CHARTERED FINANCE & LEASING LTD. (CFL)

("NBFC / B-13.02480")

Information and Cyber Security Policy

Version: V2 | Review Cycle: Annual
Approved by: Board of Directors
Date of Approval: 07th April,2026

SUMMARY OF POLICY

Particular	Details
Policy Name	Information and Cyber Security Policy
Version	V2
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	11th July, 2025	2025	RBI Regulation (DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017)	Policy adopted by Board
II	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 by Board

Information and Cyber Security Policy

1. Purpose

This Policy is framed to establish a simple and proportionate information and cyber security framework for the Company in line with applicable RBI Master Directions and guidelines relevant to NBFCs, including Master Direction DNBS.PPD.No.04/66.15.001/2016-17 dated June 08, 2017 on Information Technology Framework for the NBFC Sector, as rationalised and consolidated under the November 2025 RBI Master Directions consolidation. The focus of this IT framework is on IT Governance, IT Policy, Information & Cyber Security.

Considering the Company's limited scale of operations, low transaction volume and small staff strength, the controls under this Policy shall be practical, documented and commensurate with the nature of the business, while ensuring that the Company is not exposed to avoidable regulatory or operational risk.

2. Policy Statement

Chartered Finance & Leasing Limited ("CFL" / "the Company") shall take all necessary steps to protect information assets and information infrastructure, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation from relevant external bodies both private, public and the Government.

The objective of this Policy is to proactively identify the cyber threats and the risks manifested in information infrastructure and manage, mitigate, avoid, divert, transfer or accept the risks as per the risk appetite of the organisation.

3. Scope

This Policy applies to all systems, applications, devices, records, data, networks, outsourced technology environments and users authorised to access Company information or systems, including all data collected, processed and stored by CFL during its business operations, including co-lending activities. It extends to all trainees, employees, Board Members, Observers, Advisors, Consultants, Auditors, contractors, partners, customers and any other person who either inadvertently or in the course of its dealings with the Company obtains or collects any restricted personal data from the database of the Company. They shall collectively be termed as "Users" under this policy.

4. Information Security (IS)

Information is an asset to the Company and Information Security (IS) refers to the protection of these assets in order to achieve organisational goals. The purpose of IS is to control access to sensitive information, ensuring the access and use only by legitimate Users so that data cannot be used or compromised without proper authorisation. The Company shall ensure confidentiality, integrity, availability and authenticity of data managed by it.

The Company shall maintain reasonable information security controls suited to its scale and operations.

5. Key Components of IS Policy

5.1 Identification and Classification of Information Assets

The Company shall maintain a simple list / inventory of all information assets with clear identification, covering important systems, applications, devices and information assets.

5.2 Segregation of Functions

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 shall be segregated. The

Company shall ensure adequate staffing, skills, and tools for the information security function and clearly segregate responsibilities for system administration, database administration, and transaction processing.

Where full segregation is not practical due to small staff strength, compensating controls such as supervisory review, maker-checker or approval by senior management shall be applied.

5.3 Role-Based Access Control

Access to information should be based on well-defined user roles (system administrator, user manager, application owner, etc.). The Company shall 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. Privileged access shall be limited to authorised persons only.

5.4 Personnel Security

CFL shall implement checks and balances for authorised application owners / users who have extensive knowledge of financial institution processes and conduct rigorous background checks and screenings for personnel with privileged access (e.g., system administrators, cybersecurity personnel). Appropriate access approval and access removal on exit shall be followed for employees and other authorised users.

5.5 Physical Security

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. The Company shall create a secured environment for physical security of IS Assets such as secure location of critical data, restricted access to sensitive areas like the data centre, etc. Physical access to important systems, devices, records and backups shall be restricted.

5.6 Maker-Checker Principle

CFL shall implement a system where at least two individuals are required to complete each critical transaction to reduce errors and ensure information reliability. Maker-checker / approval controls shall be followed for important transactions and critical system changes, to the extent feasible.

5.7 Incident Management

The IS Policy defines what constitutes an incident. The Company shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents. The Company shall maintain a simple process for identifying, reporting and resolving information security incidents.

