Union Bank of Taiwan Information Security Policy

1. Purpose

To enhance the information security of Union Bank of Taiwan Co., Ltd. (hereinafter referred to as "the Bank") and ensure the security of data, systems, equipment, and networks, this policy is hereby established.

2. Objectives

The overall objective of information security is to ensure the confidentiality, integrity, and availability of the Bank’s information systems while preventing security incidents from impacting operations, thereby reducing potential operational risks.

3. Scope

This policy applies to all personnel, data, application systems, hardware equipment, data centers, network facilities, and information services of the Bank.

4. Roles and Responsibilities

None.

5. Definitions

None.

6. Operational Content

6.1 Information Security Management

The Bank’s information security management aims to prevent various potential risks and hazards caused by human error, intentional attacks, or natural disasters. The scope includes the following:

6.1.1 Division of responsibilities for information security.
6.1.2 Information security education and training.
6.1.3 Computer system security management.
6.1.4 Network security management.
6.1.5 Information asset security management.

6.1.6 System environment security management.
6.1.7 System access security management.
6.1.8 Application system development and maintenance management.
6.1.9 Physical and environmental security management.
6.1.10 Disaster recovery management for information systems.
6.1.11 Other information security management matters.

6.2 Information Security Organizational Structure

To effectively implement information security measures, the Bank adopts a three-line defense management framework for internal control:

- The **first line of defense** consists of the information technology (IT) department and all operational units, responsible for executing information security tasks.
- The **second line of defense** includes the information security unit, responsible for planning, monitoring, and implementing security policies; the legal affairs & compliance department, responsible for ensuring regulatory compliance; and the risk management department, responsible for information security risk management.
- The **third line of defense** is the audit department, which conducts security inspections and audits.

6.3 Information Security Education

Information security education and awareness training are provided for different work domains, including operations, management, IT, and security, to establish employees' information security awareness and enhance the Bank's information security governance capabilities.

6.4 Response to Information Security Incidents

In the event of an information security incident, relevant units must follow the "Information Security Incident Management Regulations" and promptly report the incident to the designated information department contact point. This allows for assessing the impact scope and formulating an appropriate response plan.

6.5 Policy Review

This policy shall be reviewed annually or upon significant changes to ensure compliance with the latest developments in laws, technology, organization, and operations, ensuring the effectiveness of information security practices.

7. Matters Not Covered

Any matters not covered in this policy shall be handled in accordance with relevant laws and the Bank's internal regulations.

8. Approval Level

This policy shall be implemented upon approval by the Board of Directors. The same applies to any amendments.

9. Related Regulations and Forms

None.