



京城銀行
King's Town Bank

Information Security Policy

File No.: IS--1001

Version: V2.1

Date of revision: 2022/05/06

Confidential level: Internal general use

Table of Content

Article 1: Purpose

Article 2: Scope of Application

Article 3: Scope of Information Security Management

Article 4: Duties and Division of Labor

Article 5: Responsibility

Article 6: Management Indicators

Article 7: Review

Article 8: Unspecified Matters

Article 9: Approval and Amendment

Article 1 Purpose

In order to protect the confidentiality, integrity, and availability of King's Town Bank's (hereinafter referred to as "the Bank") information assets, to prevent risks including inappropriate use, leakage, alteration, and damage, and to ensure the safety of the collection, handling, transmission, storage, and distribution of information.

Article 2 Scope of Application

This policy is applicable to all employees of the Bank, outsourced service vendors, and visitors.

Article 3 Scope of Information Security Management

The Bank's scope of information security management covers 14 aspects.

- I. Establishment and review of the information security policy
- II. Organization of information security
- III. Human resource security management and education training
- IV. Information asset classification management
- V. Access control
- VI. Cryptographic control measures
- VII. Physical and environmental security
- VIII. Operational security management
- IX. Communication security management
- X. System development and maintenance security
- XI. Supplier security management
- XII. Information security incident management
- XIII. Business continuity management

File No.: IS--1001

File name:Information Security Policy

Version: V2.1

Confidential level: Internal general use ☐ ☐ ☒



XIV. Compliance with applicable laws, regulations, and policies

Article 4 Duties and Division of Labor

- I. The Bank shall establish the organization of information security, coordinate the promotions of information security, and holds management review meetings at least once a year or when necessary.
- II. The Chief Information Security Officer is responsible for general affairs related to the promotion of information security policies and resource allocation.
- III. The Risk Management Department is responsible for the promotion of information security, the Information Technology Department is responsible for the execution, and the Audit Office is responsible for the audit on the promotion and execution.
- IV. The Information Security Section of the Risk Management Department is responsible for the overall management of information security implementation and shall assist the Auditing Department in reporting the results to the Board of Directors after reporting the implementation status to the Chairman of the Board every year.

Article 5 Responsibility

- I. The management shall proactively engage in and support the information security management system, and provide appropriate resources when necessary.
- II. All employees, outsourced service vendors, and visitors shall abide by this policy and are responsible for reporting information security incidents or weaknesses through appropriate reporting mechanisms.
- III. Any act that endangers information security shall be dealt with in accordance with the relevant regulations of the Bank, and the Bank

may investigate the civil and criminal liabilities according to the seriousness of the incident.

Article 6 Management Indicators

The Bank shall establish relevant management indicators to assess the achievement rate of information security goals, and shall supervise, evaluate and improve relevant matters.

Article 7 Review

- I. This Policy shall be reviewed by the Information Security Section of the Risk Management Department at least once a year, or re-examined when the organization undergoes major changes so as to comply with the latest developments in relevant laws, technology, organization, and operations.
- II. The Bank shall identify internal and external stakeholders and their feedbacks, and include those matters into the discussions at management review meetings.

Article 8 Unspecified Matters

Matters not specified in this Policy shall be handled in accordance with the relevant laws and regulations of the competent authorities and the Bank's relevant regulations.

Article 9 Approval and Amendment

The Policy shall become effective upon resolution at the board meeting, and amendments thereafter shall be approved by the Chairman.