[Translation]

ISMS Policy

1. Introduction

1.1. Objectives of the ISMS System

- To protect and ensure data and information systems security and assure confidence among stakeholders.
- To establish efficient processes for managing information security within the Company and serve as a crucial foundation for good corporate governance.
- To support business growth and Company operations.
- To establish a foundation for compliance with laws and regulations related to information security.

1.2. Scope

Encompasses the information security management system of the Company's Data Center

1.3. Definition

- "Company" refers to Thai Life Insurance Public Company Limited.
- "MR (Management Representative)" refers to the representative of the standard management system, in this case, it could be either ISMR or ISMA.
- "ISMS (Information Security Management System)" refers to the system for managing information security within the Company.
- "Internal Context" refers to internal factors that are considered when determining the scope of the ISMS system.
- "External Context" refers to external factors that are considered when determining the scope of the ISMS system.

2. Context of the Organization

The Company has defined the context of the organization, which covers the internal context, external context, and the needs and expectations of interested parties, as follows:

2.1. Internal Context

- To ensure compliance with Company policies.
- To align with the Company's strategic objectives, ensuring reliability, efficiency, responsiveness to management's needs and expectations.
- Efficient management of existing resources within the Company.
- Establishing effective processes for managing information security within the Company and laying the foundation for the implementation of information security management processes in other areas of the Company.
- To establish an information security management system for the Company in accordance with international standards (ISO/IEC 27001).

2.2. External Context

- To protect against threats and risks to information security.
- Compliance with regulations from the Office of Insurance Commission (OIC).
- Compliance with laws and regulations issued by relevant regulatory bodies.
- To build confidence in customers and users of the Company that the information system is secure.
- To prepare for emergencies and various incidents to minimize damage and enable continuous operation, such as system downtime and cyber-attacks.

2.3. Needs and expectations of interested parties:

- The expectations of management are to ensure effective governance, efficient operations, reliability, support for company growth, and customer/user confidence.
- Customers and users expect their data to be secure, confidential, not accessed, and/or changed without permission.
- Compliance with relevant laws, regulations, and agreements, such as the Computer Crime Act (No. 2) B.E. 2560, is necessary.

3. Scope of the ISMS:

Scope of the ISMS:

"The Information Security Management System applies to Data Center including Support Infrastructure, Network, and Facilities operated by Thai Life Insurance Public Company Limited. This is in accordance with the Statement of Applicability (SOA)."

Location:

Thai Life Insurance Public Company Limited.

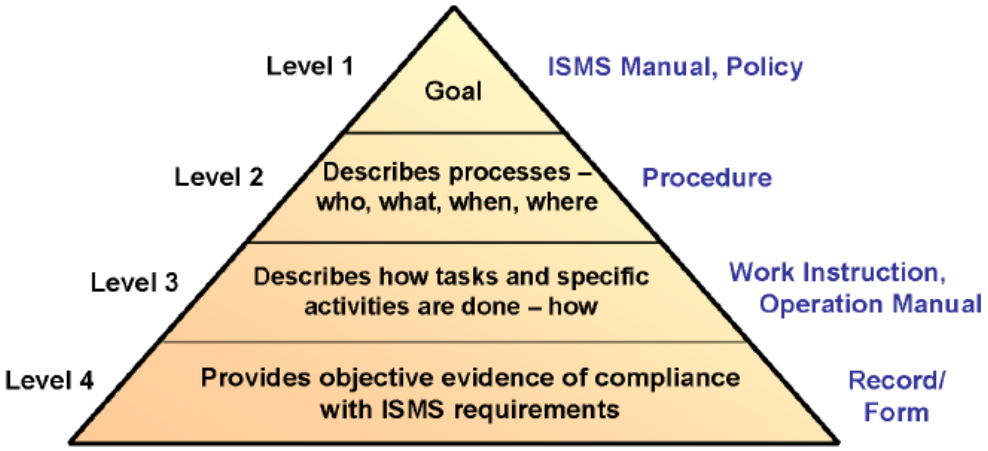
123 Ratchadaphisek Road, Dindaeng District, Bangkok 10400 Thailand

Detailed information about the assets under the scope of the ISMS of Thai Life Insurance Public Company Limited can be found in ISMS-FM-40 Inventory of Assets Data Center.

