



Avanti Finance Private Limited

Information Security Policy

This Policy was:

Version	Drafted by	Reviewed by	Committee approval date	Board approval date
Version 1	-	Mr Manish Thakkar, COO	NA	October 30, 2017
Version 2	-	Mr Manish Thakkar, COO	NA	July 24, 2020
Version 3	Mr Nagaraj Subrahmanya, CRO	Mr Manish Thakkar, COO	NA	December 19, 2022
Version 4	Mr Manish Thakkar, COO	Mr Nagaraj Subrahmanya, CRO	NA	November 08, 2024
Version 5	Mr Manish Thakkar, COO	Mr Nagaraj Subrahmanya, CRO	December 19, 2024	December 19, 2024
Version 6	Mr Manish Thakkar, COO	Mr Nagaraj Subrahmanya, CRO	March 18, 2025	March 21, 2025
Version 7	Mr Manish Thakkar, COO	Mr Nagaraj Subrahmanya, CRO	September 30, 2025	October 16, 2025
Version 8	Ms. Sonali Yadav, CISO	Mr Manish Thakkar, COO	June 29, 2026	July 06, 2026

Document Classification: **Public**

1. Scope / Purpose of the Policy

The purpose of this information security policy ("Policy") is to safeguard information belonging to the Avanti Finance Private Limited ("Company") and its stakeholders (third parties, clients or customers and the general public), within a secure environment.

This Policy informs the Company's employees, contractors, and other individuals that are entrusted with any information related to the business, of the principles governing the holding, use and disposal of information.

For the sake of clarity, the term "information" relates to:

- (i) Electronic information systems (software, computers, and peripherals) owned by the Company whether deployed or accessed on or off campus.
- (ii) The Company computer network used either directly or indirectly.
- (iii) Hardware, software and data owned by the Company.
- (iv) Paper-based materials.
- (v) Electronic recording devices (video, audio, CCTV systems).

2. Key Objectives

- (i) Information will be protected against unauthorised access or misuse.
- (ii) Confidentiality of information will be secured.
- (iii) Integrity of information will be maintained.
- (iv) Availability of information / information systems is maintained for service delivery.
- (v) Business continuity planning processes will be maintained.
- (vi) Regulatory, contractual and legal requirements will be complied with.
- (vii) Physical, logical, environmental and communications security will be maintained.
- (viii) Violation of this Policy may result in disciplinary action or criminal prosecution.
- (ix) When information is no longer of use, it is disposed of in a suitable manner.
- (x) All information security incidents will be reported to the information security manager (a leadership role that may be titled and designated based on the needs of the Company) and investigated through the appropriate management channel.
- (xi) Personal data of Data Principals shall be protected through appropriate technical and organisational security safeguards in compliance with Section 8(4) and Section 8(5) of the Digital Personal Data Protection Act, 2023, to prevent personal data breaches.
- (xii)

3. The Policy

The Company requires all users to exercise a duty of care in relation to the operation and use of its information systems, irrespective of form or media.

3.1 Authorised users of information systems

With the exception of information published for public consumption, all users of the Company's information systems must be formally authorised by appointment as an employee, contractor, or by other processes of non-disclosure specifically authorised by the person authorised to manage information security. Authorised users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

Authorised users will pay due care and attention to protect Company's information in

their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- (i) permission of the information owner.
- (ii) the risks associated with loss or falling into the wrong hands.
- (iii) how the information will be secured during transport and at its destination.

3.2 Acceptable use of information systems

Use of the Company's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people.

3.3 Information System Owners

Authorised officers, who are responsible for information systems are required to ensure that:

- (i) Systems are adequately protected from unauthorized access.
- (ii) Systems are secured against theft and damage to a level that is cost- effective.
- (iii) Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).
- (iv) Electronic data can be recovered in the event of loss of the primary source i.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).
- (v) Data is maintained with a high degree of accuracy.
- (vi) Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.
- (vii) Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers and other relevant acts concerning information and privacy.
- (viii) Any third parties (data processors) entrusted with personal data of the Company's customers or employees shall be engaged only under a valid Data Processing Agreement (DPA) that explicitly governs their obligations under the DPDP Act, 2023. Such agreements shall include obligations relating to data security standards, restrictions on sub-processing, data erasure upon instruction, audit rights, and breach notification. Non-compliance by a data processor shall constitute non-compliance by the Company as Data Fiduciary under Section 8(1) of the DPDP Act.

3.4 Personal Information

Authorised users of information systems are not given rights of privacy in relation to their use of Company information systems. Duly authorised officers of the Company may access or monitor personal data contained in any Company information system for the purposes of security, fraud prevention, legal compliance, or performance management, as permitted under Section 7(f) of the DPDP Act, 2023. Such monitoring shall be proportionate, documented, and limited to the minimum necessary data. Employees shall be informed of monitoring practices through appropriate notice.

3.5 Individuals in breach of this Policy are subject to disciplinary procedures (employee, contractor or third party) at the instigation of the officer with responsibility for the relevant information system, including referral to the Police where appropriate.

The Company will take legal action to ensure that its information systems are not used by unauthorised persons.

3.6 In the event of a confirmed or suspected personal data breach, the Company shall:

(a) Immediately initiate its incident response process; (b) Assess the scope, nature, and impact of the breach; (c) Notify the Data Protection Board of India in the prescribed form without undue delay; (d) Notify each affected Data Principal of the breach, the nature of data compromised, and remedial actions being taken, without undue delay; (e) Document all breach events, investigations, and remedial actions for audit purposes. This obligation is mandated under Section 8(6) of the DPDP Act, 2023 and non-compliance may attract a penalty of INR 200 crore.

4. Information Security Organisation Structure

The information security organisation of the Company constitutes an Information Security Committee, the composition and responsibility of which is mentioned under the Information Security Committee Charter of the Company.

5. Penal Action

Company's disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, repeat violations (either intentional or unintentional) 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, initiation of criminal proceedings or seek any other remedy as available under the applicable law against the violator(s).

6. Continual improvement

We encourage feedback from all stakeholders—employees, customers, partners regarding our information security practices. Our organisation is committed to regular internal and independent reviews to strengthen the systems and achieve continual improvement.

7. Review

CISO shall be responsible for an annual review of the compliance with this Policy and the applicable laws and regulations.

8. Ownership and Responsibility

8.1 The information security manager has direct responsibility for maintaining this Policy and providing guidance and advice on its implementation.

Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

8.2 In the event that the Company is designated as a Significant Data Fiduciary under the DPDP Act, 2023, a Data Protection Officer (DPO) shall be appointed. The DPO shall report directly to the Board of Directors and shall be responsible for: (a) overseeing DPDP Act compliance; (b) serving as the primary contact for data principals and the Data Protection Board of India; and (c) advising on Data Protection Impact Assessments. The DPO's contact details shall be published in the Company's Data Privacy and Security Policy

9. Regulatory Reference

This Policy is framed in accordance with: (i) Reserve Bank of India (Information

Technology Governance, Risk, Controls and Assurance Practices) Directions, 2023; and
(ii) The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) — in particular,
Sections 8(4) and 8(5) relating to technical and organisational security safeguards and
the prevention of personal data breaches.