HUMANICA

Information Security Management System & Privacy Information Management System Manual (ISMS & PIMS Manual)

Document Version : 4.0

Document No. : ISMS-PL-08

Document Owner: ISMR/ISMA

Last Updated: 21-06-2023

Document control

Document approvals

This document has been reviewed and approved by:

Prepared by	Reviewed by	Approved by
		
IT Security	*Head of Development*	*Chief Technology Officer*
Date: 21-06-2023	**Date:** 21-06-2023	**Date:** 21-06-2023

Version history

The following table lists all the revisions made to this document:

Version	Date	Description	Revised by
1.0	31-07-2020	Initial version	Sathaporn K.
1.1	04-09-2020	• Definitions documented information for all business related to guideline doc code. • Edit 4. Approval matrix for WI and OM process. • Definitions table of response guidelines, nonconformity, and observations.	Sathaporn K.
2.0	05-07-2021	• Amend "Action plan" in table of understanding the needs and expectations of interested parties. • Amend "ISO 31000:2018 risk management - guidelines" on the reference standard. • Annual review	Divya T.
3.0	01-07-2022	Annual review	Tosapol Y.
4.0	20-03-2023	• Update to apply ISO/IEC 27701:2019. • Amend the requirements of interested parties relevant to privacy information management system. • Amend PIMS scope • Amend Impact: Privacy information • Add risk exception management	Poonnada C.

Reference: ISO 27001:2013 & ISO/IEC 27701:2019 requirement

ISO/IEC 27001:2013 clause	ISO/IEC 27701:2019 clause	Requirement
4	5.2	Context of the organization 4.1 Understanding the organization and its context. 4.2 Understanding the needs and expectations of interested parties. 4.3 Determining the scope of the information security management system. 4.4 Information security management system
5	5.3	Leadership 5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities and authorities
6	5.4	Planning 6.1 Actions to address risks and opportunities. 6.2 Information security objectives and planning to achieve them.

ISO/IEC 27001:2013 clause	ISO/IEC 27701:2019 clause	Requirement
7	5.5	Support 7.1 Resource 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented information
8	5.6	Operation 8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment
9	5.7	Performance evaluation 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review
10	5.8	Improvement 10.1 Nonconformity and corrective action 10.2 Continual improvement
A.8.1.1	6.5.1.1	Inventory of assets
A.8.1.2	6.5.1.2	Ownership of assets
A.18.1.3	6.15.1.3	Protection of records

Table of contents

1. Security objectives

- To ensure information security management systems are applied and continually improved.
- To maintain business continuity in terms of security continuity and to reduce the risk of business damage.
- To ensure the confidentiality of Organization information is protected.
- To prevent unauthorized or undesirable person from access to and modification of the Organization information.
- To ensure that Organization systems and services is available to use when needed.
- To increase awareness and professional skills in terms of our information security management system.

2. Scope of ISMS

2.1 Context of organization

The organization defines the external and internal parameters to be taken into account when establishing information security management system.

External context

The external context is the external environment in which the organization seeks to achieve its objectives:

External context	Requirements and expectations
Legal and regulation	Comply with Thailand's computer crime law, privacy law, and cyber security law.
Natural disaster	Protect confidential information and privacy information damage from natural disasters.
Politic	Ensure business continuity aspect of security continuity during an event of political unrest.
Shareholder	Protect confidential information to maintain the trust of customers on organization's services.
Technology	Protect valuable information system from constantly changing technologies that could bring new threats to organization's systems.
Supplier/Vendor	Control the operation of suppliers to support services of organization that shall strictly follow the organization's policies.
Customer	Security and privacy contract requirements.

Internal context

The internal context is the internal environment in which organization seeks to achieve its objectives:

Internal context	Requirements and expectations
Business strategy	Develop information security management system to align with organization's business strategy.
Management direction	Develop information security management system to align with direction of management of organization.
Security organization structure	Ensure effective implementation and operation of the information security management system.
Information security policy	Review and update to reflect internal security objectives and strategy.
Information privacy policy	Review and update to reflect internal privacy objectives and strategy.
HUMANICA group	Establish information security practices that meet or exceed internal security audits.

Understanding the needs and expectations of interested parties.

The requirements of interested parties relevant to information security management system:

Interested parties	Expectations	Risk	Opportunities	Action plan
Top management	Ensure good organization governance and effective operations.	None.	Information security aligns with Business strategy.	Define objective and measure to ensure align with business strategy.
Legal and regulation	Comply with Thailand's computer crime law, privacy law, and cyber security law.	None.	Comply with applicable legal and regulation.	Develop compliance procedure and identify and follow-up for compliance program.
Shareholder	Ensure information security management system has been established and operated to protect confidential information.	None.	Gain trust of shareholder.	Establish information security program including information security policy and related documents to support ISMS activities.
Customer	Ensure customer information has been secure, non-disclosure, non-modification.	None.	Customers trust in organization services.	Monitor SLA to meet agreement with customer.
Employee	Preserve confidentiality, integrity and availability of confidential information.	Employee workload.	Employee awareness on information security.	Conduct security awareness for Employee.

