

CHARTERED FINANCE & LEASING LTD. (CFL)

("NBFC / B-13.02480")

Information Technology (IT) Policy / Information System (IS) Policy

Version: V3 | Review Cycle: Annual

Approved by: Board of Directors

Date of Approval: 07th April, 2026

SUMMARY OF POLICY

Particular	Details
Policy Name	Information Technology (IT) Policy / Information System (IS) Policy
Version	V3
Latest Approval / Review Date	07 th April,2026
Review Cycle	Annually
Approver	Board of Directors of Chartered Finance & Leasing Ltd.

VERSION HISTORY

Version No.	Approval	Version Description	Regulatory Reference	Remarks
I	Board Meeting dated 7th April, 2022	2022	RBI Regulation	Policy adopted by the Board
II	Board Meeting dated 20th May, 2025	2025	RBI Regulation	Review by the Board
III	Board Meeting dated 07 th April,2026	2026	Updated as per applicable RBI Master Directions / guidelines for NBFCs (including November 2025 consolidation)	Limited update and simplification; policy aligned to proportionate NBFC framework

Contents

1. Introduction	5
2. Framework of Policy	5
3. Information Technology Governance	5
a) Head – Information Technology (IT) / Designated IT Officer	5
b) IT Strategy Committee	6
4. Information Security	6
a) Identification and Classification of Information Assets	7
b) Segregation of Functions	7
c) Limiting Physical Access	7
d) Limiting Logical Access	7
e) Well-defined Password Policy	7
f) Role Based Access Control	8
g) Integrity of Data	8
h) Availability	8
i) Maker-Checker Concept	8
j) Incident Management	8
k) Audit Trails	8
l) Public Key Infrastructure (PKI)	8
5. Cyber Security	9
a) Cyber Security Preparedness Indicators	9
b) Cyber Crisis Management Plan	9
c) Reporting of Cyber Incidents	9
d) Awareness among Stakeholders / Top Management / Board	9
6. Mobile Financial Services / Mobile Computing	10
7. Social Media	10
8. IT Risk Assessment	10
9. Training	10
10. IT Operations	11
a) Acquiring or Developing a New System	11
b) Change Management Policy	11
11. IT Enabled Management Information System	11
12. Policy for Information System Audit (IS Audit)	12
a) Broad Framework of IS Audit	12
b) IS Audit Team	13
c) Computer-Assisted Audit Techniques (CAATs)	13
d) Periodicity and Timing	13
e) Reporting	13
13. Business Continuity Planning (BCP) and Disaster Recovery	13
a) Business Impact Analysis	13
b) Recovery Strategy / Contingency Plan	14
14. Policy for IT Services Outsourcing	14

1. Introduction

The Company, being an NBFC in the Middle Layer, is governed by Chapters I, II and V of the Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026. The Board shall approve the strategies and policies related to IT, information assets, business continuity, information security and cybersecurity (including incident response and recovery management / cyber crisis management), which shall be placed before the Board for review at least annually.

The Policy has been approved by the Board of Directors. Any material change to this Policy shall require approval of the Board. The Policy shall be reviewed at least annually.

2. Framework of Policy

The focus of this Policy is on IT Governance, Information Security, Cyber Security, IT Operations, IS Audit, Business Continuity Planning / Disaster Recovery and IT Services Outsourcing.

Information security primarily refers to protecting the confidentiality, integrity, and availability of data of the Company, whether in physical or electronic form. The purpose of this policy is to control access to sensitive information and ensure use only by legitimate users so that data cannot be read or compromised without proper authorization.

The Company shall maintain controls over confidentiality, integrity and availability of information and systems, proportionate to its business model and risk profile.

The Policy is in conformity with the Company's objectives of sound infrastructure and systems.

3. Information Technology Governance

The Board of Directors shall have overall responsibility for IT governance and oversight over information security and technology risk. The Board may discharge such oversight directly or through the Risk Management Committee / other Board Committee, wherever applicable.

Executive Management shall be responsible for implementation of this Policy.