4. Documents of the ISMS:

4.1. Types of Documents:

The ISMS documents of the Company are categorized into 4 types:



4.2. Control of Documents:

Documents of the ISMS must be adequately protected and controlled as follows:

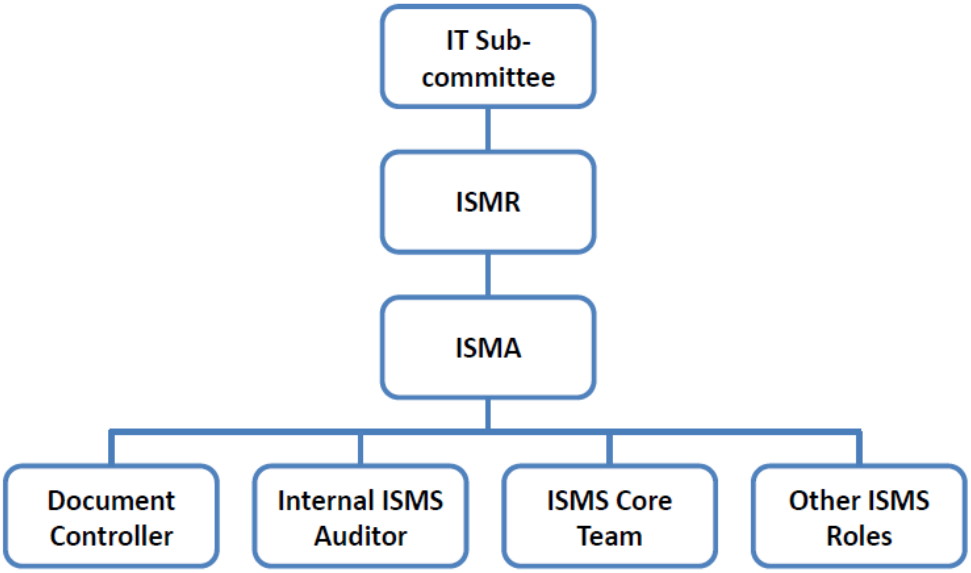
- Documents must be appropriately approved before issuance.
- Documents must be reviewed and updated regularly, with a process in place for approving new documents whenever there are changes or revisions.
- Changes to documents and the latest version must be appropriately identified in writing.
- The latest version of documents must be accessible to relevant users when needed.
- Documents must be protected against unauthorized access and use by individuals who do not have permission to use them.
- Documents must be complete and in a state ready for use.
- Documents must be managed for storage, transmission, usage, and disposal according to their confidentiality level.
- External documents used within the Company must be registered and controlled.
- Outdated versions of documents must be controlled and stored to prevent unintentional use, and if they need to be used, they must be clearly identified.
- Refer to ISMS-PC-08 Document Control Procedure.

4.3. Control of Records:

Records of the ISMS serve as evidence of ISMS operations and must be adequately protected and controlled to ensure they are complete and can be retrieved for review when needed. Furthermore, compliance with relevant laws, regulations, or regulatory requirements related to the storage, usage, and disposal of records must be adhering to the ISMS-PC-09 Record Control Procedure.

- The document must be approved before it can be published for use.

5. Structure and Responsibilities in the ISMS (Information Security Management System)



5.1. IT Sub-committee (ITSC)

The IT Sub-committee comprises senior management from relevant departments that support the establishment, implementation, review, and improvement of the Company's ISMS (Information Security Management System). The IT Sub-committee is responsible for:

- Defining the objectives of the Company's information security.
- Approving and disseminating policies for maintaining information security and related documents within the ISMS.
- Communicating to all employees the importance of data security and compliance with information security policies and related documents within the ISMS.
- Provide education and training to employees and relevant external individuals to ensure awareness and ability to adhere to information security policies and related documents within the ISMS, including appropriately monitoring the compliance of employees and relevant external individuals.
- Consider penalties for violations of information security policies and related documents within the ISMS.

- Establish criteria for risk acceptance and acceptable risk levels, including assessing the results of risk assessments and important risk mitigation plans of the Company.
- Support resources for the establishment, implementation, review, and improvement of the ISMS.
- Conduct meetings to review the operation of the ISMS to ensure that the Company's ISMS is adequate, sufficient, and effective, including considering opportunities for continuous improvement of the ISMS.

