MEENAKSHI MERCANTILES LIMITED

Information Technology Governance, Risk Controls and Assurance Practices Framework

M/s Meenakshi Mercantiles Limited (the "company") is a registered NBFC-ML carrying on the business of financing and investment activities by way of advancing Inter-Corporate Deposits and acquisition of shares and securities of its group companies. The company is committed to conducting business in accordance with an effective compliance culture and a strong compliance risk management framework.

1. PREAMBLE:

RBI vide its circular DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 dated November 7, 2023 stated that the Non-Banking Financial Company shall adopt a developed Information Technology (IT) Framework in accordance with the directives set forth in the above-mentioned RBI circular. This Policy outlines the guidelines and procedures for the secure, efficient. and compliant use of information technology resources within the company.

2. OBJECTIVES:

The primary objectives of the IT Framework are:

- To establish standards for the acquisition, deployment, and management of IT resources in alignment with RBI guidelines.
- To ensure the confidentiality, integrity, and availability of company data and systems.
- To mitigate IT-related risks and vulnerabilities.
- To comply with regulatory requirements set forth by the Reserve Bank of India (RBI) related to information security, data privacy, and IT governance.

3. SCOPE

This policy applies to all our employees (including secondees who have been seconded to the Company from other organizations), contractors, vendors and anyone who has permanent or temporary access to our systems and hardware.

The Company's staff shall sign confidentiality (non-disclosure) undertaking as a part of their employment contract. and any temporary staff (including agency staff) and secondees sign the standard confidentiality undertaking before they are permitted to use the Company's systems.

This policy covers the usage of all the Company's Information Technology and communication resources. whether they are owned or leased by the Company or are under the company's possession, custody or control. including but not limited to

- All computer-related equipment, including desktops, laptops/netbooks, terminals, workstations, wireless computing device, mobile phones, electronic storage devices such as DVDs, CDs, memory sticks, telecom equipment's, networks, databases, printers, servers, pen drives, hard drives, and all networks and hardware to which thus equipment is connected.
- All software including purchased or licensed business software applications -written applications, employee or vendor/supplier, computer operating systems/applications, firmware and any other software.
- All intellectual property and other data stored on Company's Information Technology equipment.

4. IT GOVERNANCE

The Company primarily focuses on areas of IT Governance which include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.

The Company shall put in place a robust IT Governance Framework based on the aforementioned focus areas that inter alia:

- specifies the governance structure and processes necessary to meet the Companies business/ strategic objectives;
- specifies the roles (including authority) and responsibilities of the Board of Directors (Board)/ Board level Committee and Senior Management; and
- includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks.

Enterprise-wide risk management policy or operational risk management policy shall also incorporate periodic assessment of IT-related risks (both inherent and potential risk)

Role of the Board of Directors

(a) The strategies and policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) shall be approved by the Board of Directors.

(b) Such strategies and policies shall be reviewed at least annually by the Board

IT Strategy Committee Board

The Company shall establish a Board-level IT Strategy Committee consisting of minimum of three directors as members; the chairperson of which shall be an independent director and have substantial IT expertise in managing or guiding information technology initiatives; and the members shall be technically competent.

The Committee shall meet at least on a quarterly basis.

The Committee must ensure that the company has put an effective strategic planning process in place. They must satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defines objectives and unambiguous responsibilities for each level in the organization.

The Committee should make sure that the budget allocated for the IT department, encompassing IT security and cyber security, aligns with the company's level of IT development, digital footprint, threat landscape, and industry benchmarks, and that these funds are deployed effectively to achieve the specified goals. The) must review at least on annual basis, the adequacy and effectiveness of Business Continuity Planning and Disaster Recovery Management of the company.

Senior Management and IT Steering Committee

The Senior Management of the company shall ensure the execution of the IT Strategy approved by the Board. It shall also ensure that the necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices in the company. The Company shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions. The Committee shall meet at least on a quarterly basis. The responsibilities of the Committee are as follows -

- To assist the ITSC in strategic planning, oversight of IT performance, and aligning IT activities with business needs;
- To oversee the processes put in place for business continuity and disaster recovery;
- To ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and
- To update ITSC and CEO periodically on the activities of IT Steering Committee.