The requirements of interested parties relevant to privacy information management system.

Role	Expectations	Risk	Opportunities	Action plan
Data subject Ex. Customers, Employees	- Ensure privacy information shall be processed for only purpose of the processing. - Ensure has been operated to protect information.	Misuse privacy information, Data breach.	Gain trust from data subject.	Implement ISO27701 to certify.
Data controller Ex. Customers	Ensure processes have been operated to protect privacy information.	Data breach.	Information security align with privacy information.	Establish privacy information program including privacy policy, privacy procedure and agreement.
Data processor Ex. Suppliers	Ensure processes have been operated to protect privacy information.	Data breach.	Comply with applicable agreement.	Establish privacy information agreement.
Third party Ex. The Revenue Department, Social Security Office	Ensure processes have been operated to protect privacy information. Data has accuracy.	Data breach.		Secure data transfer.

2.2 Scope

ISMS scope statement

1. HUMANICA HQ

Information security management system related to service of HUMANICA HQ (Public Company Limited) as the following details:
- HR Solutions Service including payroll service, human resource service and benefit service
- Financial solutions service
- Software development service
- Software as a service
- Data center management service

2. POS

Information security management system related to service of POS Company Limited as the following details:
- HR solutions service including payroll service, human resource service and benefit service
- Data center management service

3. FAS

Information security management system related to service of Humanica FAS Company Limited as the following details:
- Financial solutions service

- Accounting service
- Data center management service

4. TIGER

Information security management system related to service of Tiger Soft (1998) Company Limited as the following details:
- HR Solutions Service including Payroll service, Human Resource service and Benefit service
- Software Development Service
- Software as a service
- Data Center Management service

PIMS Scope

1. Humatrix software

Privacy information management system related to Humatrix software as the following details:
- HR solutions services
- Software development services

2. Workplaze software

Privacy information management system related to Workplaze software as the following details:
- HR solutions services
- Software development services

3. Tigersoft software

Privacy information management system related to Tigersoft software as the following details:
- HR solutions services
- Access solution service including face scan service and finger scan service
- Software development services

Location

- Humanica Public Company Limited, Professional Outsourcing Solutions ltd.(POS), Humanica FAS limited (FAS)

  2 Soi Rongmuang 5, Rongmuang Rd.Rongmuang, Pathumwan Bangkok, Thailand 10330

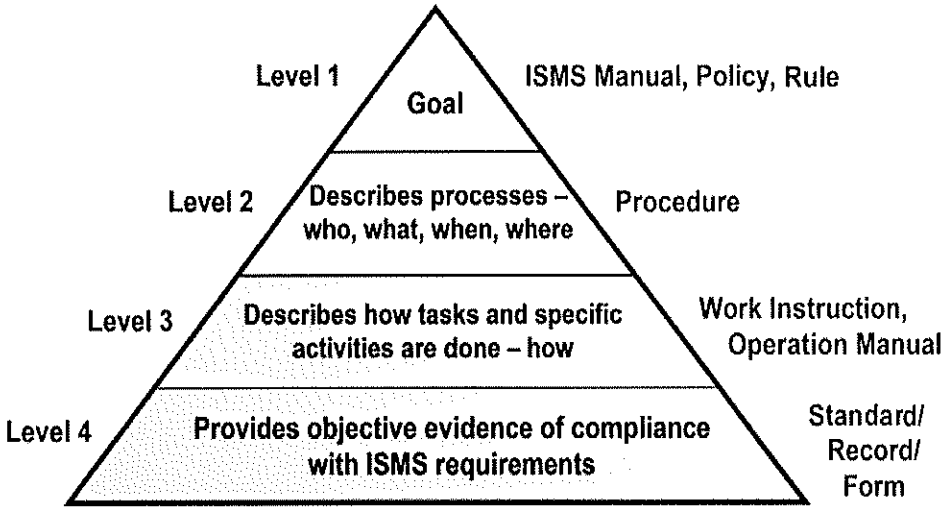
- Tiger Soft (1998) Company Limited
  7 Visionbusinesspark Building, 4-7th Floor Building 4, SOI Ramintra 55/8, Ramintra Road, Taraeng, Bangken, Bangkok 10230

  23 Visionbusinesspark Building, 1-3th, 5-6th Floor Building 11, SOI Ramintra 55/8, Ramintra Road, Taraeng, Bangken, Bangkok 10230

3. Documentation requirements of ISMS

Level of documents

ISMS documentation is a four-tier documentation structure which includes:



Control of documents

ISMS documentation shall be protected and controlled as follows:

- Approve documents for adequacy prior to issue.
- Review and update documents and re-approve documents as necessary.
- Ensure that changes and the current revision status of documents are identified.
- Ensure that relevant versions of applicable documents are available at points of use.
- Ensure that documents remain legible and readily identifiable.
- Ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification.
- Ensure that documents of external origin are identified.
- Ensure that the distribution of documents is controlled.
- Prevent unintended use of obsolete documents and apply a suitable identification if they are retained for any purpose.

Refer to *Document control procedure*

3.1 Document control procedure

Purpose

This procedure describes the process for controlling ISMS documents including established, distributed, revised, recalled, archived, and maintained all ISMS documents according to the requirement of ISO 27001.

