INFORMATION TECHNOLOGY & CYBER SECURITY POLICY

(For Base Layer NBFC – Investment and Credit Company)

1. Preamble

This Information Technology & Cyber Security Policy ("Policy") is framed in compliance with the regulatory framework prescribed by the Reserve Bank of India *(RBI)* for NBFCs under the Scale Based Regulation (SBR) framework.
The Company acknowledges that information assets, digital infrastructure, applications, and customer data are critical resources. Increasing digitization exposes NBFCs to cyber threats such as ransomware, phishing, insider fraud, malware attacks, and data breaches.

This Policy establishes a structured governance, risk management, security control, monitoring, and reporting framework to ensure:

- Confidentiality of information
- Integrity of systems and data
- Availability of critical IT services
- Compliance with RBI and statutory requirements*, including data localization and privacy laws*
- Business continuity and operational resilience

2. Objectives

The objectives of this Policy are to:

1. Establish robust IT governance aligned with RBI expectations *and the Companies Act, 2013*.
2. Define roles and accountability for cyber security *at the Board and Management levels*.
3. Mitigate cyber, operational, reputational, and legal risks.
4. Protect customer sensitive personal data *and fulfill obligations as a Data Fiduciary under the DPDP Act, 2023*.
5. Ensure secure digital lending operations *and API integrations*.
6. Provide a clear incident response and reporting framework *compliant with RBI and CERT-In timelines*.
7. Maintain business continuity in case of system disruptions.

3. Regulatory framework

This Policy is framed in accordance with:

- *Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023 (as amended up to 2025/2026)*
- *Master Direction on Outsourcing of Information Technology Services, 2023*
- RBI Master Directions for NBFCs *(Scale Based Regulation Framework)*
- RBI Cyber Security Framework for NBFCs (2017)
- Information Technology Act, 2000 *(and rules made thereunder)*
- *The Digital Personal Data Protection (DPDP) Act, 2023*
- *CERT-In Directions regarding information security practices and incident reporting (2022/latest amendments)*
- *Relevant provisions of the Companies Act, 2013 (including Sections 134, 177, and 179 regarding risk management systems)*

All amendments issued by the Reserve Bank of India *and relevant statutory bodies* shall automatically form part of this Policy.

4. Applicability

This Policy applies to:

- Board of Directors
- Senior Management
- All employees (permanent, temporary, contractual)

- Consultants and interns
- Third-party vendors*, fintech partners,* and outsourced IT service providers
- Cloud service providers
- IT infrastructure across all branches and locations
- *Digital lending applications (DLAs) and Lending Service Providers (LSPs) associated with the Company.*

5. IT governance structure

5.1 Board of Directors

The Board shall, *as part of its overall risk management oversight under Section 134 of the Companies Act, 2013*:

- Approve *the* IT & Cyber Security Policy *and review it at least annually.*
- Review *the* IT strategy and risk posture.
- Ensure adequate IT budget allocation *and resource optimization.*
- Review major cyber incidents *and post-incident analyses.*
- Ensure compliance with RBI SBR requirements *and DPDP Act provisions.*

5.2 IT Governance *(or IT Strategy)* Committee

An IT Governance Committee *(functioning as the IT Strategy Committee)* shall be constituted comprising:

- *Managing Director (Chairperson)*
- CIO / IT Head
- CISO or designated *Information Security* officer
- Chief Compliance Officer
- Heads of Credit, Finance & Operations

Responsibilities:

- Identify and monitor IT risks *and approve IT-related projects.*
- Review vulnerability assessment reports.
- Monitor cyber incident logs *and threat intelligence.*
- Oversee DRP and BCP testing.
- Recommend policy amendments *to the Board.*
- *Review the effectiveness of outsourced IT services.*

Meetings: At least quarterly and additionally during major incidents.

