THE WEST BENGAL STATE CO-OPERATIVE BANK LIMITED - A SCHEDULED BANK

The Bank for you, your business and private financial needs

Head Office: 24A Waterloo Street, Kolkata 700 069

Expression of Interest (EOI)

FOR

Empanelment of CERT-In Empaneled auditor(s) for Conducting Various IT related audits for West Bengal State Cooperative Bank for a period of Five (5) years

REF NO.: HO/MD/1235 **Date: 13/08/2025**

PARTICULARS	DEADLINE
Availability of EOI Document at Bank's website	18/08/2025
Last date for receiving queries through e-mail:	22/08/2025 up to 12:30 PM
Last date of submission of the EOI Proposal	30/08/2025 up to 12:30 PM
Date of opening of the EOI Proposal	02/09/2025 at 3:00 PM
Bank email id for EOI related communication	rfp_coopcbs2010@wbstcb.com

Disclaimer

The information contained in this scope document, or any information provided subsequently to bidder(s) whether verbally or in documentary form by or on behalf of the Bank is provided to the bidder(s) on the terms and conditions set out in this scope document and all other terms and conditions subject to which such information is provided. This scope is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this EOI is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this EOI does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability, and completeness of the information i n this EOI and wherever necessary obtain independent advice. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this EOI. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this EOI.

Contents

1. Introduction

The West Bengal State Co-operative Bank Ltd The West Bengal State Co-operative Bank Ltd. (WBSCB) is the apex cooperative banking institution in West Bengal, playing a pivotal role in the state's rural and agricultural finance ecosystem. Established in 1918 and restructured under its current name in 1967, WBSCB operates under the regulatory framework of the Reserve Bank of India and the state cooperative laws. Its primary objective is to support and strengthen the cooperative credit structure by providing financial assistance and guidance to the Central Cooperative Banks (CCBs) across the state. WBSCB facilitates short-term and medium-term credit for agriculture, rural development, and allied sectors, thereby promoting financial inclusion in underserved areas. The bank also offers a range of retail banking services, including savings and current accounts, fixed deposits, and loan products tailored for farmers, small businesses, and cooperative societies. With its head office in Kolkata and regional offices in Coochbehar, Barasat, and Diamond Harbour, WBSCB ensures statewide coverage. It has also embraced digital transformation by offering internet and mobile banking, along with integration into national payment systems like NEFT, RTGS, and UPI. Through its cooperative model, WBSCB continues to play a crucial role in empowering rural communities and supporting the socio-economic development of West Bengal.

2. Purpose of this EOI

The West Bengal State Co-operative Bank Ltd. (WBSCB) hereby invites responses from competent and CERT-In empaneled firms/organizations for the empanelment of Service Providers to conduct various IT-related audits on a need basis for a period of five (5) years.

This EOI has been issued solely for the purpose of identifying and empaneling qualified audit firms/organization. The empanelment does not guarantee the award of any specific scope of work. As and when audit requirements arise during the financial years within the contract period, WBSCB will share the detailed scope of work with the empaneled firms/organizations. Based on the scope, commercial proposals will be invited, and the selected bidder will be assigned the specific audit engagement.

WBSCB reserves the right to determine the nature and extent of audit assignments to be offered under this empanelment. It is not obligated to allocate all audit scopes exclusively to empaneled firms. WBSCB may, at its discretion, float separate tenders for specific audit requirements if deemed appropriate.

Interested and eligible firms/organizations are encouraged to submit their responses in accordance with the terms outlined in this EOI.

3. Detailed Scope of Work

The empaneled auditor must strictly adhere to the guidelines prescribed by CERT-In for empaneled Information Security Auditing Organizations (Version 3.0) and such guidelines/directives as issued by CERT-In/Regulatory Authorities from time to time. This includes maintaining high ethical standards, ensuring confidentiality, using industry-standard methodologies, and avoiding high-risk or disruptive testing practices. Auditors must obtain prior approvals for penetration testing, ensure secure handling and disposal of auditee data, and refrain from unauthorized data sharing. All audit activities must be conducted transparently, with documented approvals and secure communication protocols. The auditor must also comply with reporting obligations and maintain data storage within India, as per CERT-In norms.

