall expeditiously extinguish any such claims and shall have full rights to defend it there from. If the CBHFL is required to pay compensation to a third party resulting from such infringement, the vendor shall be fully responsible therefore, including all expenses and court and legal fees. The CBHFL will give notice to the vendor of any such claim without delay, provide reasonable assistance to the vendor in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.

VII. Other terms and conditions as specified in the Service level agreement enclosed as Annexure – G of this RFP.

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

ANNEXURE - B

FORMAT - I

Technical Proposal Covering Letter (On Company Letter Head**)**

Date:

To,
CISO
CBHFL,
6th floor, Central Bank of India,
Mumbai Main Office Building,
MG Road, Fort, Flora Fountain,
Hutatma Chowk, Mumbai – 23

Dear Sir / Madam(s),

Sub: Technical Proposal for the RFP for Cloud based Endpoint Security Solution

Having examined the Request For Proposal (RFP)_____Documents dated_____ the receipt of which is hereby duly acknowledged, we, the undersigned, offer to perform the activities mentioned in scope of the RFP, including confirmatory reviews, in terms of functional and technical expertise including all licenses required (to use any tool) and implement for in conformity with the said RFP Documents and hereby undertake that we accept all the conditions of the RFP and will provide the complete services as per the Scope of Work.

We undertake to state that we have submitted all the necessary documents / responses as per the technical proposal of this RFP.

We agree to abide by this bid for the bid validity period specified in RFP and it shall remain binding upon us and may be accepted at any time before the expiry of that period.

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

Enclosures: Annexures A, B, C, D, F, G and other supporting documents required for bid evaluation.

Yours faithfully,

Date:

Signature of the Authorised Person

Name of the Authorized Signatory:

Place:

Designation:

Name of the Organization:

Seal:

Annexure - B

FORMAT - II

Conformity Letter (On Company Letter Head)

To,
CTO
CBHFL,
6th floor, Central Bank of India,
Mumbai Main Office Building,
MG Road, Fort, Flora Fountain,
Hutatma Chowk, Mumbai – 23

Sir/Madam,

Sub: Technical Proposal for the RFP for Cloud based Endpoint Security Solutions

Further to our proposal dated_____, in response to the Request for Proposal (RFP No. _____ Here in after referred to as "RFP") dated____issued by CBHFL ("CBHFL") we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions and / or stipulations as contained in the RFP and the related annexures, addendums, corrigendum and other documents including the changes made to the original tender documents, issued by CBHFL, however that only the list of deviations furnished by us along with the technical bid which are expressly accepted by CBHFL and communicated to us in writing, shall be valid and binding part of the aforesaid RFP document. The CBHFL is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the CBHFL's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

We also hereby confirm that our prices as specified in the Annexure/s Commercial Bid are as per the terms and conditions specified in the Tender / RFP document. We agree to abide by this Tender Offer for 180 days from date of Tender / RFP (Commercial Bid) opening and our offer shall remain binding on us and may be accepted by CBHFL any time before expiry of the offer.

We also confirm that the soft-copies of the proposal submitted by us in response to the RFP and the related addendums and other documents issued by CBHFL, conform to and are identical with the hard-copies of aforesaid proposal submitted by us, in all respects.

Yours faithfully,

Date:

Signature of the Authorized Person

Name of the Authorized Signatory:

Place:

Designation:

Name of the Organization:

Seal:

Annexure – B

Format - III

Declaration for Bug Free Software

To,
CTO
CBHFL,
6th floor, Central Bank of India,
Mumbai Main Office Building,
MG Road, Fort, Flora Fountain,
Hutatma Chowk, Mumbai – 23

Sir/Madam,

Sub: Technical Proposal for the RFP for Endpoint Security Solutionement Software

1. To the best of our knowledge, our_____(Name of solution/ product) to be supplied and implemented at CBHFL is free from bug/ embedded malicious/ fraudulent code/ Malware/ covert channel in the code.

2. We have addressed and fixed all the issues based on latest Top 10 OWASP (Open Web Application Security Project) vulnerabilities.

3. There are no back doors or Trojans in the solution.

Yours faithfully,

Date:

Signature of the Authorized Person

Name of the Authorized Signatory:

Place:

Designation:

Name of the Organization:

Seal:

ANNEXURE – C

Scope of Work

The Company intends to acquire an off-the-shelf Cloud based Endpoint Security Solutions/product to protect the endpoints of the Company. The solution should be comprehensive, integrated, enterprise-wide and workflow-based solution to enhance the effectiveness of endpoint security.

1. The solution/product should among other below mentioned requirement, provide for effective protection for Cyberattacks like 1. Evasive malware and Zero-day attacks 2. File-less attacks and targeted attacks an unified dashboard view to Senior Management on compliance position of the Company as a whole.

1. This RFP is to solicit quotations from partners Cloud based Endpoint & Security Solution which includes Software, supply, support (24X7 on call support including public holidays) and installation of IT infrastructure (Software) required for setting up Endpoint Security as per the given specifications.
2. The successful bidder will be expected to provide all the necessary support for delivery of the items, warranty, solution implementation, support and required OEM co-ordination & support during the warranty period.
3. The Bidder should provide Endpoints security solution which includes Windows, MAC/IOS and non-windows Operating systems E.g.: - Cent OS, Ubuntu & Linux based OS, and for Servers includes Windows and non-windows Operating systems.
4. Software requirement for Supply, delivery, Installation and support during warranty period, Implementation and support services are as follows:
    - Bidder Technical team should work with SOC team to integrate Endpoint and server security solution with SIEM and ensure use cases are defined for the detection of potential malicious events.
    - Bidder should provide the seamless migration from current antivirus solution to proposed endpoint security antivirus solution.
5. Supply, install, integrate, test, and operationalize the Endpoint security solution on endpoints & servers in CBHFL
6. Offered products / software's should be of latest version and should not have End Of Life / End Of Support in the next five years.
7. In cases where the offered products / software's is being superseded with new product / software by OEM due to better technology / specifications etc., the successful bidder is required to offer the new product / software at no extra cost or charges to CBHFL
8. The successful bidder shall supply components as per the detailed technical specifications as asked in Annexure-B of the RFP, all necessary tools, licenses (Including operating system & required software for the solution) implement, train and handover the solution to the CBHFL
9. Bidder shall develop High-Level Design, Low-Level Design if any and Implementation Plan for end point security solution. Bidder should conduct various activities such as but not limited to:
    - BoM Verification.
    - Deployment & Installation
    - Solution Configuration

- Policy Configuration
- Integration with other security solution if any.
- Dashboard and Report Creation and Customization if any.
- Additional recommendation to improve the performance or results.
- The successful bidder shall co-ordinate with OEM to assist CBHFL
- Bidder in fixing any gaps in the deployment found out during the audit.
- The price quoted by the bidder should cover all the support to the solution including any product updates/upgrades and fixing any issues faced. Bidder should provide support onsite/remotely to fix the issues for the period of 5 Years.
- The solution provider should be able to integrate with all the required, existing and proposed and future IT systems/tools with no additional cost.
- The solution provider should provide a detailed Plan of action (POA) for implementation of Endpoint Security Solution within one week of issuance of PO or mutually agreed date with CBHFL. It should include the approach, risk, benefits and downtime (if any). Post approval of POA, solution provider should work with CBHFL's Internal teams and application or business owners to complete the implementation of the solution.
- The Bidder will deploy and validate all the features in the Endpoint Security solution including (but not limiting to) Dashboard setup, use cases of security policies/patches and report customization and share the same with CBHFL.
- Full documentation of the project is to be included in the deliverables by the successful bidder. CBHFL may provide a format for documentation to the successful bidder.
- The Selected bidder shall assign Project Manager and associated support personnel for this project.

Documentation:

10. As part of deliverables, Bidder should provide all documents to CBHFL as listed below (where applicable)

- ✓ Solution architecture.
- ✓ Project plan with milestones, resourcing, and deliverables.
- ✓ Architecture & design document including network architecture, traffic flow document between the devices.
- ✓ SOP documents.
- ✓ Product literature.
- ✓ Operating manuals.
- ✓ Documentation on troubleshooting.
- ✓ Infrastructure build document.
- ✓ IP address allocations to various components.
- ✓ Application upgradation and patches management document.
- ✓ Testing cases and test results documented before and after implementation.
- ✓ Standard operating procedures.
- ✓ Industry best practiced use cases and customization for CBHFL.
- ✓ Vendor support details and escalation matrix.
- ✓ OEM support detaizls and escalation matrix.
- ✓ Inventory list consisting hostnames, make, model, serial number.

- ✓ BCP plan and documentation.
- ✓ IT DR Solution

One-Time Implementation:

The role of Bidder/OEM in One-Time implementation includes following, but not limited to:

- ✓ The Bidder shall appoint a Project Manager (PM) at CBHFL.
- ✓ The PM will manage the entire project from project kickoff date to completion of One-time implementation. Project Manager would be the single point of contact during the project implementation period. The details of project manager shall be provided on project Kickoff date.
- ✓ The responsibilities of PM are outlined below:
- ✓ Lead implementation effort.
- ✓ Primarily accountable for successful implementation of the project.
- ✓ Act to remove critical project bottlenecks.
- ✓ Single point of contact for CBHFL.
- ✓ Ensure implementation timelines are met to achieve desired result.
- ✓ Co-ordinate with OEM/CBHFL team for successful implementation of solutions.
- ✓ Periodic reporting to CBHFL on the implementation status, issues/ challenges faced and how these are handled.

OEM Training

- The bidder should arrange OEM certified product Training directly from the OEM for minimum 4 CBHFL officials after implementation.

Acceptance:

- One-month test period will be used by CBHFL to evaluate the selected Endpoint Security solution. After the selected solution has been successfully tested and implemented, CBHFL and the Selected bidder shall agree on the start date of the Go-LIVE.
- The selected Bidder shall assign project manager and associated support personnel for this project. The number of resources provided along with their skillsets (example L1, L2, L3 implementation or Operations) will need to be shared with CBHFL as part of the final project plan.
- Bidder shall submit the manufacturer/OEM authorisation letter to confirm that product/solution is delivered from Manufacturer/OEM and Bidder is partner with OEM for the above scope of work and submit the same as part of the bid. This agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities
- The Bidder should provide the deliverables and sign off for each of the deliverables at various stages of customization and implementation.
- Termination of the Endpoint Protection and Server Security Solution and Operations Services contract in case of any the following (but not limiting to):
- Deficiency in the Endpoint Protection and Server Security Solution & Operation service in terms of performance based on daily operations, security investigation, uptime, reporting, enhancements, alerting, notifications, escalations, etc.
- Breach terms & conditions in NDA, leakage of CBHFL's Intellectual Property due to

deficiency in monitoring, misconfiguration, wrong configuration, no-action, deletion, modification, tampering of CBHFL's logs.

