Information Security & IT Policy

Company: ART Climate Finance (India) Private Ltd

Document Title: Information Security & IT Policy

Version: 1.0

Effective Date: 7th October 2025

Approved By: Board of Directors

Recommended By: Chief Executive Officer (CEO)

---

1. Introduction

ART Climate Finance (India) Private Limited ("the Company") recognises that Information Technology (IT) is a critical enabler for delivering financial services securely and efficiently. Given the increasing reliance on digital platforms, mobile applications, and outsourced IT services, safeguarding information assets has become essential to maintain operational resilience, protect customer trust, and comply with applicable regulatory requirements.

This Information Security and IT Policy ("the Policy") has been formulated in line with the Reserve Bank of India (RBI) guidelines, including the *Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices (2023)*, the *Outsourcing of IT Services Directions (2022)*, and the *Cyber Security Framework for NBFCs*. The Policy seeks to establish a robust governance framework for managing IT resources, ensuring data confidentiality, integrity, and availability, and mitigating technology-related risks.

IT governance is an integral part of corporate governance of the Company, and effective IT governance is the responsibility of the Board of Directors ("Board") of the Company and its executive management.

2. Objective

The objectives of this Policy are to:

- Establish principles for secure management of information assets
- Ensure compliance with RBI directions, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023
- Protect customer and Company information from unauthorised access, misuse, disclosure, alteration, or destruction
- Strengthen business continuity and disaster recovery preparedness.

3. Scope

This Policy applies to all:

- Employees, officers, directors, consultants, and contractors engaged by the Company
- IT infrastructure, including networks, servers, end-user devices, cloud platforms, applications, and databases
- Data generated, processed, or stored by the Company in physical or electronic form
- Third-party IT service providers and vendors engaged by the Company

4. Information Security Framework

The Company has an information security framework with the following principles:

- Identification and classification of information assets: the Company maintains a detailed inventory of information assets with distinct and clear identification of the asset.

- Functions: The information security function is adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there is a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

- Role-based access control – Access to information is based on well-defined user roles (system administrator, user manager, application owner). The Company has a clear delegation of authority to upgrade/change user profiles and permissions, and also key business parameters.

- Personnel Security - A few authorised application owners/users may have intimate knowledge of financial institution processes, and they pose a potential threat to systems and data. The Company has a process of appropriate checks and balances to avoid any such threat to its systems and data. Personnel with privileged access, like system administrators, cybersecurity personnel, etc., are subject to rigorous background checks and screening.

- Physical Security - The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. 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 like data centres, etc. and has further obtained adequate insurance to safeguard such data.

- Maker-checker is one of the important principles of authorisation in the information systems of financial entities. It means that for each transaction, there are at least two individuals necessary for its completion, as this will reduce the risk of error and ensure the reliability of information. The Company ensures that it complies with this requirement to carry out all its business operations.

- Trails – The Company ensures 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 unauthorised section, this improper activity is recorded in the audit trail.

- Mobile Financial Services – The Company has a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used by NBFC for mobile services ensures confidentiality, integrity and authenticity and provides for end-to-end encryption.

- Social Media Risks – The Company uses social media to market their products and is well-equipped to handle social media risks and threats in order to avoid any account takeover or malware distribution. The Company further ensures proper controls, such as encryption and secure connections, to mitigate such risks.

- Digital Signatures - A Digital signature certificate authenticates an entity's identity electronically. The Company protects the authenticity and integrity of important electronic documents, and also for high-value fund transfers.

- Regulatory Returns – NBFC has adequate systems and formats to file regulatory returns to the RBI on a periodic basis. Filing of regulatory returns is managed and verified by the authorised representatives of NBFC.

5. Access Controls

- Access to the Company's electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law and the Company policies, including but not limited to requirements laid down in this policy.

- 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 for protecting the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the Company, irrespective of the medium on which the information resides.

- Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person.

- Requirements:

  a) All users must use a unique ID to access the Company's systems and applications.

  b) Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

  c) Remote access to the Company's systems and applications must use two-factor authentication where possible.

  d) System and application sessions must automatically lock after 10 (Ten) minutes of inactivity.

6. Password Policy

All users are responsible for keeping their passwords secure and confidential. The password credentials of the users must comply with the password parameters ("Complexity Requirements") and standards laid down in this IT Framework. Passwords must not be shared with or made available to anyone in any manner that is not consistent with this IT Framework.

The Complexity Requirements for setting passwords are as follows:

- A strong password must be at least 8 (Eight) characters long.

- It should not contain any of the user's personal information—specifically his/her real name, user name, or even company name.

- It must be very unique from the passwords used previously by the users.

- It should not contain any word spelt completely.

- It should contain characters from the four primary categories, i.e. uppercase letters, lowercase letters, numbers, and characters.

- To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change the password every 30 (Thirty) days.

- Passwords must not be stored in readable form in computers without access control systems or in other locations where unauthorised persons might discover them. Passwords must not be written down and left in a place where unauthorised persons might discover them.