5.8 Audit Trails

The Company shall 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. Audit trails / logs available in the Company's systems shall be preserved, as relevant, for audit and review. If an employee, for instance, attempts to access an unauthorised section, this improper activity should be recorded in the audit trail.

5.9 Public Key Infrastructure (PKI)

CFL may use Digital Signature Certificate / PKI-based controls to ensure data confidentiality, access control, data integrity, authentication, and non-repudiation, wherever required for banking, statutory, regulatory and contractual purposes.

5.10 Cyber Security

The Company shall maintain basic cyber security controls such as antivirus / endpoint protection, password controls, user access controls, backup, system update / patching and incident reporting. The cyber security policy outlines strategies to combat cyber threats

based on the complexity of business and acceptable risk levels. This policy shall be reviewed regularly to ensure security concerns are addressed promptly.

6. Components of the Cyber Security Policy

6.1 Vulnerability Management

A vulnerability can be defined as an inherent configuration flaw in an organisation's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organisation. Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk and cost associated with the vulnerabilities.

The Company shall keep systems and software reasonably updated and shall address material vulnerabilities noticed by management, auditors or vendors.

6.2 Cyber Security Preparedness Indicators

The Company shall develop indicators to measure cyber resilience and conduct regular compliance checks and audits. It shall be ensured that stakeholders, including employees, are aware of these indicators. The Company may monitor a few basic indicators such as incident occurrence, antivirus status, backup status and pending user access changes.

6.3 Cyber Crisis Management Plan (CCMP)

CCMP shall address the following four aspects:

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

The Company shall take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover / contain the fallout. The Company shall be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

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.

6.4 Threat Preparedness

The Company shall be mindful of common cyber threats such as phishing, malware, ransomware, password compromise, unauthorised access and data leakage and shall maintain a simple Cyber Crisis / response plan covering detection, reporting, containment, recovery and escalation.

7. Sharing of Information on Cyber-Security Incidents with RBI

The Company is required to report all types of unusual security incidents as specified in applicable RBI Master Directions, including both successful and attempted incidents. RBI's latest template for reporting will be used. The Company shall report cyber incidents / unusual security incidents to RBI or other authority wherever specifically required under applicable regulatory instructions.

8. Cyber-Security Awareness among Stakeholders / Top Management / Board

Managing cyber risk requires the commitment of the entire organisation to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board shall also have a fair degree of awareness of the fine nuances of the threats and appropriate familiarisation may be organised.

The Company shall create basic awareness among employees regarding safe use of systems, passwords, phishing and incident reporting. Material incidents shall be reported to management / Board. The Company shall proactively promote, among its clients, vendors, lenders and other service providers and relevant stakeholders, an understanding of their cyber resilience objectives and require appropriate action to support their synchronised implementation and testing.

9. Digital Signatures

CFL has procured Digital Signature Certificates (DSC) for its authorised persons. DSCs are intended to be used for Corporate Banking, and other governmental websites like MCA, Income Tax, DGFT website authentication, PF, GST, NeSL and other regulatory websites and legal documentation of the company. The Company shall ensure authorised use and safe custody of DSCs.

10. IT Risk Assessment

The Company must undertake a comprehensive risk assessment of its IT systems at least on a yearly basis. The assessment shall make an analysis of the threats and vulnerabilities to the information technology assets of the Company and its existing security controls and processes. The outcome of the exercise should 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 Chief Risk Officer (CRO) and the Board / Risk Management Committee, and shall serve as an input for Information Security auditors.

11. Requirements with regard to Mobile Computing Policy

The mobile computing policy applies to all employees and staff provided with a company laptop or portable electronic device. It is the employee's responsibility to take proper care of the laptop computer / PED (Portable Electronic Device), data and accompanying software while using the same. Laptops, portable devices and remote access used for official purposes shall be handled securely by users. Loss, theft or compromise shall be reported immediately.

12. Social Media Risks

Employees shall not disclose confidential information, customer information or sensitive internal information on social media or public channels without approval. The following guidelines shall be adhered to:

- ✓ Usage of Social Media and restricted sites within CFL network is prohibited, unless approved specifically.
- ✓ Employees are personally responsible for the content they publish online, whether in a blog, social computing site or any other form of user-generated media.