- Non-availability of bidder's resources during the support window, downtime, upgrade.
- Implementing Service impacting changes to the Endpoint Protection and Server Security Solution without necessary approvals from CBHFL's management.
- Non-adhering to regulatory compliance for CBHFL data.
- Leakage of any confidential information.
- Not being transparent or hiding the truth or misrepresenting facts on issues relating to management and operation, security incidents to CBHFL.
- Failure to provide reporting services like daily reports, weekly report, monthly reports, half yearly reports, annual reports highlighting limitations, pending approvals, improvement, license expiry, major & critical incident detection, etc.
- In case of the bidder going insolvent, getting blacklisted, involvement in fraud, etc.
- On termination of the project, the Bidder commits to provide all necessary support in handing over the project to new incumbent identified by CBHFL, handover all documentations, provide team support during the handover period and ensure a seamless and smooth transition.

Non-Functional Requirements

Backup and Archiving

- There shall be a provision for taking backups and archive the replica of the systems' database and the application as well. There should be a provision of adequate Business Continuity Management (BCM).
- The methodology for the backing up of data and its archival may be indicated.
- The methodology or strategy used should be in alignment with CBHFL's Backup and Archival strategy.
- The Application should have a capability for easy retrieval of the backed-up data (both application and the database) with least amount of manual intervention with no data Loss events.

Security Requirements

- Provide security in compliance with CBHFL security requirements to preserve the confidentiality, integrity, and availability of the information systems.
- Develop, implement, maintain and use best in class industry proven safeguards that prevents the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems.
- Maintain a security plan that complies with industry accepted security requirements. Security Plan should be embedded within the Project Plan & approved by the CBHFL. The security plan would be reviewed by the CBHFL during the implementation phase.
- The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems.
- Selected bidder will not copy any data obtained while performing services under this

RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by CBHFL.

Deployment & Implementation

- The Bidder's resources will be required onsite during the deployment phase including the public holidays and weekends.
- The implementation phase shall be deemed as completed in all respects only after
- All applications and services are implemented as per the intent of this RFP.
- All functionalities mentioned in this RFP have gone live.
- All the related trainings are completed, and post training assessment carried out by the CBHFL.
- All documentation and reports have provided to CBHFL.

Training

- CBHFL expects the Bidder to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the training function. The training should include features, facilities, operations, implementation, troubleshooting, system administration, database administration, operating system administration, DR elements including BCP. All training will be hands-on training along with the trainer for the users. The Bidder should also provide e-learning facilities for users of the solution

Post Implementation

- The post implementation period will start after 30 days of successful "Go-Live" of the project. Post implementation will be from the day of issue of Completion Certificate by the CBHFL.

OEM Support:

- OEM should provide 24X7 Standard Support around the clock for critical business issues as per their defined severity definitions.
- Support for routine and non-critical issues should be available during normal business hours.

Bidder (SI) Support / Annual Maintenance Contract (AMC)

- The Bidder will be required to provide on-site/remote support during the 3 year of Warranty/Software Support, only when there is an issue that requires onsite support. applicable for software, respectively. Software Support shall commence from post implementation period and will start after successful "Go-Live" of the project and Completion Certificate by the CBHFL. Post implementation will be from the day for issue of Completion Certificate by the CBHFL.
- The proposed bidder should support solution in co-ordination with OEM from the date of operationalization of the system to the satisfaction of CBHFL during the support period.
- During the support period, the Bidder will have to undertake comprehensive maintenance of the software part. During the warranty period the vendor should maintain it and shall be responsible for all costs relating to maintenance.
- During the support period, the Bidder would be required to undertake all necessary modifications not falling under the purview of 'Change Management' such as updates,upgrades, bug fixes, changes in the application or any other support as and

when required at no extra cost.

- The bidder shall provide 24x7x365 telephonic and online support for the solution to address any technical Issues including configuration, breakdowns, data migration issues.
- CBHFL should be able to log calls directly by web/email or over phone to the Bidder / OEMs 24X7 during the warranty period.
- After expiry of the support, CBHFL shall have sole discretion to enter Annual Maintenance Contract (AMC) either in full or in part for maintenance.
- During the five (5) years of support period, the Bidder will be required to provide remote/on- site support when needed, if required the on-site support may be extendable at the CBHFL's discretion.
- If CBHFL desires, it could extend the onsite support (engineer will be needed onsite for any upgrades/updates/issue resolution/troubleshooting) beyond five (5) years as per the business need, Bidder should provide (Application / Software) 24X7X365 days on call support.
- During the software support Period, the selected vendor will have to provide at no additional cost to CBHFL, all software updates, releases, Version upgrades, New Versions etc within 30 days of their availability.
- The selected Bidder shall provide preventive maintenance on monthly basis.
- The selected Bidder shall design and implement to assure 99.9% uptime for the solution calculated on monthly basis.
- Where the Bidder is not the Manufacturer of certain components of the Solution, then the Bidder shall disclose the Manufacturer's warranty for such components to the CBHFL and, in the event such warranty exceeds the Bidder's warranty under this Contract in any respect, shall ensure that the CBHFL will receive the benefit of the Manufacturer's warranty

2. **Implementation timeline:** The proposed solution should be completed within a period of **30 days** from the date of issuing purchase order by CBHFL to the selectedbidder.

3. Technical Requirements:

3.1. The off-the-shelf product/solution should be free from any vulnerability, bugs, back-doors or Trojans, Vendor should provide required declaration as per Annexure B, Format III Declaration for Bug Free Software.

3.2. Regulatory /Compliance Requirements:

i. The solution should comply with extant regulatory and statutory compliance requirements.

ii. The solution should be implemented as per industry best practices. It should be customized to meet Company's requirements/Data Governance Policy and Data Retention policy.

iii. Solution should also meet "Digital Personal Data Protection Act, 2023" related Compliances.

iv. It should comply with India specific data security and access regulations and/or certifications. The Vendor has to ensure required data security andconfidentiality with no data leakage.

v. The Vendor has to provide updates/patches and fixes for all the regulatory/statutory and audit compliance requirements and observations during the contract period without any additional cost to the Company.

vi. The Vendor has to provide encryption (minimum AES 256 or latest) of the Company's data at rest and in motion.

vii. The latest and acceptable assurance certification will be required to be submitted to the Company, at periodic intervals.

3.3. Disaster Recovery Mechanism

The solution must be capable of and compatible for Disaster Recovery (DR) Implementation in active – passive mode with log shipping between Primary and DR Site, as required by the Company. The vendor needs to submit the technical architecture relating to data replication between primary and secondary site.
The company must capable of own business continuity plans & also participate in CBHFL BCP process.Authentication through Company's Active Directory should be supported.

3.4. The vendor to provide timely closure of all vulnerabilities identified in the proposed solution during Internal/External Security audit/reviews according to Company's audit schedule.

3.5. Monitoring and Audit

a) CBHFL will have the right to audit Vendor's people, processes, technology etc. as part of the Vendor Security Risk Assessment Process.

b) The periodicity of these audits will be decided at the discretion of the Company. The Vendor must provide the Company access to various monitoring and performance measurement systems. The Vendor has to remedy all discrepancies observed by the auditors at no additional cost to the Company.

c) There should also be proper audit trail of login/logout, addition, deletion, modification, activation, deactivation etc. of users and their system rights. In addition, there should also be proper audit trail of addition, deletion, modification, at the record level showing the changes, users, date and timestamp with IP capture.

d) Other terms on inspection and audit will be as per the Annexure – G, Service Level Agreement.

3.6. Software Licenses:

i. The application license(s) should be of latest and current version as of go-live date and should be in the name of the Company, CBHFL'S, Mumbai, and valid for the entire Contract period.

ii. Wherever required, the successful Vendor should submit renewal certificate in the name of Company in physical/ electronic form well in advance before the license expiry date during the Contract period.

iii. All the components used in the solution should not have end of support during the entire period of Contract.

iv. Should any components be announced end of support during the Contract period, the Vendor will have to replace the same with an equivalent or higher specification product without any additional cost.

v. The Vendor must consider the disaster recovery environment while proposing the licenses.

3.7. RTO / RPO Management:

i. The Vendor needs to maintain the below RTO (Recovery Time Objective) and RPO (Recovery Point Objective) parameters of the all the in-scope equipment's and software as mentioned below.

Recovery Time Objective (RTO)	4 Hours
Recovery Point Objective (RPO)	10 Minutes

ii. Monitor and manage the replication between the DC and DR (under supervision of CBHFL Systems Team)

iii. Generate reports to review the performance of the replication.

4. SLA & Penalties (including information security SLA terms):

- CBHFL expects that the Bidder shall be bound by the Service Levels described in this document for Endpoint Protection & Server Security Solution application and Software Performance.

Definitions

- Service Levels are calculated based on the "Business Utility" of the solution, which is described as the ratio of "System Available for Actual Business Hours" to the "Scheduled System Availability for Business".

$$BU\ (\%) = \frac{S_{BOH} - S_{BDT}}{SBOH} * 100$$

- a. Where BU = Business Utility, SBOH = Scheduled Business Operation Hours, SBDT = Business Downtime

- The "Scheduled Business Operation Hours" for a given time frame are calculated after deducting the planned downtime which can be taken on the system only with prior notice to CBHFL and with mutual consent of CBHFL and the Bidder.
- "Business Downtime" is the actual duration for which the system was not able to service CBHFL due to System or Infrastructure failure as defined by CBHFL and agreed by the Bidder. The "Business Downtime" would be calculated on daily basis and for all performance appraisals, the daily downtime would form part of core measurement for assessment/ escalation/ penalty, etc."
- The "Working Hours" would be from 8:00 AM to 9:30 PM from Monday to Saturday, even on Sunday if required, Further CBHFL expects the Bidder to recognize the fact that CBHFL might work in extended hours to provide the expected customer service as well as for statutory reporting.

Response Time: 30 minutes from the time of complaint.
Resolution Time: 1 hour from the time of complaint.

Penalties will be applicable due to downtime caused by failure in application, software, etc. which will be provided by the Vendor. However, downtime due to power or environmental failures or, due to causes attributable to CBHFL will not be taken into account. Penalties shall also be applicable in case the information security or audit related findings / vulnerabilities are not closed in a time bound manner.