5.2. Information Security Management Representative (ISMR) / Information Security Management Assistance (ISMA)

The ISMR and ISMA are representatives of the Company's management who are responsible for overseeing the establishment, implementation, review, and improvement of the Company's ISMS. The ISMR and ISMA have the following responsibilities:

- Coordinate to establish and develop the ISMS within the Company, including maintaining, reviewing, and continuously improving the system to enhance security in accordance with the information security policy and ISO/IEC 27001 standards.
- Oversee the updating of policies and related documents within the ISMS to align with changes, complying with ISO/IEC 27001 standards and recommendations received from the IT Sub-committee.
- Communicate to all employees their roles and responsibilities in adhering to policies and related documents within the ISMS.
- Monitor the Company's operations to ensure compliance with the documents of the ISMS.
- Provide consultation on information security maintenance and the implementation of various policies to employees within the Company.
- Monitor and ensure that the activities of the ISMS are carried out according to the plan and that the results align with the Company's information security objectives.

- Monitor and control changes occurring within the Company, coordinating assessments, corrections, and appropriate risk management from such changes.
- Control and oversee the effectiveness measurement of processes and controls within the ISMS.
- Supervise internal ISMS audits.
- Oversee the handling of corrections and preventive actions for ISMS vulnerabilities, including tracking and reviewing the effectiveness of such actions.
- Coordinate on meetings for management reviews of the ISMS operations and follow up on the decisions made in the meetings.
- Report the results of ISMS operations to management.
- Coordinate and find solutions for controlling and managing incidents in case of security breaches occurring within the Company.

5.3. ISMS Core Team (CT)

The ISMS Core Team comprises representatives from various departments within the scope of the ISMS, responsible for coordinating and executing ISMS-related activities within their respective departments. The ISMS Core Team has the following responsibilities:

- Communicate, advise, and oversee employees in each department to ensure proper compliance with ISMS policies and related documents.
- Establish and maintain asset registers within each department.
- Coordinate with ISMR/ISMA to conduct risk assessments and manage risks for each department.
- Coordinate with ISMR/ISMA to implement the Security Plan as outlined.
- Coordinate with ISMR/ISMA to measure the effectiveness of processes and controls within the ISMS relevant to each department.
- Maintain a record list and control records for each department.
- Coordinate with ISMR in the event of any security breaches or emergencies within the Company to control and manage the arising issues.

- Listen to complaints or suggestions related to the ISMS from employees and relevant external individuals and report to ISMR/ISMA before taking corrective and preventive actions to improve the effectiveness of ISMS operations.

5.4. Document Controller

The Document Controller is responsible for overseeing and controlling the usage of documents and records within the ISMS to comply with the requirements of ISO/IEC 27001 standards. The Document Controller's responsibilities include:

- Controlling and overseeing the process of creating new documents, modifying existing documents, and discontinuing documents.
- Assigning document number and dates to documents.
- Managing the original copies of documents or soft copies of documents.
- Maintaining the Master List of all ISMS documents and being responsible for ensuring the accuracy of data updates.
- Monitoring and ensuring that documents are reviewed and updated regularly according to appropriate schedules.

5.5. Internal ISMS Auditor

The Internal ISMS Auditor is responsible for conducting internal assessments within the Company's ISMS to identify conformity and deficiencies, leading to continuous improvement of the ISMS. The responsibilities of the Internal ISMS Auditor include:

- Planning, coordinating, and conducting internal assessments for the Company's ISMS.
- Reporting assessment results and providing recommendations for improvement to relevant parties.
- Monitoring and reviewing the implementation of corrective or preventive actions identified during internal assessments.

5.6. Asset Owner

The Asset Owner is responsible for managing asset registers, assigning data classification levels to assets, and ensuring appropriate protection of assets throughout

their lifecycle. This includes ensuring the security of assets disposal, sale, transfer, or cessation of asset use.

5.7. Risk Owner

The Risk Owner is responsible for assessing risks, planning risk mitigation, and ensuring that risks are addressed according to the plan.