  Employees are not authorised to publish or discuss the following on Social Media:

  - ✓ CFL's confidential or other proprietary information;
  - ✓ To cite or reference Customers, partners or suppliers without their approval;
  - ✓ Any unpublished confidential or price sensitive information pertaining to Customers, clients, partners or suppliers without their written approval;
  - ✓ To use CFL's logos or trademarks unless approved to do so;
  - ✓ Anything libellous and slanderous against any person / entity, in official capacity;
  - ✓ Any hate speech / statement against any entity, person, caste, creed, religion or belief and nationality.

13. IT Enabled Management Information System

CFL shall put in place MIS that assists the Top Management as well as the business heads in decision making and also to maintain oversight over operations of various business verticals and

supervisory requirements. With robust IT systems in place, CFL may have, inter alia, the following as part of an effective system-generated MIS:

13.1

A dashboard for Top Management summarising financial position vis-à-vis targets. It may include information on trend on returns on assets across categories, major growth business segments, movement of net-worth, regulatory and statutory compliances, various trackers and e-tools for generating various reports.

13.2

System-enabled identification and classification of Special Mention Accounts and NPAs as well as generation of MIS reports in this regard.

13.3

The MIS should facilitate pricing of products, especially large ticket loans.

13.4

The MIS should capture regulatory requirements and their compliance.

13.5

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).

13.6

Reports relating to treasury operations.

13.7

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 should be system driven.

13.8

Capacity and performance analysis of IT security systems.

13.9

Incident reporting, their impact and steps taken for non-recurrence of such events in the future.

14. IS Audit

14.1 Policy for Information System Audit (IS Audit)

The objective of the IS Audit is to provide insight into the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organisation's IT infrastructure. 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.

14.2 Coverage

The IS Audit shall cover the effectiveness of policy and oversight of IT systems, evaluating the adequacy of processes and internal controls, and recommend corrective action to address deficiencies and follow-up. IS Audit shall also evaluate the effectiveness of business continuity planning, disaster recovery setup and ensure that BCP is effectively implemented in the organisation. During the process of IS Audit, due importance shall be given to compliance with all applicable legal and statutory requirements. IS Audit may cover access management, backup, antivirus / endpoint controls, system controls, vendor dependency, business continuity and compliance with the Policy.

14.3 Personnel

CFL can conduct IS Audits using internal teams or engage external agencies with IT / IS audit expertise when internal skills are insufficient. Auditors need a balanced mix of technical skills and understanding of legal and regulatory standards. Independence from NBFC management is crucial for both internal and external auditors to ensure impartial assessments.

14.4 Periodicity

The frequency of IS Audits shall ideally align with the size and operations of the NBFC, typically conducted at least annually. Conducting the IS Audit before the statutory audit allows auditors to incorporate IS Audit findings into their reports promptly.

14.5 Reporting

The framework shall clearly prescribe the reporting framework, whether to the Board or a Committee of the Board viz. Audit Committee of the Board (ACB). Findings shall be reported to the Audit Committee / Board / relevant Committee, as applicable, and compliance shall be followed up.

15. Compliance

The management of the Company is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations during the IS Audit. Responsibilities for compliance / sustenance of compliance, reporting lines, timelines for submission of compliance, and authority for accepting compliance shall be delineated in the framework.

Computer-Assisted Audit Techniques (CAATs): CFL shall adopt a proper mix of manual techniques and CAATs for conducting IS audits. CAATs may be used in critical areas (such as detection of revenue leakage, treasury functions, assessing the 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.

16. Grievance Redressal

CFL is committed to addressing grievances in a timely and efficient manner. The Company remains responsible for handling customer grievances, including grievances relating to technology-enabled services. For queries or concerns, you can write to the grievance redressal email id available on our official website: https://charteredfinanceleasing.com/ and the team will respond accordingly. The responsibilities of Data Protection are carried out by the Head of Information Security.

17. Amendments

This Policy may be amended with the approval of the Board, as and when required. CFL reserves the right to amend this policy at any time. The revised policy will be made available on our official website and communicated to data subjects where applicable.

If at any point a conflict of interpretation/information between this policy and any regulations, rules, guidelines, notifications, clarifications, circulars, or Master Directions issued by relevant authorities ("Regulatory Provisions") arises, then the 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.