Purpose and Objective of SLA

- CBHFL intends to enter into a Service Levels Agreement (SLA) with the successful Bidder in order to provide complete utility of the service that could be provided to CBHFL.
- The SLA shall be included in the contract agreement as mentioned in the document and identifies the expectations of CBHFL and defines the Scope and Boundaries for the successful Bidder to provide maximum "Business Utility". Any issue could be classified under the following four categories:
    - **Level 1**: The identified issue has a material business impact (Show Stopper) and needs to be resolved immediately. This level would typically correspond to issues that result into disruption of most of the critical services to all the CBHFL, regulated entity offices and external institutions having an access.
    - **Level 2**: The identified issue has a significant business impact and needs to be taken up on top priority. This level would typically correspond to issues that result into disruption of one or more critical services to all the CBHFL, regulated entity offices and external institutions having an access.
    - **Level 3**: The identified issue has normal impact on the Business and needs to be addressed at the earliest. This level would typically correspond to issues which result into disruption of one or more services to one or more but not all CBHFL, regulated entity offices and external institutions having an access.
    - **Level 4**: The identified issue has almost no impact in terms of Business. However, issue needs the attention of the Bidder and shall be fixed on lesser priority.
- It is expected that the Bidder provides an immediate solution/ work around for "Show Stopper" issues so that CBHFL can continue to function normally and then register the issue on priority by conducting a "Root Cause Analysis".

- The selected Bidder shall design and implement to assure 99.9% uptime for the solution calculated on monthly basis

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

ANNEXURE D : Eligibility and Scoring Criteria

Format I

Minimum Eligibility Criteria

S.No.	Eligibility Criteria	Compliance (Yes/No)	Documents to be submitted
1	The bidder must be an Indian firm/Company / Organization registered under Companies Act/Partnership Act/LLP Act etc.or a foreign company, registered under applicable laws & regulations, with Sales and Support arrangement in India.		Copy of the Certificate of Incorporation issued by Registrar of Companies and full address of the registered office. Proof of Partnership/LLP. Foreign companies also to provide declaration with details of sales & support arrangement in India.
2	The Bidder must have an average turnover of minimum ₹10 crore during last 03 (three) financial year(s) i.e., FY 2021-22, FY 2022-23, and FY 2023-24		(Certificate from statutory auditor for preceding/current 03 year may be submitted.) (Refer Annexure-3)
3	The Bidder should be profitable organization on the basis of profit before tax (PBT) for at least 02 (two) out of last 03 (three) financial years i.e., FY 2021-22, FY 2022- 23, and FY 2023-24		Certificate from the statutory auditor.
4	Bidder should have completed at least 2 projects worth cumulative of at least 25 Lakhs INR (Cumulative Cost), in last 2 years for Indian Clients. The name of the Bidder (SI and/or OEM) needs to be in sync withthe credential letters / contract copies, exceptions will be madein case of divesture, M&A		Copy of the Purchase order and / or sign off report or Certificate of completion for the completed projects. All such details to be duly signed by the authorised signatory of the bidder.
5	The bidder must be ISO-27001 Certified Company, and the certificate should be valid as on date of bid submission and should also cover the proposed product/solution.		Copy of ISO-27001 certificate
6	The bidder should have priorexperience of supply and successful implementation of Endpoint Security Solution for minimum 500 users for two BFSI client organizations in India as on date.		Evidence required
7	The Bidder shall be Platinum /Gold / Silver level Partner of ESS		Evidence required
8	Bank Guarantee – 5% of the total Project cost		Performance Security in form of BG

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

Format II

Protection Category	Sub Category	Solution proposed(Y/N)
Core Protection	Antivirus	Yes
	AntiMalware	Yes
	Email Protection	Yes
	Attachment Control	Yes
	Behaviour Detection System	Yes
	Spam Protecion	Yes
	Auto Run Protection	Yes
	Safe Mode Protection	Yes
	Self Protection	Yes
	Removal of Conflicting Software	Yes
	Ransomeware Protection	Yes
	Backup & Restore	Yes
Vulnerability Scan	Vulnerability Scan	Yes
Network Protection	Firewall	Yes
	IPS/IDS	Yes
	Port Scan Attack Detection	Yes
	DDoS Attack Detection	Yes
	Source of Infection	Yes
Asset Management	System Information	Yes
	Tracking of hardware changes on Endpoints	Yes
	Tracking of software changes on Endpoints	Yes
	-Display last 4 digits of Windows OS product key	Yes

	-Display last 4 digits of Windows Office product key	Yes
	Customized Reports	
	-based on OS	Yes
	-based on application name	Yes
	-based on system manufacturer	Yes
	-based on RAM	Yes
	-based on Processor	Yes
	-based on last shutdown time	Yes
Web Secutiry	Browsing Protection	Yes
	Phishing Protection	Yes
	Browser Sandbox	Yes
	Safe Banking	Yes
	Scheduled Internet Access	Yes
	Web Filtering	Yes
Advance Device Control	Storage Device, USB	Yes
	CD/DVD	Yes
	Internal Card Reader	Yes
	Floppy Drive	Yes
	Wi-Fi	Yes
	Bluetooth	Yes
	Firewire Bus	Yes
	Serial Port	Yes
	SATA Controller	Yes
	Thunderbolt	Yes

	PCMCIA	Yes
	Card Reader Device (MTD/SCSI)	Yes
	Windows Portable Devices (Digicams, Smartphones)	Yes
	iPhone/iPad	Yes
	Blackberry	Yes
	Scanner & Imaging Devices	Yes
	Webcam	Yes
	Local Printers	Yes
	Teensy Boards	Yes
	Network Share	Yes
	Temporary USB Storage Access	Yes
Data Loss Prevention	Data Loss Prevention	Yes
	- Print Screen	Yes
	- Removable Device	Yes
	- Network Share	Yes
	- Clipboard	Yes
	- Printer Activities	Yes
	- Instant Messengers	Yes
	- File Sharing Cloud Services	Yes
	- Social Media	Yes
	- Web Browsers	Yes
	- Email Clients	Yes
	- File Types	Yes
	- Confidential Data	Yes

	- User Defined Directories	Yes
Application Control	Application Control	Yes
TuneUp	Disk Clean Up	Yes
	Registry Clean Up	Yes
	Defragmentation	Yes
Client Deployment	Active Directory	Yes
	Remote install/Uninstall	Yes
	Notify Install	Yes
	Client Packager	Yes
	Online installer	Yes
Reports Notifications & Logs	Export Reports (csv/pdf)	Yes
	Scheduled Reports	Yes
	SMS Notifications/Alerts	Yes
	Email Alerts	Yes
	News Alerts	Yes
Management	Dashboard	Yes
	Management Console	Yes
	Cloud Management Platform	Yes
	Groups & Policies	Yes
Updates	Update Manager	Yes
	Multiple Update Manager	Yes
	Scheduled Updates	Yes
Compatibility	Windows	Yes
	Mac	Yes

	Linux	Yes
Customer support	Local	Yes
2FA Authentication	Multifactor Authentication	Yes

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

ANNEXURE D : Solution Requirements

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
1	Proposed Endpoint security solution should be using a blend of advanced threat protection & detection techniques to eliminate threats entering in to CBHFL network and is delivered via an architecture that uses endpoint resources more effectively and ultimately perform considering CPU and network utilization.		
2	Solution must have Detection and Response capabilities with Insightful investigative capabilities and centralized visibility across thenetwork by using an advanced EDR, strong SIEMintegration and an open API set with threat intelligence sharing.		
3	All features asked in RFP are to be delivered all-in-one single agent with deployment option of On-Prem and/or Cloud and /or Hybrid		
4	Proposed solution should have Advanced malware and ransomware protection: Defends endpoints—on or off the corporate network—against malware, Trojans, worms, spyware, ransomware, and adapts to protect against newunknown variants and advanced threats like crypto malware and file less malware.		
5	Solution to have multiple techniques to addressknown, unknown, unpatched threats with pattern/signature based, behavior monitoring, virtually patching the vulnerabilities, highly accurate machine learning -pre-execution and runtime, Sandboxing, Application controlled etc. EDR solution should have both IOC & IOA based approach.Detection module should be mapped to MITRE ATT&CK framework		
6	Solution must have Noise cancellation techniques like reputation services and whitelist checking at each layer to reduce false positives.		
7	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually.		
	Prevention Capabilities		
8	Solution should be having Antimalware, Machine learning - pre-execution and runtime, behavior monitoring, Anti-exploit, C&C communication prevention, Virtual patching ,Application control, file less malware prevention, file/web reputation, file check mechanism to reduce false positives. Proposed solution should not only be relying on ML and Behavior based [on execution only] for prevention.		

