LAKME INVESTMENT AND FINANCE LIMITED

IT STEERING POLICY

Version Control

Document version	Description of changes	Memorandum of change	Prepared by	Proposed by	Owner Dept.	Approval Date
1.0			Operations		Operations	

Table of contents

1. Objective:

Lakme Investment and Finance Limited is an IT organizational structure commensurate with the size, scale and nature of business activities conducted. The Company has a designated a Senior Officer in-Charge of IT operations whose responsibility is to ensure implementation of IT Policy in the Company at operational level involving IT strategy, value delivery, risk management and IT resource management. To ensure technical competence at senior/middle level management of the Company, periodic assessment of the IT training requirements should be formulated to ensure that sufficient, competent, and capable human resources are available.

The entity has a broadly approved IT Policy with the following basic creeds:

- **Confidentiality**: Ensuring access to sensitive data to authorized users only.
- **Integrity**: Ensuring the accuracy and reliability of information by ensuring that there is no modification without authorization.
- **Availability**: Ensuring that uninterrupted data is available to users when it is needed.
- **Authenticity**: For IS it is necessary to ensure that the data, transactions, communications, or documents (electronic or physical) are genuine.

2. Mechanism to Control IT Processes:

- Formulating a Board approved IT policy - The policy shall be in line with the organizational objectives.
- Develop an IT organizational structure - The structure shall be commensurate with the size, scale, and nature of business activities conducted by the NBFC.
- Designate a senior Officer in-Charge of IT operations — The responsibility of such officer shall be to ensure implementation of IT Policy to the operational level involving IT strategy, value delivery, risk management and IT resource management.
- Formulate periodic assessment of the IT training requirements — To ensure technical. competence in senior/middle-level management and to ensure that sufficient, competent, and capable human resources are available.
- The Company will maintain a detailed inventory of the Assets with distinct and clear identification of assets.
- Segregation of the duties of both physical security as well as cybersecurity dealing exclusively with information systems security and the Information Technology division which actually

implements the computer systems is done and the matrix is duly approved by the Board.

- The information security function is adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there is clear segregation of responsibilities relating to system administration, database administration and transaction processing.
- **Role-based Access Control**:
  Access to information is based on well-defined user roles. The Company avoids dependence on one or a few people. There is clear delegation of authority for the right to upgrade/change user-profiles and permissions and key business parameters which is documented.
- **Personnel Security**
  A few authorized application owners/users may have intimate knowledge of financial institution processes and pose a potential threat to systems and data. Personnel with privileged access to the system administrator, cybersecurity personnel, etc. are subject to rigorous background check and screening.
- **Physical Security:** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. The Company has created a protected environment for the physical security of IS Assets such as the secure location of critical data, restricted access to sensitive areas like data centers.
- **Maker-checker** – It is one of the important principles of authorization in the information systems of financial entities. For each transaction, there are at least two individuals necessary for its completion as this will reduce the risk of error and will ensure the reliability of the information.
- **Document and IT trails:**
  The Company ensures that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating the audit, serving as forensic evidence when required and assisting in dispute resolution.

3. IT Steering Committee (“ITSC”)

a. Constitution:

IT Strategy Committee shall consist of the Chief Risk Officer, Chief Operations Officer, IT in charge and MD & CEO of the Company authorized for selecting the member/invitee of the Committee from time to time according to the requirements of various projects undertaken by the Company.

b. Meetings:

STC shall meet at an appropriate frequency on a need basis and the and the chairman of the Committee shall be MD & CEO.

c. Roles & Responsibilities:

The ITSC shall oversee and monitor the IT Governance Framework and the risk associated with it.

4. IT Governance and Risk Management:

- **Cyber-Security:** The Company has requisite cyber-security SOP illuminating the strategy comprising a suitable approach to battle cyber threats given the level of business operations and acceptable levels of risk, duly approved by their Board. NBFCs must appraise the structural measures so that the security concerns are valued, obtain adequate attention, and get escalated to appropriate levels in the hierarchy to enable quick action.
- **Vulnerability Management**: A vulnerability can be defined as an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and cost associated with the vulnerabilities. NBFCs may devise a strategy for managing and eliminating vulnerabilities and such a strategy may clearly be communicated in the Cyber Security policy.
- **Cybersecurity Preparedness Indicators**: The capability & adherence to cyber flexibility framework must be assessed & measured through the development of indicators to assess the level of risk/preparedness. These indicators should be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The alertness amongst the stakeholders, including employees, may also form a part of this assessment.
- **Cyber Crisis Management Plan:** A Cyber Crisis Management Plan (CCMP)LU should be immediately evolved and should be a part of the overall Board approved strategy. CCMP should address the following four aspects: (I) Detection (ii) Response (iii) Recovery and (iv) Containment NBFCs need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/ recover/contain the fallout. NBFCs are predictable to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. Among other things, NBFCs should take

necessary preventive and corrective measures in addressing various types of cyber threats including, but not limited to, denial of service, distributed denial of services, crypto ware, destructive malware, business email frauds containing spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

