Avanti Microfinance Private Limited

Information Technology Governance Policy

This document was:

Version	**Drafted by**	**Reviewed by**	**Board approval and adoption date**
Version 1	Mr. Manish Thakkar, Director	-	September 12, 2018
Version 2	Mr. Manish Thakkar, Director	Mr. Nagaraj Subrahmanya, Director	March 22, 2021
Version 3	Mr. Manish Thakkar, Director	Mr. Nagaraj Subrahmanya, Director	March 13, 2023
Version 4	Mr. Manish Thakkar, Director	Mr. Nagaraj Subrahmanya, Director	December 16, 2024

Document Classification**: Public**

TABLE OF CONTENTS

1. Introduction

RBI notified the updated Master Directions on Information Technology Governance, Risk, Controls and Assurance Practices ("Master Directions") on 7th November 2023, aimed at a consolidated framework across regulated entities in relation to IT governance and processes. One of the key guidelines provides for governance structure as summarized below:

I. Board of Directors ("Board"): Approval of strategies and policies related to IT function;
II. IT Strategy Committee: Ensure that a robust IT strategic plan is adopted by the Company;
III. IT Steering Committee: Assists the IT Strategy Committee in strategic IT planning and ensures that the measures taken under such planning is implemented across various functions / departments of the Company;

Chief Information Security Officer (CISO): A member of the senior management of the holding company specifically appointed to drive cyber security strategy and ensure compliance with regulatory instructions

Avanti Microfinance Private Limited (hereinafter referred to as 'the Company') has adopted the Information Technology Policy (hereafter referred to as "Information Technology Policy" or "the Policy") in accordance with statutory and regulatory requirements as applicable.

1. Purpose

The Company has laid down an IT Policy to:

- Govern operations of the IT function while aligning to the business strategy and relevant industry best practices/standards;
- Ensure compliance to all relevant statutory and regulatory requirements that are applicable to the IT function.

2. Applicability

- This policy is managed by the IT Strategy Committee (ITSC) of the Company.
- The IT policies in this document will be followed by all IT and relevant business personnel as applicable.

3. Document Maintenance and Distribution

- The IT Strategy Committee will review the information technology process and policy framework at least annually.
- It is the responsibility of the IT Strategy Committee to monitor, initiate and obtain relevant approvals for any changes/revisions required to this document.
- All editions of this policy will be version controlled.
- The IT Strategy Committee is responsible for distributing approved revisions of the document to concerned stakeholders.

4. Waiver/Exception

Waivers to the IT policy and guidelines in this document will be formally submitted to the IT Strategy Committee, including justification and benefits attributed to the waiver, and it will be approved by the IT Strategy Committee where the waiver is deemed fit for business considerations. The waiver will only be used in exceptional situations when communicating any non-compliance with the IT policy and guidelines for a specific case/period of time. At the completion of the case/time period, the need for the waiver will be reassessed and re-approved by the IT Strategy Committee, if necessary.

The waiver will be monitored by the IT Strategy Committee to ensure its concurrence with the specified period of time and exception.

5. IT Organization Structure & Governance

IT Strategy Committee is responsible for owning and delivering IT services in accordance with business objectives. IT Strategy Committee will be responsible to deliver business expectations. Keeping in view the pervasive nature of technology, it is essential that business stakeholders have appropriate involvement in making key technology decisions.

IT Strategy Committee shall develop and maintain an organizational structure reflecting business and technology needs of the company. IT Strategy Committee will establish and communicate the IT-related roles and clearly define responsibilities and accountability.

The organization structure will be established taking into consideration the following:

1. Resources required for the execution of the IT strategy
2. Key Stakeholders
3. Communication needs

4. Any applicable statutory and regulatory requirements

2. Project Management

a. A detailed project plan covering the business case for system acquisition/development will be developed for all projects as deemed necessary by the IT Strategy Committee and will include the cost-benefit analysis, success criteria, risk management, funding and resource requirements.
b. Specific risks associated with individual projects will be treated through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change.
c. Accountability for achieving the benefits, controlling the costs, managing the risks, and coordinating the activities and interdependencies of multiple projects will be clearly and unambiguously documented, assigned and monitored. Where accountability is assigned, accountability will be accepted and sufficient authority will be assigned.
d. The responsibilities, relationships, authorities and performance criteria of project team members, and sponsors will be defined.
e. Periodic monitoring of the project's progress will be carried out by the IT Strategy Committee and timely remedial actions will be taken in case of delays.