Head of IT Function

The Company will designate a highly skilled and experienced individual, possessing senior-level expertise in it matters, to serve as the Head of the IT Function.

The Head of IT Function shall, inter alia, be responsible for the following:

- Ensuring that the implementation of the IT projects and initiatives conforms to the company's IT policy and strategy;
- Establishing a robust organizational framework to facilitate the Company's IT functions effectively; and
- Implementing a reliable disaster recovery setup and business continuity strategy/plan to ensure seamless operations during unforeseen disruptions.

As the primary guardian, the Head of IT Function will oversee thorough assessment, evaluation, and management of IT controls and risks, including the establishment of resilient internal controls, to:

(i) Safeguard the Company's information assets; and

(ii) Adhere to existing internal policies, regulatory mandates, and legal obligations concerning IT matters.

5. IT INFRASTRUCTURE & SERVICES MANAGEMENT

IT Services Management

(a) The Company is committed to implementing a resilient IT Service Management Framework to uphold the operational integrity of its information systems and infrastructure, encompassing all aspects of the IT environment, including disaster recovery sites.

(b) A Service Level Management (SLM) process will be established to oversee IT operations, with a focus on ensuring the effective segregation of duties.

(c) The company will ensure the identification and mapping of the security classification of information assets based on their criticality to the company's operations taking into account aspects of Confidentiality, Integrity and Availability.

(d) To ensure smooth continuity of business operations. Responsible Entities (REs) will refrain from using outdated and unsupported hardware or software. They will also continuously monitor the end-of-support (EOS) dates of software and the Annual Maintenance Contract of IT hardware.

(e) The company will formulate a technology refresh plan to replace hardware and software in a timely manner, pre-empting their reaching end-of-support (EOS).

Third-Party Arrangements

The Company shall put in place appropriate vendor risk assessment process and controls propo1tionate to the assessed risk and materiality to, inter alia:

- mitigate concentration risk;
- eliminate or address any conflict of interests:
- mitigate risks associated with single point of failure:
- comply with applicable legal, regulatory requirements and standards to protect customer data;
- provide high availability (for uninterrupted customer service); and
- manage supply chain risks effectively.

Capacity Management

(a) The Company will guarantee that information systems and infrastructure can sustain business functions and uphold the availability of all service delivery channels.

(b) REs will conduct proactive assessments of IT resource capacity on an annual or more frequent basis. The company will ensure that IT capacity planning, covering components, services, system resources, and supporting infrastructure, aligns with historical usage patterns (peak usage), current business demands, and anticipated future needs in accordance with the company's IT strategy.

(c) The IT capacity requirements assessment and actions taken to resolve issues will undergo review by the TT Steering Committee (ITSC).

Proiect Management

(a) The Company will adhere to a consistent and formally defined project management approach for all IT projects it undertakes. This approach will facilitate appropriate stakeholder participation to effectively monitor and manage project risks and progress.

(b) When adopting new or emerging technologies, tools, or revamping existing ones in the technology stack, the Company will follow a standard enterprise architecture planning methodology or framework.

(c) Adoption of new or emerging technologies will be in line with the company's risk appetite and aligned with its overall Business/IT strategy. It will facilitate optimal creation, use, or sharing of information by the business in a secure and resilient manner.

(d) The Company will maintain an enterprise data dictionary to enable the sharing of data among applications and information systems, promoting a common understanding of data.

(e) Maintenance and necessary support of software applications will be provided by software vendors, enforced through formal agreements.

(i) The Company will obtain the source codes for all critical applications from their vendors. In cases where obtaining the source code is not possible, the company will establish a source code escrow arrangement or other suitable arrangements to adequately mitigate the risk of vendor default. All product updates and program fixes will be included in the source code escrow arrangement.