6. Information Asset Management

The Company shall:

- Maintain an updated IT asset register *(including hardware, software, networking equipment, and data).*
- Classify assets as critical / non-critical.
- Identify business-critical applications.
- Monitor *the* asset lifecycle (procurement to disposal).
- Conduct periodic reconciliation of assets.
- *Maintain a Software Bill of Materials (SBOM) for critical homegrown and third-party applications.*

Secure disposal shall include data wiping *(using recognized standard overwrite protocols)* and physical destruction where required *to prevent data leakage.*

7. Access control framework

7.1 Identity & Access Management (IAM)

- Unique User ID for each employee.
- Strict prohibition of shared IDs.
- Least privilege principle *and Zero Trust Architecture (ZTA) concepts.*
- Segregation of duties in financial systems.
- *Prompt revocation of access upon employee offboarding or role change.*

7.2 Privileged Access Management *(PAM)*

- Restricted admin access.
- Logging of all privileged actions.
- Quarterly review of privileged access *rights.*
- **7.3 Multi-Factor Authentication (MFA)**

Mandatory for:

- Core lending system
- Financial accounting systems
- Email accounts
- Remote login *(VPN)*
- Cloud platforms
- *Access to sensitive customer databases.*

8. Network & infrastructure security

The Company shall implement:

- Enterprise firewall protection.
- Intrusion Detection & Prevention Systems (IDPS).
- Secure VPN for remote users *with endpoint posture checks*.
- Network segmentation *to isolate critical databases from general corporate networks*.
- Secure Wi-Fi configuration *(WPA3 preferred)*.
- Regular firmware updates for routers and switches.
- *Data Loss Prevention (DLP) controls at the network level.*

9. Endpoint security

All desktops, laptops, and mobile devices shall:

- Have licensed antivirus/*Endpoint Detection and Response (EDR)* software.
- Be configured with automatic patch updates.
- Use disk encryption *(e.g., BitLocker)*.
- Have USB access restrictions (where applicable).
- Be monitored through endpoint protection solutions.
- *Be managed via a Mobile Device Management (MDM) solution for corporate-issued mobile devices.*

10. Application security

- Secure coding standards *(e.g., OWASP Top 10)* for internally developed applications.
- Periodic security testing *(Static and Dynamic Application Security Testing - SAST/DAST)*.
- API security controls *(authentication, rate limiting, and payload encryption)*.
- Patch management for third-party software.
- Logging and audit trails for financial transactions *with non-repudiation controls*.

11. Cyber risk management

11.1 Risk Assessment

- Annual Vulnerability Assessment & Penetration Testing (VAPT) *by CERT-In empanelled auditors*.
- Cyber risk assessment before launching new digital products *or DLAs*.
- Risk rating and mitigation tracking.
- Maintenance of *a* Cyber Risk Register.

11.2 Threat Monitoring

- Monitoring phishing trends.
- Tracking ransomware alerts.
- Monitoring suspicious login attempts.
- Continuous log monitoring *(preferably via a Security Information and Event Management - SIEM - system)*.

12. Data Protection & Privacy (DPDP Act Compliance)

12.1 Data Classification *& Consent*

Data shall be categorized as:

- Confidential (customer financial data)
- Sensitive (KYC data, *biometrics*)
- Internal (operational data)
- Public

The Company shall obtain explicit, clear, and itemized consent from Data Principals (customers) before collecting personal data, strictly adhering to the purpose limitation principle under the DPDP Act, 2023.

12.2 Encryption Standards

- Data at rest encrypted using industry standards *(e.g., AES-256).*
- Data in transit secured via TLS/SSL *(TLS 1.2 or higher).*
- Encrypted database backups.
- Secure key management procedures.

12.3 Data Retention *& Erasure* Policy

- Retention aligned with RBI and statutory norms *(e.g., KYC data retention for 5 years post-relationship termination).*
- Secure deletion post-retention *upon withdrawal of consent, unless retention is legally mandated*.
- Retention schedule approved by management.
- *Grievance redressal mechanism established for Data Principals to exercise their rights to correction and erasure.*

13. BACKUP & DISASTER RECOVERY

13.1 Backup Strategy

- Daily automated backup.
- Offsite/cloud backup redundancy *(geographically separated).*
- Backup encryption *and immutability to protect against ransomware*.
- Quarterly restoration testing.