All documents for each department other than ISMS documents should be performed according to "Guideline Doc Code" in the document master list.

Scope

All ISMS documents including:

- ISMS manual, policies and references
- Procedures
- Work instructions and operation manuals
- Standards
- Forms

All ISMS records are controlled the usage, storage and disposition in accordance with *Information Classification and Handling Policy*.

Definitions

1. Controlled document: Any document for which distribution and status are to be kept current by the issuer or document controller, to ensure that authorized holders or users have the most up-to-date version available.
2. External document: A document of external origin that provides information or direction for performing work. Examples of external documents are customer drawings, industry and governing body standards, regulations, vendor-supplied user manuals, and equipment manuals.
3. Record: A record is data or information of any kind and in any form, created or received and accumulated by an organization in the course of conducting business and subsequently kept as "evidence of activity" through incorporation into a recordkeeping system.

Procedure description

1. Established, revised, and cancelled the controlled document.
    - 1.1 Requestor prepares and submits a new document or a revision to an existing document.
    - 1.2 Requestor completes "Document action request, DAR" form indicating the reason for creating or changing the document.
    - 1.3 Document controller checks the completeness and correctness of DAR and the new/revised document.
    - 1.4 Document controller reviews & approves the document.
    - 1.5 If the result of review is not approved: Notify the reason for denial to the requestor.
    - 1.6 If the result of review is approved:
        - 1.6.1 Establish, revise, or cancel the document as per the DAR.
        - 1.6.2 Index and update the revision history.
        - 1.6.3 Update the document in the document management system.
        - 1.6.4 Store the master hard-copy document.
        - 1.6.5 Update the master list.
        - 1.6.6 Formally notify all affected departments.

Remark:

- All obsolete documents shall be clearly marked "CANCELLED" to prevent unintended use of obsolete documents.
- If the document has more than 1 language, all languages shall be revised or cancelled similarly at the same time.

2. Document Code

ISMS-YY-NN

ISMS	represent	group of documents in ISMS.
YY	represent	document type.
		(Management system manual/Policy – PL, procedure – PC, work instruction-WI, operation Manual-OM, standard – SD, form – FM)
NN	represent	running number. (2 digits)

Example of document structure

ISMS policies

ISMS-PL-01, ISMS-PL-02, ISMS-PL-03

ISMS procedures

ISMS-PC-01, ISMS-PC-02, ISMS-PC-03

ISMS standards

ISMS-SD-01, ISMS-SD-02, ISMS-SD-03

ISMS forms

ISMS-FM-01, ISMS-FM-02, ISMS-FM-03

ISMS references

ISMS-R-01, ISMS-R-02, ISMS-FM-03

3. Document version

Any changes in ISMS documents shall be revision controlled. All revisions to the ISMS documents will be documented in "Document release history" which maintained with the document. The first version number assigned shall be v1.0. If the document is revised and the change is not substantive, such as correcting a typographical error, or other minor change, the version number shall be increased by 1/10: e.g., v1.1. If the document is revised and the change is significant, the version number shall be increased to the next whole number: e.g., from v1.0 or v1.1 up to v2.0.

4. Approval matrix

All changes to the ISMS documents shall be appropriately reviewed and approved through signing or email according to the authorization level prior to issue.

	Policy, ISMS manual	Specific policy, reference	Procedure	Work instruction, operation manual	Standard	Form
Steering committee (ISMS-C)	Approve	Approve (Optional)	Approve (Optional)			
Head of BU	Review	Approve	Approve (Optional)	Approve (Optional)		
Head of department/division	Create	Review	Review & Approve	Review & Approve	Review & Approve	Review & Approve
ISMS core team	Create	Create	Create	Create	Create	Create
Staff			Create	Create	Create	Create

5. Access right

Depending on the document's content and sensitivity level, the document controller shall restrict access to and distribution of controlled documents as specified by the document owner.

6. Master list

The document controller shall maintain a master list of all controlled documents. The master list should include at a minimum the following information of each document:

- Document title
- Document code
- Date of issue
- Current version
- Document Owner

7. Periodical review of controlled document

The document controller shall be responsible for coordinating with document owner to ensure all ISMS documents are periodically reviewed (annually, at a minimum) to ensure their continued suitability to organization requirements and to ensure timely updates.

8. External document

External documents are controlled primarily for distribution purposes. All external documents and revisions shall be listed in the external document list as they are acquired and the document controller shall responsible to maintain this list. The external document list should include the following information of each document:

- Document title
- Responsible department
- Store area
  Responsible department of each document shall responsible for checking the update version and acquiring for use as appropriate.