(g) The company will obtain a certificate or written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. Such certification or confirmation will also be obtained whenever material changes to the code, including upgrades, occur.

(h) Any new IT application proposed to be introduced as a business product will undergo a product approval and quality assurance process.

Change and Patch Management

The Company will establish documented policies and procedures for change and patch management to ensure the following:

(a) Assessment of the business impact of implementing patches/changes or not implementing a particular patch/change request.

(b) Application/implementation of patches/changes in a secure and timely manner, with necessary approvals, and subsequent review.

(c) Justification of any changes to an application system or data by genuine business needs, supported by documentation, and subjected to a robust change management process.

(d) Establishment of mechanisms to recover from failed changes/patch deployments or unexpected results.

Data Migration Controls

The Company will maintain a documented data migration policy outlining a systematic process for data migration, ensuring data integrity, completeness, and consistency. This policy will include provisions regarding signoffs from business users and application owners at each stage of migration, maintenance of audit trails, and other relevant considerations.

Audit Trails

(a) Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails.

(b) The audit trails shall satisfy a company's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

(c) The Company shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorised activity.

Cryptographic controls

The Company will employ robust key lengths, algorithms, cipher suites, and protocols for transmission channels, data processing, and authentication purposes. These selections will adhere to internationally accepted and published standards that are not deprecated or demonstrated to be insecure or vulnerable. Furthermore, configurations involved in implementing such controls will comply with existing laws and regulatory instructions.

Straight Through Processing

(a) To prevent unauthorized data modification, the company will ensure that no manual intervention or modification occurs during data transfer between processes or applications, especially for critical applications.

(b) Data transfer mechanisms between processes or applications will undergo thorough testing, secure automation with necessary checks and balances, and integration through the "Straight Through Processing" methodology, incorporating appropriate authentication mechanisms and audit trails.

Physical and Environmental Controls

(a) The Company will implement appropriate physical and environmental controls in Data Centre and Disaster Recovery sites utilized by them.

(b) Data Centre (DC) and Disaster Recovery (DR) sites will be geographically well separated to mitigate the risk of both sites being affected by similar threats associated with their locations.

(c) The Company will ensure that their Data Centre and Disaster Recovery sites are equipped with necessary surveillance mechanisms.

Access Controls

(a) Access to information assets will be permitted only when a valid business need exists. The Company will maintain documented standards and procedures, approved by the JTSC and regularly updated, for administering need-based access to information systems.

(b) Personnel with elevated system access entitlements will be closely supervised, with all their system activities logged and periodically reviewed.

(c) The Company will implement multi-factor authentication for privileged users of -

- critical information systems and
- for critical activities, based on the company's risk assessment.

Controls on Teleworking

In the teleworking environment, the Company will, among other measures:

(a) Ensure the security of systems used and remote access from alternate work locations to the environment hosting company's information assets.

(b) Implement multi-factor authentication for enterprise access (logical) to critical systems.

(c) Establish a mechanism to identify all remote-access devices attached/connected to the company's systems.

(d) Ensure appropriate security measures are in place to safeguard data/information shared/presented during teleworking.

Metrics

(a) The Company will establish appropriate metrics for system performance, recovery, and business resumption, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO), for all critical information systems.

(b) For non-critical information systems, the company will adopt a risk-based approach to define suitable metrics.

(c) The Company will implement a suitable scorecard, metrics, or methodology to measure IT performance and IT maturity level.

6. IT AND INFORMATION SECURITY RISK MANAGEMENT

Periodic review of IT related risks

The risk management policy of the company will encompass IT-related risks, including Cyber Security-related risks. The Risk Management Committee of the Board (RMC), in consultation with the ITSC, will periodically review and update this policy at least on a yearly basis.

IT and Information Securit11Risk Management Framework

The Company will establish a robust IT and Information Security Risk Management Framework covering, among other aspects:

(a) Implementation of a comprehensive Information Security management function, internal controls, and processes to mitigate/manage identified risks. These controls and processes must be periodically reviewed for efficacy in a risk environment characterized by change.