5.8. Document Owner

The document owner is responsible for creating, reviewing, and updating information security policies and documents related to the ISMS to ensure they are up-to-date and usable. The document owner must support the implementation and compliance with documents to ensure that personnel can perform their duties correctly. Their responsibilities include:

- Creating, reviewing, updating, discontinuing, and versioning documents, including registering documents to the Document Controller.
- Assigning classification levels and access rights to documents for relevant parties.
- Retrieving and controlling documents that have been discontinued.
- Ensuring the correct and appropriate use of documents, including controlling the issuance of document copies.

5.9. All personnel

All employees, including external personnel such as contractors, consultants, temporary staff, partners, and service providers, who use the Company's data or information technology systems have the following responsibilities:

- Complying with the guideline 1-2/2565 on information system security.
- Protecting and safeguarding the Company's data and assets, preventing unauthorized access, modification, disclosure, or destruction.
- Fulfilling responsibilities related to information security and information technology systems as assigned.
- Reporting any abnormalities or weaknesses in security to the Company appropriately.

6. Establishing Objectives and Planning Information Security Maintenance

6.1. Establishing Objectives for Information Security of the Company

Establishing objectives for information security in accordance with the business objectives, policies, and ISMS system objectives to guide the management of information security within the Company to align with business objectives, requirements, and expectations of stakeholders.

6.2. Planning Information Security Maintenance

Developing a plan for maintaining information security within the Company to define activities necessary to achieve the objectives for maintaining information security as established.

7. Information Security Management System

The Information Security Management System (ISMS) of the Company has been established, implemented, monitored, and continuously improved according to the requirements of ISO/IEC 27001 standard. It applies risk management principles to provide confidence to stakeholders that the Company's important information and information systems are adequately protected. Additionally, the ISMS has been designed to align with the Company's management processes and organizational structure, covering the following key activities:

- Defining the Company's requirements for information security and communicating them through the issuance of information security policies, as well as ensuring awareness among relevant stakeholders.
- Assessing the Company's information security risks.
- Establishing controls that align with the Company's risks.
- Monitoring and measuring the performance of the ISMS.
- Continuously improving the ISMS based on measurement results and pre-defined objectives.

The core components of the Company's ISMS system are illustrated in the diagram below.

Figure: Core components of ISMS system

Analysis of the relevant context and determination of the scope of the ISMS system (Context of the organization)

Conduct an analysis of both internal and external contexts, including the expectations of stakeholders, to define the objectives of the Company's information security management system (ISMS) and the scope of the ISMS.

Role and responsibilities of management (Leadership)

Give importance to and support the operations of the ISMS by announcing the information security management policy, defining employee responsibilities, reviewing ISMS operations, and allocating resources for the continuous operation and improvement of the ISMS.

Planning of the ISMS operations

Planning on the maintaining of the information security of the Company to determine activities needed to achieve the objectives of the Company's information security management system (ISMS) as defined. Also, analyze information security risks, including risks that may affect the operation of the ISMS, and plan to mitigate risks by selecting appropriate control measures.

Support for ISMS Operations

Manage resources, especially human resources, to ensure they have the knowledge, skills, and awareness to comply with information security policies and ISMS processes.

ISMS Operation

Oversee the operation of the ISMS and the effectiveness of risk mitigation activities, ensuring they are in line with the planned activities. This includes monitoring risk assessments and planning risk mitigation regularly or when significant changes that may affect the Company's risks occur.

Performance Evaluation of the ISMS

Conduct reviews and evaluations of processes and control measures, comparing them against information security policies, relevant standards, indicators, and objectives related to the Company's information security. Report the results to management.

Continuous Improvement of the ISMS

Address identified deficiencies from reviews and evaluations of processes and control measures. Continuously improve the ISMS through reviewing and updating objectives related to the Company's information security and associated plans.

8. Supporting ISMS Operations

8.1. Training, Knowledge, and Skills Development

ISMR/ISMA and supervisory personnel must support training initiatives to provide knowledge to employees involved in ISMS responsibilities adequately and sufficiently for their job duties. This includes:

- Identifying the necessary skills for employees involved in ISMS-related tasks.
- Organizing training sessions or sourcing knowledgeable personnel (if necessary).
- Evaluating the effectiveness of training and taking appropriate actions.
- Maintaining records of training as well as other evidence confirming the knowledge, skills, and experiences of employees

ISMR/ISMA personnel and their superiors must ensures that employees responsible for the ISMS are aware of the importance of their roles and responsibilities in maintaining information security and contribute to the Company's in achieving its objectives.