	Antimalware		
Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
9	Solution must offer comprehensive security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.		
10	Solution must support various scanning optionsto clean dormant malwares - Real time scan, Scheduled Scan[daily/weekly/monthly] and on-Demand Scan.		
11	Solution must support customizable actions for various types ofThreats : **Clean, Delete, Rename, Quarantine, Pass.**		
12	Solution must include capabilities for detectingand removing rootkits, provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution and has capabilities to restore spyware/grayware if the spyware/grayware is deemed safe.		
13	Solution must have Assessment mode to allowfirst to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation.		
14	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: a. Terminating all known virus processes and threads in memory b. Repairing the registry c. Deleting any drop files created by viruses d. Removing any Microsoft Windows services created by viruses e. Restoring all files damaged by viruses f. Includes Clean-up for Spyware, Adware etc		
15	Should have the capability to assign a client the privilege to act as a update agent for rest of the agents in the network.		
16	Solution should have an option of Users withthe scheduled scan privileges can postpone, skip, and stop Scheduled Scan.		
17	Solution must support CPU usage performance control during scanning -Checks the CPU usagelevel configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.		
18	Solution must support safeguarding endpoint mailboxes by scanning incoming POP3/MAP email and Outlook folders for Threats.		
19	Solution should scan only those file types which are potential virus carriers (based on true file type) with option of adding program to trusted list for excluding process, if required. Should be able to detect files packed using real-time compression algorithms as executable files.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
20	Solution should provide social Engineeringattack visibility for e.g.: attackers exploiting vulnerability found in docs such as pdf.		
21	Solution must be able to scan Object Linkingand Embedding (OLE) File looking for exploit codes.		
	Highly Accurate Machine Learning		
22	Solution must have highly accurate machine learning to address unknown security threats found in suspicious file/process.		
23	Machine learning must have Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.		
24	Machine learning module should be able to extract multiple features from file for e.g.: who, when, where info, import table, header, opcode, packer existence etc and compare it with cloud/on-prim machine learning model and predict the maliciousness of the file. CBHFL is expecting to have strong machine learning module to address unknown threats.		
25	Solution must show the assigned confidence/score in terms of Percentage in the ML based detection logs to show the predictiveness of the Threat.		
26	Machine learning must support file/process andtake appropriate action in terms of quarantine/terminate. solution must have an option of adding exceptions to the machine learning engine.		
	Behavior Monitoring		
27	Solution must have behavior monitoring moduleto constantly monitor endpoints for unusual modifications to the operating systems and installed software's.		
28	Behavior monitoring must have program inspection to detect and block compromised executable files. behavior monitoring should monitor for newly encountered program downloaded from various channels like web/email/removable media.		
29	Behavior monitoring must have an **Indicator ofAttacks (IOA)** based Prevention like: • Shell modification, host file modificationlibrary injection new service process modifications duplicated system files malicious PowerShell credential access		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
30	Behavior monitoring must have **Anti-exploit** module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution etc.		
31	Anti-exploit engine must support various exploit prevention techniques but not limited to Force ASLR, Null page, Heapspray.		
32	Behavior monitoring must have multiple action parameters such as assess, allow, block, deny, terminate.		
33	Solution must support **Browser Exploit Prevention** - scan browsers for exploit/script/scan webpage and Block.		
34	Solution must have an option to Trust the process and exclude from the engine.		
	Ransomware protection		
35	Solution Should have Ransomware Protection feature with documents to be protected from unauthorized encryption or modification.		
36	Solution should have feature to take backup of ransomware infected files and restoring the same. Should support logging reporting and correlation of suspicious events.		
37	solution must block all the processes commonly associated with ransomware and should have program inspection to monitor processes and perform API hooking to identify if program is behaving abnormally.		
38	Ransomware protection must not be limited to specific ransomware behavior/variants .		
39	Solution should have capability to submit suspicious files to sandbox solution for further analysis. This is an optional feature.		
	Command & Control Prevention - Web Reputation		
40	Solution must be able to block all communication to Command & control center- bad IP/domain		
41	Solution must support adding whitelisting and Blacklisting of URL's/Domain using wildcards.		
42	Solution must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.		
43	Solution must provide by default security levels i.e. High, Med & low so that it eases the operational efforts and Solution must have an option of assessment mode ONLY so that URLs are not blocked but logged.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
44	solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list also.		
45	Solution must support malware network fingerprinting mechanism to detect unique malware family signatures within network packets and just not rely on IP addresses/domains.		
46	Solution must have damage clean-up services after detecting Command & Control communication.		
	Host Intrusion Prevention System - Vulnerability Protection		
47	Solution must have an Vulnerability Protection feature and does not only give visibility, Rules should be able to do Virtual patching of the vulnerabilities using Deep Packet Inspection and should have CVE ID mapping to the rules.		
48	HIPS should have deep packet inspection capability to identify content that may harm the application layer, Filters forbidden network traffic and ensures allowed traffic through stateful inspection.		
49	HIPS engine should have multiple configuration options i.e. Inline or tap mode-Detect only.		
50	Solution should have multiple types of rules i.e. vulnerability, exploit and smart rules.		
51	HIPS rules must also have an MITRE ATT&CK mapping for detections like : • Reverse Shell communication (ATT&CK T1071) Remote command execution via WinRM (ATT&CK T1028), Domain level -Credential dumping over DCERPC (ATT&CK T1033) WhatsApp Communication attempt (ATT&CK T1102) Remote file copy over FTP (ATT&CK T1105) Remote Service creation (ATT&CK T1050) Block Admin Share (ATT&CK T1077,T1105)		
52	Solution must have default modes of either performance or security priority.		
53	Solution should deliver the most-timely vulnerability protection in the industry across a variety of endpoints, including end-of-support (EOS) operating systems.		
	Host based Firewall		
54	Solution must support host-based firewall with stateful inspection, option to create Rules on the basis of Source/Destination/port/protocol.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
55	Solution must have an certified safe software repository to be used in Firewall rules		
56	Firewall module must have an option to bydefault Allow All/Block All/Block incoming only options and create exceptions with granularity.		
57	Firewall engine should have an Intrusion Detection - looking at pattern in network packets ,prevent intrusion like too big fragment, ping of death, syn flood,tear drop, land attack etc.		
	Endpoint Application Control		
58	Solution must have an Application Control module to enhance CBHFL defences against malware and targeted attacks by preventing unknown and unwanted applications fromexecuting on corporate endpoints with a combination of flexible, dynamic policies, whitelisting/blacklisting and Lock down capabilities		
59	It should Prevent potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).		
60	Solution should provide global and local real- time threat intelligence based on good file reputation data correlated across a global network. solution must have an option of importing application list to the management console		
61	solution should provide greater insight intothreat outbreaks with user-based visibility, policy management, and log aggregation. Enables reporting across multiple layers of security solutions.		
62	Solution must support adding application criteria on the basis of Path, hash, Certificate/Digital signature, OEM provided safe application service with allow or block actions.		
63	Solution must support importing inventory of hashes to define a Application control criteria.		
64	Solution must contain broad coverage of pre-categorized applications that can be easily selected from application catalogue (with regular updates).		
65	Solution must ensure that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change.		
66	Solution must support system lockdown to harden end-user systems by preventing new applications from being installed and executed apart from the inventory found during policyinstallation.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
	Device Control		
67	Solution must support Device control - Whitelisting/Blacking listing of devices.		
68	Solution must support Allow/Block Actions for the supported devices.		
69	Solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT ,Imaging, Prt Scrn key ,Wireless Nic		
70	Solution must support various permission -Full Access, Read only, Execute, Modify		
71	Speeds audits and enforcement with forensic data capture and real-time reporting.		
	Endpoint - Detection & Response		
72	Solution must provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack.EDR must record User and Kernel level operations - activities related to File, Process, User, Registry, DNS, Memory, IP, Port.		
73	Solution must support sending meta data/activity data to Server on frequency defined by CBHFL as per location/Branch.		
74	Solution must support Indicator of Compromise (IOC) - Sweeping on the basis of : • User File name File hash Fqdn/ip/hostname Registry -key,value name,value data cli command		
75	Solution must support Investigation using the below open standard: • STIX Open IOC YARA User Defined Repository received from Other deployed products.		
76	Solution must support Threat Investigation - Historic, Live and Scheduled ,CBHFL may use any of the option depending on the scenario.		
77	Solution must support Attack Discovery - Indicator of Attacks monitoring endpoint activity for Attackers intent and Tacti's ,Techniques and Procedures being used.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
78	Solution must support Indicator of Attacks (IOA) with MITRE ATT&CK Framework - few examples: • **Tactics:** Credential AccessAccount Creation Privilege escalation Defense evasion Execution Lateral Movement Exfiltration Persistence		
79	Solution must support live investigation to lookfor process running in memory, file existence on Disk, registry value/key on the endpoints.		
80	Solution must have an option of doing impact analysis - if specific Threat seen on endpoint can be sweeped across enterprise.		
81	Solution must support giving details like command/registry/rating of the object and isolate the Endpoints without generating Root cause/Attack chain.		
82	Solution must have Root cause analysis for simple or full Root cause/Attack chain, CBHFL expects Root Cause chain to be interactive so that immediate actions like adding to suspicious objects list, terminating, investigating further etc should be the option available in the chain. RCA should indicate objects in different coloursfor easy analysis for e.g.: malicious, suspicious, known good etc.		
83	Solution must support below **response** options: • Endpoint isolation - communicates with management only Customize rules during isolation Endpoint Restoration Terminate Process Block -IP address Block Hash Block Domain/URL Block/Quarantine - File Outbreak prevention - deny access to file/folder, ports, block write access, deny access to executables. Add to Suspicious Repository -to be shared with existing deployed products.		
84	Solution must support API for collecting logs, Investigation, Isolation/restore ,Running Root cause analysis/Sweeping.		
85	Solution should have capability to Integrate with Sandboxing Solution –submission for end to end execution and analysis. This is an optional requirement.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
86	Solution must support Open Standard – STIX/Taxii/Cybox for threat intelligence sharing.		
87	Integrates with other security products locally on your network and also to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection and reducing the spread of malware.		
	Centralized Management console and Visibility		
88	Centralized security management console should ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security.		
89	Should extend visibility and control across on-premises, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection,reduce complexity, and eliminate redundant and repetitive tasks in security administration		
90	Console should have an options of creatingcustom dashboard and report as per CBHFL's requirement. Tabs and widgets support, Threat EventsHistory (Detection over time),Threat Classifications/Types		
91	Console should have an option of creating userswith different user roles for managing the solution.		
92	Console should have operations dashboard which will give overall security posture of the endpoint security and can be drilled down by just clicking on it.		
93	Console should have an option of doing impact analysis of threat seen on endpoint and check other endpoints for the same.		
94	Management console should be able to integrate with Active Directory ,two factor authentication etc		
95	Solution must extend visibility and control across on-premises, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administrator.		
96	Management console should have an option of various alerting methods such as Email/SIEM integration.		
97	Management console should support API integration.		

Advanced Endpoint Prevention Detection & Response SolutionRequirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
98	Solution must support Reporting option with One time/Scheduled/Custom in CSV/PDF/RTF formats.		
99	Management should have option of creating suspicious object repository containing hashes/IP and also support open IOC,STIX format, YARA rules and leverage this intelligence for proactive prevention anddetection strategy for CBHFL.		
	Threat Intelligence Collaboration and Extended Detection and Response		
100	Solution must support threat Intel sharing with existing security products deployed at CBHFL environment.		
101	Solution must support Automatic sharing ofthreat intelligence across security layers enabling protection from emerging threats across the whole organization.		
102	Solution must support threat intelligence sharing with IOC/STIX/TAXII/CyBox		
103	Solution should have a provision of creating user defined repository where file/URLs/hashes can be added and shared among other security products.		
104	Solution must have an XDR [Extended Detectionand Response] option to have Native integration with products for events correlation across Endpoints,Network,Email and Cloud to reduce overall MTTD and MTTR for CBHFL.		
105	Solution must have central repository of threat intelligence - powered with 3T+ threat queries, more than 60 B threats per day, sensors and multiple sources of threat information and same should be available as update for CBHFL.		
106	The solution should have capable to protect the endpoints from Zero-day attacks.		
107	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux-RedHat,CentOS,Oracle,Debian,SUSE, Ubuntu,Amazon Linux, Cloud Linux etc		
108	The Proposed solution must support Anti-malware, HIPS, Integrity Monitoring, Host Firewall for the below mentioned server operating system:Windows ,Linux and Ubuntu		
109	Solution must have remote access tools to connect with various endpoints to troubleshoot any issue.		
110	Solution must have remote patch management tool for any update on windows & other patches deployment silently.		
111	Secures and monitors mobile devices to ensure compliance with security policies.		

