Avanti Microfinance Private Limited

Cyber Security Policy

This document was :

Version	**Drafted by**	**Reviewed by**	**Board approval and adoption date**
Version 1	Mr. Manish Thakkar, Director	Mr. Nagaraj Subramanya, Director	March 13, 2023
Version 2	Mr. Manish Thakkar, Director	Mr. Nagaraj Subramanya, Director	December 16, 2024

Document Classification**: Public**

1. Introduction

Avanti Microfinance Private Limited ("Company") provides access to information, physical assets, computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against any damages to assets or relevant legal issues emerging from unacceptable use of assets.

Over the past two decades, the proliferation of technology has enabled the cohabitation of human beings with constantly connected devices, networks, software and services. As a digital-first financial services entity, Avanti Microfinance Private Limited has built a digital lending platform that benefits both consumers and businesses from the active interactions between people and technology.

Company conducts business in a complex environment of opportunities, risks, vulnerabilities and threats. The Cyber Security Policy offers broad guidelines to Company concerning the Identification, Protection, Detection, Response, and Recovery of people and systems, building agility and resilience for the organisation.

The Reserve Bank of India has regularly issued guidelines to the sector concerning the protection of information and people. These guidelines cover aspects related to Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds. The Cyber Security Policy of Company seeks to assist its management and employees to take note of the dynamic ecosystem of technological evolution and persistent threats, remaining alert to risks and producing processes and practices to protect the organisation and its various stakeholders.

The Cyber Security Policy shall protect the interests of the business, internal and external stakeholders, including customers, business partners and employees. It also helps the organisation fulfill statutory & regulatory requirements. In instances, where the policy may not afford explicit or unambiguous guidelines on a relevant aspect of cyber security, the management and employees are encouraged to embrace leading practices borrowing from leading competitors.

Each individual and entity interacting, using or administering Company's technology and information assets shall abide by this policy. The policy serves to inform customers, employees, vendors and other authorized users of their obligatory requirements for protecting the technology and information assets of the business. The policy describes some of the user's responsibilities and privileges. The policy describes user limitations and informs users there will be penalties for violation of the policy.

2. Objectives

The objectives of the policy include but are not limited to -

- Protect the Confidentiality, Integrity and Availability of the information assets of the organisation
- Maintain the privacy of customer information and any proprietary business information
- Comply with relevant regulatory and statutory requirements in a timely manner
- Establish responsibility and accountability for cyber security in the organisation
- Ensure the effective management of related incidents
- Protect information at rest, motion, use and change

3. Scope

All employees, contractors, consultants, temporary and other workers at Company, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Company, or to devices that connect to a Company network or resides at Company's website.

The IT team, vendors and related outsourcing partners shall practice secure measures to protect the organisation. These activities shall cover the following elements –

- Network Management and Security
- Secure Configuration
- Application Security Life Cycle (ASLC)
- Patch/Vulnerability & Change Management
- User Access Control / Management
- Authentication Framework for partners and customers
- Secure mail and messaging systems
- Vendor Risk Management
- Protect Removable Media
- Anti-Phishing Measures
- Data Leak Prevention strategies
- Maintenance, Monitoring, and Analysis of Audit Logs
- Audit Log Settings
- Vulnerability Assessment and Penetration Test
- Incident Response & Management

4. Governance

The information security team shall be responsible for the day-to-day implementation of Cyber Security related measures at Company. The Information Security Committee shall be accountable for the effective management of the team. The Information Security Committee and IT Strategy Committee shall review the work performed by the team and offer oversight and support to the function. The Information Security Committee shall present the workings of the information security team to the IT Strategy Committee on an annual basis, or upon facing any severe disruption lasting more than twelve hours due to the lack of or failure of cyber security controls.

Role of the IT Strategy Committee can be referred from the Terms of reference of the IT strategy committee document.

Role of Information Security Committee

- Review cyber security incidents and relevant responses
- Ensure cyber security awareness and training for the employees of the organisation
- Review the implementation of cyber security related procedures
- Plan and implement periodic vulnerability assessment and penetration testing by independent, suitably qualified entities
- Review VAPT reports and relevant action taken measures to ensure correction and compliance within a reasonable period of time
- Ensure adequate allocation of resources for the effective implementation of cyber security controls
- Evaluate and provide approval/rejection decisions related to resource allocations
- Offer an annual report to the board setting out the security processes and mechanisms of Company, including a summary of risks and controls

5. Cyber Crisis Management Plan

The Company shall implement a Cyber Crisis Management Plan (Plan) which will encompass coordination with stakeholders such as RBI, CERT-In, etc.