The various audit engagements that may be required to perform by the emplaned Auditors are as follows:

3.1. Information System Audit

The Information Systems (IS) Audit may encompass a broad range of technical and operational areas to ensure the integrity, security, and efficiency of IT systems and processes. Key focus areas may include logical access controls, antivirus and endpoint protection, data communication infrastructure as identified by bank (such as routers/switches), and disaster recovery planning. Auditors may assess the implementation and effectiveness of the bank's Information Systems Security Policy, internet and email usage policies, and long-term IT strategy. The audit may also cover system maintenance practices, management control systems, operating system configurations, list of packaged software as identified by bank as well as parameter settings. Additional areas of review may include peripheral devices, storage media, physical access controls, environmental safeguards, and overall security management. Segregation of duties, software license compliance, system conversion and reconciliation processes, and third-party/vendor service reviews may also be evaluated. Specific operational components such as transaction processing, utility programs, wireless network security, ATM and net banking operations, cheque truncation systems (CTS), and electronic banking platforms may be included. Furthermore, the audit may examine the bank's cyber security framework, Cyber Crisis Management Plan (CCMP), daily ATM transaction reconciliation, transaction record maintenance, and mechanisms for resolving transaction disputes. These areas are indicative and may be tailored based on the specific audit engagement and risk assessment based on regulatory/supervisory/statutory directives & guidelines in vogue. Risk assessment including Risk Categorization of the open observations are also required to be performed along with Gap Analysis with respect to present IT/IS infrastructure of the Bank.

3.2. Cyber Security Audit

Core Banking Software Audit: The audit of the Core Banking Software (CBS) shall include a comprehensive review of the application's compliance with functional specifications, regulatory standards, contractual obligations, and user documentation. It will assess change management procedures, user training, feedback mechanisms, and the overall confidentiality, integrity, and availability of the CBS and its interfaces. Specific areas of focus will include authorization controls (e.g., maker-checker mechanisms, exception handling), authentication methods, user and password management, parameter maintenance, access rights, audit trail generation, and change management documentation. Additionally, the audit may cover data center operations, statutory and MIS reporting, and an overall operational review of the CBS. Security assessments will be conducted in line with OWASP guidelines, including database configuration and application-level vulnerabilities, supported by proof-of-concept (POC) screenshots where applicable.

Core IT Operations: This component will evaluate the bank's core IT operational controls, including application security, change management, incident and problem management, and IT operations governance. It will also cover internal and external system interfaces, bulk transaction posting, system-generated transactions, report generation, access controls, and infrastructure security. Compliance with regulatory requirements and data protection standards will be reviewed to ensure robust operational resilience.

IT Setup at Branches: The audit will assess network connectivity in branches and the head office as well as other areas like CBS user management, IT support mechanisms, anti-malware controls, physical security, and user awareness of information security practices. Additional areas include ATM management, environmental controls, business continuity arrangements, and governance of IT and cyber security policies, procedures, disaster recovery plans, and business continuity plans. The audit will also review IT outsourcing practices, including vendor management, SLAs, NDAs, risk

mitigation strategies, and compliance monitoring.

Cyber Security Control Review: The audit will focus on the bank's overall cyber security architecture, including network, server, and endpoint security. It will assess incident and fraud management capabilities, risk management frameworks, patch management, system hardening, encryption practices, and staff training and awareness programs. The objective is to ensure a resilient and secure IT environment aligned with industry best practices and regulatory expectations. Risk assessment including Risk Categorization of the open observations are also required to be performed along with Gap Analysis with respect to present IT/IS infrastructure of the Bank.

