

E.SUN Financial Holding Co., Ltd. Information Security Policy

Established on 2008.8.14 during the 3rd Meeting of the Third Board of Directors
Amended on 2017.11.2 during the 5th Meeting of the Sixth Board of Directors
Amended on 2021.08.20 during the 15th Meeting of the Seventh Board of Directors
Amended on 2025.6.23 during the 8th Meeting of the 24th Board of Directors

Chapter I General provisions

Article 1 E.SUN Bank adopts this Policy to ensure the confidentiality, completeness, and availability of important information of this Company and its subsidiaries, maintain accuracy and consistency of information, prevent unauthorized access, alteration, or destruction, and thereby support the sustainable operation of the Company.

Article 2 The Company and its subsidiaries shall establish relevant information security management regulations and procedures according to this Information Security Policy to serve as important bases for information security management.

Chapter II Authority and Responsibilities of Information Security

Article 3 Authority and Responsibilities of Information Security

- I. The Information Security Management Division is the primary unit responsible for overseeing information security governance, information security risk management, and information security implementation across the Company and its subsidiaries. It also regularly consolidates and reports key information security matters to the Company's Board of Directors.
- II. In order to integrate the information security resources of the Company and its subsidiaries, the "Information Security Management Committee" is in charge of the supervision and coordination of information security related policies of the Company and its subsidiaries, and the operations of related measures and mechanisms.
- III. The drafting of the Company's information security measures and technical regulations, and the research and establishment of security technology, are handled by the department assigned to implement information security for the Company.
- IV. The study, usage management, protection, and confidentiality maintenance of the Company's information and report security are handled by various related departments.

Chapter III Guiding Principles for Information Security Management

Article 4 The Company and its subsidiaries shall review the properties of their information operations, refer to the following information security management items to establish information security management system and continuously evaluate and improve them.

- I. Information security policy
- II. Authority and responsibilities of information security
- III. Staff security management
- IV. Computer systems security management
- V. Network security management
- VI. System access control
- VII. System development and maintenance security management
- VIII. Physical and environmental security management
- IX. Business Continuity Management Security Principles
- X. Third-Party Information Security Management Requirements
- XI. Information security incident emergency reporting procedure, response and drill mechanism
- XII. Monitoring, Assessment, reporting and response mechanism regarding information security threats and information

Article 5 The information management departments of the Company and its subsidiaries must list all its application systems and information security operating procedures, and assign administrative staff to be in charge of the systems' management, operation, and maintenance.

Article 6 The Company and its subsidiaries must strictly comply with the system's information security operation procedures so as to comply with the Company's information security requirements.

Article 7 All employees of the Company and its subsidiaries are required to comply with this policy and related information security regulations, and are responsible for safeguarding information security and protecting data.

Article 8 When an important information system of the Company and its subsidiaries is being developed or revised, relevant information security protection measures must be taken into consideration.

Article 9 The Company must establish information security defense mechanisms for the business, transactions, and exchange and use of information with and between its subsidiaries.

Article 10 For business operations involving third-party access and outsourcing of data and information systems, the Company and its subsidiaries shall establish information security requirements that third-party personnel or vendors must comply with, as well as enforce confidentiality responsibilities and obligations regarding business secrets.

Chapter IV Supplementary Provisions

Article 11 The Policy shall be reviewed at least once a year to reflect the latest developments in government regulations, technology and business to ensure the effectiveness of information security practices.

Article 12 Any matters not covered in the Policy shall be handled in accordance with relevant laws and regulations and the Company's relevant regulations.

Article 13 The Policy shall come into effect once approved by the board of directors.