Supporting document

1. Document Action Request (DAR)
2. Document Master List
3. External Document List
4. Information Classification and Handling Policy

Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. Records shall remain legible, readily identifiable and retrievable. The controls needed for the storage, protection, retrieval, and disposition of records have been documented in *Information Classification and Handling Policy.* For the identification, storage, retention time of records have been documented in *Inventory of Assets.* Retention period of each type Refer to *Retention time table.*

Retention time table

Record	Retention (Minimum)
ISMS documents: Policies/Procedures/Standard	3 years
ISMS records	3 years
Logs	90 days
Employment contract & record	Refer to ISMS-FM-04_Inventory of assets (HR)
Financial information	Refer to ISMS-FM-04_Inventory of assets (Financial)
Customer information	Depend on contractual/Agreement

4. ISMS organization structure and responsibility

Refer to *Role and Responsibility*

5. Information security objective and planning

To plan, define and maintain information security procedures by relevant department to align with business objectives, information security policy objectives and ISMS objectives.

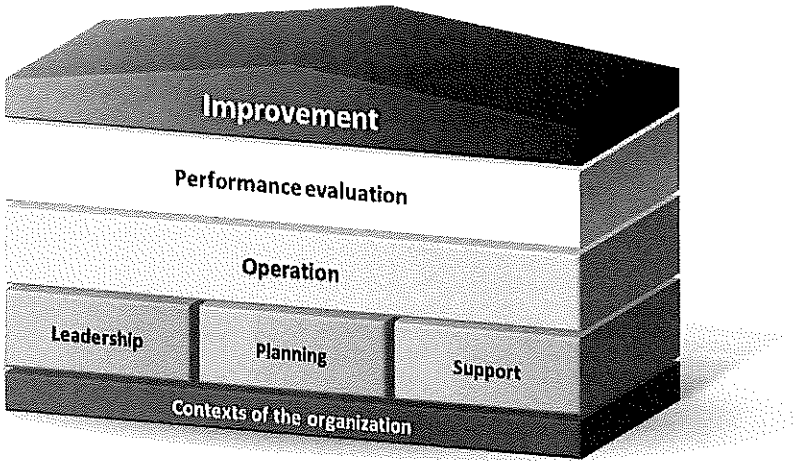
Refer to *Effectiveness Measurement*

6. Information security management system

The ISMS has been established to document, implement, maintain and continually improve information security effectiveness in accordance with the requirements of ISO 27001 standards. The ISMS used risk management in order to ensure the organization's information and systems will be protected. The ISMS has been designed to align information security processes with the organization's objectives by:

- Determining the organization's information security requirements and enforcement of information security policy including the communication process.
- Considering the organization's information security risk assessments.
- Establishing controls that manage information security risk.
- Auditing and evaluating performance of ISMS.
- Continual improvement to align the results of performance evaluation with organization objectives.

The main elements of organization's ISMS are:



Context of the organization and ISMS scope

Determine the internal and external context including expectation of related person in order to define information security objective of organization and ISMS scope.

Leadership

Management shall emphasize and sponsor the ISMS by enforcing the information security policy, assigning role of ISMS, reviewing ISMS operations and providing the resources to operate and continually improve ISMS.
Refer to *Information Security Policy*

Planning

Define activities to achieve information security objectives and address any issues identified by the information security risk assessment.

Support

Ensure the ISMS is supported by adequate resources that have the proper competencies and awareness to achieve ISMS objectives.

Operation

Implement, monitor and control ISMS procedures to protect the Organization's information security assets. Conduct risk assessment activities and identify risk treatment plans regularly.

Performance evaluation

Audit and evaluate the effectiveness of processes and controls compared with information security policy, relevant standards, metrics and information security objectives of Organization and report to management.

Improvement

Correct issues found in the audit and process evaluations, identify lack of ISMS controls and continually improve the suitability, adequacy and effectiveness of the information security management system of the organization.

7. Supporting of ISMS operation

7.1 Training, awareness and competency

ISMR/ISMA shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

- Determining the necessary competencies for personnel performing work effecting the ISMS.
- Providing training or, if necessary, employing competent personnel to satisfy these needs.
- Evaluating the effectiveness of the training provided and actions taken.
- Maintaining records of education, training, skills, experience and qualifications.

They shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

7.2 Communication

Develop an internal and external security communication plan in order to ensure that all associates, visitors and third parties understand the need to comply with the Organization's information security policy.
In particular:

- Internal communications refer to communication between HUMANICA IT departments and relevant departments.
- External communications refer to communication between organization and external parties such as partners, third party services or government agencies.

Refer to *Security Communication Plan*

8. Risk management

Risk management is a systematic process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. Risk management process is an integral part of the ISMS that provides continuous process improvement. Because risk can never be completely eliminated, the organization shall continuously review all identified risks as well as carry out assessments for new risks.

Reference standards

- NIST SP 800-30, Risk management guide for information technology systems
- ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management
- ISO 31000:2018 Risk management - Guidelines

Acceptable level of risk and criteria for accepting Risk

The organization separates risk into 5 levels which are Very High, High, Medium, Low and Very Low. The acceptable levels of risk are Low and Very Low level. Formal risk acceptance shall be performed and all key stakeholders shall be made aware of, and agree if it is necessary to accept the risk higher than Low. Criteria for accepting risk could be:

- The cost of implementing a control outweighs the potential loss through the risk occurring.