3.3. Vulnerability Assessment and Penetration Testing Audit

This audit will focus on various applications and systems used by WBSCB such as but not limited to *(Mobile Banking Application, IMPS, UPI, AML, CKYC, Micro ATM Application at PACS device, Micro ATM CSP Application, Website of the Bank, NSDL Application, SFMS setup etc)* in alignment with industry standards such as the OWASP guidelines, NIST Standard. The VAPT exercise should include proof-of-concept (POC) screenshots and cover a wide range of security aspects including application design flaws, password vulnerabilities, backdoor detection, denial-of-service (DoS/DDoS) resilience, and network penetration risks etc. Auditors may assess vulnerabilities such as IP spoofing, buffer overflows, session hijacking, injection flaws, and cross-site scripting. The review should also include SSL certificate validation, firewall rule base configuration, intrusion detection systems (IDS), logical access controls, and remote server management. Additional focus areas include system patching, backup infrastructure, biometric authentication, proxy server configuration, and monitoring tools. Compliance with RBI and NABARD guidelines, data confidentiality, and legal and regulatory considerations must also be evaluated to ensure robust cyber security posture across the bank's digital assets. The detected vulnerabilities are also required to be categorized as per respective criticalities (with CVSS score) with recommended remediation measures.

3.4. General Data Protection and Regulation (GDPR) Audit

The empaneled auditors may be required to conduct GDPR (General Data Protection Regulation) audits to assess the Bank's compliance with applicable data protection laws and privacy standards, particularly in relation to the handling of personal data of individuals. The audit will involve a comprehensive review of data collection, processing, storage, sharing, and disposal practices across the Bank's systems and operations. Auditors may be expected to evaluate the Bank's data protection existing process/policy, consent management mechanisms, data subject rights (such as access, rectification, erasure, and portability), and procedures for handling data breaches. The audit should also assess the adequacy of technical and organizational measures in place to ensure data security, including encryption, access controls, data minimization, and retention policies. Special attention should be given to data transfers, third-party data processing. All findings must be supported by verifiable evidence and aligned with GDPR principles of lawfulness, fairness, transparency, accountability, and data integrity. The scope of each engagement will be defined by the Bank based on operational needs and regulatory requirements.

3.5. Other IT Related Audits

The empaneled auditors may be required to undertake various other IT-related audits based on the evolving operational, regulatory, and strategic needs of the Bank. The scope of each audit engagement will be defined by the Bank at the time of requirement and may vary depending on the nature of the systems, regulatory mandates, and risk assessments.

4. Compliance Verification and Submission of Reports

For all audit engagements undertaken by the empaneled auditors, a structured reporting and compliance process shall be followed. Upon completion of the initial audit activities, the auditor will submit a Draft Observation Report to the Bank, highlighting preliminary findings, potential risks, and areas of concern. The Bank will then review the observations and provide a formal compliance response, detailing corrective actions taken, clarifications, or mitigation plans. Based on the Bank's response, the auditor will finalize the audit review and submit a Final Audit Report, incorporating validated findings, compliance status, and actionable recommendations for improvement. The final report shall include supporting evidence such as logs, screenshots, reconciliation statements, and relevant documentation. This process ensures transparency, accountability, and alignment with regulatory and operational standards. The Bank may also request follow-up reviews or verification audits to confirm the implementation of recommended measures, as deemed necessary.

5. Eligibility Criteria

Sr. No.	Eligibility Criteria	Supporting Documents
Mandatory Bidder Eligibility Criteria		
1	The bidder should be a legal entity registered in India, under the Indian Companies Act 1956 or Partnership/LLP Act 2013 as per the Companies Act, and should be in existence for last 5 years from the date of EOI.	Certificate of Incorporation/Partnership deed. Copy of certificate of GST Registration and PAN card
2	The Bidder should have average annual turnover of 1 crore in the last three financial years, viz., 2022-23, 2023-24 and 2024-25.	Audited Financial Statements for the financial years 2022-23, 2023-24 and 2024-25. If Audited financial statements not available for 2024-25 then certified provisional financial statement for FY 2024-25 to be provided from Auditor with UDIN.
3	The Bidder should have a positive profit before tax in each of the last three financial years, viz., 2022-23, 2023-24 and 2024-25.	Audited Financial Statements for the financial years 2022-23, 2023-24 and 2024-25. If Audited financial statements not available for 2024-25 then certified provisional financial statement for FY 2024-25 to be provided from Auditor with UDIN.
4	The Bidder should not have been blacklisted/debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs). Also, the Bidder has neither been convicted nor is any criminal case pending against it before any court in India.	Self-declaration by the competent authority of the Bidder.
5	The bidder should be empaneled by CERT-In as an Information Security Audit Organization at least for last 3 years as on EOI submission date.	Copy of Certificate. Proof of CERT-In empanelment of last three years.

