REQUEST FOR PROPOSAL

CYBER SECURITY OPERATIONS CENTRE

MONITORING AND REPORTING MAN POWER SUPPORT

Ref.No: TMB/ITD/RFP/2023-2024/002 Dated: 14.11.2023

TAMILNAD MERCANTILE BANK LTD
Information Technology Department
Plot No: 4923, AC-16, Second Avenue,
Anna Nagar West, Chennai – 600040.

The information provided by the bidders in response to this RFP Document will become the property of the Bank and will not be returned. The Bank reserves the right to amend, rescind or reissue this RFP Document and all amendments will be advised to the bidders and such amendments will be binding on them. The Bank also reserves its right to accept or reject any or all the responses to this RFP Document without assigning any reason whatsoever.

This document is prepared by Tamilnad Mercantile Bank Ltd., (TMB) for availing SOC Manpower Support Services at Chennai. It should not be reused or copied or used either partially or fully in any form.

Disclaimer

While the document has been prepared in good faith, no representation or warranty, express or implied, is or will be made, and no responsibility or liability will be accepted by Tamilnad Mercantile Bank Ltd., (TMB) or any of its employees, in relation to the accuracy or completeness of this document and any liability thereof expressly disclaimed. The RFP is not an agreement and is not an offer by TMB, but an invitation for bidder's responses. No contractual obligation on behalf of TMB, whatsoever, shall arise from the offer process unless and until a formal contract is signed and executed by duly authorized officials of TMB and the Bidder.

Index

REQUEST FOR PROPOSAL (RFP) FOR CYBER SECURITY OPERATIONS CENTRE MONITORING AND REPORTING MAN POWER SUPPORT

INTRODUCTION

M/s Tamilnad Mercantile Bank Ltd.,(therein after referred as "Bank") is a leading old private sector bank in India established during the year 1921 having registered office at 57, V.E. Road, Thoothukudi – 628 002. Presently, the Bank has a network of 536 Branches and over 1483 ATMs all over India. Bank intends to invite Bids for service provider to provide full-fledged services for managing and monitoring the Cyber Security Operations Centre (C-SOC).

1. Scope of Work – CSOC Service Provider

The overall scope of work would be C-SOC operation which is monitoring and managing SOC devices including SIEM, WAF, DAM, PAM, etc. It includes monitoring, performance tuning, optimization and maintenance of SIEM and security tools, SIEM log backup, troubleshooting, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEMs and any other activities related to or connected to the Information Technology / Cyber security solutions, devices and technologies.

2. Eligibility Criteria

- The applicant should possess the requisite experience, resources and capabilities in providing the services necessary to meet the requirements of the Bank. The applicant must also possess the technical know-how and the financial wherewithal that would be required to successfully execute the replication solution and support services sought by the Bank for the entire period of contract

- The Applicant shall not subcontract or permit anyone other than its personnel or the OEM supplier to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank
- The application must be complete in all the aspects and should cover the entire scope of work as stipulated in the document
- Applicant should have experience in C-SOC management and monitoring for minimum 3 years in servicing banks / financial institutions.
- Applicant should provide satisfactory performance certificates from two customers to whom the applicant is currently providing C-SOC services (24X7) for similar requirements, at least 1 year as on 30.09.2023.
- The Applicant should not be currently blacklisted by any bank / institution in India or abroad
- The Applicant is required to provide factually correct responses to the RFP, adequate justification for the response (including technical and other requirements) as a part of the response. In case the bank finds any response to be inadequate, the Bank has the right to ask for additional explanation / justification.
- The professionals identified for managing and monitoring C-SOC should possess essential qualification and should have exposure to the field of work.
- The professionals for managing and monitoring C-SOC should be capable of performing gap analysis, recommending C-SOC measures to bridge regulatory compliance material weaknesses, broad understanding of global and local regulatory compliance policies and the ability to manage host / provide ongoing support.