Risk assessment

Risk assessment is an analysis of risk involving identification of threats that may cause harm to the assets, identification of vulnerabilities that can be exploited by threats and assessment of the probability of the unwanted event occurring and its impact.
Refer to *Risk Management Procedure*

Risk treatment

Risk treatment is a process which involves selecting, evaluating and implementing the appropriate risk-reducing and cost-effective controls to decrease risk to an acceptable level. The possible options for treatment of risk include:

- Reduction
- Transfer
- Avoidance
- Acceptance

Refer to *8.2 Risk Management Procedure*

Review of risk assessment

The risk assessment result shall be reviewed at planned intervals (at least once a year) or when a major change occurs to ensure that the results are correct and up to date.

Remark: Major change can consist of:

- Organization
- Technology
- Business objectives and processes
- Identified new threats.
- Effectiveness of the implemented controls.
- External events such as environmental, social and political

Example

- Widening the scope to other units of the organization.
- Changes in the external environment (legal, competitive, technological ...).
- Consideration of new risk scenarios.

8.1 Asset management procedure

Purpose

- To ensure that any addition, change and cancellation made to assets within ISMS system are properly controlled and the Inventory of Assets is always correct and up to date.
- To ensure that all assets are appropriately classified in terms of their value which lead to the risk assessment and risk treatment in proper means.

Scope

- This procedure applies to employees, contractors, consultants, temporary workers, and other workers, including all affiliated third parties.

Definitions

1. Asset: Anything that has value to the organization which include organization personnel or capability. Assets include anything that can contribute to the delivery of a service.

Procedure description

1. Monitor any change to asset.

ISMS-T monitors asset changes once a year, monitoring any changes made to all 5 asset categories:

I. Information asset
II. Hardware asset
III. Software asset
IV. Personal asset
V. Services and environmental asset

2. Classify asset change.

ISMS-T classifies asset changes to classify asset changes into one of the following 3 categories:

I. Addition of asset
II. Change of asset
III. Cancellation of asset

3. Collect data of new assets.

ISMS-T collects data of all assets recently added into the system in according to requirements of Inventory of assets.

4. Identify classification of information assets.

ISMS-T identifies classification level of information asset to indicate the degree of asset sensitivity in terms of its confidentiality.

5. Collect data of asset change.

ISMS-T collects data of asset changes to update inventory of assets in case of any change occurred to assets.

6. Collect data of asset cancellation.

ISMS-T collects data of asset cancellation to collect data of asset cancellation e.g. reasons of cancellation, date of cancellation and so forth.

7. Fill data in Inventory of assets.

ISMS-T fills data in Inventory of assets, filling data collected from step 3-6 in Inventory of assets to make it up to date and also defining the details of adjustment in "Track changes" as well as updating version of it.

8. Uploads "Inventory of asset" into common folder.

ISMS-T sends the latest version of 'Inventory of assets' file to document control in order to upload into share drive in each department and upload on the "ISO 27001" web portal for ISMS documents.

9. Report asset change to ISMR/ISMA.

Document control informs reviews asset changes to ISMR/ISMA, informs ISMR/ISMA with regard to asset changes for taking actions in accord with risk management process.

Supporting documents

1. Inventory of Assets

8.2 Risk management procedure

Purpose

- To ensure the assessor can appropriately carry out risk assessment.
- To ensure the result of risk assessment is correct, repeatable and comparable.
- To ensure the risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks.

Scope

This policy applies to:

- ISMS-T, asset owner, ISMR/ISMA and steering committee who involve the risk management Procedure of ISMS
- All resources, information, information processing facilities and assets, which concern to the risk management procedure of ISMS.

Definition

1. Risk management: coordinated activities to direct and control with regard to risk.
2. Risk assessment: overall process of risk analysis and risk evaluation.
3. Risk analysis: systematic use of information to identify sources and to estimate the risk.
4. Risk evaluation: process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
5. Risk treatment: process of selection and implementation of measures to modify risk.

Procedure description

1. Identify assets

ISMS assets consist of 5 asset categories:

I. Information asset
II. Hardware asset
III. Software asset
IV. Personal asset
V. Services and environmental asset

2. Identify possible threat to assets

A threat can cause an unwanted incident which could result in harm to the organization and its assets. This harm can occur from an attack on the organization's information, e.g. resulting in its unauthorized disclosure, modification, corruption, destruction and unavailability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit one or more vulnerabilities of the systems, applications or services used by the organization in order to successfully cause harm to assets. Threats may originate from within the organization as well as external to it.
Few examples of threat include;

- Fire
- Theft
- Non-availability of critical resources
- Un-authorized access
- Data leakage
- Hacking
- Cyber crime
- Hardware malfunction
- Power failures

3. Identify vulnerability and existing control

A weakness (vulnerability) which may be a threat to cause damage to the asset and existing control which protect damage to the asset, based on data from Vulnerability catalog or other sources such as incident report, security website, etc.,
Few examples of vulnerability catalog include;

- Lack of information protection (e.g. data leakage/loss, data management, mobile device)
- Lack of hardware control (e.g. configuration, change, maintenance, obsolescence, theft, capacity, log, disaster & recovery)
- Lack of software control (e.g. management, development, testing, capacity, obsolescence, license, source code, hacking, malicious)
- Lack of resource control (e.g. people, training, compliance, business continuity, internal auditor, budget, forensic evidence)
- Lack of Service control (e.g. contract, network, power, maintenance, vendor)
- Lack of process control (e.g. communication, disposal, encryption, backup, maintenance)
- Lack of protection system (e.g. fire, flood, water leak, earthquake, terrorism)

4. Assess impact

ISMS-T assesses impact of each threat and weaknesses that identified in previous step according to impact table below.