In addition, the following positions/committees shall play an important role in the Company's IT Governance framework.

a) Head – Information Technology (IT) / Designated IT Officer

The Company shall appoint a sufficiently senior level, technically competent and experienced official in IT related aspects as Head of IT Function, who shall be responsible for ensuring that the execution of IT projects / initiatives is aligned with the IT policy and IT strategy, ensuring an effective organisational structure to support IT functions, putting in place an effective DR setup and business continuity strategy / plan, and, as a first line of defence, ensuring effective assessment, evaluation and management of IT controls and IT risk.

The designated IT function shall be responsible for:

- ✓ maintaining the Company's systems, devices, applications and user administration;
- ✓ implementing Board / management approved IT controls;
- ✓ ensuring backup, password, access and basic cyber hygiene controls;
- ✓ maintaining records of major incidents and changes; and
- ✓ escalating material IT / cyber issues to management and the Board / Committee, as applicable.

b) IT Strategy Committee

In accordance with the Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, the Company has constituted a Board-level IT Strategy Committee (ITSC). The ITSC shall have a minimum of three directors (including its Chairperson) as members; the Chairperson shall be an

independent director having substantial IT expertise, i.e., a minimum of seven years' experience in managing information systems and/or leading/guiding technology/cybersecurity initiatives/projects, with an understanding of the business processes at a broader level and the impact of IT on such processes; and the members shall be technically competent, i.e., able to understand and evaluate information systems and associated IT/cyber risks.

The Committee shall review IT strategy, material technology issues, cyber security matters, major incidents, IS audit observations and significant outsourcing arrangements. The Committee shall meet at least on a quarterly basis.

The Committee's deliberations shall be placed before the Board.

Roles and Responsibilities of the IT Strategy Committee:

The ITSC shall: (1) ensure that the Company has put an effective IT strategic planning process in place; (2) guide in preparation of IT strategy and ensure that it aligns with the overall strategy of the Company; (3) satisfy itself that the IT governance and information security governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well-defined objectives and unambiguous responsibilities for each level; (4) ensure that processes for assessing and managing IT and cybersecurity risks are in place; (5) ensure that budgetary allocations for the IT function, including IT security / cybersecurity, are commensurate with the Company's IT maturity, digital depth, threat environment and industry standards; (6) review, at least on an annual basis, the adequacy and effectiveness of business continuity planning and DR management; (7) review the assessment of IT capacity requirements and measures taken; and (8) approve documented standards and procedures for administering need-based access to an information system.

The Company shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions, which shall meet on a quarterly basis and shall assist the ITSC in strategic IT planning, oversight of IT performance and aligning IT activities with business needs; oversee the processes for business continuity and DR; ensure implementation of a robust IT architecture meeting statutory and regulatory compliance; and update the ITSC and MD / CEO periodically on its activities.

An Information Security Committee, under the oversight of the ITSC and headed by an official from the risk management vertical, shall be formed with the CISO and representatives from business, IT and other relevant functions, as decided by the ITSC. A senior level executive shall be designated as the Chief Information Security Officer, who shall not have any direct reporting relationship with the Head of IT Function, shall not be given any business targets, shall be a permanent invitee to the ITSC and IT Steering Committee, shall directly report to the Executive Director or equivalent executive overseeing the risk management function, and shall place a review of cybersecurity risks / arrangements / preparedness before the Board / Risk Management Committee of the Board / ITSC at least on a quarterly basis.

The Company shall implement a suitable scorecard / metrics / methodology to measure IT performance and IT maturity level, covering, inter alia: (a) availability / uptime of critical information systems and service delivery channels; (b) number and severity of IT and cyber incidents and the time taken to resolve them; (c) success rate of changes and patches deployed in the production environment; (d) delivery of IT projects against approved timelines and budgets; (e) status of closure of IS audit, VA / PT and other audit observations; and (f) a periodic self-assessment of IT maturity against the IT strategy of the Company. The scorecard shall be reviewed by the IT Steering Committee and placed before the ITSC periodically.

