Nan Shan Life Insurance Company Limited

Information Security Policy

Enacted: November 4, 2014

Amended: March 21, 2019

March 29, 2022

August 28, 2025

Article 1. Purpose

This Policy is hereby established to ensure the confidentiality, integrity, availability, and legality of the Company's information assets during operations and service delivery. To prevent internal and external intentional or accidental threats, a continuous improvement management model based on the "Plan-Do-Check-Act" (PDCA) cycle is adopted, and an information security management system compliant with relevant regulations is established.

Article 2. Scope of Application

This Policy applies to all information operation activities performed by information users.

Article 3. Definitions

The terms used in this Policy are defined as follows:

(1). Confidentiality:

Ensuring that information is not made available or disclosed to unauthorized individuals, and access is limited to authorized personnel only.

(2). Integrity:

Protecting the accuracy and completeness of information to ensure it is correct, reliable, and unaltered.

(3). Availability:

Ensuring that information and related services are accessible and usable by authorized individuals when needed.

(4). Legality:

Conducting all information-related activities in accordance with applicable regulations set forth by competent authorities.

(5). Information Assets:

Includes information systems, software, hardware, environments, documentation, communication systems, data, and personnel.

(6). Information Users:

Individuals authorized to use or manage information assets, including but not limited to employees, sales agents, contractors or temporary staff, vendors (e.g., implementation and maintenance vendors, outsourced IT service providers, and cloud service providers).

Article 4. Policy Compliance

All information users must comply with this Policy.

Article 5. Compliance Requirements

(1). The following declarations are made under this Information Security Policy:

a. The Company has established an information system management system based on relevant regulations set forth by competent authorities. Through periodic internal and external audits, the Company ensures continuous improvement and strengthens security controls over its information assets, including but not limited to information systems, software, hardware, environments, documents, communications, and data, etc.

b. All information users are responsible for implementing the requirements of this Policy through appropriate procedures and must uphold the responsibility of maintaining information security.

c. All information users when utilize information assets must adhere to confidentiality obligations and follow all relevant policies and procedures.

d. The Company establishes information security standards and relevant contractual terms with business partners and information operation vendors (e.g., outsourced IT service providers, cloud service providers, etc.). Through conducting

information security reviews or audits, the Company ensures their compliance with its information security policies, thereby safeguarding the integrity of the information security supply chain. The vendors shall observe the following:

- Comply with confidentiality obligations and relevant laws.
- Take appropriate security measures to protect the services provided to the Company.
- Bear liability for any damages caused by security incidents.
- Ensure proper transfer, deletion, or destruction of data upon service termination.

e. The Company enforces strict measures to protect personal data, financial data, and operational records from unauthorized access, tampering, or disclosure in accordance with the "Personal Data Protection Act" and relevant financial supervisory regulations.

f. Both internal personnel and vendor suppliers must stay alert to potential weaknesses or threats, and report any incidents or suspicious issues through the appropriate reporting channels in accordance with the Information Security Incident Reporting and Management Procedure.

g. In the event of a material information security incident, the Company shall process in accordance with the "Information Security Incident Reporting and Management Procedure" and the "Nanshan Life Insurance Co., Ltd. Material Contingency Event Handling Guidelines." Incident handling shall be transparent and communicated to affected stakeholders with timely updates and remediation measures. Post-incident, a comprehensive vulnerability assessment and root cause analysis shall be conducted, and relevant personnel may be subject to disciplinary or legal action based on the severity of the incident.

(2). To effectively implement information security management and protection throughout the data lifecycle, the Company shall adopt the following information security control measures:

a. Identify data, information, and corresponding access rights, and establish appropriate access control procedures.
b. Conduct periodical risk assessments and risk management for information assets.
c. Ensure proper backup and management of critical information and records.
d. Maintain the security of work areas and operational equipment to prevent damage that may disrupt normal operations.
e. Ensure the correct and secure operation of information equipment.
f. Establish and periodically conduct business continuity plans, and update them in line with organizational development and operational needs.
g. Implement secure controls for communication networks.
h. Ensure the acquisition, development, and maintenance of information systems comply with the Company's internal standards.
i. Enforce management protocols for information service vendors.
j. Establish internal control procedures in compliance with applicable laws and regulations and conduct periodic information security audits.
k. Conduct periodical information security training programs to promote awareness of the information security policy and relevant implementation guidelines.

(3). The Company shall appoint a person at the level of Vice President or above, or an individual with equivalent responsibilities, to concurrently serve as the Chief Information Security Officer (CISO), responsible for overseeing the promotion of information security policies and the coordination of related resources. The CISO shall report the overall implementation status of information security to the Board of Directors once a year. The Company shall also establish a dedicated information security unit with independent authority, which shall not concurrently engage in

information operations or other affairs that may create conflicts of interest. A person at the level of Associate Vice President or above, or with equivalent responsibilities, shall be appointed as the head of this dedicated unit, responsible for planning, monitoring, and executing information security management operations. Appropriate human resources and equipment shall be allocated to this unit. Personnel in the dedicated information security unit shall perform tasks assigned by the head of dedicated information security unit related to information security management.

(4). This Policy shall be reviewed at least annually or revised as needed in response to regulatory requirements or technological developments, to ensure the effectiveness and feasibility of the information security management system.

(5). Matters not covered in this Policy shall be handled in accordance with relevant laws, the self-regulatory standards published by the Life Insurance Association of the Republic of China, and the Company's internal regulations. If any updates to laws or self-regulatory standards conflict with the provisions of this Policy, the most recent legal or self-regulatory requirements shall prevail, even before the Policy is officially revised.

Article VI. Implementation

This Policy shall be approved by the Board of Directors, and any subsequent amendments to the policy also require board approval.