Impact table

Impact value		CIA				Privacy
		Disruption of operation	Reputation	Financial (THB)	Legal and regulation compliance	Privacy information
5	Very high	More than 24 hours	Serious impact on reputation and loss of customer confidence	> 300,000	Numerous major litigations	Privacy information whose unauthorized disclosure, modification, loss or destruction can affect the existence or the health, freedom and life of the PII principal (Ex. information about commitment to an institution, a sentence, personnel reviews, health data, unserviceable debts, or if the PII principal is at risk of becoming a victim in a criminal case)
4	High	8 – 24 hours	Significant impact on reputation and may cause termination of contract	~150,000	Single major litigation or numerous moderate litigations	Privacy information whose unauthorized disclosure can affect the reputation of the data subject
3	Medium	4 – 8 hours	Moderate impact on reputation and may loss customer's trust	~75,000	Single moderate litigation or numerous minor litigations	Privacy information that requires a legitimate interest for access (Ex. restricted public files or the members of a distribution list)
2	Low	Less than 4 hours	Insignificant impact on reputation and customer's trust	~30,000	Single minor litigation	Privacy information that publicly accessible (Ex. in telephone directories, address books or selection list)
1	Very low	No impact	No impact	< 3,000	Threat of litigation requiring small compensation	No impact

5. Assess probability.

ISMS-T assesses the level of probability, threat can be caused by damage to the asset vulnerability as table below.

Likelihood Table

Probability		Criteria/Description
5	Extremely likely	The possibility is almost certain. Potential of it occurring more than once a day.
4	Likely	Very likely, the event is expected to occur in most circumstances as there is a history of regular occurrence at the similar organization/ environment. (Once a month)
3	Possible	There is a strong possibility that the event will occur as there is a history of frequent occurrence at similar organization/ environment. (Once a year)
2	Rare	The event might occur at some time as there is a history of casual occurrence at the similar organization/environment. (1-2 times in 5 years)
1	Unlikely	Rare, but it may occur in exceptional circumstances. It could happen, but probably never will. (One in 10 years)

6. Calculate Risk Level

Risk Level refers to Risk Level table as below.

Risk Level Table

Risk Map		Impact				
		Very Low	Low	Medium	High	Very High
Likelihood		1	2	3	4	5
Unlikely	1	1	1	2	2	3
Rare	2	1	2	2	3	3
Possible	3	2	2	3	4	4
Likely	4	2	3	4	4	
Extremely Likely	5	3	3	4		

7. Require treatment

Considering whether the risks that need to correct and control, organization defined risk acceptable levels without risk treatment for risk level are "Low" only.

7.1 If the risk level is higher than "Low", follow "Step 8 Determine risk treatment plan"

7.2 If the risk equals "Low" or "Very Low", end process.

Risk treatment action table

Risk level	Required action
Very high	Risk cannot be accepted. Immediate action is needed to implement or improve controls on urgent basis.
High	Risk cannot be accepted. Action is needed to implement or improve controls within appropriate time.
Medium	Risk is in moderate level. Correction needs to be considered but with justification, it can be considered accepting the risk.
Low	Risk can be accepted. Unlikely to require specific or significant application resources.
Very low	

8. Determine risk treatment solution

ISMS-T considers the appropriate solution in order to correct and control the risk with the following points should be considered.

8.1 Details of the solution to use. Difficulty in the implementation, appropriate and compatible with the organization.

8.2 Resources required in terms of budget, staff, time and etc.

8.3 Laws, regulations, policies or agreements relevant

8.4 Performance of treatment and control risk

8.5 Priority of actions and plan

Priority action table

Priority action table	
High priority	Immediate action with senior management involvement and regular status reporting to implement or improve controls on an urgent basis.
Medium priority	Seek to implement additional/improved controls to reduce risk impact and/or likelihood.
Low priority	Manage risk by routine procedures ensuring existing controls operating as expected, unlikely to require specific or significant application of resources.

9. Possible and valuable treatment

ISMS-T considers the possibility and value of risk treatment solution and proposes to request for management's approval as appropriate.

9.1 If possible, to implement a solution to control the risk and appropriate cost, follow "step 10 Summarize risk treatment plan"

9.2 If unable to control risk or over budget, follow "step 13 Accept risk"

10. Summarize risk treatment plan

Summarize and create risk treatment plan (RTP) in order to request management support and approval which risk treatment plan details as below;

- Risk treatment solution
- Responsibility
- Resource need (budget, personnel)
- Timeline
- Priority

11. Approve risk treatment plan

Steering Committee considers approving risk treatment plan and provision of appropriate resource to support.