Note : Each of the requirements above has value one so in technical evaluation each partner sum of these values

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

ANNEXURE E

Commercial Proposal Covering Letter (On Company Letter Head**)**

Date:

To
CTO ,
CBHFL,
6th floor, Central Bank of India,
Mumbai Main Office Building,
MG Road, Fort, Flora Fountain,
Hutatma Chowk, Mumbai – 23

Dear Sir/ Madam(s),

Sub: Commercial Proposal for RFP for Endpoint Security Cloud based solution

Having examined the Request For Proposal (RFP) Documents dated _ the receipt of which is hereby duly acknowledged, we, the undersigned, offer our services, as mentioned, conformance with the scope of work of said RFP documents and as per the attached Commercial Proposal and hereby undertake that we accept all the terms and conditions of the RFP.

We further undertake, if our bid is accepted, to deliver the services accordance with the delivery schedule finalized.

Our commercial proposal shall be binding upon us, subject to the modifications resulting from contract negotiations, up to expiration for the validity period of the Proposal.

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

Enclosure- Commercial Bid

Yours faithfully,

Date:

Place:

Signature of the Authorized Person

Name of the Authorized Signatory:

Designation:

Name of the Organization:

Seal:

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

Commercial Bid Format (On Company Letter Head)

Sr. No.	Off-the-shelf End point Security solution for the period of 3 years	Amount in Rs. Excl. of taxes
1	**One time implementation cost**	
2	**Yearly Subscription/Support Cost #**	
3	**Endpoints Count -200 and Server Count -20**	
Total Cost in Rs. (excl. of taxes)		

Yearly subscription/support cost will be fixed for the entire period of contract of 5 years

Yours faithfully,

Date:

Place:

Signature of the Authorized Person

Name of the Authorized Signatory:

Designation:

Name of the Organization:

Seal:

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

Annexure – F

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made at_____ between:

CBHFL., a company incorporated under the Companies Act, 1956; bearing CIN U65922MP1991PLC006427 and having its Registered Office at 6th floor, Central Bank of India, Mumbai Main Office Building, MG Road, Fort, Flora Fountain, Hutatma Chowk, Mumbai – 400023 (hereinafter referred to as "Client" / "CBHFL" which expression includes its successors and assigns) of the ONE PART;

And

_____ a private/public limited company/LLP/Firm *< remove or strike off whichever is not applicable>* incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 *< remove or strike off whichever is not applicable>*, having its registered office at _____ (hereinafter referred to as "_____" which expression shall unless repugnant to the subject or context thereof, shall mean and include its successors and permitted assigns) of the OTHER PART;

And Whereas

1. _____ is carrying on business of providing _____, has agreed to_____for CBHFL and other related tasks.

2. For purposes of advancing their business relationship, the parties would need to disclose certain valuable confidential information to each other (the Party receiving the information being referred to as the "Receiving Party" and the Party disclosing the information being referred to as the "Disclosing Party. Therefore, in consideration of covenants and agreements contained herein for the mutual disclosure of confidential information to each other, and intending to be legally bound, the parties agree to terms and conditions as set out hereunder.

NOW IT IS HEREBY AGREED BY AND BETWEEN THE PARTIES AS UNDER

1. Confidential Information and Confidential Materials:

(a) "Confidential Information" means non-public information that Disclosing Party designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential. "Confidential Information" includes, without limitation, information relating to developed, installed or purchased Disclosing Party software or hardware products, the information relating to general architecture of Disclosing Party's network, information relating to nature and content of data stored within network or in any other storage media, Disclosing Party's business policies, practices, methodology, policy design delivery, and information received from others that Disclosing Party is obligated to treat as confidential. Confidential Information disclosed to Receiving Party by any Disclosing Party Subsidiary and/ or agents is covered by this agreement

(b) Confidential Information shall not include any information that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed to Disclosing party; (ii) becomes known to Receiving Party free from any confidentiality

obligations prior to Disclosing Party's disclosure of such information to Receiving Party; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party and without confidentiality restrictions on use and disclosure; or (iv) is independently developed by Receiving Party.

(c) "Confidential Materials" shall mean all tangible materials containing ConfidentialInformation, including without limitation written or printed documents and computer disks or tapes, whether machine or user readable.

2. Restrictions

(a) Each party shall treat as confidential the Contract and any and all information ("confidential information") obtained from the other pursuant to the Contract and shall not divulge such information to any person (except to such party's "Covered Person" which term shall mean employees, contingent workers and professional advisers of a party who need to know the same) without the other party's written consent provided that this clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract, which is already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause). Receiving Party will have executed or shall execute appropriate written agreements with Covered Person, sufficient to enable it to comply with all the provisions of this Agreement. If the Service Provider appoints any Sub-Contractor (if allowed) then the Service Provider may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving CBHFL an undertaking in similar terms to the provisions of thisclause. Any breach of this Agreement by Receiving Party's Covered Person or Sub-Contractor shall also be constructed a breach of this Agreement by Receiving Party.

(b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), providedReceiving Party shall give Disclosing Party reasonable notice (provided not restricted by applicable laws) prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

i. the statutory auditors of the either party and
ii. government or regulatory authorities regulating the affairs of the parties and inspectors and supervisory bodies thereof

(c) Confidential Information and Confidential Material may be disclosed, reproduced, summarized or distributed only in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder. Receiving Party agrees to segregate all such Confidential Material from the confidential material of others in order to prevent mixing.

3. Rights and Remedies

(a) Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use.

(b) Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option, certify destruction of the same.

(c) Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (including but not limited to as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

i. Suspension of access privileges
ii. Change of personnel assigned to the job
iii. Termination of contract

(d) Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.

4. <u>Miscellaneous</u>

(a) All Confidential Information and Confidential Materials are and shall remain the sole and of Disclosing Party. By disclosing information to Receiving Party, Disclosing Party does not grant any expressed or implied right to Receiving Party to disclose information under the Disclosing Party's patents, copyrights, trademarks, or trade secret information.

(b) Confidential Information made available is provided "As Is," and disclosing party disclaims all representations, conditions and warranties, express or implied, including, without limitation, representations, conditions or warranties of accuracy, completeness, performance, fitness for a particular purpose, satisfactory quality and merchantability provided same shall not be construed to include fraud or willful default of disclosing party.

(c) Neither party grants to the other party any license, by implication or otherwise, to use the Confidential Information, other than for the limited purpose of evaluating or advancing a business relationship between the parties, or any license rights whatsoever in any patent, copyright or other intellectual property rights pertaining to the Confidential Information.

(d) The terms of Confidentiality under this Agreement shall not be construed to limit either party's right to independently develop or acquire product without use of the other party's Confidential Information. Further, either party shall be free to use for any purpose the residuals resulting from access to or work with such Confidential Information, provided that such party shall maintain the confidentiality of the Confidential Information as provided herein. The term "residuals" means information in non-tangible form, which may be retained by person who has had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, the foregoing shall not be deemed to grant to either party a license under the other party's copyrights or patents.

(e) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequently to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, its agents, or employees, except by an instrument in writing signed by an authorized officer of Disclosing Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.

(f) In case of any dispute, both the parties agree for neutral third party arbitration. Such arbitrator will be jointly selected by the two parties and he/she may be an auditor, lawyer, consultant or any other person of trust. The said proceedings shall be conducted in English

language at Mumbai and in accordance with the provisions of Indian Arbitration and Conciliation Act 1996 or any Amendments or Re-enactments thereto. Nothing in this clause prevents a party from having recourse to a court of competent jurisdiction for the sole purpose of seeking a preliminary injunction or any other provisional judicial relief it considers necessary to avoid irreparable damage. This Agreement shall be governed by and construed in accordance with the laws of Republic of India. Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of Mumbai.

(g) Subject to the limitations set forth in this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and assigns.

(h) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(i) The Agreement shall be effective from____ ("Effective Date") and shall be valid for a period of 3 year(s) thereafter (the "Agreement Term"). The foregoing obligations as to confidentiality shall survive the term of this Agreement and for a period of five (5) years thereafter provided confidentiality obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

5. <u>Suggestions and Feedback</u>

Either party from time to time may provide suggestions, comments or other feedback to the other party with respect to Confidential Information provided originally by the other party (hereinafter "feedback"). Both parties agree that all Feedback is and shall be entirely voluntary and shall not in absence of separate agreement, create any confidentially obligation for the receiving party. However, the Receiving Party shall not disclose the source of any feedback without the providing party's consent. Feedback shall be clearly designated as such and, except as otherwise provided herein, each party shall be free to disclose and use such Feedback as it sees fit, entirely without obligation of any kind to other party. The foregoing shall not, however, affect either party's obligations hereunder with respect to Confidential Information of other party.

Dated this_____day of_____(Month) 20___at_____(place)

For and on behalf of _____

Name		
Designation		
Place		
Signature		

For and on behalf of _____

Name		
Designation		
Place		
Signature		

सेन्ट बैंक होम फायनेन्स लिमिटेड
Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी Subsidiary of Central Bank of India

Annexure - G

SERVICE LEVEL AGREEMENT

FOR

Cloud based Endpoint Security Solution

BETWEEN

CBHFL AND

[_____]

Date of Commencement :

Date of Expiry :

This agreement ("**Agreement**") is made at _____ (Place) on this _____ day of _____ 2023.

BETWEEN

CBHFL, a company incorporated under the Companies Act, 1956; bearing CIN U65922MP1991PLC006427 and having its Registered Office at 6th floor, Central Bank of India, Mumbai Main Office Building, MG Road, Fort, Flora Fountain, Hutatma Chowk, Mumbai – 400023, hereinafter referred to as "the **Company**" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of First Part:

AND

_____ a [private/public limited company/LLP/Firm] ~~<strike off whichever is not applicable>~~incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932 ~~<strike off whichever is not applicable>~~, having its registered office at _____ hereinafter referred to as "**Service Provider/ Vendor**", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS

(i) The Company is carrying on the business of Standalone Primary Dealership operations and is desirous of availing services for Endpoint Security Solution

(ii) Service Provider is in the business of providing [ ] and has agreed to provide the product/services as may be required by the Company mentioned in this Agreement.