Sr. No.	Eligibility Criteria	Supporting Documents
6	The bidder should have conducted **Cyber Security Audit as well as at least two (2)** type of Audits from below mentioned in **at least one (1)** Public Sector Bank / Private Bank / Small Finance Bank / Regional Rural Bank / Cooperative Bank) in **last 3 years**. a. IS Audit b. VAPT Audit c. GDPR Audit	PO/ Credential letter from client mentioning the organization name, date of execution and scope of work. Multiple client letter accepted.
7	The Bidder should have at least one (1) CISA Certified professional having three years of experience and at least three (3) professionals having valid certification of CISSP/CISM/CA/CEH/OSCP etc. along with three or more years of Audit experience.	Self-Declaration of Bidder confirming at least 4 resources under its payroll. Resume/Profile of at least two (2) professionals, including copies of their relevant certifications (CISSP /CISM/CA/CEH/OSCP etc.) Resume/Profile of one (1) professional, including copies of their relevant certifications (CISA)

Notes:

- The eligibility criteria is made for empanelment of Audit only.
- Each Financial Year Bank will ask Empaneled auditors to submit:
  - Valid CERT-In empanelment certificate.
  - Non-Blacklisting Declaration.
  - Declaration for eligibility criteria 6.
  - Declaration for eligibility criteria 7.
  - Positive Profit Before tax of the previous financial year.
- Consortium is not allowed between two auditors for the empanelment.

6. Evaluation Procedure

— Eligibility Evaluation

— Bank may empanel all the audit firms/organization based on the eligibility qualification of the Bidders.

7. Financial Proposal

The financial quotes are not required to be submitted at the time of EOI submission by the Auditor Firms/Organizations. Financial quotations will be invited by the bank from empaneled Auditor during the period of empanelment based on bank's requirements. Bank as a part of closed tendering process may ask the empaneled auditor to submit their commercials for the specified scope of work. However, Bidder to note that no advance payment will be made for any audit work. The payment will be made only after completion of the job

8. Introduction to the Bidders

8.1. Bidder's Liability

i. The Language of Bid should be in English.

ii. The EOI not submitted with the eligibility information or incomplete in any aspect is liable for rejection. The Bank is not responsible for non-receipt of bid within the specified date and time due to any reason including Holidays.

8.2. Limitation of Liability

The aggregate liability of the vendor in connection with this EOI, will be the services provided by the bidder for the specific scope of work document, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise) and including any and all liability shall be the actual limited to the extent of the total contract value.

8.3. Indemnity

The bidder shall, at its own cost and expenses, defend and indemnify the bank against all third-party claims including those of the infringement of intellectual property rights, including patent, trademark, logo, copyright, trade secret or industrial design rights, arising from the performance of the contract.

The bidder shall expeditiously meet any such claims and shall have full rights to defend itself therefrom. If the bank is required to pay compensation to a third party resulting from such infringement etc., the bidder will bear all expenses including legal fees.

Bank will give notice to the bidder of any such claim and shall provide reasonable assistance to the Bidder in disposing of the claim.

The bidder shall also be liable to indemnify the bank, at its own cost and expenses, against all losses/damages, which bank may suffer on account of violation by the bidder of any or all applicable national/ international trade laws. This liability shall not ensue if such losses/ damages are caused due to gross negligence or willful misconduct by the bank or its employees.

8.4. Document to be submitted with Bid

The Bidders shall submit the following documents along with Bid in PDF file.

Sr.No.	Particulars	Annexure / Document
1	Letter for EOI Participation	Annexure – 1
2	Bidder's Information	Annexure – 2
3	Confirmation to Eligibility Criteria	Annexure – 3
4	Non-Disclosure Agreement	Annexure – 4

8.5. Force Majeure

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

For purposes of this Clause, "Force Majeure" means an event beyond the control of the bidder and not involving the bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of the Bank in its sovereign capacity, wars or revolutions, fires, floods, epidemics, and quarantine restrictions.