13.2 Disaster Recovery Plan (DRP)

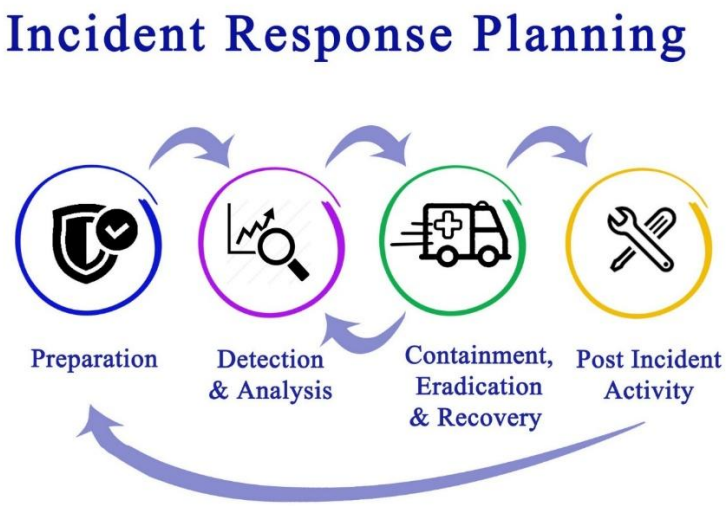
- Clearly defined Recovery Time Objective (RTO).
- Clearly defined Recovery Point Objective (RPO).
- Annual DR drill *involving primary to DR site switchover*.
- Documentation of DR test results *and presentation to the Board/IT Committee*.

14. BUSINESS CONTINUITY MANAGEMENT (BCM)

The Company shall:

- Identify critical processes *via a Business Impact Analysis (BIA).*
- Define alternate arrangements.
- Maintain *an* emergency contact matrix.
- Ensure continuity of customer service during outages.
- Integrate IT DRP with *the* overall BCP.

15. Incident response framework



Getty Images

15.1 Incident Response Team (IRT)

The IRT shall:

- Detect and classify incidents.
- Contain affected systems.
- Preserve evidence *(forensic readiness)*.
- Initiate recovery.
- Escalate as per severity.

15.2 Incident Reporting to RBI *and CERT-In*

- Significant cyber incidents shall be reported to the Reserve Bank of India within prescribed timelines *(typically within 24 hours of notice)*.
- *Severe cyber security incidents (as classified by CERT-In) must be mandatorily reported to CERT-In within 6 hours of noticing or being brought to notice.*
- **15.3 Root Cause Analysis (RCA)**
- Identify source of breach.
- Implement preventive controls.
- Update risk assessment.
- Report corrective action to *the* Board.

16. Outsourcing & third-party risk

In alignment with RBI IT Outsourcing Directions:

The Company shall:

- Conduct IT security due diligence before vendor onboarding.
- Include *comprehensive* security clauses *and Right to Audit clauses* in contracts.
- Ensure confidentiality *and Non-Disclosure* agreements *(NDAs)*.
- Monitor vendor compliance *periodically*.
- Review cloud data storage location compliance *(All customer and financial data must be stored on servers located within the geographical borders of India).*
- *Maintain an inventory of all outsourced IT services and report material IT outsourcing arrangements to the IT Governance Committee.*

17. Cyber security awareness

- Mandatory annual training for all employees *and new joiners*.
- Phishing simulation exercises.
- Awareness sessions on password hygiene *and social engineering*.

- Special training for privileged users *and IT personnel.*
- *Dissemination of cyber hygiene tips to customers to prevent digital lending fraud.*

18. Audit & assurance

18.1 Internal Audit
(To be conducted by an independent Information Systems Audit team or external firm)
- Review of access control logs.
- VAPT compliance verification.
- Data backup verification.
- Incident management audit.

18.2 External Audit
- Annual independent IT audit *(preferably by a CISA-qualified auditor).*
- Compliance certification *submitted to the Board and RBI (if mandated).*

19. Documentation & record keeping

The Company shall maintain:
- Incident register.
- Access review logs.
- Audit reports.
- VAPT reports.
- DR drill reports.
- IT asset inventory.

· *Consent logs as required under the DPDP Act.*

20. Policy review

This Policy shall be reviewed:

- Annually; or
- Upon significant regulatory or technological changes.

Any amendments require Board approval.

21. Effective date

This **INFORMATION TECHNOLOGY & CYBER SECURITY POLICY** has been approved by the Board of Directors of THIRUKOCHI FINCAP LIMITED at its meeting held on 12/03/2026.

Effective Date: 12/03/2026

Version:1