

LAKME INVESTMENT AND FINANCE LIMITED

Regd Office: No. 1, Anna Pillai Street, Chennai – 600 001.

Corporate Office: No.1, Padiyur Road, Pudupatti, Dindigul – 624 005.

CIN: U65993TN1995PLC033288 | Email ID: compliance@lakmefinance.com | Mobile No: 8925975497

INFORMATION TECHNOLOGY (IT), INFORMATION SECURITY AND CYBER SECURITY POLICY

Board Approval Date: 20.03.2026

Sl No	INDEX	Page
1	PREAMBLE	2
2	OBJECTIVES	2
3	APPLICABILITY	2
4	IT GOVERNANCE FRAMEWORK	3
5	INFORMATION SECURITY PRINCIPLES	3
6	IT ORGANISATION STRUCTURE	3
7	INFORMATION ASSET MANAGEMENT	4
8	USER ACCESS MANAGEMENT	4
9	PASSWORD MANAGEMENT	4
10	CYBER SECURITY FRAMEWORK	4
11	MAKER-CHECKER CONTROLS	5
12	DATA SECURITY AND CUSTOMER INFORMATION PROTECTION	5
13	IT VENDOR MANAGEMENT	5
14	DIGITAL LENDING CONTROLS	6
15	INFORMATION SECURITY INCIDENT MANAGEMENT	6
16	IT RISK ASSESSMENT	6
17	BUSINESS CONTINUITY PLAN (BCP)	6
18	DISASTER RECOVERY (DR)	7
19	DATA BACKUP POLICY	7
20	DATA MIGRATION CONTROLS	7
21	TRAINING AND AWARENESS	7
22	INFORMATION SYSTEMS AUDIT (ISA)	8
23	RECORD RETENTION	8
24	REPORTING TO THE BOARD	8
25	POLICY REVIEW	9
26	BOARD APPROVAL	9

1. PREAMBLE

Lakme Investment and Finance Limited ("the Company") recognizes that Information Technology plays a critical role in lending operations, customer servicing, accounting, regulatory reporting, information security and business continuity.

This Policy establishes a framework for governance, management and protection of the Company's information systems and technology assets in a manner commensurate with the size, scale and complexity of its operations.

This Policy is framed considering:

- a. RBI Master Direction – Non-Banking Financial Company , as amended from time to time;
- b. RBI Information Technology Governance and Risk Management guidance applicable to NBFCs;
- c. RBI Cyber Security and Information Security advisories;
- d. RBI Digital Lending Guidelines, wherever applicable;
- e. Information Technology Act, 2000;
- f. Applicable statutory and regulatory requirements.

The Policy follows the principle of proportionality applicable to Base Layer NBFCs.

2. OBJECTIVES

The objectives of this Policy are:

- a. To ensure secure and efficient use of Information Technology.
- b. To safeguard customer information and Company data.
- c. To protect the confidentiality, integrity and availability of information assets.
- d. To manage technology and cyber security risks.
- e. To establish appropriate IT governance and oversight.
- f. To ensure continuity of business operations during disruptions.
- g. To comply with applicable RBI and statutory requirements.

3. APPLICABILITY

This Policy shall apply to:

- a. Directors;
- b. Employees;
- c. Consultants;
- d. Contract staff;
- e. Outsourced service providers;
- f. IT vendors;
- g. Business Correspondents;
- h. Recovery Agents having access to Company systems or information.

4. IT GOVERNANCE FRAMEWORK

The Board of Directors shall have overall responsibility for Information Technology Governance. The Board shall:

- a. Approve the IT Policy.
- b. Review major technology risks.
- c. Review Information Systems Audit findings.
- d. Review significant cyber incidents.
- e. Ensure adequate resources for IT operations and security.
- f. Review Business Continuity arrangements.

The day-to-day implementation of this Policy shall be overseen by a designated IT Officer or senior employee responsible for technology operations.

5. INFORMATION SECURITY PRINCIPLES

The Company shall ensure:

Confidentiality

Information shall be accessible only to authorized persons.

Integrity

Information shall be protected against unauthorized modification.

Availability

Information and systems shall be available whenever required for business operations.

Authenticity

Users and transactions shall be appropriately authenticated.

Accountability

Activities performed within systems shall be traceable through audit logs and records.

6. IT ORGANISATION STRUCTURE

The Company shall designate a responsible officer to oversee:

IT operations;
Information security;
Vendor coordination;
Data backup management;
User access management;
Incident reporting
Disaster Management.

Depending on business requirements, these functions may be outsourced to qualified service providers under appropriate agreements.

However, accountability shall remain with the Company.

7. INFORMATION ASSET MANAGEMENT

The Company shall maintain and periodically update:

- a. Hardware Asset Register;
- b. Software Register;
- c. Application Inventory;
- d. User Access Register;
- e. Vendor Register;
- f. Data Backup Register.

All critical information assets shall be appropriately identified and protected.

8. USER ACCESS MANAGEMENT

The Company shall implement Role-Based Access Control (RBAC).

The following controls shall be maintained:

- a. Unique User IDs.
- b. Password Protection.
- c. Role-Based Permissions.
- d. Access Authorization.
- e. Maker-Checker Controls.
- f. Segregation of Duties.
- g. User Access Review.

Access shall be granted strictly on a need-to-know basis.

User access rights shall be reviewed at least annually and immediately upon employee resignation, transfer or termination for amendment and/or cancellation.

9. PASSWORD MANAGEMENT

The Company shall establish password standards covering:

- a. Minimum password complexity.
- b. Periodic password changes.
- c. Restricted password sharing.
- d. Protection against unauthorized access.

