[Translation]

Information Security Policy

1. Introduction

1.1. Objectives

To secure assets of Thai Life Insurance Public Company Limited (the "Company"), particularly information assets utilized in business operations, by protecting from threats and risks regarding information technology both inside and outside of the Company. To protect against illegal action or cause of damage to other persons whether by intentionally or unintentionally. To reduce the damage that may occur from security breaches, and to maintain the ability to operate the business continuously.

1.2. Scope

- All information (both in the form of physical documents and/or electronic information) which is stored, used, disclosed and/or utilized for communication of the Company's operations.
- Internal personnel including directors, sub-committees, non-executive directors, executives, full-time employees, and temporary employees; external personnel including third parties employed by the Company, business partners, companies or contracting counterparties, business representatives, service providers including personal representatives and Company's sale agent, who involve in the use of the Company's information and information systems.
- All assets which is related to information and used to store, transfer or process information, including servers, software, programs, electronic information, publications, tools, facilities as well as the services received.

1.3. Definition

- "MR" means Management Representative which is ISMR or ISMA (Refers to ISMS-PL09 ISMS Manual)

2. Policy

2.1. Information Security Policy

1) To prevent information (regardless of the form of the storage) from any breach which may affect the confidentiality, integrity and availability of the information
2) To comply with ISO/IEC 27001 standard and other standards, as well as the information Security Policy set by the Company for information security
3) To comply with any other applicable laws and regulations.

The Company has the policies as follows:

1) The Company's essential information must be protected from unauthorized access.
2) The Company's essential information must be properly maintained in its confidentiality.
3) The Company's essential information must be accurate and complete.
4) The Company's essential information must always be available.
5) All relevant laws, rules, and regulations must be complied accurately and completely.
6) The Company must prepare a complete and comprehensive report of information assets that includes assets relating to equipment and computers, information systems and information.
7) Internal personnel should receive information security training.
8) Internal personnel must perform their duties with awareness of the information security.
9) Providing the IT Risk and Cybersecurity management that are related to the security of information technology systems and the Company’s information.
10) Providing management plan to facilitate the continuing operation of the Company, as well as maintaining and testing the plan appropriately.

11) Providing a set of information security policy documents and relevant supporting documents to establish rules and regulations, and operational guidelines on secure information usage.
12) Providing an appropriate procedure for reporting, examining, investigating, mitigating, and managing information security breaches. Any breach of information security, abnormality, and other suspicious events must be reported to MR for further investigation and remedy, the Board of Directors or sub-committees, and legal external authorities in case of major incidents.

2.2. Compliance with Policies and Auditing

1) Internal personnel and other relevant personnel must acknowledge the Company's Non-Disclosure Agreement and/or other related guidelines to agree that the information obtained and used during operation duty is the Company's asset and cannot be used for any other purpose without permission. Upon any use of the Company's information, it is considered that the person acknowledged and agreed to comply with all conditions under this policy.

2) Intentional access to information systems without permission, deliberately providing incorrect information and intentional changes to information without permission are prohibited. Failure to comply with this Information Security Policy is considered a disciplinary offense. In order to ensure that this policy is strictly followed, the Company has established a process to monitor employees' and other relevant personnel's performance from time to time through the assessment of internal audit function and the audit of related Security Logs / Audit Trails. The Company reserves the right to take any action that is considered necessary to manage and protect the security of the Company's data and information systems.

2.3. Reviewing and Updating Policy

Information Security Policies, procedures, and any other guidelines shall be reviewed and updated by management at least once a year to ensure that its content is complete, effective, and can be used appropriately.

2.4. Penalties

Any breach, violation, negligence, or non-compliance with the policy, work instruction, and relevant supporting documents whether intentional or not, the Company may consider penalties at its discretion or disciplinary action in accordance with the Company's policies. Any breach or violation of the policy is deemed to be an illegal act, the Company may consider further legal proceedings.

(The policy shall be effective as of 22 August 2023 onwards.)