O-Bank Information Security Policy

June 23, 2025: Implementation approved by resolution of the 19th session of the 9th Board of Directors of the Company.

Article 1 Basis and Purpose

In accordance with Article 3 of BAROC (The Bankers Association of the Republic of China) Cyber Security Defense Standards of Financial Institutions, this Policy is established to ensure the confidentiality, integrity, availability, and legality of O-Bank's (hereinafter referred to as "the Bank") information assets, and to protect the Bank from internal and external intentional or accidental threats, and to consider the business needs of the Bank.

Article 2 Scope of application

All staff of the Bank (incl. all employees, contract employees, dispatched personnel), third-party vendors shall comply with this policy.

Article 3 Definitions

1. Information assets: The assets related to information processing, including hardware, software, data, documents, and personnel, classify into information assets.
2. Confidentiality: Ensure that the information is only accessed by authorized users.
3. Integrity: Ensure the degree of accuracy and completeness of information and processing methods.
4. Availability: Ensure that authorized users have timely access to information and related assets when they needed.

Article 4 Information security objectives

The information security objectives of the Bank are as follows:

1. Ensure the confidentiality of the Bank's information assets, implementation of the data access controls. And the information access is restricted to authorized personnel.
2. Ensure the integrity of the Bank's information assets to avoid unauthorized changes.
3. Ensure business continuity of the Bank's information activities.
4. Ensure the Bank's information activities to meet the requirements of relevant laws and

regulations.

Article 5 Information security controls

The information security controls of the Bank are as follows:

1. Management shall be committed to maintaining information security, continuously improving the quality of information security management system to address information security risks, and reducing information security incidents to protect the rights and interests of clients.

2. All personnel of the Bank are under obligation to protect the information assets in their procession, custody, and use.

3. To prevent unauthorized changes and the misuse of information or service, task assigning shall consider the division of labor, and the duties and the areas of responsibility shall be segregated.

4. The Bank shall review and publicize the Bank's information security policies to the third-party vendors that have rights to access the Bank's information assets in accordance with the contracts. The vendors shall comply with this policy and BAROC's Directions for Risk Management of Cyber Systems and Service Supply Chain of Financial Institutions, and be responsible for protecting the Bank's information assets they access, keep and use.

5. Ensure the security of the workplace to prevent theft and damage of information assets.

6. Implement communication security management.

7. In principle, those who need to get remote access to the Bank shall use Virtual Desktop Infrastructure (VDI) or Virtual Private Network (VPN) by granting minimum privilege, and comply with the Bank's regulations related to information security.

8. The Bank shall actively monitor cybersecurity risks, respond to cybersecurity threats and be attention of the information security incidents, security vulnerabilities and the possibility of security policy violations whether they happened, and report the information security incidents, responding to incidents promptly, and implementing mitigation measures in accordance with the process. It shall instantly disclosure the situation of incidents to affected stakeholders when information incidents occur, and outline following actions to address incidents and to prevent related future risks.

9. Adopt mobile device security controls to manage the risks associated with the use of mobile devices.

10. Establish an organization for information security management to maintain the operation of the information security management system, identify the internal and external issues of the information security management system, determine requirements and expectations of stakeholders for the Bank. Regularly conduct the tasks of information asset classification, risk assessment and information security objectives. Comply with the external and internal laws and regulations, establish appropriate control process and timely update, and periodically conduct an information security audit.

Article 6 Annual review

This policy shall be reviewed at least once a year to conform to laws, regulations and the latest developments in information business, and amended if necessary.

Article 7 Supplementary provision

1. The procedures related to this policy shall be formulated by the information departments and implemented after approved by the president, and the same applies when amended.

2. This policy implements after approved by the Board, and the same applies when amended.