If a Force Majeure situation arises, the bidder shall promptly notify the Bank in writing of such condition and the cause thereof within fifteen calendar days. Unless otherwise directed by the Bank in writing, the bidder shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not

prevented by the Force Majeure event.

8.6. Bidder's Integrity

The bidder is responsible for and obliged to conduct all contracted activities in accordance with the contract using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the contract.

8.7. Bidder's Obligation

The bidder is obliged to work closely with the Bank's staff, act within its own authority and abide by directives issued by the Bank and implementation activities.

The bidder is responsible for managing the activities of its personnel or its representatives and will hold itself responsible for any misdemeanors. The bidder is under obligation to provide consultancy services as per the contract.

The bidder will treat as confidential all data and information about the Bank, obtained in the execution of their responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

8.8. Information Ownership

All information processed, stored, or transmitted by Vendor equipment belongs to the Bank. By having the responsibility to maintain the equipment, the vendor does not acquire implicit access rights to the information or rights to distribute the information. The vendor understands the civil, criminal, or administrative penalties may for failure or protect information appropriately.

8.9. No Legal Relationship

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

8.10. Errors and Omissions

Each Recipient should notify WBSCB of any error, omission, or discrepancy found in this EOI document.

8.11. Acceptance of Terms

A recipient will, by responding to WBSCB for EOI, be deemed to have accepted the terms of the Introduction and Disclaimer. If the submission does not include all the information required or is incomplete, the proposal is liable to be rejected.

All submissions, including any accompanying documents, will become the property of WBSCB. Recipients shall be deemed to license, and grant all rights to WBSCB to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients and to disclose and/or use the contents of the submission as the basis for processing of EOI, notwithstanding any copyright or other intellectual property right that may subsist in the submission or accompanying documents.

8.12. Termination for Convenience

The Bank reserves the right to terminate the empanelment of auditors, in whole or in part, at its sole discretion and for its convenience, by providing a written notice of fifteen (15) days to the concerned empaneled auditor(s). The notice shall explicitly state that the termination is being effected for the Bank's convenience.

Additionally, the Bank may terminate the empanelment with immediate effect in the event of any credible information or reports indicating:

- A breach or failure in audit responsibilities in any organization associated with the auditor, or
- Debarment or blacklisting of the auditor by the Indian Computer Emergency Response Team (CERT-In) or any other competent authority.

8.13. Applicable Law and Jurisdiction of Courts

The Contract with Bidder shall be governed in accordance with the Laws of India for the time being enforced and will be subject to the exclusive jurisdiction of Courts in Kolkata / Honorable High Court at Kolkata (with the exclusion of all other Courts).

8.14. Clarification of EOI

A prospective bidder requiring any clarification of the EOI may notify the Bank in writing, by e - mail at the Bank's mailing address indicated in the Expression of Interest (EOI). The Bank will respond in writing to any request for clarification of the EOI which it receives prior to the date of EOI Submission.

2 Annexure - 1 - Letter for EOI Participation

REF NO.: HO/MD/1235 Dated 13/08/2025

To,
The Managing Director,
The West Bengal State Co-operative Bank Ltd.
24A, Waterloo Street,
Kolkata – 700 069

Sub: Expression of Interest (EOI) for Empanelment of CERT-In Empaneled auditor(s) for Conducting Various IT related audits for West Bengal State Cooperative Bank for a period of Five (5) years

Having examined the Expression of Interest including all annexure, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to deliver services in conformity with the said EOI.

We undertake, if our proposal is accepted and if we get empaneled, then we agree to deliver the services as and when Scope of Work is given by Bank.

We agree to abide by this bid for the period of 5 years if selected and it shall remain binding upon us and may be accepted at any time before the expiration of the period.

We undertake that, in competing for (and, if the award is made to us, in executing) the Letter of Intent, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We understand that the bank is not bound to accept the proposal even if eligibility qualified until formal Letter of Intent is given to the Auditor Firm/Organization.