12. Perform risk treatment activity

ISMS-T implements the specified solution in the risk treatment plan. Using the resource as defined in the plan and action to be completed within due date. The progress and problem of implementation shall be informed to management at intervals.

13. Accept risk decision

Summarize risks that need to accept, limitation and reason why it is unable to treat and control the risks. These risks have to record in the Risk acceptance document in order to request steering committee to consider and endorse to accept risk.

Supporting Document

1. Risk Assessment Treatment

9. Performance evaluation

Performance evaluation is an important process which enables the organization to assess how well it is doing in implementing information security and the effectiveness of its policies, supporting documents and controls selected from ISO 27001. This process shall cover the measurement of both ISMS processes (described in clauses 4-10) and the controls (described in Annex. A) of ISO 27001.

Refer to *Effectiveness measurement procedure*

9.1 Effectiveness measurement procedure

Purpose

- To ensure that the effectiveness of ISMS meet the expectation.
- To ensure the continuity of ISMS development.
- To provide solutions in case of ISMS effectiveness does not meet the expectation.

Scope

This policy applies to:

- ISMS-T, ISMR/ISMA and steering committee who use the information security policy.
- All resources, information, information processing facilities and assets, which concern to the ISMS scope.

Definitions

1. Metric: A measure of how well the ISMS processes are performing and how they achieve the organization's objectives and requirements, or a measure of one or more controls that are implemented in the ISMS, indication whether they achieve their identified information security objectives and risk reduction.

Procedure description

1. Consider controls and ISMS requirements grouping.

Grouping controls and ISMS requirements shall be assigned to the following persons:

- ISMS-T shall consider the controls in their responsibility.
- ISMR/ISMA shall consider all of ISMS requirements and the controls in their responsibility.

Criteria for grouping the controls and ISMS requirements are:

- Similar purpose
- Ability to treat the same risk
- Similar level of value of asset

For example, effectiveness of using firewall and IDS to protect assets from cyber-attacks can be evaluated by finding out the amount of attacks per month.
When finish grouping, responsible persons shall be assigned and recorded in measurement list.

2. Define criteria of Effectiveness measurement

ISMS-T and ISMR/ISMA shall define criteria for measuring the effectiveness of controls and ISMS requirements.

Effectiveness measurement criteria

Field	Data
Metric	Define name, id, description
Objective	Define objective of the metric
Method	Define how to calculate measurement result
Target	Define a satisfactory measurement result
Frequency	Define frequency of measure
Data Source	Define where the data is collected from
Report format	Define how the result will be reported
Responsible	Define responsible person

When the criteria are completely defined, the details shall be recorded in measurement method as the example below;

Field	Data
Metric	Information security awareness, education and training
Objective	To ensure all employees in ISMS scope obtained security awareness training
Method	(Total of employees in ISMS scope attended security awareness training * 100) / Total of employees in ISMS scope
Target	100% = good <100% = improve
Frequency	Annually
Data Source	Training record
Report format	Document
Responsible	HR

3. Execute the effectiveness measurement

Effective measurement shall be carried out following defined criteria and the finding shall be recorded in measurement log.

4. Analysis and summary the effectiveness measurement

Responsible persons shall analyze and summary their measurement when the result of measurement is lower than expectation level, responsible persons shall follow corrective action procedure to improve and correct that measurement.

5. Report the ISMS effectiveness

ISMS-T and ISMR/ISMA shall report the effectiveness of ISMS to the steering committee at least once a year.

Supporting documents

1. Effectiveness Measurement Form
2. Corrective Action Procedure

10. Internal ISMS Audit

An Internal ISMS audit shall be conducted at planned intervals, at least once a year, to determine whether the control objectives, controls, processes and procedures of the ISMS:

- Conform to the requirements of ISO 27001 and relevant legislation or regulations.
- Conform to the identified information security requirements.
- Are effectively implemented and maintained.
- Perform as expected.

An audit program shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work. The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records shall be refer to *Internal ISMS audit procedure*. The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes.

10.1 Internal ISMS audit procedure

Purpose

This procedure describes the process for performing the Internal ISMS Audit according to the requirements of ISO 27001 in order to ensure that the organization effectively operates in accordance with the specified policies, procedures and all relevant requirements.

Scope

All departments that form part of the organization information security management system.

Definitions

1. Nonconformity (NC): Non-fulfillment of a requirements. Deviation or failure to meet one or more requirements of applicable standards, regulations or established documents of the organization.
2. Observation (OBS): A statement of opinion to improve a process. A minor findings with no objective evidence to prove as nonconformity. Though it is not booked as nonconformity, it calls management attention to an area that requires improvement/action, lest it be elevated to nonconformity in the future audits.
3. Table of response guidelines, nonconformity, and observations.

Type	Time to respond	Time to closed
Nonconformities (Major NC)	15 days	30 days (Acceptance letter: head BU)
Nonconformities (Minor NC)	15 days	90 days
Observations (OBS)	15 days	- 180 days - 1 year In the event that the duration of time affected by external factors such as external training courses or purchasing problems, etc.
Opportunity for Improvement (OFI)	Optional	Optional

Procedure description

1. Audit schedule

ISMR/ISMA shall create the audit schedule that contains all scheduled and potential audits related to the ISMS for the whole calendar year. This shall include internal ISMS audits, audit performed by clients and third party audits.
Internal ISMS audits shall be scheduled at least once a year or as the need arises.

