E.SUN Bank Policy on Internal Control System

Established on the 15th meeting of the 6th Term by the Board of Directors on November 15, 2007

Approved on the 9th meeting of the 7th Term by the Board of Directors on November 12, 2009

Amended on the 7th meeting of the 8th Term by the Board of Directors on March 16, 2012

Amended on the 5th meeting of the 9th Term by the Board of Directors on November 14, 2014

Amended on the 11th meeting of the 9th Term by the Board of Directors on August 21, 2015

Amended on the 23rd meeting of the 9th Term by the Board of Directors on March 24, 2017

Amended on the 25th meeting of the 9th Term by the Board of Directors on April 28, 2017

Amended on the 9th meeting of the 10th Term by the Board of Directors on August 10, 2018

Amended on the 17th meeting of the 10th Term by the Board of Directors on November 13, 2019

Amended on the 20th meeting of the 10th Term by the Board of Directors on April 24, 2020

Amended on the 16th meeting of the 11th Term by the Board of Directors on November 12, 2021

Amended on the 7th meeting of the 12th Term by the Board of Directors on November 13, 2023

Amended on the 13th meeting of the 12th Term by the Board of Directors on August 16, 2024

Chapter I General Principles

Article 1 This system is formulated in accordance with the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries," "Regulations Governing Establishment of Internal Control Systems by Public Companies," "Guidelines for Bank Corporate Governance," and the "Code of Practice for the Three Lines of in Internal Control of Banks."

Article 2 The basic objectives of this system are to promote sound operations and sustainable development and, through joint compliance by the Board of Directors, management, and all personnel, to reasonably ensure that the following objectives are achieved:

(1) Effectiveness and efficiency of operations;

(2) Reliability, timeliness, transparency and compliance of reporting; and

(3) Compliance with applicable rules and regulations.

The objective of effectiveness and efficiency of operations referred to in subparagraph 1 of the preceding paragraph includes objectives such as profits, performance, and safeguarding asset security.

The reporting referred to in subparagraph 2, paragraph 1 includes internal and external financial reporting and non-financial reporting of a financial holding company or banking business. The objective of external financial reporting includes ensuring that financial reports presented to external users are prepared in accordance with the generally accepted accounting

principles and that all transactions are properly approved.

Chapter II Principles and Scope

Article 3 The Board of Directors shall approve and annually review overall business strategies, sustainable development, and major policies. The Board of Directors should also be aware of the operational risks faced by the company or business, supervise its operating results and bears the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective internal control system.

Article 4 The control environment of the Bank includes integrity and ethical values, the governance oversight responsibilities of the Board of Directors and the audit committee, organizational structure, assignment of authority and responsibility, human resources policy, performance measures, awards and disciplines, and sustainable operation objectives. The Board of Directors and management should establish internal code of conduct, including code of conduct for directors and code of conduct for employees.

Article 5 The internal control system should enable effective management. The management should consider the impact of changes in the external environment and within its own business model, as well as sustainable development and possible fraud scenarios. The risk assessment results can assist the Bank in designing, correcting, and implementing necessary controls in a timely manner.

Article 6 Control operations are actions of adopting proper policies and procedures based on the risk assessment results to control risks within a tolerable range. Control operations shall be performed at all levels of a financial holding company or business, at various stages of business processes, and over the technological environment, appropriate segregation of duties and that management and employees should avoid assuming conflicting responsibilities.

Article 7 The internal control system must have mechanisms to generate information necessary for planning, implementation, and supervision and to enable timely access to information by those who need it, and the system should maintain comprehensive internal financial, operational and compliance data. An effective internal control system shall also establish effective channels of communication.

Article 8 The operating units and business management units of the Bank shall

perform ongoing evaluations, meaning routine evaluations of their operational processes. Internal auditors should conduct individual evaluations and communicate any identified deficiencies of the internal control system to senior management, the Board of Directors, and the audit committee, and improvements shall be made in a timely manner.

If audit personnel and compliance officers propose improvement suggestions for significant deficiencies or illegal activities in the internal control system that are not adopted by management, potentially causing substantial losses to the bank, they shall promptly report and notify independent directors or the audit committee. Simultaneously, they should report to the competent authority immediately.

Article 9 The internal control system should cover the Bank's operational activities and the management of sustainability-related information, in compliance with industry regulations, including controls for various types of transaction cycles. Proper policies and procedures should be formulated and promptly revised. The Bank’s organizational codes or business guidelines, including organizational systems, departmental responsibilities, business scope, and hierarchical authorization methods, should be defined. Each department should establish the following business-related regulations and manuals:

(1) Cashier, saving, exchange, loaning, foreign currency, trust, insurance, and new financial products.

(2) Investment guidelines and shares management.

(3) Customer data confidentiality.

(4) Regulation on interested party transactions.

(5) Management of board meetings.