Place:

Dated: this day of 2025.

……
……Signature) (In the Capacity of)

Duly authorized to sign bid for and on behalf of

3 Annexure – 2 Bidder's Information

Name of the Bidder	
Constitution & Year of Establishment	
Registered Office/Corporate office Address	
GST Registration No. & PAN	
Mailing Address	
Name and designations of the persons authorized to make commitments to the Bank against the EOI Response	
Telephone e-mail	
Name & Addresses of Directors/Promoters	
Net Profit Based on the Audited Financial Statement of the Bidder: FY 2022-23: FY 2023-24: FY 2024-25:	
CERT-IN Empanelment Details	
Turnover of the Bidder Financial Statement of the Bidder: FY 2022-23: FY 2023-24: FY 2024-25:	

4 Annexure – 3 Confirmation to Eligibility Criteria

Sr. No.	Eligibility Criteria	Supporting Documents	Documents Attached (Yes/No)
Mandatory Bidder Eligibility Criteria			
1	The bidder should be a legal entity registered in India, under the Indian Companies Act 1956 or Partnership/LLP Act 2013 as per the Companies Act, and should be in existence for last 5 years from the date of EOI.	Certificate of Incorporation/Partnership deed. Copy of certificate of GST Registration and PAN card	
2	The Bidder should have average annual turnover of 1 crore in the last three financial years, viz., 2022-23, 2023-24 and 2024-25.	Audited Financial Statements for the financial years 2022-23, 2023-24 and 2024-25. If Audited financial statements not available for 2024-25 then certified provisional financial statement for FY 2024-25 to be provided from Auditor with UDIN.	
3	The Bidder should have a positive profit before tax in each of the last three financial years, viz., 2022-23, 2023-24 and 2024-25.	Audited Financial Statements for the financial years 2022-23, 2023-24 and 2024-25. If Audited financial statements not available for 2024-25 then certified provisional financial statement for FY 2024-25 to be provided from Auditor with UDIN.	
4	The Bidder should not have been blacklisted/debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs). Also, the Bidder has neither been convicted nor is any criminal case pending against it before any court in India.	Self-declaration by the competent authority of the Bidder.	
5	The bidder should be empaneled by CERT-In as an Information Security Audit Organization at least for last 3 years as on EOI submission date.	Copy of Certificate. Proof of CERT-In empanelment of last three years.	
6	The bidder should have conducted **Cyber Security Audit as well as at least two (2)** type of Audits from below mentioned in **at least one (1)** Public Sector Bank / Private Bank / Small Finance Bank / Regional Rural Bank / Cooperative Bank) in **last 3 years** a. IS Audit b. VAPT Audit	PO/ Credential letter from client mentioning the organization name, date of execution and scope of work. Multiple client letter accepted.	

Sr. No.	Eligibility Criteria	Supporting Documents	Documents Attached (Yes/No)
	c. GDPR Audit		
7	The Bidder should have at least one (1) CISA Certified professional having three years of experience and at least three (3) professionals having valid certification of CISSP/CISM/CA/CEH/OSCP etc. along with three or more years of Audit experience.	Self-Declaration of Bidder confirming at least 4 resources under its payroll. Resume/Profile of at least two (2) professionals, including copies of their relevant certifications (CISSP /CISM/CA/CEH/OSCP etc.) Resume/Profile of one (1) professional, including copies of their relevant certifications (CISA)	

5 Annexure – 4 Non-Disclosure Agreement

(Duly stamped on stamp paper INR 500/-)

This Non-Disclosure Agreement ("Agreement") effective from xx xx 2025 ("Effective Date") is formed between The West Bengal State Co-operative Bank Ltd., having head office at The West Bengal State Co-operative Bank Ltd, 24A Waterloo Street, Kolkata 700069 ("Customer") and ..... ("Company") having its Registered office at ..... to share Confidential Information for the purpose of assessing potential business relationships ("Purpose").
Parties agree as follows:

