CHARTERED FINANCE & LEASING LIMITED

IT POLICY

CHARTERED FINANCE & LEASING LIMITED

IT POLICY

POLICY VERSION CONTROL:

VERSION NO.	APPROVED BY BOARD ON	REMARKS
1.0	07-Apr-2022	Policy adopted by the Board

IT POLICY

1. Introduction

- **Objective**: This section outlines the purpose of the IT policy, including ensuring compliance with RBI guidelines, ensuring the security of financial transactions, and supporting business continuity.
- **Scope**: Covers all IT systems, software, hardware, networks, and personnel within the organization.

2. Governance Structure

- **IT Governance**: Define roles and responsibilities of the IT governance framework, including the IT steering committee, Chief Information Security Officer (CISO), and other key stakeholders.
- **Board and Senior Management**: The policy should stress that the Board of Directors and senior management must actively oversee and implement the IT governance framework.

3. IT Security Policy

- **Data Protection**: Ensure the security of financial data, sensitive customer information, and personal data as per regulatory requirements like **Data Privacy Laws** (e.g., **GDPR**, **IT Act 2000**, **RBI Cyber Security Framework**).
- **Encryption Standards**: Specify encryption standards for data at rest and in transit.
- **Access Control**: Define access control mechanisms to ensure only authorized personnel can access sensitive systems and data. This includes Multi-factor Authentication (MFA) and Role-Based Access Control (RBAC).
- **Authentication**: Ensure strong authentication methods for all users accessing critical systems.

4. Risk Management

- **Cybersecurity Risk Assessment**: Conduct periodic assessments to identify vulnerabilities and mitigate risks associated with IT systems.
- **Incident Response**: Define a response plan for IT security incidents, including data breaches or cyber-attacks. It should outline how the organization identifies, mitigates, and reports incidents.
- **Third-Party Risk Management**: Ensure that third-party service providers (outsourcing vendors, cloud services, etc.) comply with the NBFC's security requirements and undergo regular risk assessments.

5. Business Continuity & Disaster Recovery (BCDR)

- **Backup and Restoration**: Regular backups of all financial data, software, and critical systems to ensure they can be restored quickly in case of a disaster.
- **Business Continuity Plan**: Define the procedures for ensuring that essential financial services can continue in the event of a disaster (e.g., server failure, network disruption).
- **Disaster Recovery Plan**: The IT policy should detail the steps and timelines for recovering from disasters affecting IT systems.

6. Data Privacy & Confidentiality

- **Data Classification**: Define data classification based on sensitivity (e.g., confidential, internal use, public), and how each class of data should be protected.
- **Compliance with RBI and Other Regulations**: Ensure the IT policy aligns with the RBI's requirements on data privacy and confidentiality, including **the RBI Cyber Security Framework** and **Data Localization Requirements**.

7. IT Infrastructure Management

- **Software & Hardware Management**: Define the management process for procuring, installing, and maintaining IT infrastructure (hardware and software) to ensure they meet business and regulatory needs.
- **Patch Management**: Implement a strategy for regular updates and patching of software to protect against security vulnerabilities.
- **Network Security**: Ensure firewalls, intrusion detection/prevention systems (IDS/IPS), and secure communication protocols are in place.

8. Compliance with RBI Cybersecurity Framework

- **Cybersecurity Framework**: Align the IT policy with the **RBI Cyber Security Framework for NBFCs**, which includes guidelines on IT security governance, the protection of critical systems, and compliance monitoring.
- **Audit and Reporting**: Conduct regular internal and external audits of IT systems and practices to ensure compliance with RBI guidelines and to identify areas for improvement.

9. Audit and Compliance Mechanism

- **Internal Audits**: Establish processes for periodic internal audits of IT systems, networks, and cybersecurity measures to ensure compliance with both RBI regulations and internal policies.
- **External Audits**: Engage third-party auditors to assess compliance with regulatory guidelines and identify potential gaps.
- **Reporting**: Ensure timely reporting to the RBI and other relevant authorities about compliance status and any significant IT incidents.

10. Employee Training and Awareness

- **Training Programs**: Regular training and awareness programs on IT security, data privacy, and compliance requirements for all employees.

- **Employee Access Controls**: Define roles and responsibilities, access levels, and training requirements for employees handling financial data or critical systems.

11. Software Usage and Licensing Compliance

- Ensure that all software used by the NBFC is properly licensed and that it complies with legal standards, including software audits.

12. Incident Management & Reporting

- Define a structured incident management process, which includes detection, containment, resolution, and reporting of any cybersecurity incidents.
- Specific timelines and procedures for reporting incidents to the **RBI** or other regulatory bodies should be mentioned.

13. IT Procurement and Vendor Management

- Define guidelines for selecting IT vendors and service providers based on security, reliability, and compliance with RBI standards.
- Include provisions for monitoring and managing third-party risks, especially those related to critical systems and customer data.

14. Technology Change Management

- Ensure structured change management procedures for updates, upgrades, or any technological changes that could impact the security or performance of financial systems.

15. Review and Updates of IT Policy

- Define the process for periodic reviews and updates of the IT policy to ensure it remains aligned with regulatory changes and industry best practices.