8.2. Internal and External Communication

Develop a communication plan (ISMS-FM-38 Security Communication Plan) to disseminate information related to information security management to both internal and external stakeholders of the Company.

- Internal communication within the Company includes communication between departments and reporting to management.
- External communication involves communication between the Company and external entities such as partners, external service providers, or relevant government agencies, as well as communication between the Company and external individuals such as customers or the general public.

8.3. Oversight of External Service Providers

Oversight external service providers engaged in activities or processes related to information security management for the Company. This involves controlling activities or processes in accordance with the Company's information security policy, as well as other relevant supporting documents. Additionally, conduct evaluations of external service providers and support continuous improvement efforts.

9. Risk management

Risk Management is a systematic process involving risk identification, assessment, and control measures to maintain risks at acceptable levels for the Company. It is considered a crucial aspect that enables a Company's ISMS to uphold information security. Risk management involves ongoing activities to address and mitigate risks arising from internal and external changes within the Company. In addition to managing risks, it is also essential to consider opportunities.

Standard serves as a reference for the Company's risk management practices.

- ISO 31000:2009, Risk Management – Principles and guidelines
- ISO/IEC 27005:2011, Information technology - Security techniques – Information security risk management

- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- AS/NZS 4360

The criteria for accepting risks and the acceptable levels of risk

The Company categorizes risk levels into four levels: High (H), Significant (S), Moderate (M), and Low (L). The levels that the Company can accept without the need for corrective action and risk control are Low (L) and Moderate (M). Any risk exceeding these levels must be addressed explicitly and must receive approval from relevant management personnel. The criteria for accepting risks that are deemed feasible include:

- Investment required for risk mitigation does not justify the potential maximum impact.
- Risks cannot be mitigated to the Low (L) or Moderate (M) levels.
- Management decision not to mitigate the risk. This required to be supported by appropriate rationale.

The risk management and opportunity management

The risk management and opportunity management process consist of three main activities:

9.1. Risk Assessment and Opportunity Assessment

Risk assessment involves analyzing potential risk scenarios by considering possible threats and vulnerabilities. Then, the likelihood of these risk scenarios occurring and the impact they would have are evaluated, following the ISMS-PC-06 Risk Assessment Procedure.

Opportunity assessment entails analyzing potential opportunity scenarios that could benefit the Company. Then, the likelihood and impact of these opportunities are evaluated.

9.2. Risk Treatment

Risk treatment involves finding appropriate methods or tools to mitigate and control risks to a level that the Company can accept. Possible approaches for risk treatment include:

- Risk Mitigation
- Risk Acceptance
- Risk Avoidance
- Risk Transfer or sharing with other properties
- Accepting increased risk for business opportunities

The selection of risk treatment approaches must consider their suitability and the resources required. Risk mitigation actions should refer to controls outlined in Annex A of the ISO/IEC 27001 standard, following the ISMS-PC-05 Risk Treatment Procedure.

9.3. Review of Risk Assessment:

The results of risk assessments must be reviewed at appropriate intervals, at least once a year or when significant changes occur. This ensures that the methods used and the results of risk assessments align with the current situation.

10. Performance Evaluation:

Performance evaluation is a crucial process that demonstrates the effectiveness and continuous improvement of the ISMS. It helps the Company understand the effectiveness of policies, supporting documents, processes, controls, and risk management strategies employed. This evaluation covers both ISMS requirements (Clause 4-10) and the controls selected for implementation (Annex A) of the ISO/IEC 27001 standard.

Measurement indicators used for performance evaluation include both lead indicators (before an event) and lag indicators (after an event) to provide comprehensive data. The results of performance evaluations are reported to management and relevant stakeholders for consideration in implementing corrective actions or improvements to the ISMS. This process is outlined in the ISMS-PC-10 Effectiveness Measurement Procedure.