- Immediately upon assignment of the initial password and in case of password "reset" situations, the password must be immediately changed by the user to ensure the confidentiality of all information.
- Under no circumstances shall the users use another user's account or password without proper authorisation.

- Under no circumstances should the user share his/her password(s) with other user(s), unless the said user has obtained from the concerned official the necessary approval in this regard. In cases where the password(s) are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password was shared.

7. Cyber Security

- The Company takes effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions to respond/recover/contain the fallout. Among other things, the Company takes necessary preventive and corrective measures in addressing various types of cyber threats which includes 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 and password related frauds.

- The Company realises that managing cyber risk requires the commitment of the entire organisation to create a cyber-safe environment. This requires a high level of awareness among staff at all levels. The Company ensures that the top management and the Board have a fair degree of awareness of the fine nuances of the threats. The Company shall conduct periodic training and awareness programs to sensitise employees on information security risks, phishing attempts, safe email practices, and incident reporting procedures.

- Further, it also proactively promotes, among their customers, vendors, service providers and other relevant stakeholders, an understanding of their cyber resilience objectives, and ensures appropriate action to support their synchronised implementation and testing.

8. Confidentiality

- The Company, along with preservation and protection of the security (as set out in detail above), also ensures confidentiality of customer information in the custody or possession of the service provider.

- Access to customer information by employees of the service provider to the Company is on 'need to know' basis, i.e., limited to those areas where the information is required in order to perform the outsourced function.

- The Company further ensures that the service provider isolates and clearly identifies the Company's customer information, documents, records and assets to protect the confidentiality of the information. The Company has strong safeguards in place so that there is no comingling of information/documents, records and assets.

- The Company ensures that it immediately notifies RBI in the event of any breach of security and leakage of confidential customer-related information.

9. Business Continuity Planning (BCP)

- BCP forms a significant part of any organisation's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP at the Company is also designed to minimise the operational, financial, legal, reputational and other material consequences arising from a disaster.

- The Company requires its service providers to develop and establish a robust framework for documenting, maintaining and testing business continuity and recovery procedures. The Company ensures that the service provider periodically tests the Business Continuity and Recovery Plan and occasionally conducts joint testing and recovery exercises with its service provider

- In order to mitigate the risk of unexpected termination of the outsourcing agreement or liquidation of the service provider, the Company retains an appropriate level of control over its outsourcing and the right to intervene with appropriate measures to continue its business operations in such cases without incurring prohibitive expenses and without any break in the operations of the Company and its services to the customers.

- The Company ensures that service providers are able to isolate the Company's information, documents and records and other assets. In appropriate situations, the Company can remove all its assets, documents, records of transactions and information given to the service provider from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

- The Company is responsible for formulation, review and monitoring of BCP to ensure continued effectiveness, including identifying critical business verticals, locations and shared resources to prepare a detailed business impact analysis.

- After the vulnerabilities and interrelationships between various systems, departments and business processes are identified, there should be a recovery strategy available to minimise losses in case of a disaster. The Company also has the option of alternate service providers and would be able to bring the outsourced activity back in-house in case of an emergency.

- The Company also has in place necessary backup sites for their critical business systems and Data centres.

- These plans are also tested by the Company on a regular basis.

10. Back-Up of Data with Periodic Testing

- In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out.

- Restoration testing on a time-to-time basis is done as both hard disks and magnetic tapes are prone to errors. As a general rule, daily full backup happens for all critical business applications and a complete weekly full backup is carried out, including file servers/old data kept on servers.

11. Incident Response and Reporting

An Incident Response Plan shall be established to detect, contain, investigate, and remediate security incidents. All employees must promptly report suspected or confirmed security incidents to the In-Charge of Information/IT Security. Material cybersecurity incidents shall be reported to the RBI and other regulators in accordance with prescribed timelines. Lessons learned from incidents shall be incorporated into policies and procedures.

12. Outsourcing and Third-Party Management

Where IT services are outsourced, the Company shall comply with RBI's Outsourcing of IT Services Directions (2022). Contracts with service providers shall contain robust clauses on confidentiality, data protection, regulatory access, and incident reporting. The Company shall retain ultimate responsibility for outsourced activities and conduct periodic risk assessments of service providers.

13. Information Systems Audit

- The Company shall conduct annual audits by competent personnel to ensure compliance with the information security policies, procedures, standards and guidelines.
- Such audits should test the effectiveness of technical and operational security control measures implemented in IT networks and systems.
- Audits performed shall include cyber cybersecurity assessment of the company's information systems to comply with regulatory requirements.
- Procedures shall be followed for planning and reporting audits and audit findings, and ensuring the implementation of a prompt and accurate remedial action.
- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
- All instances of non-compliance related to Information security shall be communicated and discussed with the Board of Directors.
- The IS Audit shall be performed before the statutory audit so that the statutory auditors can incorporate comments, if applicable, in the audit reports.

14. Policy Review

This Policy shall be reviewed at least annually, or earlier if necessitated by changes in business processes, regulatory requirements, or the technology environment. Amendments shall be approved by the Board of Directors.