Default passwords shall be changed immediately upon deployment.

10. CYBER SECURITY FRAMEWORK

The Company shall implement cyber security controls proportionate to the nature and scale of its operations.

Minimum controls shall include:

- a. Antivirus protection.
- b. Firewall protection.
- c. Endpoint security.

- d. Malware protection.
- e. Secure email controls.
- f. System update and patch management.
- g. Data encryption where appropriate.
- h. Secure internet usage controls.

The Company shall periodically review emerging cyber threats.

11. MAKER-CHECKER CONTROLS

The Company shall ensure maker-checker controls for critical activities including:

- a. Loan disbursement.
- b. Loan closure.
- c. Customer master modification.
- d. User creation.
- e. Accounting entries.
- f. Bank transactions.
- g. Data migration activities.

No individual shall independently complete critical transactions without appropriate authorization.

12. DATA SECURITY AND CUSTOMER INFORMATION PROTECTION

Customer information shall be treated as confidential.

The Company shall ensure:

- a. Restricted access to customer information.
- b. Secure storage of records.
- c. Encryption of sensitive information wherever feasible.
- d. Protection against unauthorized disclosure.
- e. Secure disposal of information.

Customer information shall not be disclosed except:

- a. With customer consent;
- b. Under legal or regulatory requirements;
- c. For legitimate business purposes.

13. IT VENDOR MANAGEMENT

Before engaging any IT vendor or service provider, the Company shall assess:

- a. Technical competence;
- b. Security controls;
- c. Financial stability;
- d. Reputation;
- e. Service capability.

Vendor agreements shall include:

- a. Confidentiality obligations;
- b. Data storage and protection requirements;
- c. Business continuity requirements;
- d. Audit rights of the Company.

Vendor performance shall be reviewed periodically.

14. DIGITAL LENDING CONTROLS

Where digital lending activities are undertaken, the Company shall ensure:

- a. Customer consent capture.
- b. Audit trails.
- c. Data privacy controls.
- d. Secure transmission of customer information.
- e. Compliance with RBI Digital Lending Guidelines

15. INFORMATION SECURITY INCIDENT MANAGEMENT

Any incident involving:

- a. Unauthorized access;
- b. Malware infection;
- c. Data leakage;
- d. System compromise;
- e. Customer information breach;
- f. Fraud involving IT systems;

shall be reported immediately to Management.

The incident shall be documented, investigated and corrective action taken.

A register of information security incidents shall be maintained.

16. IT RISK ASSESSMENT

The Company shall conduct an IT Risk Assessment at least annually.

The assessment shall cover:

- a. Information security risks;
- b. Cyber security risks;
- c. Vendor risks;
- d. Data protection risks;
- e. Operational technology risks.

The findings shall be placed before the Board.

17. BUSINESS CONTINUITY PLAN (BCP)

The Company shall maintain a Business Continuity Plan to ensure continuity of critical operations during:

- a. System failures;
- b. Power outages;
- c. Natural disasters;
- d. Cyber incidents;
- e. Communication failures.

The BCP shall be reviewed annually.

18. DISASTER RECOVERY (DR)

The Company shall maintain arrangements for recovery of critical systems and data.

The Company shall ensure:

- a. Regular backups of critical data.
- b. Secure storage of backups.
- c. Periodic backup verification.
- d. Restoration testing at least annually.

Recovery procedures shall be documented and tested.

19. DATA BACKUP POLICY

The Company shall maintain:

- a. Daily backup of critical systems and databases.
- b. Secure storage of backup media.
- c. Access restrictions for backup repositories.
- d. Periodic verification of backup integrity.

Backup records shall be maintained.

20. DATA MIGRATION CONTROLS

Any migration of data between systems shall be subject to:

- a. Management approval.
- b. Data mapping documentation.
- c. Validation checks.
- d. User acceptance testing.
- e. Audit trail maintenance.
- f. Rollback procedures.

Post-migration verification shall be performed before system go-live.

21. TRAINING AND AWARENESS

The Company shall conduct periodic awareness programs covering:

- a. Information security.
- b. Cyber security.
- c. Password protection.
- d. Phishing risks.
- e. Data privacy.
- f. Incident reporting.

Training records shall be maintained.

22. INFORMATION SYSTEMS AUDIT (ISA)

The Company shall conduct an Information Systems Audit at least once every year through:

- a. Internal Auditor; or
- b. External IT Auditor; or
- c. Qualified Information Systems Auditor.

The audit shall cover:

- a. Access controls;
- b. Information security;
- c. Cyber security controls;
- d. Data backup arrangements;
- e. Vendor management;
- f. System controls.

Audit observations shall be placed before the Board.

23. RECORD RETENTION

The Company shall maintain:

- a. System logs;
- b. Audit trails;
- c. Incident reports;
- d. Backup records;
- e. Audit reports;
- f. Vendor assessment records;

for a minimum period of eight years or such longer period as required under applicable laws.

24. REPORTING TO THE BOARD

Management shall place before the Board at least annually:

- a. IT Risk Assessment Report;
- b. Information Systems Audit Report;
- c. Cyber Security Incidents, if any;
- d. Vendor Risk Review;
- e. BCP/DR Testing Status;
- f. Corrective Action Taken Report.

Material incidents shall be reported immediately to the Board.

25. POLICY REVIEW

This Policy shall be reviewed annually or earlier in the event of:

- a. Changes in RBI regulations;
- b. Significant technology changes;
- c. Major cyber incidents;
- d. Audit observations;
- e. Business expansion.

Any amendments shall require approval of the Board of Directors.

26. BOARD APPROVAL

This Policy approved by the board at the Board Meeting held on 20.03.2026.