CHARTERED FINANCE & LEASING LTD. (CFL)

(“NBFC/ B-13.02480”)

SUMMARY OF POLICY

Particular	Details
Policy Name	Information and Cyber Security Policy
Version	V1
Latest Approval/Review Date	11th July, 2025
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	Policy Adopted by Board

Information and Cyber Security Policy

1. Purpose

This Policy is framed in compliance to Master Direction DNBS.PPD.No.04/66.15.001/2016-17 of RBI dated June 08, 2017 on Information Technology Framework for the NBFC Sector, that are expected to enhance safety, security, efficiency in processes leading to benefits for NBFCs and their customers. The focus of this IT framework is on IT Governance, IT Policy, Information & Cyber Security.

2. Policy Statement

Chartered Finance & Leasing Limited ("CFL/ the Company") shall take all necessary steps to protect information and information infrastructure in internet/cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize 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 organization.

3. Scope

This policy applies to all data collected, processed and stored by CFL during its business operations, including colending activities, and extends to its all trainees, employees, employers, 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 collect any restricted personal data from the database of the Company . They shall be 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 organizational 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 authorization. The Company shall ensure confidentiality, integrity, availability and authenticity of data managed by it.

5. Key Components of IS Policy:

1.1. **Identification and Classification of Information Assets:** Maintain a detailed inventory of all information assets with clear identification.

1.2. **Segregation of Functions:** Separate the duties of the Security Officer/Group (responsible for information systems security) from the Information Technology division (responsible for implementing computer systems). 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.

1.3. **Role-Based Access Control:** Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), NBFCs shall avoid dependence on one or few persons for a particular job. There should be clear delegation of authority for right to upgrade/change user profiles and permissions and also key business parameters (eg. interest rates) which should be documented.

1.4. **Personnel Security :** CFL shall implement checks and balances for authorized 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).

1.5. **Physical Security:** The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. The Company needs to create a secured environment for physical security of IS Assets such as secure location of critical data, restricted access to sensitive areas like data center etc.

1.6. **Maker-Checker Principle:** CFL shall implement a system where at least two individuals are required to complete each transaction to reduce errors and ensure information reliability.

1.7. **Incident Management:** The IS Policy should define what constitutes an incident. The Company shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.

1.8. **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. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.

1.9. **Public Key Infrastructure (PKI):** CFL may increase the usage of PKI to ensure data confidentiality, access control, data integrity, authentication, and non-repudiation.

1.10. **Cyber Security:** The cyber security policy outlines strategies to combat cyber threats based on the complexity of their business and acceptable risk levels. This policy should be reviewed regularly to ensure security concerns are addressed promptly and must be approved by the board and clearly define the approach to managing cyber threats.

6. Components of the Cyber Security Policy

1.11. **Vulnerability Management:** A vulnerability can be defined as an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization. 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.

1.12. **Cyber Security Preparedness Indicators:** Company shall develop indicators to measure cyber resilience and conduct regular compliance checks and audits. It should be ensured that stakeholders, including employees, are aware of these indicators.

1.13. **Cyber Crisis Management Plan (CCMP):** CCMP should address four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment.

1.13.1. Company need to take effective measures to prevent cyber-attacks and to promptly detect any cyberintrusions so as to respond / recover / contain the fall out and must be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

Among other things, CFL 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), ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, driveby downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

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 Annex I of the Master Directions including both successful and attempted incidents. RBI's latest template for reporting will be used.

8. Cyber-security awareness among stakeholders / Top Management / Board

It should be realized that managing cyber risk requires the commitment of the entire organization to create a cyber-safe environment. This will require a high level of awareness among staff at all levels. Top Management and Board should also have a fair degree of awareness of the fine nuances of the threats and appropriate

familiarization may be organized. The Company should proactively promote, among their Clients, vendors, Lenders and other service providers and other relevant stakeholders an understanding of their cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing.

9. Digital Signatures

CFL has procured Digital Signature Certificates (DSC) for its Authorised persons/ and is 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.

10. IT Risk Assessment

Company must undertake a comprehensive risk assessment of their IT systems at least on a yearly basis. The assessment should make an analysis on the threats and vulnerabilities to the information technology assets of the NBFC 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 appropriate mitigation of risks. The risk assessment should be brought to the notice of the Chief Risk Officer (CRO), and the Board and should serve as an input for Information Security auditors.

11. Requirements with regards 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.

12. Social Media Risks

12.1. Usage of Social Media and restricted sites within CFL network is prohibited, unless approved specifically.

12.2. Employees are personally responsible for the content they publish on- line, whether in a blog, social computing site or any other form of user- generated media.

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

12.3.1. CFL's confidential or other proprietary information

12.3.2. To cite or reference Customers, partners or suppliers without their approval

12.3.3. Any Unpublished Confidential or Price Sensitive Information pertaining to Customers, Clients, partners or suppliers without their written approval

12.3.4. To use CFL's logos or trademarks unless approved to do so.

12.3.5. Anything libelous and slanderous against any person/ entity, in official capacity

12.3.6. 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 assist the Top Management as well as the business heads in decision making and also to maintain an 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 the 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 NPA 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 an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization'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: IS Audit should cover effectiveness of policy and oversight of IT systems, evaluating adequacy of processes and internal controls, recommend corrective action to address deficiencies and follow-up. IS Audit should also evaluate the effectiveness of business continuity planning, disaster recovery set up and ensure that BCP is effectively implemented in the organization. During the process of IS Audit, due importance shall be given to compliance of all the applicable legal and statutory requirements.

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 should 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 should clearly prescribe the reporting framework, whether to the Board or a

Committee of the Board viz. Audit Committee of the Board (ACB)

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 should 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. For queries or concerns, you can write to grievance redressal email id available on our website https://charteredfinanceleasing.com/ and the team will respond to the same. The responsibilities of DPO are carried out by the head of Information Security.

17. Amendments

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.