

Information Security Objectives

# 1. Introduction

**1.1 Purpose**

The purpose of this document is to define, communicate, and document the information security objectives of ABC-FinTech. These objectives are designed to support the overall Information Security Management System (ISMS), ensuring alignment with the Information Security Policy and compliance with ISO 27001:2022 standards.

**1.2 Scope**

This document applies to all relevant functions, levels, and departments within ABC-FinTech. It includes specific objectives for each department and process involved in the protection of information assets.

# 2. Information Security Objectives

The following information security objectives have been established for ABC-FinTech:

**2.1 Objective 1: Improve Protection Against Cyber Attacks**

* **Objective:** Reduce the number of successful cyber attacks on ABC-FinTech’s systems by 30% within 12 months.
* **Measurement:** Track the number of detected and successfully mitigated cyber incidents.
* **Justification:** Consistent with the Information Security Policy’s focus on protecting the organization from external and internal threats.
* **Applicability:** IT Security Team, SOC (Security Operations Center), Risk and Compliance.

**2.2 Objective 2: Strengthen Data Encryption Across All Systems**

* **Objective:** Achieve 100% encryption of sensitive data both at rest and in transit within 6 months.
* **Measurement:** Monitor the percentage of encrypted databases and secure communications.
* **Justification:** Supports confidentiality and integrity of sensitive data as outlined in the Information Security Policy.
* **Applicability:** IT Security Team, Database Administrators, Product Development.

**2.3 Objective 3: Ensure 100% Compliance with ISO 27001 Requirements**

* **Objective:** Maintain 100% compliance with ISO 27001 controls, with no major non-conformities during annual audits.
* **Measurement:** Results from internal and external ISO 27001 audits.
* **Justification:** Reflects the company’s commitment to regulatory compliance and continual improvement.
* **Applicability:** Risk & Compliance Team, Information Security Steering Committee, Management.

**2.4 Objective 4: Reduce Third-Party Risks**

* **Objective:** Ensure 100% of third-party vendors have completed security assessments within the next 9 months.
* **Measurement:** Track the number of vendors who complete security assessments and meet compliance requirements.
* **Justification:** Mitigates risks posed by third-party vendors as identified in the risk assessment.
* **Applicability:** Vendor Management, IT Security Team, Risk & Compliance.

**2.5 Objective 5: Increase Employee Security Awareness**

* **Objective:** Achieve 95% participation in security awareness training across all employees and contractors within 3 months.
* **Measurement:** Attendance rates and post-training security awareness test scores.
* **Justification:** Supports the Information Security Policy’s focus on insider threat mitigation and reducing human error.
* **Applicability:** HR, IT Security Team, All Departments.

# 3. Planning to Achieve Information Security Objectives

For each of the objectives, the following steps will be taken:

**3.1 Objective 1: Improve Protection Against Cyber Attacks**

* **What will be done:** Implement enhanced threat detection systems, conduct red team/blue team exercises, and upgrade firewall and intrusion prevention systems (IPS).
* **Resources Required:** Budget for new security systems, personnel for threat intelligence and testing.
* **Who is Responsible:** IT Security Team.
* **Completion Date:** 12 months from approval of this document.
* **Evaluation:** Results will be evaluated by tracking the number of successfully mitigated cyber incidents and periodic vulnerability assessments.

**3.2 Objective 2: Strengthen Data Encryption Across All Systems**

* **What will be done:** Implement AES-256 encryption for data at rest, upgrade SSL/TLS to the latest version for data in transit, conduct regular encryption audits.
* **Resources Required:** Encryption software, IT personnel for system upgrades, and training.
* **Who is Responsible:** IT Security Team, Database Administrators.
* **Completion Date:** 6 months from initiation.
* **Evaluation:** Periodic audits of encryption across all systems, verification through external audits.

**3.3 Objective 3: Ensure 100% Compliance with ISO 27001 Requirements**

* **What will be done:** Conduct internal ISO 27001 audits, review and update policies, perform gap analysis before the external audit.
* **Resources Required:** Auditors, Risk & Compliance Team resources.
* **Who is Responsible:** Risk & Compliance Manager.
* **Completion Date:** Ongoing; no major non-conformities during annual audit.
* **Evaluation:** Success will be measured through audit results and management reviews.

**3.4 Objective 4: Reduce Third-Party Risks**

* **What will be done:** Develop and implement third-party security assessment protocols, ensure contracts include security requirements.
* **Resources Required:** Vendor Management team resources, security assessment tools.
* **Who is Responsible:** Vendor Management Lead, IT Security Team.
* **Completion Date:** 9 months from the start of the assessments.
* **Evaluation:** Percentage of third-party vendors that meet security compliance, monitored via vendor management platform.

**3.5 Objective 5: Increase Employee Security Awareness**

* **What will be done:** Develop comprehensive security awareness training programs, require mandatory participation for all employees, and conduct regular phishing simulation tests.
* **Resources Required:** HR personnel, IT Security Team trainers, security awareness materials.
* **Who is Responsible:** HR Manager, IT Security Team.
* **Completion Date:** 3 months for full participation.
* **Evaluation:** Success measured through attendance rates, test scores, and post-training phishing simulation results.

# 4. Communication and Documentation

**4.1 Communication**

These information security objectives will be communicated to all relevant departments and personnel through:

* Internal memos and announcements.
* Regular management meetings.
* Security awareness programs and team briefings.

**4.2 Documentation**

Documented information on these objectives and progress toward achieving them will be maintained in ABC-FinTech’s document management system and reviewed quarterly by the Information Security Steering Committee. Updates to the objectives will be made as required based on evolving risks, business needs, and regulatory changes.

# 5. Monitoring and Review

**5.1 Monitoring**

Each objective will be tracked using the following methods:

* Periodic reports from responsible departments.
* Metrics and KPIs defined for each objective.
* Internal audits and compliance checks.

**5.2 Review and Updates**

Information security objectives will be reviewed on an annual basis or when significant changes occur in the organization’s risk landscape. Adjustments will be made based on feedback from audits, risk assessments, and performance reviews.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 17 Jan 2024**