4. Information Security

Information is an important asset of the Company. The Company shall establish and maintain basic information security controls to protect information in physical and electronic form.

The information security framework shall be based on the following principles:

- ✓ Confidentiality – access only to authorised persons;
- ✓ Integrity – prevention of unauthorised change;

- ✓ Availability – information and systems available when required; and
- ✓ Authenticity – users, transactions and records to be genuine.

a) Identification and Classification of Information Assets

The Company shall maintain an inventory of information assets and shall ensure identification and mapping of the security classification (in terms of confidentiality, integrity and availability) of information assets based on their criticality to its operations.

b) Segregation of Functions

The Company shall put in place a Service Level Management process to manage IT operations while ensuring effective segregation of duties, and areas of possible role conflicts and accountability gaps shall be specifically identified and eliminated or managed. The Company shall ensure reasonable maker-checker / supervisory review / approval controls in critical areas such as access creation, transaction processing, parameter changes and vendor payments.

c) Limiting Physical Access

The Company shall restrict physical access to laptops, systems, records, backups, server / network devices and other important IT assets.

The Company has created a secure environment for physical security of information assets such as secure location of critical data, restricted access to sensitive areas and has obtained adequate insurance to safeguard such data.

d) Limiting Logical Access

The Company shall grant system access only on a need basis and with approval. User IDs shall be unique. Access rights shall be removed / modified promptly on role change or exit.

- ✓ All users must use a unique ID to access the Company's systems and applications.
- ✓ Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.
- ✓ The Company shall implement multi-factor authentication for enterprise (logical) access to critical systems from alternate work locations, and, based on risk assessment, two-factor or multi-factor authentication for privileged users of critical information systems and for critical activities. Personnel with elevated system access entitlements shall be closely supervised, with all their system activities logged and periodically reviewed.
- ✓ System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

e) Well-defined Password Policy

The Company shall maintain basic password controls including minimum complexity, confidentiality of passwords, prohibition on sharing and periodic change, wherever applicable. All users are responsible for keeping their passwords secure and confidential.

f) Role Based Access Control

Access to systems and information shall be role-based to the extent feasible. Administrative / privileged access shall be restricted.

The Company would, as far as possible, avoid dependence on one or few persons for a particular job. There shall be clear delegation of authority for the right to upgrade / change user profiles and permissions and also key business parameters (e.g. interest rates), which shall be documented.

g) Integrity of Data

The Company shall maintain data accuracy and reliability through maker-checker controls, authorised system changes, reconciliations and record retention. The Company shall ensure

that data, transactions, communications or documents (electronic or physical) generated are authentic and genuine.

The Company shall maintain enterprise data dictionary to enable the sharing of data among applications and information systems and promote a common understanding of data.

In order to prevent unauthorised modification of data, the Company shall ensure that there is no manual intervention or manual modification in data while it is being transferred from one process to another or from one application to another, in respect of critical applications. Data transfer mechanism between processes or applications must be properly tested, securely automated with necessary checks and balances, and properly integrated through 'Straight Through Processing' methodology with appropriate authentication mechanism and audit trails.

h) Availability

The Company shall ensure availability of important systems and information through appropriate backup, antivirus / endpoint protection, vendor support and recovery arrangements.

i) Maker-Checker Concept

The Company shall follow a maker-checker / checker-approval concept for critical transactions and important system changes, to the extent feasible. This helps minimise the risk of error and ensures reliability of information.

j) Incident Management

The Company's cyber incident response and recovery management framework shall address classification and assessment of incidents, a clear communication strategy and plan to manage such incidents, and measures to contain exposures and achieve timely recovery. Cyber incidents shall be analysed (including through forensic analysis, if necessary) for severity, impact and root cause. The Company shall have written incident response and recovery procedures including identification of key roles of staff / outsourced staff, and clear communication plans for escalation and reporting of incidents to the Board and Senior Management as well as to customers, as required.

Common incident types include delay in services due to hardware/software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, data integrity issues, etc.