1. The party disclosing Confidential Information is a Discloser and the party receiving Confidential Information is Recipient.
2. Confidential Information means information of a party that is identified with either a restrictive legend, or where the circumstances surrounding disclosure indicate the information is confidential. Confidential Information includes proprietary information, personal data and sensitive personal data of individuals, and other information relating to financing strategies, organizational strategies, trade secret information, financial information, pricing policies, operational methods, marketing information and other business affairs of Company relating to the business. oral, visual or written communication made to each other shall be considered to be Confidential.
3. The Recipient may disclose Confidential Information only to (a) its employees, agents, subcontractors, majority owned affiliates; (b) those having a need to know the Confidential Information for the Purpose or otherwise for the benefit of the Discloser, where the above persons/entities are bound by confidentiality obligations as stringent as those contained herein.
4. Information disclosed under this Agreement will be governed by this Agreement for five (5) years following the initial date of disclosure. Upon the request of the Discloser, all Confidential Information, in possession of the Recipient and other items which contain, disclose and/or embody any Confidential Information (including, without limitation, all copies, reproductions, summaries and notes of the contents thereof), shall be returned to Discloser or destroyed by the Recipient, and the Recipient will certify that the provisions of this paragraph have been complied with.
5. The Recipient will use at least the same care, but no less than reasonable care, to avoid disclosure of the Discloser's Confidential Information as it uses with its own Confidential Information and will use the Discloser's Information only for the purpose for which it was disclosed.
6. This Agreement will not apply to any information that (a) is or becomes publicly available without breach of this Agreement; (b) is known by the Recipient without any confidentiality obligation, (c) is rightfully received from a third party who did not acquire such information by a wrongful or tortuous act; (d) is independently developed by the Recipient or (e) is authorized by the Discloser for release. Notwithstanding anything to the contrary, this section will not apply to any personal data or sensitive personal data processed by either party arising out of the relationship by the parties, unless permitted by law.
7. If a governmental entity or legal authority requires the Recipient to disclose Confidential Information, the Recipient will give the Discloser prompt written notice sufficient to allow the Discloser to seek a protective order. The Recipient will also use reasonable efforts to obtain confidential treatment for any such Confidential Information.
8. No rights are granted to use the Confidential Information except for the express limited rights stated in this Agreement. The Confidential Information remains the exclusive property of the Discloser.
9. This Agreement shall be governed by the laws of India, and both parties further consent to jurisdiction by the courts in **Kolkata, India**.
10. Either party may terminate this Agreement by providing thirty (30) days written notice to the other party. Any terms of this Agreement, which by their nature extend beyond its termination remain in effect until fulfilled and apply to respective successors and assignees.
11. The parties will comply with all applicable export and import laws and regulations to the extent they apply to

the Confidential Information.

12. All right, title and interest (and associated intellectual property rights) in the Confidential Information and derivatives shall belong to Discloser and its licensors (as case maybe).
13. The receipt of Confidential Information under this Agreement will not limit the Recipient from providing or developing products or services which may be competitive with products or services of the Discloser or assigning responsibilities to its employees, agents or subcontractors provided the Recipient does not breach any of the terms of this Agreement.
14. In case of breach, the affected party shall have the right to seek injunctive relief, which relief shall not exclude any other recourse provided by law.

15. This Agreement is the entire agreement regarding the use and disclosure of Confidential Information and replaces any prior oral or written communications between us regarding these disclosures. By signing below, each party agrees to the terms of this Agreement. This Agreement may only be altered or modified by written instrument duly executed by both parties. Once signed, any reproduction of this Agreement made by reliable means (for example, photocopy facsimile or digital image) is considered an original. All waivers shall be in writing. If any provision(s) hereunder is unenforceable, the remaining provisions shall be held valid and enforceable. Notices shall be in writing and to the addresses captured herein or notified by the other party. The undersigned represent that they are duly authorized representatives of the parties and have full authority to bind the parties. This Agreement will be effective as of the Effective Date.

<Bidder's Name>	The West Bengal State Cooperative Bank Limited
Sign:	Sign:
Name:	Name:
Designation:	Designation:
Date:	Date:
Seal:	Seal: