CHARTERED FINANCE & LEASING LTD. (CFL)

(“NBFC/ B-13.02480”)

SUMMARY OF POLICY

Particular	Details
Policy Name	Information Technology (IT) Policy / Information System (IS) Policy
Version	V2
Latest Approval/Review Date	20th May, 2025
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

Contents

1. Introduction

The Reserve Bank of India in its relevant Master Direction has stipulated that NBFCs shall have a Board approved Information Technology (IT) Policy / Information System (IS) Policy to ensure that the IT framework in NBFCs is benchmarked to best practices.

The Policy has been approved by the Board of Directors. Any changes to this Policy would require the approval of the Board. The Policy will be reviewed annually.

2. Framework of policy

The focus of the proposed IT framework is on IT Governance, IT Policy, Information & Cyber Security, IT Operations, IS Audit, Business Continuity Planning 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.

With increasing use of technology in the Company's operations, there is a need to ensure security of data which is in digital form, i.e., in computers, devices, networks, server etc. Accordingly, in addition to Information Security, this Policy also encompasses effective IT and cyber security procedures.

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

3. Information Technology Governance

The basic principles of value delivery, IT Risk Management, IT resource management and performance management form the basis of the Company's governance framework. Given the criticality of the IT, the company has followed relevant aspects of such prudential governance standards that have found acceptability in the industry.

The Board of Directors and the Risk Management Committee of the Board will have overall responsibility of ensuring information security of the Company. The Managing Director of the Company shall be responsible for the development and implementation of an effective risk management function, in line with the requirements stipulated by RBI and this Policy. The Board/ the Risk Management Committee of the Board (RMCB) would exercise oversight.

Effective IT Governance would be the responsibility of the Board of Directors and Executive Management. The Company would develop an IT organizational structure, which would be commensurate with the size, scale and nature of the business activities carried out.

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

a) Chief Technology Officer (IT)

The Company would designate a senior executive as the Chief Technology Officer (CTO) operations whose responsibility would be to ensure implementation of this Policy on an operational level, involving IT strategy, value delivery, risk management and IT resource management.

b) IT Strategy Committee

The Company would form an IT Strategy Committee. An independent director would be the chairman of the committee and the Chief Technology Officer (CTO) would be a part of the committee. The IT Strategy Committee would meet at an appropriate frequency but the gap between two meetings will not be more than six months. The Committee shall work in partnership with the Risk Management Committee of the Board, other Board committees and Senior Management to provide inputs to them. It will also carry out review and amend the IT strategies in line with the corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance. The Committee's deliberations will be placed before the Board.

Roles and Responsibilities of IT Strategy Committee:

- Approving IT strategy and policy documents and Ensuring that the management has put an effective IT strategic planning process in place;
- Ascertaining that management has implemented processes and practices that ensure that the 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 provide high-level direction for sourcing and use of IT resources;
- Ensuring proper balance of IT investments for sustaining the Company's growth and becoming aware about exposure towards IT risks and controls.

For the purpose of effective implementation of this Policy, the Company would ensure technical competence at senior/middle level management of the Company. The Chief Technology Officer would also be responsible for periodic assessment of the IT training requirements to ensure the availability of sufficient, competent and capable human resources in the Company.

4. Information Security

Information and the knowledge based on it have increasingly been recognized as 'information assets', which are vital inputs of business operations. The Company believes that it is important to provide adequate levels of protection to such information assets.

This Policy is based on the following tenets:

a) Confidentiality – Ensuring access to sensitive data to authorized users only.
b) Integrity – Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.
c) Availability – Ensuring that uninterrupted data is available to users when it is needed.
d) Authenticity –Ensuring that the data, transactions, communications or documents (electronic or physical) are genuine.

The Company's Information Security Framework is based on the following key tenets:

a) Identification and Classification of Information Assets

The Company shall maintain a detailed inventory of its Information Assets with distinct and clear identification of the asset.

b) Segregation of functions

There would be segregation of the duties of the Security Officer (both physical security as well as cyber security)/ Group dealing exclusively with information systems security and the Information Technology division which actually implements the computer systems. The information security function would be adequately resourced in terms of the number of staffs, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there would be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

c) Limiting physical access

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 further obtained adequate insurance to safeguard such data.

The Company would put in place adequate controls to limit physical access (i.e. access to the office, meeting rooms and physical IT assets).

d) Limiting logical access

Persons or entities with access to the Company's electronic information and information systems are accountable for all activities associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the Company. Personnel with privileged access like system administrators, cyber security personnel, etc. would be subject to rigorous background check and screening.

The Company would also put in place controls to limit logical access (i.e. access to computer networks, system files and data). These would be done by a process that enables authenticating and authorizing users who are permitted to use the said network and data.

- 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 a two-factor authentication, where possible
- System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

e) Well-defined password policy

A well-defined password policy would be implemented to ensure that confidentiality of data is maintained. All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters and standards laid down in this Policy. Passwords must not be shared with or made available to anyone in any manner that is not consistent with the Policy.

f) Role based Access Control

Access to information would be based on well-defined user roles (system administrator, user manager, application owner etc.) The Company would, as far as possible, avoid dependence on one or few persons for a particular job. There would be clear delegation of authority for right to upgrade / change user profiles and permissions and also key business parameters (e.g. Interest rates), which would be documented.

The Company would ensure that access to sensitive information and data is available to authorized users only.

g) Integrity of data

The Company would maintain accuracy and reliability of information by ensuring that there is no modification without authorization. The Company would ensure that the data, transactions, communications or documents (electronic or physical) generated are authentic and genuine.

h) Availability

It would also be ensured that uninterrupted data is available to users when it is needed.

i) Maker- checker concept

The Company would follow a Maker-Checker concept. For each transaction, there would be at least two individuals for its completion. This would help minimize the risk of error and would ensure reliability of information. The Company would ensure that it complies with this requirement to carry out all its business operations.

j) Incident Management

Incident management is the process of developing and maintaining the capability to manage incidents within the Company so that the risk is contained and proactive control measures are taken within a specified time. The Company would develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

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 CTO. These incidents/ violations of security policies would be reported to the Board/RMCB. If these breaches related to digital information, the same would be reported to the IT Strategy Committee as well. Wherever appropriate, required communication would be sent to customers.

k) Audit Trails

The Company would ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity would be recorded in the audit trail.

l) Public Key Infrastructure (PKI)

The Company would strive to increase the usage of PKI 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 would adopt an appropriate approach to combat cyber threats, given the level of complexity of business and acceptable levels of risk. The Company would review organizational arrangements so that security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick response and suitable action.

Vulnerability management is an integral part of Cyber Security. Vulnerability would mean an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by any person to gather sensitive information about the functioning of the organization. The company would devise appropriate strategies for managing and eliminating vulnerabilities.

a) Cyber security preparedness indicators

The adequacy of and adherence to cyber resilience framework would be assessed and measured through development of indicators to assess the level of risk/preparedness. These indicators would be used for comprehensive testing through independent compliance checks and audits carried out by qualified and competent professionals. The awareness among the stakeholders including employees may also form a part of this assessment.

b) Cyber Crisis Management Plan

As part of the Board approved strategy, the Company would put in place a Cyber Crisis Management Plan (CCMP). The CCMP would need to be approved by the IT Strategy Committee. It would address the following four aspects:

- (i) Detection
- (ii) Response
- (iii) Recovery and
- (iv) Containment.

The Company would take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the adverse effects.

The Company would strive to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks. The Company would 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), ransom-ware / crypto ware, 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) Sharing of information on cyber-security incidents with RBI

The Company would report all types of unusual cyber security incidents, as prescribed by RBI.

d) Awareness among stakeholders / Top Management / Board

The Company would strive to create awareness about cyber security among its stakeholders, top management and the Board of Directors. Its stakeholders would include the Board of Directors, Risk Committees, the Chief Technology Officer. Head Technology/ Head IT and business executives.

The Company would proactively promote, among their customers, vendors, service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronised implementation and testing.

6. Mobile Financial Services

a) Mobile Applications

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

b) Privacy Policy:

As personal information would be collected from the borrowers, the Company would have a comprehensive and compliant privacy policy available publicly. Details of any third parties, that are allowed to collect personal information via the lending app, would also be disclosed. Privacy practices of the Company would be disclosed on the app at every stage, i.e., before requesting user permission to use personal data, during account sign up or login page, payment page, etc.

c) Cloud Infrastructure:

The Company would make sure that cloud vendors comply with commensurate regulatory standards. The app would have specific technological safeguards to prevent frauds.

In case the Company engages digital lending platforms as its agents, the applicable directions of RBI in this regard will be adhered to.

7. Social Media

Whenever the Company uses social media to market its products, proper controls such as encryption and secure connections would be put in place to mitigate risks.

8. IT Risk Assessment

The Company would undertake a comprehensive risk assessment of its IT systems on a yearly basis. The assessment would make an analysis on the threats and vulnerabilities to the information technology assets of the Company and its existing security controls and processes. The outcome of the exercise would 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 Technology Officer/ Head (IT), the Chief Risk Officer and the Board/ RMCB of the Company and would serve as an input for Information Security auditors.

9. Training

The Company would develop an information security awareness programme. The programme would be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information security framework. There would be a mechanism to track the effectiveness of training programmes through an assessment / testing process. The Company would maintain an updated status on user training and awareness relating to information security.

10. IT Operations

The Company would aim to put in place IT systems which would 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

While developing or acquiring a new system, the Company would identify system deficiencies and defects at the system design, development and testing phases. The Company would establish a steering committee, consisting of business owners and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

b) Change Management Policy

The Company would realign its IT systems on a regular basis in line with the changing needs of its customers and business. The changes would be carried out in such a way that adverse incidents and disruption to services are minimized while maximizing value for the customers. For this purpose, the Company would develop, with the approval of their Board, a Change Management Policy that encompasses the following:

a) prioritizing and responding to change proposals from business,
b) cost benefit analysis of the changes proposed,
c) assessing risks associated with the changes proposed,
d) change implementation, monitoring and reporting.

It would be the responsibility of the senior management to ensure that the Change Management Policy is being followed on an on-going basis.

11. IT Enabled Management Information System

The IT function of the Company would support a robust and comprehensive Management Information System (MIS) in respect of various business functions. It would take care of information needs at all levels in the business. The Company would put in place an MIS that would assist the top management in decision making and also to maintain an oversight over operations of various business verticals. The MIS would facilitate pricing of products, especially large ticket loans.

The following information would be part of the system:

- A dashboard for the 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 etc.
- 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. (also 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.
- Capacity and performance analysis of IT security systems
- Incident reporting, their impact and steps taken for non-recurrence of such events in the future.

The Company's IT system would capture regulatory requirements and compliance thereof enabling the Company to file the required regulatory returns with RBI. All regulatory/ supervisory returns would be system driven, so that there is a seamless integration between the MIS of the Company and reporting to RBI under COSMOS. Further, it would be ensured that "Read Only" access would be provided to RBI Inspectors.

12. Policy for Information System Audit (IS Audit)

The Company would put in place an Information System Audit process. The objective of the IS Audit would be to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the Company's IT infrastructure. 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. IS Audit would form an integral part of Internal Audit system of the Company.

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

The broad framework of the IS Audit, as stated below, has been approved by the Board. While designing the detailed scope, the Company would refer to guidance issued by Professional bodies like ISACA, IIA, ICAI in this regard.

a) Broad framework of IS Audit

The IS Audit should evaluate the following aspects:

- Effectiveness of policy and oversight of IT systems,
- Adequacy of processes and internal controls,
- Effectiveness of business continuity planning, disaster recovery set up
- Compliance with all legal and statutory requirements.

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

The Audit Committee of the Board, along with the IT strategy committee, would outline the responsibilities for compliance/sustenance of compliance, reporting lines, timelines for submission of compliance, authority for accepting compliance in the IS Audit framework. The Audit Committee of the Board would ensure that appropriate action is taken in response to reported observations and recommendations during the IS Audit.

Audit-mode access would be provided for auditors/ inspecting/ regulatory authorities.

b) IS Audit Team

The IS Audit would be conducted by an internal team of the Company. In case of inadequate internal skills, the Company may appoint an outside agency having enough expertise in area of IT/IS audit for the purpose. It would 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 should act independently of the Company' Management both in attitude and appearance. In case of engagement of external professional service providers, the Company would ensure that independence and accountability issues are properly addressed.

c) Computer-Assisted Audit Techniques (CAATs)

The Company would adopt a proper mix of manual techniques and CAATs for conducting IS Audit. CAATs would 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 would be conducted once in a year. IS Audit would 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

The IS audit report would be submitted to the Audit Committee of the Board.

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 would put in place a BCP Policy, duly approved by the Board. The BCP would be designed to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster.

The Company would 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 would consider the need to put in place necessary back-up sites for its critical business systems and data centres.

The Board of Directors shall be responsible for formulation, review and monitoring of BCP to ensure continued effectiveness.

The BCP would have the following salient features:

a) Business Impact Analysis

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

b) Recovery strategy/ Contingency Plan

The Company would try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP would come up with the probabilities of various failure scenarios. Evaluation of various options would be done for recovery and the most cost-effective, practical strategy would be selected to minimize losses in case of a disaster.

The Company shall test the BCP either 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 should be based on 'worst case scenarios'. The results along with the gap analysis would be placed before the Board/ RMCB. The GAP Analysis along with Board's insight would form the basis for construction of the updated BCP.

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 would be done. The Company's decision to outsource IT Services would be within its overall strategic plan and corporate objectives.

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

The Board and senior management would be ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. The Board of Directors of Company is responsible for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions. The Board and IT Strategy committee have the responsibility to institute an effective governance mechanism and risk management process for all IT outsourced operations.

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

15. REVIEW:

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

If at any point a conflict of interpretation / information between this policy and any regulations, rules, guidelines, notification, clarifications, circulars, master circulars/ 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.