All security incidents or violations of security policies should be brought to the notice of the designated IT Officer. These incidents / violations shall be reported to the Board / Risk Management Committee, as applicable.

k) Audit Trails

The Company shall ensure that every IT application / system that can access or affect critical or sensitive information has necessary audit logging capabilities and provides audit trails sufficiently detailed to facilitate audits, serve as forensic evidence and assist in dispute resolution, including for non-repudiation, and shall put in place a system for regularly monitoring audit trails and system logs to detect, understand or recover from any unauthorised activity or attack.

l) Public Key Infrastructure (PKI)

The Company may use digital signatures / PKI wherever required, for banking, statutory, regulatory and contractual purposes, to ensure confidentiality of data, access control, data integrity, authentication and non-repudiation.

5. Cyber Security

Cyber Security is an integral part of this Policy. The Company shall maintain reasonable preventive and detective controls against cyber threats, proportionate to its size and digital exposure. The Company shall review organisational arrangements so that security concerns receive adequate attention and are escalated to appropriate levels in the hierarchy.

Vulnerability management is an integral part of Cyber Security. The Company shall devise appropriate strategies for managing and eliminating vulnerabilities in its IT base, whether hardware or software.

The Company shall conduct vulnerability assessment at least once in every six months and penetration testing at least once in 12 months for critical information systems and / or those in the De-Militarised Zone having customer interface, and also pre-implementation, post-implementation and after changes, through appropriately trained and independent information security experts / auditors; for non-critical systems a risk-based approach shall be adopted. Identified vulnerabilities shall be fixed in a time-bound manner, and a documented approach for VA / PT covering scope, coverage and vulnerability scoring mechanism shall be maintained, including for systems hosted in a cloud environment.

a) Cyber Security Preparedness Indicators

The Company may monitor basic indicators such as antivirus status, system update / patch status, incident occurrence, backup status and user access review completion. These shall be used for periodic compliance checks and audits carried out by qualified and competent professionals.

b) Cyber Crisis Management Plan

The Company shall maintain a simple Cyber Crisis Management / response process covering the following four aspects:

- ✓ Detection
- ✓ Response
- ✓ Recovery
- ✓ Containment

The Company shall take effective measures to prevent cyber-attacks and promptly detect any cyber-intrusions so as to respond / recover / contain adverse effects. The Company shall 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 (DDoS), ransomware / cryptoware, destructive malware, business email frauds including 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.

c) Reporting of Cyber Incidents

The Company shall report cyber incidents to RBI within six hours of detection on the DAKSH platform (<https://daksh.rbi.org.in>) and shall also pro-actively notify CERT-In regarding cyber incidents.

d) Awareness among Stakeholders / Top Management / Board

The Company shall conduct basic awareness for employees and inform the Board / management about major cyber risks and incidents. The Company shall proactively promote, among its customers, vendors, service providers and other relevant stakeholders, an understanding of their cyber resilience objectives, and require appropriate action to support synchronised implementation and testing.

6. Mobile Financial Services / Mobile Computing

The Company shall maintain reasonable controls over laptops, portable devices and remote access used for official work.

a) Mobile Applications: The Company also uses mobile applications for providing Financial Services. It shall develop a mechanism for safeguarding information assets used by mobile applications to provide services to customers. The technology used for mobile services shall ensure confidentiality, integrity, authenticity and shall provide for end-to-end encryption.

b) Privacy Policy: As personal information is collected from borrowers, the Company shall maintain a comprehensive and compliant privacy policy available publicly. Details of any third parties allowed to collect personal information via the lending app shall also be disclosed. Privacy practices shall be disclosed on the app at every relevant stage.

c) Cloud Infrastructure: Where the Company uses cloud services for storage, computing and movement of data, it shall comply with the Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, including documenting the services that can be moved to the cloud, ensuring that the IT outsourcing arrangements address the entire lifecycle of data, selecting CSPs based on a comprehensive risk assessment, implementing role-based access with multi-factor authentication for cloud applications, and maintaining an exit strategy. In case the Company engages digital lending platforms as its agents, the applicable directions of the RBI in this regard shall be adhered to.

7. Social Media

Employees shall not disclose confidential information, customer information or sensitive business information on social media or public platforms without authority. Whenever the Company uses social media to market its products, proper controls such as encryption and secure connections shall be put in place to mitigate risks.

8. IT Risk Assessment

The Company shall undertake an IT risk assessment at least annually, in a simple documented manner, covering key systems, vendors, access, backup, antivirus / endpoint protection, data protection and recovery arrangements. The assessment shall analyse threats and vulnerabilities to the information technology assets of the Company and its existing security controls and processes.

The outcome of the exercise shall be to find out the risks present and to determine the appropriate level of controls necessary for the mitigation of risks. The risk assessment shall be brought to the notice of the Designated IT Officer, the Chief Risk Officer and the Board / Risk Management Committee, and shall serve as an input for Information Security auditors.

The risk management policy of the Company shall include IT related risks, including cybersecurity related risks, and the Risk Management Committee of the Board, in consultation with the ITSC, shall review and update the same at least on an annual basis. The risk assessment for each information asset shall be guided by appropriate security standards / IT control frameworks, and the security infrastructure and security policies shall be reviewed at least annually.

9. Training

The Company shall develop an information security awareness programme. The programme shall be periodically updated, keeping in view changes in information technology systems, threats/vulnerabilities and / or the information security framework.

The Company shall provide basic awareness and training to staff on password hygiene, phishing, safe system usage, incident reporting and data confidentiality. There shall be a mechanism to track the effectiveness of training programmes through an assessment/testing process. The Company shall maintain an updated status on user training and awareness relating to information security.

10. IT Operations

The Company shall maintain simple and effective controls over IT operations. The Company shall aim to put in place IT systems which support processing and storage of information such that the required information is available in a timely, reliable, secure and resilient manner.

For seamless continuity of business operations, the Company shall avoid using outdated and unsupported hardware or software and shall monitor software end-of-support (EOS) dates and Annual Maintenance Contract (AMC) dates of IT hardware on an ongoing basis. The Company shall develop a technology refresh plan for the replacement of hardware and software in a timely manner before they reach EOS.

The Company shall ensure that information systems and infrastructure are able to support business functions and ensure availability of all service delivery channels. The Company shall proactively assess capacity requirement of IT resources at least annually, and more frequently where warranted by business growth or significant changes in the IT environment. The Company shall ensure that IT capacity planning across components, services, system resources, supporting infrastructure is consistent with past trends (peak usage), the current business requirements and projected future needs as per the IT strategy of the Company.

a) Acquiring or Developing a New System

Any new system or material application change shall be approved by management and implemented only after considering business need, security, access controls, user testing and vendor support. The Company shall identify system deficiencies and defects at the system design, development and testing phases.

The Company shall follow a consistent and formally defined project management approach for IT projects, a standard enterprise architecture planning methodology while adopting new or emerging technologies, and shall ensure that any new IT application proposed for introduction as a business product undergoes the prescribed product approval and quality assurance process.

b) Change Management Policy

Important system changes, parameter changes and access changes shall be documented and approved. The Company shall realign its IT systems on a regular basis in line with the changing needs of its customers and business. The changes shall be carried out in such a way that adverse incidents and disruption to services are minimised while maximising value for customers.

For this purpose, the Company shall develop, with the approval of the Board, a Change Management Policy that encompasses:

- ✓ Prioritising and responding to change proposals from the business;
- ✓ Cost-benefit analysis of the changes proposed.
- ✓ Assessing risks associated with the changes proposed;
- ✓ Change implementation, monitoring and reporting.
- ✓ Testing and validation of proposed changes prior to deployment in the production environment, with a documented rollback/contingency plan in case of failure.

The Change Management Policy shall also cover patch management and ensure that the business impact of implementing (or not implementing) patches / changes is assessed; patches / changes are applied and reviewed in a secure and timely manner with necessary approvals; and a mechanism is established to recover from failed changes / patch deployment.