3. IT Strategy

IT Strategy Committee:

1. Will consider the current organization's environment, business processes and future objectives to arrive at the conclusion for the direction of the IT strategy.

2. Will understand the business strategy of the Company and develop an IT strategy which aligns with the business strategy and objectives, and this will be reviewed at least once a year.

3. Will also consider any criteria that are based on industry factors, applicable legal and regulatory requirements.

4. IT Budgeting

a. IT investment requirements in support of business/IT strategy will be identified, categorized, prioritized, and agreed upon.

b. IT investment programs will specify the following:

- The business benefit expected and performance to be achieved
- The method for measuring outcomes
- Accountability for achieving the outcomes
- The expected delivery schedule for each outcome

c. A decision-making process will be followed to prioritize the allocation of IT resources for operations, projects and maintenance to optimize the return on the enterprise's portfolio of IT investment programs and other IT services and assets.
d. Costs incurred by IT will be identified along with their allocation across the IT budget and projects.

e. A formal IT budget will be defined and implemented.

f. The relevant costs and benefits for IT investments will be reviewed and approved by the Board.

g. Variances between budgeted and actual costs will be analyzed and reported to relevant stakeholders by the Finance Team.

h. Monitoring and reporting costs against the budget and managing costs will be done through the yearly review and the budget utilization report will be maintained by the Finance Team.

5. IT Resource Management

The Company will maintain and annually review an inventory for all IT assets including but not limited to hardware and software.

Performance of critical IT systems/Infrastructure along with IT partners' service level performance will be monitored periodically by the IT Strategy Committee.

6. IT Operations

IT Strategy Committee:

1. Will manage appropriate processes and activities required to deliver the IT strategy and ensure that it adds value to the organization's IT requirements.

2. Will develop procedures and standards/guidelines as necessary to support its endeavour in implementing the information systems.

3. Recognize the maker-checker concept to reduce the risk of error and misuse and to ensure reliability of data/information.

4. Will enable the provision of system-generated reports for the management team summarizing financial position including operating and non-operating revenues and expenses, cost-benefit analysis of segments/verticals, cost of funds, etc.

5. Conduct a gap analysis exercise once a year against the current statutory/regulatory requirements as necessary to formulate and implement an appropriate remediation plan.

6. Will manage the following under IT operations (including but not limited to the following):

a. IT asset/ Equipment management & configuration
b. Backup and restoration
c. Network Management
d. Change & Release management
e. Define & manage IT third-party services
f. System and Software development
g. Database implementation and support
h. Access Control
i. Manage problems and IT events and incidents
j. Filing of regulatory returns to RBI (where applicable)

7. IT Risk Management

IT Operations and business risks will be managed during the project lifecycle by the IT Steering Committee and relevant business heads. Also, the IT Steering Committee will lay down procedures for the assessment and treatment of IT risks and drive the annual IT risk assessments with the involvement of relevant stakeholders from business functions.

8. IT Security Management

1. Purpose

The broad purpose of IT security management shall be to respond to security incidents within agreed timelines and mitigate any damage from security incidents (Cybersecurity Events). Additionally, the following goals are also sought to be addressed herein:

1. To set up a channel for quick reporting of Cybersecurity Events and make employees aware of the point of contact for reporting incidents;

2. To set up an internal team to correct or recover from the incident based on agreed parameters; and

3. Ensure that event reporting and escalation procedures are in place;

The steps outlined herein apply to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, other third parties who have access to services systems of Company (for the purpose of this Section 8, the aforementioned personnel shall be referred to as "Personnel").

Approved Information Security (IS) policy of the organization will be followed and implemented with necessary controls which are defined by Information Security Committee (ISC) along with CISO.

2. Reporting Procedure

Personnel can report Cybersecurity Events by any of the following means:

1. Sending mail to isms@avantimicrofinance.in
2. Call the helpdesk at 080-41689310 in case the incident requires immediate attention.

Personnel should make sure that any Cybersecurity Event, even if it is of a minor nature, is not left unreported, as it may cause harm if left unattended over a period of time.

As an indicative illustrative list of what may constitute a Cybersecurity Event, the following may be referred:

1. Virus attack
2. Denial of Service
3. Unauthorized access
4. Modification of information/data
5. Compromise of user/Personally identifiable information (PII) data
6. Loss of sensitive information
7. Misuse of information & computing resources
8. Incidents related to physical security such as but not limited to, laptop lost, unauthorized entry into premises, assault, etc.

