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	07th 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 07th 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

The Reserve Bank of India, through its Master Directions on IT Framework for the NBFC Sector and the subsequent Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023 (effective April 1, 2024), as rationalised and consolidated under the November 2025 RBI Master Directions consolidation, requires NBFCs to maintain a Board-approved Information Technology (IT) Policy / Information System (IS) Policy to ensure that the IT framework is benchmarked to best practices and is proportionate to the scale, complexity and risk profile of the NBFC.

Considering the size of operations, limited transaction volume and small staff strength of the Company, the IT framework shall be simple, practical and proportionate to the scale and complexity of the business, while ensuring compliance with applicable regulatory expectations.

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 designate a responsible officer / senior employee / outsourced support arrangement for day-to-day IT administration and implementation of this Policy. Depending on the size and structure of the Company, a separate Chief Technology Officer may not be required.

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

The Company may constitute an IT Strategy Committee if required under applicable regulatory instructions or if considered necessary by the Board. In case a separate IT Strategy Committee is not constituted, the Board / Risk Management Committee may discharge the related oversight functions.

Where constituted, the Committee shall review IT strategy, material technology issues, cyber security matters, major incidents, IS audit observations and significant outsourcing arrangements. The gap between two meetings shall ordinarily not exceed six months.

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

Roles and Responsibilities of the IT Strategy Committee:

- ✓ Approving IT strategy and policy documents and ensuring that management has put an effective IT strategic planning process in place;
- ✓ Ascertaining that management has implemented processes and practices that ensure IT delivers value to the business;
- ✓ Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable;
- ✓ Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and providing high-level direction for sourcing and use of IT resources;
- ✓ Ensuring a proper balance of IT investments for sustaining the Company's growth and becoming aware of exposure to IT risks and controls.

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 a simple inventory of critical information assets, systems, applications, devices and data.

b) Segregation of Functions

Considering the small staff strength, full segregation may not always be feasible. The Company shall, however, 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.
- ✓ Remote access to the Company's systems and applications must use two-factor authentication, where possible.

- ✓ 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.

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 shall maintain a simple process for identification, reporting, escalation and closure of IT / information security incidents. Major incidents shall be brought to the notice of senior management and the Board / relevant Committee, as applicable.

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 audit trails / system logs, as available in the applications / systems used by it, are enabled and preserved for review and audit purposes, serving as forensic evidence when required and assisting in dispute resolution.

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.

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 all types of unusual cyber security incidents to RBI or other authority, as prescribed under applicable Master Directions / guidelines. Both successful and attempted incidents shall be reported using RBI's latest prescribed template.

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: The Company shall ensure that cloud vendors comply with commensurate regulatory standards. 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.

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.

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.

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.

✓

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.

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 IS Audit shall be conducted at least once in a year, or at such interval as may be considered appropriate by the Board / Audit Committee based on size and risk profile. 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.

The Company shall ensure regular oversight of the BCP by way of periodic reports (at least once every year) put up to the Board of Directors. 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.

14. Policy for IT Services Outsourcing

Prior to commencement of any outsourcing arrangement, careful consideration of risks, threats of contractual arrangements and regulatory compliance obligations shall be done. The Company's decision to outsource IT Services shall be within its overall strategic plan and corporate objectives.

Before outsourcing material IT services, the Company shall carry out basic due diligence on the service provider and ensure that the agreement covers at least: scope of service, confidentiality, access rights, incident reporting, backup / recovery support, termination and handover provisions.

The terms and conditions governing the contract between the Company and the outsourcing service provider shall be carefully defined in written agreements and vetted by the Company's legal counsel. The contractual agreement shall have provisions as prescribed in the RBI directions.

Outsourcing shall not dilute the Company's accountability for compliance, customer protection and information security. The Board and senior management shall be ultimately responsible for outsourcing operations and for managing risks inherent in such outsourcing relationships.

The Board and IT Strategy Committee shall have the responsibility to institute an effective governance mechanism and risk management process for all IT outsourced operations. The role of the IT Strategy Committee in respect of outsourced operations shall include:

- ✓ Instituting an appropriate governance mechanism for outsourced processes, comprising risk-based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end-to-end manner;
- ✓ Defining approval authorities for outsourcing depending on the nature of risks and materiality of outsourcing;
- ✓ Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope and complexity of outsourcing arrangements;
- ✓ Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements;
- ✓ Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board;
- ✓ Periodically reviewing the effectiveness of policies and procedures;
- ✓ Communicating significant risks in outsourcing to the Company's Board on a periodic basis;
- ✓ Ensuring an independent review and audit in accordance with approved policies and procedures;
- ✓ Ensuring that contingency plans have been developed and tested adequately.

The Company shall ensure that its business continuity preparedness is not adversely compromised on account of outsourcing. The Company shall adopt sound business continuity management practices and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

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.