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for other valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree to the following terms and conditions hereinafter contained:-

1) DEFINITIONS & INTERPRETATIONS:

A. Definition:

Certain terms used in this Agreement are defined hereunder. Other terms used in this Agreement are defined where they are used and have the meanings there indicated. Unless otherwise specifically defined, those terms, acronyms and phrases in this Agreement that are utilized in the information technology services industry or other pertinent business context shall be interpreted in accordance with their generally understood meaning in such industry or business context, unless the context otherwise requires/mentions, the following definitions shall apply:

a) "**Company**" shall mean the CBHFL (including branches).

b) "**Confidential Information**" shall have the meaning set forth in Clause 14.

c) "**Deficiencies**" shall mean defects arising from non-conformity with the mutually agreed specifications and/or failure or non-conformity in the Scope of the Services.

d) "**Documentation**" will describe in detail and in a completely self-contained manner User Manuals, Technical design documents, FAQs , Trouble Shooting documents etc.

e) "**Effective Date**" shall mean the date on which this Agreement takes effect.

f) "**Intellectual Property Rights**" shall mean, on a worldwide basis, any and all: (a) rights associated with works of authorship, including copyrights &moral rights; (b) Trade Marks; (c) trade secret rights; (d) patents, designs, algorithms and other industrial property rights; (e) other intellectual and industrial property rights of every kind and nature, however designated, whether arising by operation of law, contract, license or otherwise; and (f) registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

g) "**Project Cost**" means the price payable to Service Provider over the entire period of Agreement (i.e., INR [●]/- **(Rupees in words** [●])[or PO reference may be given] for the full and proper performance of its contractual obligations.

h) '**Services**' shall mean and include the Services offered by Service Provider under this Agreement more particularly described in Clause 2 of this Agreement.

B. Interpretations:

In construing the Agreement:

a) Reference to a person includes any individual, firm, body corporate, association (whether incorporated or not) and authority or agency (whether government, semi government or local).
b) The singular includes the plural and vice versa.
c) Reference to any gender includes each other gender.
d) The provisions of the contents table, headings, clause numbers, italics, bold print, and underlining is for ease of reference only and shall not affect the interpretation of this Agreement.
e) The Schedules, Annexures and Appendices to this Agreement shall form part of this Agreement.
f) A reference to any documents or agreements (and, where applicable, any of their respective provisions) means those documents or agreements as amended, supplemented or replaced from time to time provided they are amended, supplemented, or replaced in the manner envisaged in the relevant documents or agreements.
g) A reference to any statute, regulation, rule, or other legislative provision includes any amendment to the statutory modification or re-enactment or, legislative provisions substituted for, and any statutory instrument issued under that statute, regulation, rule, or other legislative provision.
h) Any agreement, notice, consent, approval, disclosure, or communication under or pursuant to this Agreement is to be in writing.

C. Commencement, Term & Change in Terms:

a) This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from [_____] (**Effective Date**).
b) This Agreement shall be in force for a period of 5 years from Effective Date, unless terminated by the Company by notice in writing in accordance with the termination clauses of this Agreement.
c) The Company shall have the right at its discretion to renew this Agreement in writing, for a further term of 5 years on the mutually agreed terms & conditions.
d) Unless terminated earlier in accordance with this Agreement, the Agreement shall come to an end on completion of the term specified in the Agreement or on expiration of the renewed term.

e) Either Party can propose changes to the scope, nature or time schedule of services being performed under this Service Level Agreement. Such changes can be made upon mutually accepted terms & conditions maintaining the spirit (Purpose) of this Service Level Agreement.

2) Scope of Work:

The scope and nature of the Services which the Service Provider has to provide to the Company is described in the Annexure – 'A' of this Agreement. The Company may, at its sole discretion, provide remote access to its information technology system in order to facilitate the performance of the Services. Such remote access to the Company's information technology system shall be subject to the following:

a) Service Provider shall ensure that the remote access to the Company's information technology system is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.
b) Service Provider shall ensure that only its authorized employees/representatives access the Device.
c) Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Company's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Company's representative may inspect. Service Provider shall facilitate and/ or handoverthe Device to the Company or its authorized representative for investigation and/or forensic audit.
d) Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Company's network is performed, effectively against unauthorized access, malware, malicious code, and other threats in order to ensure the Company's information technology system is not compromised in the course of using remote access facility.
e) In case of VPN access:
    i. Service Provider shall be required to get the Device hardened/configured as per the Company's prevailing standards and policy.
    ii. Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Company's prescribed format before such remote access is provided by the Company.

3) Fees, Taxes, Duties & Payments:

A. **<u>Professional fees:</u>**

i. Service Provider shall be paid fees and charges in the manner **detailed in here under**, the same shall be subject to deduction of income tax thereon wherever required under the provisions of the Income Tax Act by the Company. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Company as per the laws and regulations for the time being in force. Nothing in the Agreement shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Agreement.

ii. All duties and taxes (excluding GST or any other tax imposed by the Government in lieu of same), if any, which may be levied, shall be borne by Service Provider and the Company shall not be liable for the same. All expenses, stamp duty and other charges/ expenses in connection with execution of this Agreement shall be borne by Service

Provider. Goods & Services Tax or any other tax imposed by the Government in lieu of same shall be borne by the Company on actual upon production of original receipt wherever required.

iii. Service Provider shall provide a clear description quantifying the service element and goods element in the invoices generated by them.

B. Payments:

i. The Company will pay properly submitted valid invoices within reasonable period but not exceeding 45 days after its receipt thereof. All payments shall be made in Indian Rupees.

ii. The Company may withhold payment of any product/services that it disputes in good faith and may set-off penalty amount or any other amount which Service Provider owes to the Company against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, the Company shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidence, if any, within 21 days. Penalty or damages, if any, recoverable from Service Provider shall be recovered by the Company through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, the Company shall have right to withhold the payment or set-off penal amount from current invoices.

4) Liabilities/Obligation:

i. The Company's Duties /Responsibility (if any)
   a. Processing and authorizing invoices
   b. Approval of Information

ii. Service Provider Duties
   a. Service Delivery responsibilities.
   b. To adhere to the service levels/timelines documented in this Agreement and RFP

iii. Service Provider shall ensure that Service Provider's personnel and its sub-contractors (if allowed) will abide by all reasonable directives issued by the Company, including those set forth in the Company's then-current standards, policies, and procedures (to the extent applicable), all on-site rules of behaviour, work schedules, security procedures and other standards, policies and procedures as established by the Company from time to time.

iv. Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable laws for the time being in force including but not limited to Information Technology Act, 2000 and rules thereof and directions issued by RBI concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

Security Responsibility

i. Service Provider shall maintain the confidentiality of the Company's data, resources, and other intellectual property rights.

ii. Service Provider shall implement and maintain reasonable security practices and procedures as defined under Section 43A of Information Technology Act, 2000 and rules thereof.

iii. Without the Company's prior written permission, Service Provider shall not store or share Company's materials including Confidential Information outside the geographical boundary of India or in/with a public cloud.

iv. Service Provider shall first obtain the Company's approval of the content of any filing, communications, notices, press release or reports related to any security breach prior to any publication or communication thereof to any third party. Service Provide shall maintain a well understood reporting procedure for security incidents and a copy of such procedure shall be made available to the Company.

v. Service Provider should secure the Company's data (if shared) while transiting, processing, at the store, during backup and archival, over external media, etc. with latest & secured encryption standards.

vi. Service Provider should define proper access control for protecting the Company's data (if shared) and access to the data is strictly on a need-to-know Basis.

vii. The Service Provider will comply with the directions issued from time to time by the Company and the standards related to the security and safety as per best practices and standards relevant in the industry, to the extent as it applies to the provision of the Services.

viii. Both parties to the service level agreement shall use reasonable endeavors to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the project's data, assets, facilities, or confidential information.

ix. The Service Provider shall upon reasonable notice by the Company or its designated agency participate in regular meetings when safety and information technology security matters are reviewed.

x. The parties under the service level agreement shall promptly report in writing to each other any act or omission (which they are aware could have an adverse effect on the Services and proper conduct of safety and information technology security at project's locations

xi. The Service Provider shall promptly inform in writing to the Company all material adverse events in the nature of data breaches, denial of service, service unavailability, etc. to enable the Company to take prompt risk mitigation measures and ensure compliance with statutory guidelines.

5) Representations & Warranties:

i. Each of the Parties represents and warrants in relation to itself to the other that:

a) It has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement and has been fully authorized through applicable corporate process to do so.

b) The authorised person(s) signing this Agreement on behalf of the Parties have the necessary authority and approval for execution of this document and to bind his/their respective organization for due performance as set out in this Agreement. It has all necessary statutory and regulatory permissions, approvals and permits for the running and operation of its business.

c) It has full right, title, and interest in and to all software, copyrights, trade names, trademarks, service marks, logos symbols and other proprietary marks (collectively 'IPR') (including appropriate limited right of use of those owned by any of its vendors, affiliates, or subcontractors) which it provides to the other Party, for use related to the Services to be provided under this Agreement.

d) It will provide such cooperation as the other Party reasonably requests in order to give full effect to the provisions of this Agreement.

e) The execution and performance of this Agreement by either of the Parties does not and shall not violate any provision of any of the existing Agreement with any of the party and any other third party.

f) Service Provider warrants that the technical quality and performance of the Services provided will be consistent with the mutually agreed standards during the entire contract period.

g) Any defect found will be evaluated by the service provider(s) to establish the exact cause of the defect. Service Provider to provide technical support to the Company for related deficiencies.

ii. Additional Representation and Warranties by Service Provider

a) Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency, and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material, and methods.

b) Service Provider has the requisite technical and other competence, sufficient, suitable, qualified, and experienced manpower/personnel, and expertise in providing the Services to the Company.

c) Service Provider shall duly intimate to the Company immediately, the changes, if any in the constitution of Service Provider.

d) Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the Services provided by Service Provider to the Company do not violate or infringe any patent, copyright, trademarks, trade secrets or other intellectual property rights of any third party. Also, the Service Provider has not received any notice of violation of any Intellectual Property Right in relation to the Services being provided by the Service Provider under this Agreement.

e) Service provider shall ensure that all persons, employees, workers, and other individuals engaged by or sub-contracted (if allowed) by Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by Service provider unless such person is found to be suitable in such verification and Service Provider shall retain the records of such verification and shall produce the same to the Company as and when requested. Further, the Service Provider agrees and undertakes that upon request by the Company it shall provide information to the Company regarding such third parties engaged by the Service Provider in relation to the Services under this Agreement.

f) Service Provider represents and warrants that its personnel shall be present at the Company premises or any other place as the Company may direct, only for the Services and follow all the instructions provided by the Company; act diligently, professionally and shall maintain the decorum and environment of the Company; comply with all occupational, health or safety policies of the Company.

g) Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provided fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Company shall have no liability in this regard.

h) Service Provider agrees that it shall communicate to the Company well in advance along with detail plan of action, if any changes in Service Provider's environment/infrastructure is of the nature that may have direct or indirect impact on the Services provided under this Agreement or operations of its Services.

i) Service Provider shall ensure confidentiality, integrity, and availability of the Company's information at all times and shall ensure that information security risks related to outsourcing of Services to any other party, if permitted by the Company, shall be assessed, and managed regularly, to the satisfaction of the Company.

