Alpha Fintech Private Limited

Policy Name – Information Security Governance and Compliance Policy

Version – 1.0

.

DOCUMENT CONTROL			
Policy Name	Information Security Governance and Compliance Policy	**Document Version**	First Version

Description	Name	Date
Document creation date	-	14-08-2025
Prepared By	Rajat Sah	14-08-2025
Reviewed By	Aniket Pathak	10-10-2025
Approved By	Vijay Kuppa	13-10-2025

DOCUMENT REVISION HISTORY

Version No.	Change Description	Date of Change	Change Author	Change Reviewer	Change Approver
1	First Version				

Status	Working Draft	Approved Policy	Implemented Policy

K. Vijay Krishna

ALPHA FINTECH PRIVATE LIMITED

Date: 13-10-2025

Signature:

.

Contents

Disclaimer

This document forms a part of the Information Security Management System (ISMS) of **Alpha Fintech Private Limited,** developed in accordance with the ISO/IEC 27001 standard. It outlines internal policies, procedures, and controls designed to protect the confidentiality, integrity, and availability of information assets.

The contents of this document are strictly confidential and intended solely for internal use by authorized personnel of **Alpha Fintech Private Limited.** Unauthorized access, reproduction, modification, distribution, or disclosure of any part of this document is strictly prohibited and may result in disciplinary or legal action.

While every effort has been made to ensure the accuracy, completeness, and relevance of the information contained herein, **Alpha Fintech Private Limited** reserves the right to update or revise this document at any time to reflect changes in regulatory requirements, organizational practices, or security threats.

This document should be read in conjunction with other ISMS documents and is not intended to be a standalone reference for legal or compliance purposes. For any clarifications related to this policy and procedure document with respect to its interpretation, applicability, and implementation, please write to **ciso@incredmoney.com.**

Purpose

The purpose of this policy is to establish a structured governance framework for information security, ensuring that security objectives, policies, and controls are effectively developed, implemented, reviewed, and enforced. It defines requirements for creating, maintaining, and independently reviewing information security policies while ensuring compliance with applicable rules, standards, and contractual obligations

Scope

This policy applies to all employees, contractors, consultants, vendors, and third-party service providers engaged with the organization. It encompasses all information systems, applications, networks, and assets, whether hosted on-premises, in the cloud, or within hybrid environments. Furthermore, the scope includes all forms of information—digital, physical, and intellectual property—that are owned, processed, or controlled by the organization.

Objectives

To ensure:

- Formalized, documented, and approved information security policies aligned with business and regulatory requirements.
- Independent reviews to assess adequacy and effectiveness of information security governance.
- Strict adherence to information security policies, rules, and standards across the organization.
- Continuous improvement of security governance through monitoring, audits, and corrective actions.

Policy Statement

Policies for Information Security

- The organization has established, documented, approved, and maintained an overarching Information Security Policy framework, supported by subsidiary policies and procedures.
- All policies are fully aligned with ISO/IEC 27001:2022, applicable laws, regulatory requirements, and contractual obligations.
- Information security policies have been:
    - Approved by the Chief Executive Officer (CEO) and Chief Technology Officer (CTO).
    - Made accessible to all employees via the organization's Google Drive policy repository.

- Communicated through formal circulation of “Dos and Don’ts” guidelines, with employee acknowledgements recorded.

- Policies have been reviewed annually by top management and updated when required due to changes in technology, regulations, or business operations.
- Version control and change history have been maintained for all policies.

Independent Review of Information Security

- The Information Security Management System (ISMS) is independently reviewed at defined intervals, with a minimum frequency of once per year.
- These reviews have been carried out by:
  - Internal audit functions independent of ISMS implementation.
  - Accredited external auditors as part of the annual Vulnerability Assessment and Penetration Testing (VAPT) exercise.
- Each review has confirmed:
  - Policy alignment with business objectives, regulatory obligations, and risk management requirements.
  - Adequacy and effectiveness of implemented controls.
- All findings, risks, and non-conformities have been documented, tracked, and addressed through corrective actions with defined deadlines, and closure has been verified by the CISO.

Compliance with Policies, Rules, and Standards for Information Security

- All employees, contractors, and third-party providers have complied with established information security policies, rules, and standards.
- Compliance has been ensured through:
  - Mandatory information security training, including an information security exam for employees.
  - Policies being readily available to all staff via Google Drive.
  - Circulation of “Dos and Don’ts” guidelines with acknowledgement tracking.
  - Random monitoring of activities and observation of employees to verify adherence.
- Regular internal audits and spot checks are being conducted, with continuous oversight by the Department Heads.

- Non-compliance incidents have been recorded, investigated, and resolved in accordance with the Incident Management Policy.
- Repeated or wilful violations have resulted in disciplinary measures, up to and including termination of employment or contract.

Roles and Responsibilities:

Chief Executive Officer (CEO)

- Formally approves the overarching Information Security Policy framework.
- Provides top-level commitment and resources to ensure information security is integrated into business strategy.
- Holds ultimate accountability for compliance with legal, regulatory, and contractual obligations.

Chief Technological Officer (CTO)

- Leads the design, implementation, and ongoing management of the ISMS.
- Ensures regular independent reviews, audits, and assessments are carried out.
- Tracks findings, risks, and non-conformities, ensuring corrective actions are completed on time.
- Provides periodic security performance reports to senior management.

Chief Information Security Officer (CISO)

- Establishes governance structures, committees, and reporting lines to ensure information security responsibilities are clearly defined and monitored.
- Aligns security and compliance initiatives with organizational objectives, ensuring that controls are business-enabling rather than restrictive.
- Engages with regulators, auditors, and external stakeholders to demonstrate compliance and maintain trust in the organization's security posture.
- Sponsors security improvement programs, ensuring adequate investment in technology, people, and processes to address evolving threats.

Department Heads

- Enforce compliance with policies and standards within their respective teams.
- Ensure staff complete required training and understand their security responsibilities.
- Monitor daily operations for policy adherence and escalate issues promptly to the CISO.
- Support investigations into incidents or non-compliance within their departments.

Employees, Contractors, and Third Parties

- Follow all approved information security policies, procedures, and "Dos and Don'ts" guidelines.
- Participate in mandatory security awareness training and examinations.

- Report any suspected security incidents, policy violations, or weaknesses immediately.
- Protect organizational information assets and avoid negligent or wilful non-compliance.

Non-Compliance:

Failure to comply with this policy could result in security vulnerabilities, unauthorized access, data breaches, and reputational damage. Non-compliance shall be addressed with corrective actions, including potential disciplinary measures.

Policy Review and Approval

This policy shall be reviewed annually or upon significant changes to legal, regulatory, or business requirements, such as updates to ISO/IEC 27001, or changes in organizational operations.

The **CTO/CISO** is responsible for initiating the review, incorporating necessary updates, and presenting the revised draft for approval. The review procedure includes:

- Review Initiation: Triggered annually or based on relevant change.
- Update and Drafting: The policy is updated within 10 business days of review initiation.
- Stakeholder Feedback: Key departments (e.g., Legal, HR, IT, Compliance) provide feedback within 5 business days.
- Final Approval: The finalized policy is submitted to the IT committee after incorporating feedback.
- Publication: Once approved, the updated policy is published and communicated to relevant personnel.

All approved versions shall be maintained in the organization's Policy Repository, with clear version control and audit trails.

ISO 27001:2022 Reference Controls

A.5.01 - Policies for information security

A.5.35 - Independent review of information security

A.5.36 - Compliance with policies, rules and standards for information security

---------- End of Document ----------