(6) Management of the preparation process of financial statements, including management of the application of International Financial Reporting Standards, procedures for professional accounting judgments, and processes for making changes in accounting policies and estimates.

(7) Management of administration of general affairs, information, and personnel affairs (including regulations for regular transfer and vacation).

(8) Management of operations for disclosing information externally.

(9) Outsourced operations management.

(10) Management of financial examination reports.

(11) Management of protection of financial consumers.

(12) Mechanism for anti-money laundering and combating the financing of terrorism and management of compliance with relevant laws and regulations, including the management mechanism for identifying, assessing, and monitoring anti-money laundering and combating the financing of terrorism risks, and anti-money laundering and combating the financing of terrorism plans based on risk assessment results.

(13) Management of shareholder services operations.

(14) Management of personal data protection.

(15) Management of audit committee meetings.

(16) Mechanism for handling major contingencies.

(17) Management of internal control systems related to simultaneous operations of securities business.

(18) Internal credit rating management.

(19) Other operational guidelines and operating procedures.

The stipulation, revision, or abolition of all operational and management regulations mentioned above should be coordinated with changes in laws, business items, and process flows, reviewed and revised at least annually, and requiring the participation of legal compliance, internal audit, and risk management agencies when necessary.

Article 10 The self-assessment of the internal control system should incorporate effectiveness evaluation items of the internal control system.

Chapter III The Three Lines of Defense in Internal Control

Article 11 The Bank shall establish a three lines of defense framework for internal control, clearly defining the scope of responsibilities for each line of defense. This framework allows various units to understand their specific roles within the overall risk and control structure of the bank, enhancing communication and coordination in risk management and internal control tasks. Each line of defense shall perform its respective duties.

Article 12 The Board of Directors and executive management should actively assist and guide the establishment of the three lines of defense. They must clearly define the roles, functions, and responsibilities of each line of defense,

continuously ensure that the organizational structure aligns with the principles of the three lines of defense, and oversee the effective operation of this framework, bearing ultimate responsibility for its effectiveness.

When establishing the three lines of defense framework, executive management should consider the nature, size, complexity, and risk conditions of various operational activities to make necessary adjustments, while ensuring the effectiveness of the three lines of defense.

Section 1 The First Line of Defense

Article 13 The first line of defense refers to the various units within the Bank that are responsible for the risks arising from their daily operations and functions. Each unit is tasked with identifying and managing these risks and designing and implementing effective internal control procedures tailored to the specific nature of these risks, covering all related operational activities.

Article 14 The first line of defense is responsible for and continuously manages the risks generated by operational activities, including the following aspects:

(1) Continuously identify, evaluate, control, and mitigate risks associated with their operational activities to ensure that these activities are aligned with the Bank's objectives and mission.
(2) Control risks within the unit’s capability to handle and, when necessary, report exposures to the second line of defense.
(3) Develop and implement internal control procedures.
(4) Implement and maintain effective internal controls and risk management processes.
(5) Propose improvement plans immediately if processes and control procedures are found to be inadequate.

The first line of defense shall conduct regular or occasional self-assessments on the above responsibilities to ensure that risks are appropriately managed.

Section 2 The Second Line of Defense

Article 15 The second line of defense is independent from the first line and distinct from the third line, consisting of other functions and units that assist and supervise the first line in identifying and managing risks. The second line of defense includes risk management, legal compliance, information security, and other specialized units (such as financial control, human

resources, legal, etc.). These units are responsible for formulating the overall risk management policy, overseeing the bank's risk-taking capacity and current risk exposure, and reporting risk control situations to the Board of Directors or executive management.

Article 16 The function of the second line of defense is to establish overall policies and create management systems, assisting and supervising the first line of defense in managing risks and conducting self-assessments. Depending on the nature of its functions, the responsibilities of the second line of defense include helping to identify and measure risks, defining risk management roles and responsibilities, providing a risk management framework, and regularly reporting risk management results to the executive management.

Article 17 To comply with legal regulations, a compliance system should be established, managed, and executed by the compliance unit. This unit is responsible for developing the assessment content and procedures for legal compliance and overseeing periodic self-assessments of compliance by various departments. A senior executive should be appointed as the chief compliance officer of the head office to oversee compliance-related matters. This officer should report at least every six months to the Audit Committee and the Board of Directors. If any major legal violations are found or if the financial supervisory authorities reduce the institution's rating, the Board should be immediately notified, and compliance matters should be reported to the board.

The chief compliance officer of the head office may concurrently serve as the head of the unit responsible for anti-money laundering and counter-terrorist financing, but may not concurrently serve as the head of the legal department or hold any other internal positions.

Article 18 The Bank shall formulate appropriate risk management policies and establish an independent and effective risk management mechanism to evaluate and oversee the overall risk-taking capacity and current risk exposure of the bank and its subsidiaries, determine risk response strategies, and ensure adherence to risk management procedures.