3. Detailed Scope of Work

- Manage and monitor Cyber SOC 24 * 7 * 365 days.
- Monitoring and raising tickets for security incidents / attacks into / on / against Bank's IT assets and follow up with concerned team till closure.
- Manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
- Provide proactive threat intelligence and threat hunting.
- To fix the security loopholes identified through security incident monitoring.
- Ensure adherences to Bank's Information Security Policy and Cyber Security Policy.
- Risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and applications under the scope of C-SOC.
- Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.
- Provide forensics support as per the requirement of Bank in case of any incident.
- Dashboard for reporting and SLA management.
- Rapid response to incidents and forensics.
- Participation in Cyber Drills and identifying the attacks and its remedial action.
- The C-SOC team shall support for internal / external and regulatory / compliance requirements of the Bank.
- Forwarding the IOCs received from threat intel forums like CERT-IN,

VISA, IB-CART, NPCI, etc., to the respective Bank's teams as tickets.

- 24 * 7 * 365 monitoring of Security Incident and Event Management tool for the following event resources.
- Creation of new use cases, policies, rules, custom parsers and fine tuning.

S. No	SIEM Data Source Type
1.	Web Application Firewall (WAF)
2.	Database Activity Monitoring (DAM)
3.	Privileged Access Management (PAM)
4.	Firewalls
5.	Network Devices / Routers
6	Web Gateway
7	Messaging Gateway
8.	Antivirus / EDR
9.	IDS / IPS / NAC
10	Honeypot / Deception Solution
11	Data Leakage Prevention Solution
12	Critical Applications and Databases
13	Servers

Device Management requirements

Security Operations/ Tool Management		
S. No	Device Type	Quantity
1.	IBM Q-Radar – Security Incident and Event Management(SIEM)	1
2	F5 – Web Application Firewall (WAF)	1
3	IBM Guardium – Database Activity Monitoring(DAM)	1
4	Arcos-Privileged Access Management(PAM)	1
5	OTRS – Ticketing Tool	1

4. Proposed C-SOC manpower team structure

- The C-SOC skilled manpower requirement is for 9 (6 L1 + 2 L2+ 1 L3) resources. However, the Bank reserves the right to increase / decrease this number, anytime during the contract period.
- The applicant is expected to quote for the supply of manpower for minimum of these 9 resources for C-SOC operations. The job descriptions, responsibilities and skill sets are as per this document.
- The L1 resources are expected to work in three shifts 24X7, they will do the 1st level incident analysis and alerting.
- L2 resources should do the next level incident analysis, resolution and closure of tickets, threat hunting, trend analysis and reporting. They shall work to cover maximum peak business hours of Bank working days.
- L3 resource shall perform system configuration, adding / removing data sources, device management, updates, creation / fine tuning of use cases, policies, custom parsers based on the requirement. L3 resource shall also works on all Bank working days. L2 resources shall also assist L3 on the above works.
- The L1, L2 and L3 resources engaged shall be retained for a minimum period of one year (Lock-in Period).

5. C-SOC manpower skill requirement

Type of Engineer	C-SOC L1 support	C-SOC L2 Support	C-SOC L3 Suppot
Location	TMB C-SOC (onsite)	TMB C-SOC (onsite)	TMB C-SOC (onsite)
Skills, Requirements	-B.Sc (CS / IT) / BCA / B.E./ B.Tech / MCA / M.Sc (CS / IT)	- B.E./ B.Tech / MCA / M.Sc (CS / IT) -Total 3 Years of	- B.E / B.Tech / MCA / M.Sc (CS / IT) -Total 4 Years of

	- Minimum of 2 years of experience in C-SOC services conducting security device administration and management - Minimum 1 year in operating a SIEM product and other security tools - CEH / CompTIA certifications Preferred.	experience out of which, minimum 2 years' experience in C-SOC services conducting security device administration and management and minimum 2 years in SIEM tool and other security tools. - Certification in at least one industry leading SIEM product and other certifications.	experience out of which, minimum 3 years' experience in C-SOC services conducting security device administration and management and minimum 2 years in SIEM tool and other security tools – Certification in at least one industry leading SIEM product. Other leading certifications in security, such as CISA, CEH, CISSP, CISM, CRISC is preferred.