(b) Definition of roles and responsibilities of stakeholders (including third-party personnel) involved in IT risk management. Areas of possible role conflicts and accountability gaps must be specifically identified and eliminated or managed.

(c) Identification of critical information systems within the organization and fortification of the security environment of such systems.

(d) Definition and implementation of necessary systems, procedures, and controls to ensure secure storage, transmission, and processing of data/information.

Information Security Policy and Cyber Security Policy

(a) The Information Security Policy will encompass aspects such as objectives, scope, ownership, and responsibility for the Policy; information security organizational structure; exceptions; compliance review; and penalties for non-compliance of Policies. Additionally, the company will establish a Cyber Security Policy and Cyber Crisis Management Plan (CCMP).

(b) An Information Security Committee (ISC), overseen by the ITSC, will be established to manage cyber/information security. The constitution of the ISC, including the Chief Information Security Officer (CISO) and other representatives from business and IT functions, will be determined by the TTSC. The head of the ISC will be from the risk management vertical. The major responsibilities of the ISC will include:

- Developing information/cyber security policies, implementing policies, standards, and procedures to ensure that all identified risks are managed within the company's risk appetite.
- Approving and monitoring information security projects and security awareness initiatives.
- Reviewing cyber incidents, information systems audit observations, monitoring, and mitigation activities.
- Providing periodic updates to the ITSC and CEO on the activities of the ISC.

(c) A senior-level executive, preferably in the rank of a General Manager or an equivalent position, will be designated as the Chief Information Security Officer (CISO). The CISO will not have any direct reporting relationship with the Head of IT Function and will not be assigned any business targets. The Company will ensure the following:

- The CISO possesses the requisite technical background and expertise.
- She/He is appointed for a reasonable minimum term.
- The CISO's Office is adequately staffed with personnel having the necessary technical expertise, commensurate with the business volume, extent of technology adoption, and complexity.
- The budget for information/cyber security is determined considering the current/emerging threat landscape.

(d) The Company shall ensure that the roles and responsibilities of the CISO are clearly defined and documented, covering, at a minimum, the following points:

- The CISO shall be responsible for driving cybersecurity strategy and ensuring compliance with extant regulatory/statutory instructions on information/cybersecurity.
- The CISO shall enforce the policies used by the company to protect its information assets, in addition to coordinating information/cybersecurity-related issues within the company and with relevant external agencies.
- The CISO shall be a permanent invitee to the JTSC and IT Steering Committee.
- The CISO's Office shall manage and monitor the Security Operations Centre (SOC) and drive cybersecurity-related projects.
- The CISO's office shall ensure the effective functioning of the security solutions deployed.
- The CISO shall directly report to the Executive Director or equivalent executive overseeing the risk management function.
- The CISO shall present a review of cybersecurity risks/arrangements/preparedness of the company before the Board/RMCB/ITSC at least on a quarterly basis.

Risk Assessment

(a) The Risk Assessment for each information asset within the company's scope will be guided by appropriate security standards/IT control frameworks.

(b) The Company will ensure that all staff members and service providers comply with the extant information security and acceptable-use policies applicable to them.

(c) The Company will conduct annual reviews of their security infrastructure and security policies, taking into account their own experiences and emerging threats and risks. The Company will take steps to adequately address cyber-attacks, including phishing and spoofing attacks, and mitigate their adverse effects.

Cyber Incodent Response and Recovery Management

(a) The cyber incident response and recovery management policy will encompass the classification and assessment of incidents. It will also include a clear communication strategy and plan to manage such incidents, mitigate exposures, and achieve timely recovery.

b) The Company will analyse cyber incidents, including conducting forensic analysis if necessary, to determine their severity, impact, and root cause. Measures, both corrective and preventive, will be taken to mitigate the adverse impact of incidents on business operations.

(c) The company will establish written incident response and recovery procedures, which will include the identification of key roles of staff/outsourced staff responsible for handling such incidents.