11. Internal Audit of the ISMS

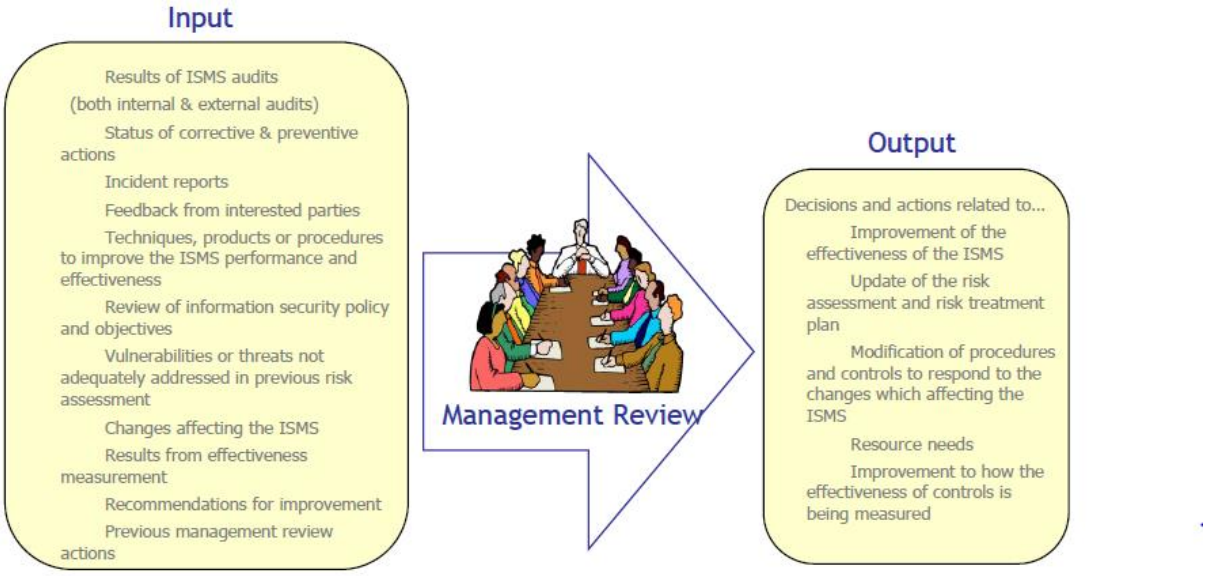
The Company ensures that internal audits of the ISMS are conducted at least once a year to ensure that:

- Operations of the ISMS comply with the requirements of the ISO/IEC 27001 standard and relevant laws and regulations.
- Operations align with the requirements and documentation of the Company's ISMS.
- Operations are carried out effectively.

Planning for internal audits considers the importance of processes, departments, or areas to be audited and the results from previous audits. Auditors must receive appropriate training and selection, ensuring that they do not audit areas where they have involvement. Planning, testing, reporting, and monitoring corrective actions follow the IA-ISO-PC-01 Internal Audit Procedure. Department managers involved in audited areas must cooperate in identifying causes and implementing corrective actions for identified deficiencies.

12. Review of the ISMS by Management:

The IT Sub-committee must hold meetings to review the operations of the ISMS at least once a year. This ensures that the Company's ISMS operations are appropriate, sufficient, and effective. Such reviews should consider opportunities for improving the ISMS and necessary changes. Additionally, they should involve reviewing and revising the information security policies and objectives of the Company. The outcomes of these reviews are adequately documented for reference.



13. Corrective Action

The Company has established a corrective action process to address issues or non-conformities identified within the ISMS (Information Security Management System) to prevent recurrence. All actions must be communicated to relevant personnel, and there must be follow-up and review of the outcomes to ensure that the objectives of the corrective actions are achieved. This process is referenced in the ISMS-PC-12 Corrective and Preventive Action Procedure.

14. Statement of Applicability (SOA)

The Statement of Applicability (SOA) is a document that identifies the application of controls from all 114 requirements of the ISO/IEC 27001 standard within the Company. It specifies:

- Controls selected for implementation in the ISMS (Information Security Management System), along with explanations of their application or references to related documents that can explain the implementation of controls.
- Controls that are not applied, along with the reasons for not applying them.

15. Continuous Improvement of ISMS

The Company emphasizes continuous improvement of the ISMS to ensure effective maintenance of information security. This enables the protection of assets, data, and critical information systems from constantly evolving threats. Regular internal and external context reviews, along with input from stakeholders, are conducted to enhance the objectives of maintaining information security and the Company's information security maintenance plans, annually.

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