The risk management policies should be approved by the Board of Directors and reviewed and revised as necessary.

Article 19 The risk management unit shall report on risk control to the Board of Directors at least quarterly. Immediate measures should be taken, and the

board informed if significant exposures that endanger financial or business conditions or compliance with laws are discovered.

Article 20 The bank shall establish appropriate information security policies and an independent and effective information security management system to promote, coordinate, supervise, and improve the operation of the bank's information security management system. This aims to effectively control information security risks and meet the overall operational needs of the company.

A dedicated information security unit with operational independence shall be established to plan, monitor, and execute information security management operations, headed by a designated information security unit officer who oversees all information security matters.

The information security policy shall be approved by the Board of Directors and reviewed and revised as necessary.

Section 3 The Third Line of Defense

Article 21 The third line of defense consists of the internal audit unit, which shall conduct audit activities with an independent and objective mindset. This unit assists the Board of Directors and executive management in verifying and assessing the effectiveness of risk management and the internal control system, measuring operational efficiency, and evaluating the effectiveness of risk monitoring by the first and second lines of defense. It shall also provide timely improvement recommendations to ensure the continuous and effective implementation of the internal control system and serve as a basis for reviewing and revising the internal control system.

Article 22 The bank shall establish an internal audit unit that reports directly to the Board of Directors and define the organization, staffing, and responsibilities of internal audits. The Chief Audit Executive shall oversee audit activities independently and objectively, reporting to the audit committee and the Board of Directors at least quarterly.

Article 23 The internal audit unit shall compile internal audit work manuals and working papers, which should at least include assessments of the internal control system's provisions and business processes to determine whether current procedures have appropriate internal controls, whether all units are effectively implementing these controls, and whether the controls' effectiveness is reasonable. Improvement suggestions should be provided

as needed.

Article 24 The internal audit unit shall continuously track and review audit comments or deficiencies identified by financial inspection authorities, auditors, internal audit units (including parent company internal audit units), and internal units, as well as items listed in internal control declarations that require improvement. The tracking results should be reported in writing to the Board of Directors or audit committee and included as key factors in evaluating the performance and rewards or penalties of individual units.

Article 25 Following an inspection by competent authorities or receipt of an inspection report from local authorities of overseas branches, the internal audit unit at headquarters shall immediately inform the directors of any significant findings and report at the next board meeting. The report should include the contents of the inspection communication meeting, major inspection deficiencies, downgrades by financial authorities, significant improvement plans required by the authorities, or potential disciplinary measures.

Article 26 Internal auditors shall perform their duties with an independent and objective attitude, adhering to professional diligence. In addition to reporting audit activities to the audit committee quarterly, the chief auditor should also attend board meetings to report.

Prohibited Conduct for Internal Auditors:

(1) Concealing or making false disclosures about operating activities, reports, and compliance conditions that directly harm stakeholders, despite knowing such conditions exist.
(2) Neglect of duty that results in harm to the Bank or stakeholders.
(3) Engaging in actions beyond audit responsibilities or other improper conduct, including disclosing information obtained for personal gain or to the detriment of the bank.
(4) Auditing departments where they were previously employed within the past year.
(5) Failing to recuse themselves from auditing activities for tasks they previously executed or where there is a conflict of interest.
(6) Directly or indirectly offering, promising, requesting, or accepting unreasonable gifts, hospitality, or other forms of improper benefits from Bank personnel or clients.
(7) Failing to cooperate in audit matters instructed by competent

authorities or providing relevant information.

(8) Engaging in activities prohibited by laws or regulations or stipulated as forbidden by competent authorities.

The bank shall continuously check whether internal auditors are violating the above regulations. If any violations are found, their duties shall be adjusted within one month from the date of discovery.

Section 4 Coordination Among the Three Lines of Defense

Article 27 Coordination among the three lines of defense, based on their respective roles in the risk management and internal control framework, shall be governed by the following principles:

(1) The construction of risk management and control processes shall follow the three lines of defense framework.

(2) Each line of defense shall accurately execute and manage relevant tasks based on their defined roles and responsibilities.

(3) The lines of defense should coordinate with each other to enhance effectiveness and efficiency.

(4) Results from the risk management and control functions of each line of defense should be shared to facilitate all functions in effectively fulfilling their duties.

Chapter IV Supplementary Provisions

Article 28 If managers or related personnel violate the provisions of this system, they shall be disciplined in accordance with the "E.SUN Bank Employee Reward and Disciplinary Guidelines."

Article 29 The Bank shall ensure the confidentiality of financial inspection reports. Unless permitted by law or approved by the competent authorities, neither responsible officers nor employees shall view, disclose, deliver, or publicize any part of the financial inspection reports to personnel not related to the execution of their duties.

The bank shall formulate internal management regulations and operational procedures related to financial inspection reports and submit these for approval by the Board of Directors.

Article 30 The Policy shall be implemented after being approved by the Board of Directors