6) General Indemnity:

i. Service Provider agrees and hereby keeps the Company indemnified against all claims, actions, loss, damages,, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which the Company may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any willful misconduct and gross negligent acts on the part of employees, agents, representatives or subcontractors (if allowed) of Service Provider. Service Provider agrees to make good the loss suffered by the Company.

ii. Service Provider hereby undertakes the responsibility to take all possible measures, at no additional cost, to avoid or rectify any issues which thereby results in non-performance of Service Provider systems including deliverables within reasonable time. The Company shall report as far as possible all material defects to Service Provider without undue delay. Service Provider also undertakes to co-operate with other service providers thereby ensuring expected performance covered under scope of work.

7) Contingency Plans:

i. Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other contingency plans to meet any unexpected obstruction to the Service Provider or any employees or sub-contractors (if allowed)

of Service Provider in rendering the Services or any part of the same under this Agreement to the Company. Service Provider at Company's discretion shall cooperate with the Company in case on any contingency.

ii. Service Provider shall have defined business continuity management and disaster recovery procedures in place for effective handling of critical business processes in situation of any incident disrupting the Services under this Agreement. Service Provider shall carry out periodic drill activity to ensure the effectiveness of business continuity management and disaster recovery procedures and reports of such activities shall be shared with the Company. Further, Service Provider shall have consider identifying skilled resources who provide core services as 'essential personnel' and are necessary to operate critical functions on site during exigencies (including pandemic situations) to limit the number of staff that may be required during such exigencies (including pandemic situations).

8) Transition Requirement:

i. In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Company at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Company shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work.

ii. During the transition phase, the existing Service Provider shall render all reasonable assistances to the new Service Provider within such period prescribed by the Company, at no extra cost to the Company, for ensuring smooth switch over and continuity of Services, provided where transition services are required by the Company or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement.

iii. If existing Service Provider is found to be in breach of this obligation, they shall be liable for paying a penalty of INR 5% on demand to the Company, which may be settled from the payment of invoices or bank guarantee for the contracted period.

9) Liquidated Damages:

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this Agreement, the Company may, without prejudice to its other remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 1% of order value for delay of each week or part thereof maximum up to 5% of order value. Once the maximum deduction is reached, the Company may consider termination of the Agreement.

10) Relationship Between the Parties:

i. It is specifically agreed that Service Provider shall act as independent service provider and shall not be deemed to be the Agent of the Company except in respect of the transactions/services which give rise to Principal - Agent relationship by express agreement between the Parties.

ii. Neither Service Provider nor its employees, agents, representatives, Sub Contractors (if allowed) shall hold out or represent as agents of the Company.

iii. None of the employees, representatives or agents of Service Provider shall be entitled to claim any absorption or any other claim or benefit against the Company.

iv. This Agreement shall not be construed as joint venture. Each Party shall be responsible for all its obligations towards its respective employees. No employee of any of the two Parties shall claim to be employee of other Party.

v. All the obligations towards the employee(s) of a Party on account of personal accidents while working in the premises of the other Party shall remain with the respective employer and not on the Party in whose premises the accident occurred unless such accidents occurred due to gross negligent act of the Party in whose premises the accident occurred.

vi. For redressal of complaints of sexual harassment at workplace, Parties agree to comply with the policy framed by the Company (including any amendment thereto) in pursuant to the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 including any amendment thereto.

11) Sub-Contracting:

As per the scope of this Agreement subcontracting is not permitted.

i. However, if the Service Provider subsequently wishes to subcontract the scope of work, it will have to obtain specific written permission from the Company before contracting any work to subcontractors. The Company at its own discretion may permit or deny the same.

ii. In case subcontracting is permitted by the Company, the contracting vendor will be responsible for all the services provided to the Company regardless of which entity is conducting the operations. The contracting vendor is also responsible for ensuring that the subcontractor comply with all security requirements of the contract and the Company may obtain independent audit report for the same in accordance with Clause 2 of this Agreement. In such a case, the Service Provider shall provide subcontracting details to the Company and if require, the Company may evaluate the same.

iii. Before engaging Sub-Contractor, the Service Provider shall carry out due diligence process on sub-contracting/ sub-contractor to the satisfaction of the Company and Company shall have access to such records.

iv. In the event of sub-contracting the Service Provider shall ensure that suitable documents including confidentiality agreement are obtained from the sub-contractor and the Service Provider shall ensure that the secrecy and faith of Company's data / processes is maintained.

v. In the event of sub-contracting, the Service Provider shall ensure that the sub-contractor shall subsume all the rights and obligations of the Service Provider as envisaged under this Agreement.

vi. Notwithstanding approval of the Company for sub-contracting, the Service Provider shall remain liable to the Company for all acts/omissions of sub-contractors.

12) Intellectual Property Rights:

i. For any technology / software / product used by Service Provider for performing Services for the Company as part of this Agreement, Service Provider shall have right to use as well as right to license such technology/ software / product. The Company shall not be liable for any license or IPR violation on the part of Service Provider.

ii. Without the Company's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Company's rights under this Agreement.

iii. Subject to clause 12.4 and 12.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Company against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Company the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Company all amounts paid by the Company to Service Provider under this Agreement.

iv. The Company will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Company, unless such settlement releases the Company fully from such claim, (ii) Service Provider shall promptly provide the Company with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Company with respect to the defence and settlement of any such claim, and (iv) in any litigation to which the Company is also a party, the Company shall be entitled to be separately represented at its own expenses by counsel of its own selection.

v. Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Company's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an Infringement Claim and Service Provider did not inform the Company of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Company.

vi. Subject to payment of requisite service fee in accordance with clause 3 (B) of this Agreement, Service Provider grants CBHFL an irrevocable, non-exclusive, subscription-based license throughout the territory of India to access, replicate, modify and use software provided by Service Provider including its upgraded version during the term of this Agreement.

13) Inspection and Audit:

i. It is agreed by and between the parties that Service Provider shall be subject to annual audit by internal/external Auditors appointed by the Company/ inspecting official from the CBHFL or anyregulatory authority, covering the risk parameters finalized by the Company/ such auditors in the areas of productsand Services etc. provided to the Company and Service Provider shall submit such certification by such Auditors to the Company. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Company) shall facilitate the same. The Company can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/datato them. All costs for such audit shall be borne by the Company. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Company shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

ii. Where any Deficiency has been observed during audit of Service Provider on the risk parameters finalized by the Company or in the certification submitted by the Auditors, it is agreed upon by Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the Deficiencies. It is also agreed that Service Provider shall provide certification of the auditor to the Company regarding compliance of the observations made by the auditors covering the respective risk parameters against which such Deficiencies observed.

iii. Service Provider further agrees that whenever required by the Company, it will furnish all relevant information, records/data, books/logs, alerts to such auditors and/or inspecting officials of the Company / Reserve Bank of India and/or any regulatory authority(ies) and provide access to the business premises to the inspecting officials of the Company. The Company reserves the right to call for and/or retain any relevant information / audit reports on financial and security reviews with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/ data not related to Services under the Agreement (e.g., internal cost breakup etc.).

14) Confidentiality:

i. "Confidential Information" mean all information which is material to the business operations of either party or its affiliated companies, designated as being confidential or which, under the circumstances surrounding disclosure

out to be treated as confidential, in any form including, but not limited to, proprietary information and trade secrets, whether or not protected under any patent, copy right or other intellectual property laws, in any oral, photographic or electronic form, whether contained on computer hard disks or floppy diskettes or otherwise without any limitation whatsoever. Without prejudice to the generality of the foregoing, the Confidential Information shall include all information about the party and its customers, costing and technical data, studies, consultants reports, financial information, computer models and programs, software code, contracts, drawings, blueprints, specifications, operating techniques, processes, models, diagrams, data sheets, reports, and other information with respect to any of the foregoing matters. All and every information received by the parties and marked confidential hereto shall be assumed to be confidential information unless otherwise proved. It is further agreed that the information relating to the Company and its customers is deemed confidential whether marked confidential or not.

ii. All information relating to the accounts of the Company's customers/constituents/counterparty(s) shall be confidential information, whether labelled as such or otherwise.

iii. All information relating to the infrastructure and Applications (including designs and processes) shall be deemed to be Confidential Information whether labelled as such or not. Service Provider personnel/resources responsible for the project are expected to take care that their representatives, where necessary, have executed a Non-Disclosure Agreement similar to comply with the confidential obligations under this Agreement.

iv. Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential Information is required by law, legal process, or any order of any government authority. Service Provider in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of Company and the Company's per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law, legal process, or order of a government authority.

v. Each party, including its personnel, shall use the Confidential Information only for the purposes of achieving objectives set out in this Agreement. Use of the Confidential Information for any other purpose shall constitute breach of trust of the same.

vi. Each party may disclose the Confidential Information to its personnel solely for the purpose of undertaking work directly related to the Agreement. The extent of Confidential Information disclosed shall be strictly limited to what is necessary for those particular personnel to perform his/her duties in connection with the Agreement. Further each Party shall ensure that each personnel representing the respective party agree to be bound by obligations of confidentiality no less restrictive than the terms of this Agreement.

vii. The non-disclosure obligations herein contained shall not be applicable only under the following circumstances:

a) Where Confidential Information comes into the public domain during or after the date of this Agreement otherwise than by disclosure by a receiving party in breach of the terms hereof.

b) Where any Confidential Information was disclosed after receiving the written consent of the disclosing party.

c) Where receiving party is requested or required by law or by any Court or governmental agency or authority to disclose any of the Confidential Information, then receiving party will provide the other Party with prompt notice of such request or requirement prior to such disclosure.

d) Where any Confidential Information was received by the receiving party from a third party which does not have any obligations of confidentiality to the other Party.

e) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

viii. Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

ix. Service Provider shall not, without the Company's prior written consent, make use of any document or information received from the Company except for purposes of performing the Services and obligations under this Agreement.

x. Any document received from the Company shall remain the property of the Company and shall be returned (in all copies) to the Company on completion of Service Provider's performance under the Agreement.

xi. Upon expiration or termination of the Agreement, all the Company's proprietary documents, customized programs partially or wholly completed and associated documentation, or the Company's materials which are directly related to any project under the Agreement shall be delivered to the Company or at the Company's written instruction destroyed, and no copies shall be retained Service provider without the Company's written consent.

xii. The Company reserves its right to recall all the Company's materials including Confidential Information, if stored in Service Provider system or environment, at any time during the term of this Agreement or immediately upon expiry or termination of Agreement. Service Provider shall ensure complete removal of such material or data from its system or environment (including backup media) to the satisfaction of the Company.

xiii. The foregoing obligations (collectively referred to as "Confidentiality Obligations") set out in this Agreement shall survive the term of this Agreement and for a period of (5) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

15) Ownership

i. Service Provider agrees that the Company owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all intellectual property rights, copyrights. Any work made under this Agreement shall be deemed to be 'work made for hire' under any Indian or any other applicable copyright laws.

ii. All information processed by Service Provider during Services belongs to the Company. Service Provider shall not acquire any other right in respect of the information for the license to the rights owned by the Company. Service Provider will implement mutually agreed controls to protect the information. Service Provider also agrees that it will protect the information appropriately.

