

Information Security Policy

**1. Purpose**

The purpose of this Information Security Policy is to ensure that ABC-FinTech operates in a secure environment that protects the confidentiality, integrity, and availability of all information assets. This policy establishes the framework for setting information security objectives and outlines the company’s commitment to achieving and maintaining compliance with relevant legal, regulatory, and contractual requirements. It also emphasizes continual improvement of the Information Security Management System (ISMS).

**2. Scope**

This policy applies to all employees, contractors, consultants, and third parties who have access to ABC-FinTech’s information systems, data, and infrastructure. It covers all information assets, including but not limited to customer data, financial records, intellectual property, and company operational information.

**3. Information Security Objectives**

ABC-FinTech’s primary information security objectives are to:

* Ensure the confidentiality, integrity, and availability of all information assets.
* Prevent unauthorized access, disclosure, alteration, or destruction of sensitive data.
* Safeguard customer trust by adhering to industry standards and best practices.
* Maintain continuous compliance with ISO 27001, PCI-DSS, GDPR, and other applicable regulations.
* Implement and maintain a secure and resilient IT infrastructure that supports the company's innovative financial services.

**4. Commitment to Satisfy Applicable Requirements**

ABC-FinTech is committed to:

* Meeting all applicable legal, regulatory, and contractual obligations related to information security, including ISO 27001, PCI-DSS, and GDPR.
* Ensuring that security policies and procedures are in place to mitigate risks associated with the company’s financial products and services.
* Protecting customer data through robust encryption, access controls, and regular security reviews.
* Conducting regular audits and assessments to verify compliance and make necessary improvements.

**5. Continual Improvement of the Information Security Management System**

ABC-FinTech acknowledges that the threat landscape is continually evolving, and we are committed to the continual improvement of our Information Security Management System (ISMS). This will be achieved by:

* Regularly assessing risks, vulnerabilities, and incidents, and implementing corrective and preventive actions.
* Reviewing and updating security policies, procedures, and controls in response to emerging threats and changes in the business environment.
* Providing ongoing training and awareness programs for employees to ensure that security remains a priority across the organization.
* Monitoring security metrics and performance to evaluate the effectiveness of the ISMS.

**6. Governance and Accountability**

The Information Security Steering Committee (ISSC) is responsible for overseeing the implementation and ongoing management of the ISMS. The committee will regularly review and update the security objectives and this policy to ensure alignment with business goals and regulatory requirements.

The Chief Information Security Officer (CISO) is responsible for the day-to-day management of information security risks and for ensuring that security policies and controls are effectively implemented across the organization.

**7. Communication**

This Information Security Policy is to be communicated to all employees, contractors, and relevant third parties to ensure full awareness and compliance. It will be reviewed annually or whenever significant changes occur in the business environment or the regulatory landscape.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 9 Jan 2024**