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

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.

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. 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 or information security related policies of the Company and its subsidiaries, and the operations of related measures and mechanisms.

II. 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.

III. 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 to establish information security management regulations and procedures which include part or all of the information security management items listed below:

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. Information security incident emergency reporting procedure, response and drill mechanism
X. Assessment, reporting and response mechanism regarding information security 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 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 8 The Company must establish information security defense mechanisms for the business, transactions, and exchange and use of information with and between its subsidiaries.

Chapter IV Supplementary Provisions

Article 9 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 10 Any matters not covered in the Policy shall be handled in accordance with relevant laws and regulations and the Company's relevant regulations.

Article 11 The Policy shall come into effect once approved by the board of directors.