16) Termination:

i. The Company may, without prejudice to any other remedy for breach of Agreement, by written notice of 30 (thirty) days, terminate the Agreement in whole or in part:

   a) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement, or any extension thereof granted by the Company.
   b) If Service Provider fails to perform any other obligation(s) under the Agreement.
   c) On happening of any termination event mentioned herein above in this Agreement.

   Prior to providing a written notice of termination to Service Provider under clause 16(i) (a) to 16 (i) (c), the Company shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Company shall have right to initiate action in accordance with above clause.

ii. The Company, by written notice of not less than 60 (sixty) days, may terminate the Agreement, in whole or in part, for its convenience, provided same shall not be invoked by the Company before completion of half of the total Contract period (including the notice period). In the event of termination of the Agreement for the Company's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

iii. In the event the Company terminates the Agreement in whole or in part for the breaches attributable to Service Provider, the Company may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to **clause 22** Service Provider shall be liable to the Company for any increase in

costs for such similar Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

iv. The Company shall have a right to terminate the Agreement immediately by giving a notice in writing to Service Provider in the following eventualities:

a) If any Receiver/Liquidator is appointed in connection with the business of the Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider.

b) If Service Provider applies to the Court or passes a resolution for insolvency or voluntary winding up of or any other creditor / person files a petition for insolvency or winding up or dissolution of Service Provider.

c) If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors, or representatives, in the reasonable opinion of the Company tantamount to fraud or prejudicial to the interest of the Company or its employees.

v. In the event of the termination of the Agreement, Service Provider shall be liable and responsible to return to the Company all records, documents, data, and information including Confidential Information pertains to or relating to the Company in its possession.

vi. In the event of termination of the Agreement for material breach, the Company shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations.

vii. Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

17) Dispute Redressal Mechanism:

i. All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement (including dispute concerning interpretation) or in discharge of any obligation arising out of the Agreement (whether during the progress of work or after completion of such work and whether before or after the termination of this Agreement, abandonment, or breach of this Agreement), shall be settled amicably.

ii. If the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any party notifying the other regarding the disputes, either party (the Company or Service Provider) shall give written notice to other party clearly setting out there in, specific dispute(s) and/or difference(s), and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance thereof shall be binding on the parties.

iii. In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and the arbitration shall be conducted in accordance with the Arbitration and Conciliation Act, 1996.

iv. Service Provider shall continue providing the Services under the Agreement during the arbitration proceedings, unless otherwise directed by the Company or unless the matter is such that the Services cannot possibly be continued until the decision of the arbitrator is obtained.

v. Arbitration proceeding shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

18) Governing law & Jurisdiction:

i. This Agreement shall be governed by laws in force in India. Subject to the arbitration clause above, all disputes arising out of or in relation to this Agreement, shall be subject to the exclusive jurisdiction of the courts at Mumbai only.

ii. In case of any change in applicable laws that has an effect on the terms of this Agreement, the Parties agree that the Agreement may be reviewed, and if deemed necessary by the Parties, make necessary amendments to the Agreement by mutual agreement in good faith, in case of disagreement obligations mentioned in this clause shall be observed.

19) Severability:

If any part or any provision of this Agreement is or becomes illegal, invalid, or unenforceable, that part or provision shall be ineffective to the extent of such invalidity or unenforceability only, without in any way affecting the validity or enforceability of the remaining parts of said provision or the remaining provisions of this Agreement. The Parties hereby agree to attempt to substitute any invalid or unenforceable provision with a valid or enforceable provision, which achieves to the greatest extent possible the economic, legal, and commercial objectives of the invalid or unenforceable provision.

20) Powers to vary or omit work:

i. No alterations, amendments, omissions, additions, suspensions, or variations of the Services (hereinafter referred to as variation) under the Agreement shall be made by Service provider except as directed in writing by Company. The Company shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct Service provider to make any variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of Service provider, if carried out, prevent them from fulfilling any of their obligations under the Agreement, they shall notify the Company, thereof, in writing with reasons for holding such opinion and Company shall instruct Service provider to make such other modified variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If Company confirms their instructions Service provider's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in cost occasioned by such variation shall be mutually agreed between the parties. In any case in which Service provider has received instructions from the Company as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in the opinion of Service provider, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

ii. If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of reduction in payment to be made to Service Provider before Service provider proceeding with the change.

21) Waiver of rights:

i. Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedyunder this Agreement will not automatically operate as a waiver of such right, power or remedy or any other right,power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power, or remedy by either Party hereunder on one occasionwill not be construed as a bar to a waiver of any successive or other right, power, or remedy on any other occasion.

22) Limitation of Liability:

i. The maximum aggregate liability of Service Provider, subject to clause 22(iii), in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total amount payable to the Service Provider in the twelve months period.

ii. Under no circumstances shall either Party be liable for any indirect, consequential, or incidental losses, damages or claims including loss of profit, loss of business or revenue.

iii. The limitations set forth in Clause 22(i) shall not apply with respect to:

a) claims that are the subject of indemnification pursuant to Clause 12 (infringement of third-party Intellectual Property Right).
b) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider.
c) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations.
d) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Company, provided such guidelines were brought to the notice of Service Provider.

For the purpose of clause 22.iii(b)

"Gross Negligence" means "any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith."

"Willful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

23) Force Majeure:

i. Notwithstanding anything else contained in the Agreement, neither Party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

ii. For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or sub-contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

iii. If Force Majeure situation arises, the non-performing Party shall promptly notify to the other Party in writing of such conditions and the cause(s) thereof. Unless otherwise agreed in writing, the non-performing Party shall continue to perform its obligations under the Agreement as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

iv. If the Force Majeure situation continues beyond 9**0 (ninety) days**, either Party shall have the right to terminate the Agreement by giving a notice to the other Party. Neither Party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

24) Notices:

i. Any notice or any other communication required to be given under this Agreement shall be in writing and may be given by delivering the same by hand or sending the same by prepaid registered mail, postage prepaid, to the relevant address set forth below or such other address as each Party may notify in writing to the other Party from

time to time. Any such notice given as aforesaid shall be deemed to be served or received at the time upon delivery (if delivered by hand) or upon actual receipt (if given by postage prepaid).

ii. A notice shall be effective when it is delivered or on the effective date of the notice, whichever is later.

iii. The addresses for Communications to the Parties are as under.

In the case of the Company	In case of Service Provider
CS Contact Address: [●]	

In case there is any change in the address of one Party, it shall be promptly communicated in writing to the other Party.

25) General Terms & Conditions:

TRAINING: Service Provider shall train CBHFL officials on the configuration, operation/ functionalities, maintenance, support & administration for software, application architecture and components, installation, troubleshooting processes of the proposed Services as mentioned in this Agreement.

PUBLICITY: Service Provider may make a reference of the services rendered to the Company covered under this Agreement on Service provider's Web Site or in their sales presentations, promotional materials, business plans or news releases etc., only after prior written approval from the Company.

SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other party, or aid any third person to do so, without the specific written consent of the other party. However, nothing in this clause shall affect the Company's regular recruitments as per its recruitment policy and not targeted to the employees of Service provider.

SEVERABILITY: The invalidity or unenforceability of any provision of this Agreement shall not in any way effect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

MODIFICATION: This Agreement may not be modified or amended except in writing signed by duly authorized representatives of each party with express mention thereto of this Agreement.

CO-OPERATION IN CASE OF INSOLVENCY OF COMPANY: The Service Provider shall co-operate with the relevant authorities in case of insolvency / resolution of the Company.

ENTIRE AGREEMENT: This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior written agreements, undertakings, understandings, and negotiations, both written and oral, between the Parties with respect to the subject matter of the Agreement, except which are expressly annexed or attached to this Agreement and saved by this Agreement.

No representation, inducement, promise, understanding, condition, or warranty not set forth herein has been made or relied upon by any Party hereto.

The following documents along with all addenda/corrigenda issued thereto shall be deemed to form and be read and construed as integral part of this Agreement and in case of any contradiction between or among them the priority in which a document would prevail over another would be as laid down below beginning from the highest priority to the lowest priority:

a) This Agreement
b) Annexure(s) of Agreement if any
c) Purchase Order No._____dated _____

PRIVITY: Neither this Agreement nor any provision hereof is intended to confer upon any person/s other than the Parties to this Agreement any rights or remedies hereunder.

DUE AUTHORISATION: Each of the undersigned hereby represents to the other that she/ he is authorized to enter into this Agreement and bind the respective parties to this Agreement.

COUNTERPART: This Agreement is executed in duplicate, and each copy is treated as original for all legal purposes.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date and day first mentioned above.

CBHFL
By:
Name:
Designation:
Date:
WITNESS:
1.

2.

Service Provider
By:
Name:
Designation:
Date:

SLA-Annexure-A : Deliverables/Scope Of Work

As per Annexure-C "Scope of Work" of this RFP

SLA-Annexure-B : Escalation Matrix

To be provided by the Service Provider at the time of signing of SLA

Other Instructions for submission of BID :

The documents in connection with the Technical Bid and Commercial BID shall be provided separately in two different envelops with super scribed with the type of BID (Commercial/Technical).

Further, the above mentioned two envelopes must be placed together inside another larger envelope/cover. The outer envelope/cover containing the Two envelopes must be super scribed with the following information:

Details of the RFP : "RFP response for Endpoint Security Solution"
Name of Bidder:
Name of the Authorized Person along with contact details including email Id of the bidding entity.

Further, the large envelope containing Technical and Commercial Bid should reach to the following address on or before last date of Bid submission i.e. 24th December, 2024 by 17:00 P.M.

Cent Bank Home Finance Limited.
6th floor, Central Bank of India, Mumbai Main Office Building,
MG Road, Fort, Flora Fountain, Hutatma Chowk,
Mumbai – 400 023.
Contact Number: 022-69519323 /9028658694

If the outer cover of the Bid is not sealed and marked appropriately, CBHFL will assume no responsibility for the bid's misplacement or premature opening. The deficiency in documentation may result in the rejection of the Bid. Any decision in this regard by CBHFL shall be final, conclusive, and binding on the Bidder.

Any addendum and corrigendum, if any, will be published only on the website, not in newspapers. So, please keep visiting our website for any updation.

== End of the Document ==

'

== End of the Document ==


Cent Bank Home Finance Limited
सेन्ट्रल बैंक ऑफ इण्डिया की अनुषंगी
Subsidiary of Central Bank of India