The Company shall follow a documented, systematic process for data migration ensuring data integrity, completeness and consistency, with audit trails and sign-offs from business users and application owners at each stage.

11. IT-Enabled Management Information System

The Company shall maintain such MIS as is necessary for management oversight, regulatory compliance, basic risk monitoring and operational control. The MIS shall assist top management in decision-making and maintain oversight over the operations of various business verticals.

The following information shall be part of the system:

- ✓ A dashboard for Top Management summarising financial position vis-à-vis targets, including information on trend on returns on assets across categories, major growth business segments, movement of net-worth, regulatory and statutory compliances and various trackers / e-tools for generating reports.
- ✓ System-enabled identification and classification of Special Mention Accounts and NPAs as well as generation of MIS reports in this regard.
- ✓ Regulatory requirements and their compliance.
- ✓ Financial Reports including operating and non-operating revenues and expenses, cost benefit analysis of segments/verticals, cost of funds, etc. (including regulatory compliance at transaction level).
- ✓ Reports relating to treasury operations.
- ✓ Fraud analysis — Suspicious transaction analysis, embezzlement, theft or suspected money-laundering, misappropriation of assets, manipulation of financial records, etc. The regulatory requirement of reporting fraud to RBI shall be system-driven.
- ✓ Capacity and performance analysis of IT security systems.
- ✓ Incident reporting, its impact and steps taken for non-recurrence of such events in the future.

The Company's IT system shall capture regulatory requirements and compliance thereof, enabling the Company to file the required regulatory returns with RBI. Wherever applicable, all regulatory/supervisory returns shall be system-driven so as to enable seamless integration between the MIS of the Company and reporting to RBI. Further, it shall be ensured that 'Read Only' access is provided to RBI Inspectors.

12. Policy for Information System Audit (IS Audit)

The objective of an IS Audit is to review the adequacy and effectiveness of IT controls, access management, information security, backup, business continuity and vendor controls. The IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure, such as server architecture, local and wide area networks, physical and information security, telecommunications, etc. The IS Audit shall form an integral part of the Internal Audit system of the Company.

The Company shall have adequately skilled personnel in its Audit Committee who can understand the results of the IS Audit.

The Audit Committee of the Board shall be responsible for oversight of IS Audit and shall approve, and review at least annually, the provisions of this section describing the mandate, purpose, authority, audit universe and periodicity of IS Audit. The Company shall have a separate IS Audit function or resources possessing the required professional skills within the Internal Audit function; where external resources are used, responsibility and accountability shall remain with the competent authority within the Internal Audit function. IS Audit planning shall adopt a risk-based approach.

a) Broad Framework of IS Audit

The IS Audit shall evaluate the following aspects:

- ✓ Effectiveness of policy and oversight of IT systems;
- ✓ Adequacy of processes and internal controls;
- ✓ Effectiveness of business continuity planning and disaster recovery setup;

- ✓ Compliance with all legal and statutory requirements.

The IS Audit shall recommend corrective action to address deficiencies and follow-up. The IS Audit shall ensure that BCP is effectively implemented in the Company.

The Audit Committee of the Board, along with the IT Strategy Committee, shall outline the responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, and authority for accepting compliance in the IS Audit framework.

b) IS Audit Team

IS Audit may be carried out by an internal team of the Company or by external professionals having relevant competence and independence. It shall be ensured that there is a right mix of skills and understanding of legal and regulatory requirements so as to assess the efficacy of the framework vis-à-vis these standards. IS Auditors shall act independently of the Company's management both in attitude and appearance.

c) Computer-Assisted Audit Techniques (CAATs)

The Company shall adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs shall be used in critical areas (such as detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported), particularly for critical functions or processes having financial / regulatory / legal implications.

d) Periodicity and Timing

The periodicity of IS Audit shall be as approved by the Audit Committee of the Board under this section, and IS Audit shall in any case be conducted at least once a year. IS Audit shall be undertaken prior to the statutory audit so that IS Audit reports are available to the statutory auditors well in time for examination and for incorporating comments, if any, in the audit reports.

e) Reporting

IS Audit findings shall be placed before the Audit Committee of the Board / relevant Committee, as applicable, and compliance shall be tracked.