(d) The Company will have clear communication plans for escalation and reporting incidents to the Board and Senior Management, as well as to customers, as required. Proactive notification to CERT-In and RBI regarding incidents will be carried out in accordance with regulatory requirements. Additionally, the Company is encouraged to report incidents to Indian Banks - Centre for Analysis of Risks and Threats (IB-CART) set up by IDRBT.

(e) The Company will establish processes to enhance incident response and recovery activities and capabilities by learning from past incidents and conducting tests and drills. This includes ensuring the effectiveness of the crisis communication plan/process through the conduct of periodic drills and testing with stakeholders, including service providers.

7. BUSINESS CONTINUITY AND DISASTER RECOVERY MANAGEMENT

The Business Continuity Policy (BCP) and Disaster Recovery (DR) Policy will adopt best practices to guide its actions in reducing the likelihood or impact of disruptive incidents and maintaining business continuity. The policy will be regularly updated based on major developments and risk assessments.

The Company's BCP/DR capabilities will be designed to effectively support its resilience objectives and enable it to rapidly recover and securely resume its critical operations, including security controls, following cyber-attacks or other incidents.

Disaster Recovery Management

(a) The periodicity of DR drills for critical information systems shall be at least on a half-yearly basis, and for other information systems, as per the Company's risk assessment.

(b) Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of the drill before the next cycle.

(c) The DR testing shall involve switching over to the DR/alternate site and using it as the primary site for a sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered.

(d) The Company shall regularly test the BCP/DR under different scenarios for possible types of contingencies to ensure that it is up-to-date and effective.

(e) The Company shall backup data and periodically restore such backed-up data to check its usability. The integrity of such backup data shall be preserved, along with securing it from unauthorized access.

(f) The Company shall ensure that DR architecture and procedures are robust, meeting the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for any recovery operations in case of a contingency.

(g) The Company should prioritize achieving minimal RTO (as approved by the company's ITSC) and a near-zero RPO for critical information systems.

(h) In a scenario of non-zero RPO, the company shall have a documented methodology for reconciliation of data while resuming operations from the alternate location.

(i) The Company shall ensure that the configurations of information systems and deployed security patches at the DC and DR are identical.

(j) The Company shall ensure BCP and DR capabilities in critical interconnected systems and networks, including those of vendors and partners. REs shall ensure demonstrated readiness through collaborative and coordinated resilience testing that meets the REs' RTO.

8. INFORMATION SYSTEMS (IS) AUDIT

(a) The Audit Committee of the Board (ACB) will be responsible for overseeing the IS Audit of the Company.

(b) The Company will establish an IS Audit Policy containing a clear description of its mandate, purpose, authority, audit universe, periodicity of audit, etc. This policy will be approved by the ACB and reviewed at least annually.

(c) The ACB will review critical issues highlighted related to IT/information security/cybersecurity and provide appropriate direction and guidance to the company's Management.

(d) The company will have a separate IS Audit function or resources possessing the required professional skills and competence within the Internal Audit function. In cases where external resources are used for conducting IS audits in areas where skills are lacking within the Company, the responsibility and accountability for such external IS audits will remain with the competent authority within the Internal Audit function.

(e) The company will carry out IS Audit planning by adopting a risk-based audit approach.

(t) The Company may consider, wherever possible, a continuous auditing approach for critical systems, performing control and risk assessments on a more frequent basis.

9. CONCLUSION

Adherence to this framework is crucial for maintaining the security, integrity, and availability of IT resources, protecting sensitive information, and ensuring compliance with the RBI circular directives. All employees, contractors, and third-party vendors are expected to familiarize themselves with the provisions of this framework and adhere to its guidelines.

10. MONITORING AND REVIEW OF THE FRAMEWORK

The IT Steering Committee or the Board of Directors of the Company will review the policy periodically to ensure its effectiveness, relevance, and alignment with the RBI circular directives and changing business needs and must act accordingly to add, amend, modify this policy as and when it deems necessary in terms with statutory amendments.