6. Ongoing C-SOC Approach:

6.1 Security Incident and Event Management (SIEM)

- TMB's critical devices including servers, network devices, applications are already integrated with SIEM system that provides all the security related information to the SIEM system.
- The raw log information received by SIEM tool will be filtered, correlated based on default and custom rules defined in the SIEM system.
- All the incidents / alerts shall be sent out to the Bank's IT Team as per the agreed communication matrix.
- Integrity of log data is maintained with confidentiality and online archival of 9 months is done along with an offline archival of 27

months, a total of three years.

- Monitoring is done on role-based access and audit log is maintained for keeping track of the activities done by C-SOC team.
- C-SOC team shall monitor the SIEM console for security events.
- For the monitored security incidents, severities of incidents are classified based on the following parameters
    - Threat Severity
    - Vulnerability Information
    - IT asset business criticality

By correlating the above parameters, severity score for incidents shall be calculated. Based on the severity scores, the C-SOC team will respond to the incidents.

- As per priority of the monitored incident, the tickets shall be raised and the incident shall be assigned to incident manager for analysis and resolution.
- The analysis shall be communicated to respective IT stake holders as alerts and for resolution purposes.
- The C-SOC team shall follow-up with respective stake holders/ third parties to take necessary actions to close the incident.
- SIEM incident fix shall be validated and closed after monitoring the incident for a day.
- Provisioning of log collection from newly rolled out systems.
- Creation of new use cases, policies, rules, custom parsers and fine tuning.
- Periodical threat hunting.

6.2 Web Application Firewall

- 24 * 7 Monitoring of device availability and performance alerts.
- To monitor attacks, server errors and other unauthorized activities.

- To proactively block attacks through proper policy / rule configuration.
- To take actions during suspicious activities / attacks like drop requests and responses, block the TCP session, block the application user, or block the IP addresses etc.,
- Ensure HTTP and SSL web applications are also protected without terminating or changing HTTPS connections.
- Ensure XML contents are also protected.
- Administration of WAF device using the web console provided by OEM and OOB management in case of device not accessed through network.
- Prepare compliance reports and share with TMB team.
- Creation / Fine tuning of WAF policies / use cases / rules.

6.3 Database Activity Monitoring (DAM)

- Adding / removing databases / instances for database activity monitoring.
- Setting up the alerts for Database incidents.
- Creation / fine tuning of DAM policies / use cases / rules.
- Blacklisting / White listing
- Monitor and report on Data Manipulation Language (DML) commands.
- Capture and report on Data Definition Language (DDL) commands.
- Report on detailed SQL, including the source of the request, the actual SQL commands, the database user name when the request was sent and what database objects the command was issued against.
- Create custom reports, understand detail levels.
- Group objects (sensitive and financial) and activities for use in reporting
- Capture and report access to sensitive objects.
- Alert real time on specific execution of an SQL command.
- Report on database access including logins, client IP, Server IP and

source program information.

- Perform audits on specific user and review all the commands executed.
- Alert on multiple failed logons

6.4 Privilege Access Management (PAM)

- Conduct role engineering to design the access policies for servers and network devices.
- Configure and fine tune access policies for servers and network devices.
- Configure end user accounts and associated access policies and manage their privileges.
- Design and configure PAM reports and dashboard.
- Generate daily, weekly, monthly PAM reports.
- Monitor and analyze PAM alerts and perform incident management.
- Analyze PAM recordings for incident analysis.

6.5 Security Event / Incident Severity

Event Severity: Events severity is defined as High / Medium / Low depending on the impact it has in the Bank's environment.

Asset Criticality: Asset criticality is defined by identifying what systems directly impact the Bank's environment. All the assets are assigned criticality level of High/Medium/Low depending on the impact they have on working of the Bank.