13. Business Continuity Planning (BCP) and Disaster Recovery

BCP forms a significant part of an organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. The Company shall put in place a BCP Policy, duly approved by the Board. The BCP shall be designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.

Reports on the functioning of the BCP shall be placed before the Board at least annually, and the ITSC shall review the adequacy and effectiveness of business continuity planning and DR management at least on an annual basis. The Company shall consider the need to put in place necessary back-up sites for its critical business systems and data centres.

a) Business Impact Analysis

The Company shall identify critical business verticals, locations, shared resources, systems, records and processes to come up with a detailed Business Impact Analysis. The process shall envisage the impact of any unforeseen natural or man-made disasters on the Company's business. The business impact areas in order of priority shall be clearly listed.

b) Recovery Strategy / Contingency Plan

The Company shall maintain basic backup and recovery arrangements, alternate contact points and vendor support details for recovery of important systems and data. The Company shall try to fully understand vulnerabilities associated with interrelationships between various systems, departments and business processes.

The Company shall test the BCP at least annually, or when significant IT or business changes take place, to determine if the Company could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test shall be based on 'worst case scenarios'. The results along with the gap analysis shall be placed before the Board / Risk Management Committee.

The Company's BCP and DR arrangements shall adopt best practices (e.g., ISO 22301). DR drills for critical information systems shall be conducted at least on a half-yearly basis, and for other systems as per risk assessment, involving switching over to the DR site for at least a full working day. Backed-up data shall be periodically restored to check usability. The Company shall prioritise achieving minimal RTO, as approved by the ITSC, and near zero RPO for critical information systems, ensure that configurations and security patches at DC and DR are identical, and that DC and DR sites are geographically well separated.

The Company shall define suitable metrics for system performance (such as availability and response time), recovery (such as RTO, RPO and the outcome of DR drills and backup restoration tests) and business resumption (such as the time taken to resume critical business processes at an acceptable level), for all critical information systems. The RTO and RPO values for critical information systems shall be: an RTO not exceeding 4 (four) hours and an RPO not exceeding 15 (fifteen) minutes, for critical information systems including the loan management system, the accounting / ERP system and the treasury / investment management system. For non-critical information systems, the Company shall adopt a risk-based approach to define suitable metrics.

The further business continuity and disaster recovery requirements applicable to the Company are set out in section 6.5 of the Company's Information and Cyber Security Policy.

14. Policy for IT Services Outsourcing

Outsourcing of IT services shall be governed by this section, read with Chapter IV of the Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, covering the matters specified therein.

For third-party arrangements in the information technology / cybersecurity ecosystem which are not within the applicability of the Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025, the Company shall put in place appropriate vendor risk assessment process and controls proportionate to the assessed risk and materiality to, inter alia: (1) mitigate concentration risk; (2) eliminate or address any conflict of interests; (3) mitigate risks associated with single point of failure; (4) comply with applicable legal, regulatory requirements and standards to protect customer data; (5) provide high availability (for uninterrupted customer service); and (6) manage supply chain risks effectively.

15. Review

This Policy shall be reviewed at least annually.

The Company shall review and refine the Information Technology & Information Security Policy as may be required periodically, based on its own experience and fresh guidelines, if any, issued by the RBI in this regard.

If at any point a conflict of interpretation / information between this policy and any regulations, rules, guidelines, notifications, clarifications, circulars, Master Directions issued by relevant authorities ("Regulatory Provisions") arises, then interpretation of the Regulatory Provisions shall prevail. In case of any amendment(s) and/or clarification(s) to the Regulatory Provisions, this policy shall stand amended accordingly from the effective date specified as per the Regulatory Provisions.