- **Cyber-Security Awareness Among Stakeholders / Top Management / Board:** It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require an elevated level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarization may be organized. NBFCs should proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives and require and ensure the appropriate action to support their synchronized implementation and testing.
- **Digital Signature:** A Digital Signature Certificate authenticates an entity's identity electronically. It also provides an elevated level of security for online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. NBFCs may consider the use of digital signatures to protect the authenticity and integrity of important electronic documents and also for high- value fund transfer.
- **IT Risk Assessment:** NBFCs should undertake a comprehensive risk assessment of their IT systems at least on a yearly basis. The assessment should make an analysis of the threats and vulnerabilities to the information technology assets of the NBFC and its existing security controls and processes. The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), CIO and the Board of the NBFC and should serve as an input for Information Security Auditors.
- **Mobile Financial Services**: NBFCs that are already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to-end encryption.
- **Social Media Risks:** NBFCs using social media to market their products must be well equipped in treating social media risks and threats. As social media is vulnerable to account

takeovers and malware distribution, proper controls, such as encryption and secure connections, should be prevalent to mitigate such risks.

- **Training:** Human link is the weakest link in the information security chain. Hence, there is a vital need for an initial and ongoing training and information security awareness program. The program may be periodically updated keeping in view changes in the information technology system, threats/vulnerabilities, and/or the information security framework. There needs to be a mechanism to track the effectiveness of training programs through an assessment/testing.
- process. At any point in time, NBFCs need to maintain an updated status on user training and awareness relating to information security.

5. Business continuity and Disaster Recovery plan:

The Company shall Conduct a thorough assessment of potential risks that could impact IT systems, such as natural disasters, cyber-attacks, power outages, hardware failures, and human errors.

It shall evaluate the potential impact of these risks on IT operations, financial transactions, customer service, regulatory compliance, and overall business continuity.

Define acceptable downtime and data loss thresholds for critical IT systems and processes.

Implement regular backups of critical data and systems, ensuring redundancy and encryption. Store backups securely off-site or in the cloud.

Establish alternative IT infrastructure options to quickly restore IT operations if primary systems are unavailable.

Formulate an incident response team with clearly defined roles and responsibilities. Include IT personnel, management, and key stakeholders.

Develop communication protocols for internal and external stakeholders during IT disruptions, ensuring transparency and timely updates.

Outline procedures for containing incidents, minimizing damage, and initiating IT system recovery.

6. Periodic IT audit:

Cybersecurity Controls: Assess the effectiveness of firewall configurations, antivirus software, intrusion detection/prevention systems, and security incident response procedures.

Data Protection: Review encryption methods, access controls, data masking techniques, and compliance with data privacy regulations.

IT Governance: Evaluate IT policies, procedures, and controls to ensure alignment with business objectives and regulatory requirements.

Vendor Management: Assess risks associated with third-party IT vendors and service providers, including contract management and compliance.

Data migration controls:

- Data migration controls in IT systems are essential to ensure the safe and accurate transfer of data from one system or storage location to another.
- Clearly outline the goals and scope of the data migration project, including the types of data to be migrated and the target systems or repositories. Conduct a thorough risk assessment to identify potential risks and challenges associated with data migration, such as data loss, corruption, or unauthorized access.
- Create a detailed data mapping document that defines the source and destination of each data element, ensuring accurate mapping and transformation rules. Cleanse and normalize data to ensure consistency and accuracy before migration.
- Implement validation checks during the migration process to verify data integrity and completeness.
- Develop procedures to handle errors and discrepancies encountered during data migration, including mechanisms for data rollback or recovery.
- Restrict access to migration tools and data repositories to authorized personnel only.
- Implement strong authentication mechanisms to ensure only authorized users can initiate and oversee data migration processes.
- Enable detailed audit logging to track activities related to data migration, including access, changes, and errors.
- Conduct thorough testing in a non-production environment to validate migration processes and ensure compatibility between source and target systems.
- Perform parallel runs where feasible, migrating a subset of data to verify accuracy and identify potential issues before full-scale migration.
- Validate data integrity and functionality in the target system after migration to ensure that all data has been transferred correctly and is usable.