3. Response Procedure

Upon reporting a Cybersecurity Event, the IT Steering Committee may record the details and further delegate the response (with regard to the severity of the reported incident) to

any authorized personnel in this regard. In any case, the following information shall be recorded:

- Date and time of the incident;
- Location of the incident;
- Type of incident (security breach/weakness/malfunction);
- Brief description of the incident;
- Name and designation of the person reporting the incident;
- Name and designation of the person receiving the report of the incident;
- Name and designation of a person to whom any task with respect to investigation or otherwise is delegated;
- Identification of the root cause of the incident;
- Action taken by the person authorized to do so;
- The Root cause analysis to develop preventive approaches to avoid similar incidents; and
- Close date in respect of the incident.

Conduct an awareness programme for employees and other related stakeholders about Information Security and incident management on a quarterly basis. This shall be delivered either digitally or physically.

9. Information Security Committee (ISC)

The ISC is established under the oversight of the IT Strategy Committee (ITSC) to ensure the effective management of cyber and information security within the organization. The ISC is responsible for overseeing security initiatives, ensuring compliance with regulatory requirements, and mitigating cybersecurity risks in alignment with the organization's risk appetite. For a detailed structure and operational framework of the ISC, refer to the ISC Charter.

10. Appointment and Responsibilities of CISO

The Chief Information Security Officer (CISO) is responsible for articulating the IS Policy that the Company uses to protect the information assets apart from coordinating the security related issues within the Company as well as relevant external agencies.

Responsibilities of CISO:

a. The CISO is responsible for driving cyber security strategy and ensuring compliance to the extant regulatory/ statutory instructions on information / cyber security.

b. The CISO is responsible for enforcing the policies that Company uses to protect its information assets apart from coordinating information/ cyber security related issues within the Company as well as with relevant external agencies.

c. The CISO is a permanent invitee to the ITSC and IT Steering Committee.

d. The CISO's office manage and monitor Security Operations Centre (SOC) and drive cyber security related projects.

e. The CISO's office ensures effective functioning of the security solutions deployed.

f. The CISO shall directly report to the CEO or CRO of the Company; and

g. CISO reviews the cyber security risks/ arrangements/ preparedness of the Company before the Board/ ITSC on a quarterly basis.

h. Reporting to CERT-In:
On the occurrence of any Cybersecurity Event, the Company shall as soon as possible, through the CRO, report such event to the Computer Emergency Response Team of India (CERT-In) in accordance with the Information Technology (Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

i. Establish and maintain security policies and standards for the organization to follow.

j. Directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology risks.

k. Ensure that disaster recovery and business continuity plans are in place and tested.

l. Arrange for backup of data with periodic testing.

m. Enable independent investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar vulnerabilities.

n. Maintain a current understanding of the IT threat landscape for the industry.

o. Ensure compliance with the changing laws and applicable regulations, and translate that knowledge to the identification of risks and actionable plans to protect the business.

p. Schedule periodic security audits internally.

q. Provide training and mentoring to security team members.

r. On reporting of a Cybersecurity Event, CISO may initiate action by directing any authorized personnel or set of such personnel to respond, correct and prevent similar incidents in future. A detailed report of the critical incident will be made by the CISO.

11. Change and Patch Management

All proposals for new features and/or changes to IT systems will go through a systematic approval process which includes cost benefit analysis of the change, risk assessment of the proposed changes and monitoring plan for the proposed changes. In addition, the Company will evaluate all changes in a test environment first prior to taking it live. The Company governs this process through the Board approved Change Management policy of the organization.

12. Data Migration Policy

In instances where there is a need for Data Migration, the detailed rationale, process and monitoring plan for the same will be presented to the IT Strategy Committee for approval prior to implementation. The CISO will be responsible for the execution of the data migration and will report back to the IT Strategy Committee once the migration is completed

13. Digital Signatures

When using digital signatures, the Company endeavors to use such Digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

14. Mobile Financial Services

The Company shall develop mechanisms for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to-end encryption.

15. Use of social media

Where the Company uses any relevant social media to market its products, Company shall ensure that its social media accounts(s) are safeguarded with proper controls such as encryption and secure connections to prevent risks such as account takeover and/or malware attack / disruption.