Security Incident Severity: Security incident severity is derived using the 3*3 matrix of Asset criticality and event severity given below:

Incident Severity Matrix		**Asset Criticality Levels**		
		Critical / High	**Medium**	**Low**
Event	**Critical /**	**HH**	**HM**	**HL**

Severity Levels	**High**			
	Medium	**MH**	**MM**	**ML**
	Low	**LH**	**LM**	**LL**

Description of proposed Security Incident Severity level is given below:

Incident Severity	**Coverage**	**Description**
Low – S3	LH / LM/ LL	Events that cannot be definitively identified as attacks and have no effect on operations. ❖ Isolated and non-repeated scans or pings from an external uncontrolled network. ❖ Malware detected and removed prior to begin placed on a network.
Medium – S2	MH/ MM/ ML	Incident that have no effect on operations and comprise identified but unsuccessful attempts to actively breach an information security policy ❖ Accidental failure to physically secure systems overnight. ❖ Repeated active probes or port mappings from an external network. ❖ Malware that has been successfully contained or removed.
Critical / High – S1	HH/ HM/ HL	Incidents made up of any successful attempt to actively breach an information security policy and might result in a minor

		or moderate effect on operation. ❖ Unauthorized access acquired or attacks. ❖ Malware found on more than one system or an inability to contain and remove the code. ❖ The defacement, alteration or deletion of Web server files.

The severity definitions will be fine-tuned after discussion with Bank's team during transition phase.

6.6 Security event list / reports

Below is indicative list of security incidents that are required to be monitored in the Bank's environment, additional events would be required as per current threat scenario

Sl. No	Event Type for servers
1	Login of privileged accounts after office hours
2.	Attempted logins with default / disabled accounts
3.	Repeated failed login with privileged accounts
4.	System stop
5	Program installation / removal
6.	Failure / Enabling / Disabling of logging services
7	Changes in system time
8	Creation / Deletion of user accounts
9.	Disabling of Anti-Virus
10.	Changes to critical system files
11.	Login with privileged accounts
12.	Service Start / Stop

13.	Escalation of privileges (e.g use of Su in Unix)
14	Repeated failed logins after office hours
15	Deletion of log files
16	Repeated failed login with privileged accounts
17	Reset / change of admin passwords
18	Login with user accounts
19	Repeated attempts to access non-allowed services
20	Failed authorization to allowed services
21	Violations of set policies
22	Assigning of privileged to user accounts
23	Access to specific files
24	Changes to specific files
25	Copying of specific files
26	Deletion of specific files
27	I/O device attachment / detachment
28	Login to users accounts after office hours
29	System Start

Sl. No	**Gateways(Both internal & external) – Firewalls and Gateways**
1.	Login with privileged accounts
2.	Login of user accounts after office hours
3.	Attempted login with default / disabled accounts
4.	Repeated failed login with privileged accounts
5.	Repeated failed login with user accounts
6.	Repeated failed login after office hours
7.	System Start/stop
8.	Service Start/stop

9	Failure of logging services
10	Enabling / Disabling of logging services / changes to logging level
11	Changes to system time
12	Escalation of privileges
13	Assigning of privileges to user accounts
14	Creation / Deletion of user accounts
15	Reset / change of passwords
16	Repeated attempts to access non-allowed services on device
17	Repeated failed attempt to access allowed service on device
18	Access attempts to the device from unauthorized hosts(Internal hosts)
19	Configuration changes with access permitted from Internet (On access control gateways)
20	Configuration changes with access permitted on all ports (On access control gateways)
21	Mail spoofing(Internal)
22	Virus infected mails originating from internal networks
23	Probes from External networks
24	Probes from Internal networks
25	Spyware
26	SPAM mails originating from Internal
27	SPAM mail originating from Outside
28	Repeated attempts to access non-allowed services (From external networks)
29	Repeated attempts to access non-allowed services(From internal networks)
30	Large traffic observed from internal system due to mis-configured

	systems.
31	Large traffic observed from internal system due to virus infected systems.

