First Financial Holding Co., Ltd. Information Management and Information Security Policy

Article 1 **(Objective)**

First Financial Holding Co., Ltd. ("the Company") has established the Information Management and Information Security Policy ("this Policy") for improving the overall operating performance, **developing the information resource sharing mechanism of the Financial Holding Group ("the Group") and strengthening the information security management, so as to achieve the information security objectives such as confidentiality, integrity, availability, and legitimacy of information operations**.

Article 2 **(Organization and duties)**

A Chief Information Security Officer ("CISO") has been established in the Company, who is responsible for establishing and implementing the information security system, and supervising the information management, information security and other relevant business operations. The Information Technology Division shall be the execution and management unit.

The information security risk management and inspection shall continue to be managed, coordinated and followed up by the relevant competent units in accordance with its authorities.

Article 3 **(Information development and investment plan reviews)**

The Group's comprehensive information business development plan and the information plan among subsidiaries are overall organized by this Company. The subsidiaries may be entrusted to handle the aforementioned plans in accordance with actual operational needs.

Subsidiaries' information development and investment plan and the modification of such a plan shall be submitted to the Information Technology Department of the Company for review.

Article 4 **(Information resource and service sharing)**

The information resource and service sharing mechanism is overall organized by this Company. The subsidiaries may be entrusted to

handle the establishment, management, and maintenance operations in accordance with actual operational needs.

Article 5 **(Appointment of information operations)**

If a contract is entered into between the Company and its subsidiary or between subsidiaries **with respect to** the mutual entrustment of information processing among each other, the contract shall **clearly** regulate the rights and obligations of both parties, the scope of use, cost allocation, and information confidentiality agreements.

Article 6 **(Network integration and sharing)**

Relevant protection and authority management mechanisms shall be established for network integration and sharing between the Company and its subsidiary or between subsidiaries.

Article 7 **(Data and information exchange)**

For the exchange of transaction data and information among different information systems between the Company and its subsidiary or between subsidiaries, an authority management mechanism shall be **established** in order to regulate the access scope of relevant personnel.

Article 8 **(Customer relationship management and cross-selling)**

When it is necessary to disclose, refer or exchange customer information for the purposes of cooperating with the Group's customer relationship management and cross-selling, it shall comply with relevant laws and regulations and an appropriate access authority mechanism shall be established.

Article 9 **(Scope of information management and information security regulations)**

In order to support the overall business development of the Group and ensure the effective use of information resources, and also consider the security of information systems and operations, the Company and its subsidiaries shall establish relevant information management **and information security** regulations in accordance with industry characteristics. The main content shall include the

following:

1. Software management **including system development and maintenance management (subcontracting development is included)**

2. **Information operating entity and environmental management**

3. Network **and communication security** management

4. Data and documentation management **including backup and data exchange**

5. **Information equipment authorization and protection management**

6. Internet application management

7. Information operations related personnel management

8. Information security defense, monitoring, and detection

9. Use of emerging technology management

10. Information security education and training

11. Crisis handling **including information security incident** management

12. **Information operation continuing management**

13. Regularly perform information security self-check operations and follow up on management improvement issues

14. Other information security management matters

The relevant information management **and information security** regulations of **each subsidiary** should be submitted to the Company for reference.

Article 10 (Information security enhancement measures and reporting information security incident)

The Company and its subsidiaries shall, in accordance with the development trends of information technology, take appropriate information security enhancement measures to reduce the risk of data being stolen, tampered with, damaged or leaked.

During information operations, the Company and its subsidiaries

shall report any abnormal information security incident in accordance with applicable regulations.

Article 11 (Information operation outsourcing management)

When outsourcing information operations, the responsibilities and confidentiality requirements of the service provider for information management and information security shall be incorporated into the contract. Furthermore, the liabilities for a breach of contract shall be clearly specified.

Article 1**2** **(Information system redundancy and disaster recovery plan)**

The Company and its subsidiaries shall establish a information system redundancy and disaster recovery plan, and conduct regular drills**.** The results of the drills shall be recorded for future reference.

Article 1**3** **(Compliance with other information operation management regulation)**

If subsidiaries must establish separate information operation management regulations due to cooperation with the competent authority's requirements or participation in the joint systems of international organizations, governments, enterprises or banks**,** it shall be handled in accordance with such regulations.

Article 1**4** **(Policy evaluation)**

This Policy shall be evaluated at least once per year or reassessed when there is a material change, so as to make sure that this Policy complies with applicable legislations and technologies, and is suited to the most current organizational and operational business practices.

Article 1**5** **(Other regulations)**

Matters not covered in the Policy shall be processed in accordance with the applicable laws of the competent authorities and the related regulations of the Company.

Article 1**6** **(Appendix)**

This Policy, and any amendment hereto**,** shall be issued and

implemented once it has been approved by the Board of Directors.

Article 1**7** **(Dates of enforcement and amendment)**

This Policy was established on March 18, 2004.

The first amendment was made on April 21, 2022.