16. Password Policy

Passwords are an important aspect of IT security. A poorly chosen password may result in unauthorized access and/or exploitation of the resources of the Company. This section details the standard for the creation, maintenance and change cycle for strong passwords. All users, including employees, contractors, vendors and all other stakeholders with access

to systems of the Company are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

a. Password Construction

Strong passwords have the following characteristics:

1. Contain at least three of the five following character classes:
2. Lowercase characters
3. Upper case characters
4. Numbers
5. Punctuation
6. “Special” characters (for example: @#$%^&*()_+|~-=\`{}[]:";'<>/, etc.)
7. Contain at least 8 alphanumeric characters.

b. **Password Protection Standards**

a) Change cycle**:**
   (i) All cloud service management passwords must be changed at least once every 90 days.
   (ii) All administrative passwords for the platform must be changed at least once every 180 days.
   (iii) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least once every 365 days.
b) Personnel shall use different passwords for official and personal accounts.
c) Personnel shall not share official passwords with anyone.
d) Passwords should never be written down or stored online without encryption.
e) Personnel shall not reveal their password in email, chat, or other electronic communication; or speak about a password in front of others.
f) If someone demands a password, refer them to this document and direct them to the CRO of holding company.
g) Passwords should be changed immediately in case of password leakage is noticed or suspected.
h) If an account or password compromise is suspected, report the incident to isms@avantimicrofinance.in.

17. Business Continuity

Company shall ensure that:

1. It identifies critical business verticals, locations and shared resources to come up with the detailed business impact analysis. Due regard shall be given to account for any impact of any unforeseen natural or man-made disasters on the Company's business;
2. It understands the vulnerabilities associated with interrelationships between various systems, departments and business processes. It shall endeavor to come up with the probabilities of various failure scenarios and evaluate various options for recovery and minimization of losses in case of a disaster;
3. It considers the need to put in place necessary backup sites for its critical business systems and data centres; and
4. It tests the business continuity plan annually as well as when significant IT or business changes take place.
5. Review cloud service arrangements and SLA for business continuity once every six months.

IT Steering Committee will approve and oversee the annual business continuity plan strategy and road map. Business continuity plans are reviewed and maintained periodically to incorporate any significant changes to process, human resources and technology. The Company's business continuity plan is in line with the guidelines issued by RBI and is subject to annual review by the Board of Directors.

Company understands the environment in which it operates in and the associated risks, hence the Company has developed and implemented business recovery strategies and infrastructure to ensure recovery and continuity of critical IT operations as per agreed timelines and acceptable service levels. The plan is designed to facilitate the continuity of the critical business processes in the event of defined disaster scenarios. The same is tested periodically to address any gaps.

In a significant disruption scenario: During a significant disruption or a disaster, if a customer's usual access to Company's services is affected, the customer may connect with the Company through its customer care number (1800-3095021). Customer care number of the Company is published on the Company's website. If a customer is not able to contact the company through its customer care number, customer could visit its website at www.avantimfin.in and send queries/complaints/requests through online contact links published on the website.

18. Value Delivery

a. Value delivery will be an integral form of IT service delivery to the organization.

b. Business functions will be able to register formal service complaints to be addressed to the IT team.

c. All service complaints will be recorded by IT, investigated, addressed, reported and formally closed.

d. Business functions will be able to escalate cases wherein a complaint is not resolved by IT as per the agreed service levels.

e. Satisfaction of business needs and managing the business relationships will be the responsibility of the COO of holding company within the applicable business constraints.

f. Measures will be put in place to satisfy business needs and actions for improvement will be identified, recorded and updated in a continual service improvement plan.

19. IT Compliance and Audit

1. Compliance

Compliance functions include the following: Evaluate, define the compliance parameters based on internal and regulatory requirements, assess the reported observations, recommendations and perform timely corrective actions to ensure compliance to identified requirements.

2. Information System (IS) Audit

Auditing of Information Systems will take into consideration the risks and the impacts on all the in-scope systems (e.g. potential for disruption). The Information systems will be audited at least once a year. Auditing requirements will include:

- Audit requirements for access to systems and data should be agreed with appropriate management;
- Computer Assisted Auditing Techniques (CAATs) will be used wherever feasible;
- The scope of technical audit tests should be agreed and controlled;
- Audit tests should be limited to read-only access to software and data requirements for special or additional processing should be identified and agreed; audit tests that could affect system availability should be run outside business hours;
- All access should be monitored and logged to produce a reference trail.

The findings of the audit shall be shared with each relevant stakeholder for remedial action or an adequate management response. IT Steering Committee of the Board shall review the progress and action taken on the audit findings during their quarterly review.

20. Regulatory reference

This policy is framed as per the following regulatory references and in accordance with leading industry practice:

Reserve Bank of India (Information Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023

21. Policy Review updated

This Policy shall be reviewed by the Board of the Company, and shall be reviewed at least once a year. Reviews shall also account for any significant business changes and/or any regulatory requirements.