Sl. No	Network Devices (Routers, NIDS)
1.	Login with privileged accounts
2.	Login of user accounts after office hours
3.	Attempted login with default / disabled accounts
4.	Repeated failed login with privileged accounts
5.	Repeated failed login with user accounts
6.	Repeated failed logins after office hours
7.	System start/stop
8.	Service Start/Stop
9.	Failure of logging services
10	Enabling / Disabling of logging services/changes to logging level
11.	Changes to system time
12	Escalation of privileges
13	Assigning of privileges to user accounts
14	Creation / Deletion of user accounts
15	Reset / Change of passwords
16	Access attempts to the device from unauthorized hosts(Internal hosts)
17	Repeated attempts to access non-allowed services(From internal networks)
18	Large traffic observe from internal system due to mis-configured systems.
19	Large traffic observed from internal system due to virus infected

	systems.
20	Vulnerability exploitation (External)
21	Vulnerability exploitation (Internal)
22	Violation of Security Policies

The above-mentioned events are as per the log availability. But further during the operation at our Bank's SOC we can define more events as per the log availability and custom rule creation.

6.7 Reporting:

- The events / reports mentioned above are indicative only. Reports should be prepared / submitted as per our Bank requirement / Industry best practice / controlling authority / regulator requirement based on the logs and SOC tools output availability.
- The operation team should continue the existing reporting frequency, reporting metrics or parameters on which the reports are getting generated.
- Each report will have a clear description of its purpose, audience and data source
- Security Incident Management reporting
- Other information security related activity report

6.8 Proposed SLA & KPIs

Security Incident Management SLAs

Severity	Response Time
Critical / High	< 15 Minutes
Medium	< 30 Minutes
Low	< 45 Minutes

6.9 Roles and Responsibilities

Bank's Team responsibility

- Provide relevant documentation and information needed by the SOC team.
- Bank will provide required infrastructure like workstation, network connectivity and required access to Bank's resources, phone and desk to the SOC resource working in Bank's location.
- Bank will manage and coordinate the communication with stakeholders, out sourced vendor applicant shall provide assistance if required.
- Bank will facilitate issue resolution, scope of work, definition of requirement of deliverable and acceptance of deliverables.
- Provide Bank's documentation and information needed by the team.

SOC team responsibility

- Protect the confidentiality of Bank's information.
- Maintain the project delivery as per mutually agreed Project Plan.
- Provide regular projects progress updates against approved time frames and notify at the earliest, of any action or problem foreseen that jeopardize the successful completion of the project or the performance of the Project Team

6.10 Penalties

Severity	Response Time	Penalty
Critical / High	< 15 Minutes	Events along with the remediation / mitigation steps should be alerted to the Banks teams' else penalty will be as under: Within 15 minutes of the event identification, Update should be provided every 30 minutes, Penalty for missing will be as follows: 1-2 events :2% 3-4 events :4%

		5-6 events :5% 7 and above events :10% Of the total monthly billing value
Medium	< 30 Minutes	Within 30 minutes of the event identification, Update should be provided every 4 hours Penalty for missing will be as follows: 1-3 events : 1% 4-6 events :2% 7-10 events :3% 11 and above events : 5% Of the total monthly billing value
Low	< 45 Minutes	Within 45 minutes of the event identification, Update should be provided every day or as desired by the Bank till closure of the event.

a. Audit observations to be closed within mutually agreed timeframe. Penalty of 1%, with a cap of 10% of Monthly charges, for each repeat observation

b. Manpower services – Penalty of 0.5% for absence per day of L1 / L2 resources and 1% in case of L3 resource.

6.11 Payment Terms

Invoice shall be raised at the end of Quarter (in arrears) and payment shall be released within 30 days from invoice date.

7. TERMS & CONDITIONS

7.1SCHEDULE OF BIDDING PROCESS

No	Description of Information/ Requirement	Information/Requirement
1	Tender Reference	Bid for C-SOC Service Provider **1.Commercial Proposal** **2.Technical Proposal**

2	Date of Issue of RFP	**14.11.2023**
3	Bid Submission Mode.	Sealed envelopes through Courier / Speed Post, duly super scribing **Ref.No: TMB/ITD/RFP/2023-2024/002 C-SOC Service Provider**
4	Last Date and Time for submission of bids along with supporting document	**27.11.2023**
5	Contract period	**3 Years**
6	Address for Communication / Submission of Bids	The General Manager, Tamilnad Mercantile Bank Ltd., Information Technology Department, II Floor, Pearl Towers, AC-16, 2nd Avenue, Anna Nagar Chennai – 600 040
7	Contact E-mail Address.	dc_admin@tmbank.in

Note:

1. This document is the property of the Bank & is not transferable.
2. If a holiday is declared on the dates mentioned above, the bids shall be received / opened on the immediate next working day at the same time specified above and at the same venue unless communicated otherwise.