This Plan will form an integral part of Company's Information Technology Governance Policy and shall, at minimum, require the following:

a. Incident Management:
   The Company shall use the existing incident management system/ process adopted and implemented for information security.
b. Reporting:
   The Company shall proactively report cyber security incidents to RBI, CERT-In, and other applicable authorities within the timeline as may be notified from time to time.

6. Monitoring & Review

The policy and procedures related to cyber security shall be reviewed at least once annually. In the event of a significant systems change (including process, hardware and software) or an unplanned disruption lasting more than twelve hours, the policy and procedures shall be called into review with immediate effect, irrespective of the date of the previous review.

Observations and incidents shall be recorded in Jira at the instance they reach the attention of an employee, partner or any other stakeholder internal or external to the business. These incidents shall be assigned relevant priority and addressed effectively by the cyber security team. All changes to the systems, processes and controls shall be submitted to the Information Security Committee for their review each month.

A thorough VAPT by a suitably qualified entity shall be conducted at least once in six months or at any significant change/event, whichever occurs earlier.

Individuals or entities, including the senior management of the organisation, violating the cyber security policy, procedures or controls shall be presented to the Information Security Committee for a violation review. The committee shall exercise its collective powers to initiate and complete appropriate disciplinary action, including termination from services, where necessary without any limitation or hindrance. The aggrieved entity can appeal the decision made by the Information Security Committee (ISC) through an immediate appeal to the IT Strategy Committee. Any appeal shall be made within twelve hours of the ISC decision. In the interim period between the initial verdict and the consideration of the appeal, the aggrieved entity shall remain disallowed from any form of access to the information assets of the organisation. Further and final action can be communicated and implemented with no further internal recourse to the entity violation policy, procedure or controls. If any member or chair of a particular committee is deemed to commit such a violation, they shall excuse themselves from the duties of the committee till a final decision is implemented by the organisation.

The cyber security team shall collect and report a summary of cyber security incidents to the RBI and any other relevant statutory body proactively

The next section of this policy document shall cover key elements of interest for Company and its stakeholders, with a view to strengthening and sustaining a strong cyber security culture for the organisation.

I. Confidential Data

Company defines "confidential data" as:

- Unreleased and classified financial information
- Customer, supplier, and shareholder information
- Customer leads and sales-related data
- Patents, business processes, and/or new technologies
- Employees' passwords, assignments, and personal information
- Company contracts and legal records

II. Device Security

Company Use

To ensure the security of all company-issued devices and information, Company employees are required to:

- Keep all company-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters)
- Device should be locked when left unattended
- Refrain from sharing private passwords with coworkers, personal acquaintances, senior personnel, and/or shareholders
- Regularly update devices with the latest security software

Personal Use

Company recognizes that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 6 characters for mobile, 8 characters for other handheld or desktop equipment and devices)
- Ensure all personal devices used to access company-related systems are password protected
- Lock all devices if left unattended
- Ensure all devices are protected at all times
- Always use secure and private networks

III. Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, Company requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name
- Avoid opening suspicious emails, attachments, and clicking on links
- Look for any significant grammatical errors
- Avoid clickbait titles and links
- Contact isms@avantimicrofinance.in upon receipt of any suspicious emails.

IV. Data Transfer

Company recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties
- Only transfer confidential data over Company networks, use Cloud services related access controlled links
- Obtain the necessary authorization from senior management
- Verify the recipient of the information and ensure they have the appropriate security measures in place
- Adhere to Company data protection guidelines and non-disclosure agreements
- Immediately alert isms@avantimicrofinance.in of any breaches, malicious software, and/or scams

7. Disciplinary Action

Violation of this policy can lead to disciplinary action, up to and including termination. Company's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, repeat violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the circumstances of the case.

8. Awareness

The management shall ensure that stakeholders have access to the policy and awareness of their responsibilities toward the organisation. An awareness session shall be conducted at least once in six months. Awareness shall be considered an ongoing effort and stakeholders shall be informed of the relevant risks and controls regularly using media such as emails, internal meetings and discussions.

9. Regulatory Reference

Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, 2023

This Policy was:
I. Drafted on behalf of the Company by: Ms Nalini Chinta
II. Internally reviewed by: Mr Nagaraj Subrahmanya, Director of the Company and Mr. Manish Thakkar, Director of the Company