

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	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	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 the Reserve Bank of India (Non-Banking Financial Companies – Cybersecurity, Technology: Risk, Resilience and Assurance Framework) Directions, 2026, as amended from time to time. The focus of this IT framework is on IT Governance, IT Policy, Information & Cyber Security.

The Company, being an NBFC in the Middle Layer, shall comply with Chapters I, II and V of the said Directions, and this Policy constitutes the Company's Information Security Policy and Cybersecurity Policy referred to therein.

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. 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.

This Policy is owned by the Chief Information Security Officer (CISO), who shall be responsible for its maintenance, for monitoring its implementation and for initiating its periodic review. The information security organisational structure shall comprise the Board, the ITSC, the Information Security Committee and the CISO. Exceptions to this Policy shall be approved by the Information Security Committee on the recommendation of the CISO; every exception shall be recorded with the reasons, the compensating controls and the period of validity, shall be time-bound, and shall be reviewed on or before its expiry. Compliance with this Policy shall be reviewed at least annually, and non-compliance shall attract appropriate disciplinary action.

A senior level executive shall be designated as the Chief Information Security Officer with the requisite technical background, appointed for a reasonable minimum term, without any direct reporting relationship with the Head of IT Function and without business targets. The CISO shall drive cybersecurity strategy, enforce information security policies, manage and monitor the Security

Operations Centre, be a permanent invitee to the ITSC and IT Steering Committee, directly report to the Executive Director or equivalent executive overseeing the risk management function, and place a review of cybersecurity risks / arrangements / preparedness before the Board / RMCB / ITSC at least quarterly. An Information Security Committee under the oversight of the ITSC, headed by an official from the risk management vertical, shall develop and implement information security / cybersecurity policies, approve and monitor security projects and awareness initiatives, and review cyber incidents and IS audit observations.

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.

The Company shall identify and map the security classification (in terms of confidentiality, integrity and availability) of information assets based on their criticality to its operations.

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.

Areas of possible role conflicts and accountability gaps shall be specifically identified and eliminated or managed, and IT operations shall be managed through a Service Level Management process ensuring effective segregation of duties.

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.

The Company shall put in place appropriate physical and environmental controls for securing critical assets including DC and DR sites from natural and man-made threats; DC and DR sites shall be geographically well separated and subjected to e-surveillance.

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's cyber incident response and recovery management framework shall address classification and assessment of incidents, a clear communication strategy and plan, and measures to contain exposures and achieve timely recovery. The Company shall analyse incidents for severity, impact and root cause; shall maintain written incident response and recovery procedures identifying key roles of staff / outsourced staff; and shall conduct periodic drills / testing of the crisis communication plan with stakeholders including service providers.

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.

Every IT application / system that can access or affect critical or sensitive information shall have audit logging capabilities, and the Company shall regularly monitor audit trails and system logs to detect, understand or recover from any unauthorised activity or attack.

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.

The key length, algorithms, cipher suites and protocols used in transmission channels, processing of data and authentication shall be strong, adopting internationally accepted and published standards that are not deprecated or demonstrated to be insecure.

The Company shall ensure that software vendors provide maintenance and necessary support of software applications and shall enforce the same through formal agreements. The Company shall obtain the source codes for all critical applications from its vendors. Where obtaining of the source code is not possible, the Company shall put in place a source code escrow arrangement or other arrangements to adequately mitigate the risk of default by the vendor. The Company shall ensure that all product updates and programme fixes are included in the source code escrow arrangement.

The Company shall obtain a certificate or a written confirmation from the application developer or vendor stating that the application is free of known vulnerabilities, malware, and any covert channels in the code. The Company shall also obtain such a certificate or a written confirmation whenever material changes to the code, including upgrades, occur. The definition

of material changes can be mutually agreed upon between the Company and its vendor. 'Material Changes' refer to significant modifications to the software code that could impact the application's functionality, security, or performance. This, however, excludes routine maintenance activities such as minor bug fixes, performance optimisations, and updates that do not alter the application's core functions, security posture, or compliance status. It is essential to conduct a risk assessment when determining whether a change is material.

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 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 DMZ having customer interface, and throughout their lifecycle, through appropriately trained and independent experts; adopt a risk-based approach for non-critical systems; fix identified vulnerabilities in a time-bound manner; and maintain documented change and patch management procedures.

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.

6.5 Business Continuity and Disaster Recovery

In addition to the business continuity planning and disaster recovery provisions in section 13 of the Company's IT / IS Policy, the Company's BCP and DR arrangements shall adopt best practices (e.g., ISO 22301) to guide its actions in reducing the likelihood or impact of disruptive incidents and maintaining business continuity and shall be updated based on major developments and risk assessments. The Company's BCP and DR capabilities shall be designed to effectively support resilience objectives and enable rapid recovery and secure resumption of critical operations including key cybersecurity controls post cyber-attacks / other incidents aligned with recovery time objectives while ensuring the security of processes and data.

Any major issues observed during the DR drill shall be resolved and tested again to ensure successful conduct of drill before the next cycle. The DR testing shall involve switching over to the DR / alternate site and thus using it as the primary site for sufficiently long period where usual business operations of at least a full working day (including Beginning of Day to End of Day operations) are covered. The Company shall regularly test the BCP / DR, at least on a half-yearly basis for critical information systems and as per the Company's risk assessment for other information systems, under different scenarios for possible types of contingencies, to ensure that it is up-to-date and effective.

The integrity of backed-up data shall be preserved along with securing it from unauthorised access. The Company shall ensure that DR architecture and procedures are robust, meeting the defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for any recovery operations in case of contingency. In a scenario of non-zero RPO, the Company shall have a documented methodology for reconciliation of data while resuming operations from the alternate location.

The Company shall ensure BCP and DR capabilities on critical interconnected systems and networks including those of vendors and partners. The Company shall ensure demonstrated readiness through collaborative and co-ordinated resilience testing that meets the Company's RTO.

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

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.

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.

IT related risks, including cybersecurity risks, shall form part of the Company's risk management policy, which the Risk Management Committee of the Board, in consultation with the ITSC, shall review and update at least annually; the security infrastructure and security policies shall be reviewed at least annually.

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.

In the teleworking environment, the Company shall ensure that systems used and remote access are secure, implement multi-factor authentication for enterprise (logical) access to critical systems, put in place a mechanism to identify all remote-access devices connected to its systems, and ensure that data shared in teleworking is secured.

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 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.

The Audit Committee of the Board shall exercise 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 with required skills within the Internal Audit function and shall plan IS Audit using a risk-based approach.

14.2 Coverage

The IS Audit shall cover the effectiveness of policy and oversight of IT systems, evaluate 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

IS Audit shall be conducted at the periodicity approved by the Audit Committee of the Board under this section, and in any case at least once a year. 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.