Note: Bank reserve its right to reject any bid, which is not in line with these conditions.

7.2 BIDDER'S INQUIRIES ON RFP & BANK'S RESPONSE:

All enquiries from the bidders, related to this RFP must be directed in writing to dc_admin@tmbank.in. Any clarifications / query received there after shall not be considered and will be ignored. The preferred mode of delivering written

questions, to the aforementioned contact person would be through email followed by letter in writing. In no event, Bank will be responsible for acknowledging receipt of enquiries.

Bank makes no commitment on its part to accept all the queries / suggestions / requests submitted by the bidders. Bank on reviewing the enquiries received from the bidders, wherever needed, will carry out necessary amendment to its RFP clauses, if any, and the same will be informed through separate communication to individual bidders.

7.3 FURNISHING OF INFORMATION

The Bidder is expected to examine all instructions, forms, terms and specifications in these documents. Failure to furnish all information required by the documents or to submit a bid not substantially responsive to the documents in every respect will beat the Bidder's risk and may result in the rejection of its bid.

7.4 FORMAT AND SIGNING OF BIDS

The original Technical and Commercial bids shall be typed and shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the contract. The person or persons signing the bid shall initial all pages of the offer.

7.5 AUTHENTICATION OF ERASURES / OVERWRITING ETC:

Any inter-lineation, erasures, or overwriting shall be valid only if the person or persons signing the bid initial them.

7.6 AMENDMENTS TO RFP TERMS AND CONDITIONS:

Banks reserves its right to issue any amendments to the terms and conditions, technical specification of the RFP at any time prior to the deadline for opening of the technical bids. Such amendments to RFP shall be communicated separately and shall be deemed to form part of this RFP.

7.7 CONFIDENTIALITY:

Successful bidder 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, the concepts, know-how, techniques, data, facts, figures and information whatsoever concerning or relating to the Bank and its affairs to which they said employees have access in the course of the performance of the contract. Non-disclosure agreement as per format provided in **Annexure I** should be signed by the Bidder.

7.8 CLARIFICATION

During evaluation of the bids (technical), the Bank may, at its discretion, ask the Bidder for any clarification on its bid. The request for clarification and the response shall be in writing / email, and no change in the prices shall be sought, offered, or permitted after submission of the bid.

7.9 ASSIGNMENT

The Successful Bidder/s shall not assign / sub contract, in whole or in part, its obligations to perform under this Contract, except with the Bank's prior written consent.

7.10 FORCE MAJEURE

Notwithstanding the provisions of clauses the Bidder shall not be liable for

penalty or termination for default if and to the extent that it's delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure. For purposes of this clause, "Force Majeure" means an event 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, wars or revolutions, fires, floods and epidemics.

If a Force Majeure situation arises, the Bidder shall promptly notify the Bank in writing of such condition and the cause thereof. 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 of performance not prevented by the Force Majeure event

Similarly, Bank shall also be not liable for any delay or failure in providing required infrastructure or support to the successful bidder to perform its obligations under the contract where such delay or failure is the result of an event of Force Majeure. For purposes of this clause, "Force Majeure" means an event beyond the control of the Bank and not involving the Bank's fault or negligence and not foreseeable. Such events may include, but are not restricted to, wars or revolutions, fires, floods and epidemics.

7.11 RESOLUTION OF DISPUTES, JURISDICTION & ARBITRATION:

In case of any disagreement or dispute between the Bank and the successful bidder, the dispute will be resolved in a manner as outlined hereunder.

The Bank and the successful bidder shall make every effort to resolve amicably by direct informal negotiations any disagreement or dispute between them on any matter connected with the contractor in regard to the interpretation of the context thereof. If, after thirty (30) days from the commencement of informal negotiations, the Bank and the successful Bidder

have not been able to resolve amicably a contract dispute, such differences and disputes shall be referred, at the option of either party, to the arbitration of one single arbitrator to be mutually agreed upon and in the event of no consensus, the arbitration shall be done by three arbitrators, one to be nominated by the Bank, one to be nominated by the successful bidder and the third arbitrator shall be nominated by the two arbitrators nominated as above. Such submission to arbitration will be in accordance with the Arbitration and Conciliation Act 1996. Upon every or any such reference the cost of and incidental to the references and award shall be at the discretion of the arbitrator or arbitrators or Umpire appointed for the purpose, who may determine the amount thereof and shall direct by whom and to whom and in what manner the same shall be borne and paid.

Courts of Chennai city shall alone have jurisdiction to the exclusion of all other courts, in respect of all differences and disputes envisaged above.

****

ANNEXURE - I

NON-DISCLOSURE AGREEMENT

THIS RECIPROCAL NON-DISCLOSURE AGREEMENT (the "Agreement") is made at …….…… (place) between:

TAMILNAD MERCANTILE BANK a Banking Company under the Companies Act 1956, having its Registered Office at 57 V.E. Road, Thoothukudi 628 002 (hereinafter referred to as "Bank" which expression includes its successors and assigns) of the ONE PART;

And

……. (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 the Bank 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. 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 setout hereunder.

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

1. Confidential Information and Confidential Materials:

(a) "Confidential Information" means nonpublic 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 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 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; or (iv) is independently developed by Receiving Party.

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

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 own employees and other persons and then only to those employees and persons 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 its employees and consultants specifically assigned and/or otherwise, sufficient to enable it to comply with all the provisions of this Agreement. If the Contractor shall appoint any Sub-Contractor then the Contractor may disclose confidential information to such Sub-Contractor subject to such Sub Contractor giving the Customer an undertaking in similar terms to the provisions of this clause.

(b) Receiving Party may disclose Confidential Information in accordance with judicial or other governmental order to the intended recipients (as detailed in this clause), provided Receiving Party shall give Disclosing Party reasonable notice prior to such disclosure and shall comply with any applicable protective order or equivalent. The intended recipients for this purpose are:

(1) The statutory auditors of the Customer and

(2) Regulatory authorities regulating the affairs of the Customer and inspectors and supervisory bodies thereof

(c) The foregoing obligations as to confidentiality shall survive any termination of this Agreement

(d) 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.

(e) Receiving Party may not reverse engineer, decompile or disassemble any software disclosed to Receiving Party.

3. <u>Rights and Remedies</u>

(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 (as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

- Suspension of access privileges
- Change of personnel assigned to the job
- Financial liability for actual, consequential or incidental damages
- 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. Miscellaneous

(a) All Confidential Information and Confidential Materials are and shall remain the property 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 patents, copyrights, trademarks, or trade secret information.

(b) Any software and documentation provided under this Agreement is provided with RESTRICTED RIGHTS.

(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 Chennai and in accordance with the provisions of Indian Arbitration and Conciliation Act 1996 or any Amendments or Reenactments thereto.

(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) All obligations created by this Agreement shall survive change or termination of the parties' business relationship.

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

(a) 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 party 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..... 202 at .....
(month) (place)

For and on behalf of …….

Name :

Designation :

Place :

Signature with Seal

For and on behalf of …….

Name :

Designation :

Place :

Signature with Seal

ANNEXURE - II

SELF DECLARATION – BLACK LISTING
(To be provided in Company's Letter Head)

Dear Sir,

We, (Name of the Company/LLP/OEM) here by certify that, we have not been debarred / black listed in any Statutory body / Central Government / PSU / Banking / Insurance company in India or abroad as on date of the RFP.

Date:
Place: (Signature of Authorized Signatory)
Company Seal: Name with Designation