Lead auditor/Auditor

For each internal ISMS audit, ISMR/ISMA shall appoint all audit team members including lead auditors and auditors. All appointed auditors shall pass internal audit training and have adequate knowledge of ISO 27001 requirements and controls. Selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work. In case the audit area/process needs specific IT knowledge, the appropriate IT personnel shall be selected.

2. Audit program

ISMR/ISMA and lead auditors shall prepare the audit program taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit program shall be approved by steering committee and consists of:

- audit objective
- audit scope
- audit standards and/or regulations
- audit date
- audit team members (lead auditors/auditors)
- audit areas/processes
- audit criteria/requirements/controls for each area/process

All areas/processes applicable to the ISMS shall be audited at least annually.

3. Audit preparation

Lead auditors/auditors shall review ISO 27001 requirements, controls, relevant regulations and ISMS documents impacting the area/process to be audited prior to the audit and then prepare a checklist. In addition, audit reports, nonconformities and corrective actions taken for related past audits shall also be considered for preparing the audit checklist.

4. Audit execution

4.1 Lead auditor inform auditee at least 3 working days in advance of the audit.

4.2 Lead auditor conduct opening meeting to confirm the objective, scope, standards and regulations for this audit.

4.3 Lead auditor/auditor perform the audit using the prepared checklist, verifying what is happening in practice and seeking evidence that the documents/requirements are being complied with by using below techniques:

- reviewing documents/records
- observing pertinent activities
- interviewing related personnel

(Auditor shall not be limited to the prepared checklist)

4.4 Lead auditor/Auditor consolidate, review and classify all findings (NC & OBS) within audit teams.

4.5 Lead auditor conduct closing meeting to report the findings (NC & OBS) and recommendations for improvement. (All queries shall be resolved)

- IF any NC not found, Issue audit report to auditee and ISMR/ISMA
- IF found any NC, Issue audit report and CAR to auditee and ISMR/ISMA (CAR shall be handled according to the corrective action procedure)

Remark: Lead auditors/Auditors shall update all audit findings in audit checklist and attach with audit report before sending to ISMR/ISMA.

5. Audit reporting

ISMR/ISMA shall maintain all audit reports and review the results to ensure that the internal ISMS audit is conducted effectively. All internal ISMS audit results shall be summarized for input into the management review meeting.

Supporting documents

1. Audit Program (Audit Plan)
2. Audit Checklist
3. Audit Report

11. Management review of the ISMS

Steering committee shall conduct management review meetings at least once a year to ensure ISMS continual suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained.

The management review shall include consideration of:

a) The status of actions from previous management reviews.

b) Changes in external and internal issues that are relevant to the information security management system.

c) Feedback on the information security performance, including trends in:

1) Nonconformities and corrective actions
2) Monitoring and measurement results
3) Audit results
4) Fulfilment of information security objectives.

d) Feedback from interested parties.

e) Results of risk assessment and status of risk treatment plan.

f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

12. Corrective action

Corrective actions shall be appropriately conducted to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. Lessons learned from the security experiences of other companies and those of the organization itself shall be applied. All actions and improvements shall be communicated to all interested parties with an appropriate level of detail. Follow-up activities shall include the verification of the actions taken and the reporting of verification results to ensure that the actions and improvements achieve their intended objectives.

Refer to *Corrective action procedure*

12.1 Corrective action procedure

Purpose

This procedure describes the process for undertaking corrective actions to eliminate the causes of actual or potential nonconformities.

Scope

All ISMS related nonconformities or potential nonconformities observed either during supervision, review and audit including all customer or third-party complaints whether written or verbal.

Definitions

1. Correction: Action implemented by a stakeholder to eliminate the causes of nonconformities in order to prevent recurrence.
2. Corrective action: Action implemented by a stakeholder to eliminate the causes of potential nonconformities in order to prevent their occurrence ;or evaluation of patterns/trends through corrective actions and taking steps to prevent their re-occurrence.

Procedure description

1. Possible sources of correction/Corrective action

Corrective action request (CAR) shall be issued for handling nonconformities, potential nonconformities or improvements to the ISMS which are observed in any of the following situations:

Situations	Raise CAR by
Internal audits	Lead auditor/Auditor
External audits	ISMR/ISMA
During operations (e.g. non-monitoring of required logs, non-implementation of a security procedure, error in coding, non-attainment of SLAs,...)	Staff who observed the event
Customer or third-party complaints	Staff who responsible for receiving the complaint
Information security incident (after the remediation steps have been accomplished)	Incident response team or ISMR/ISMA

2. Corrective action request

2.1 Requestor raises CAR to the concerned department manager. (1 CAR per case)
2.2 ISMR/ISMA register CAR information to CAR log and running the request number.
2.3 Department Manager (who received CAR)
  2.3.1 Review and investigate the causes of observed or potential nonconformities or complaint.
  2.3.2 Obtain inter-departmental help if necessary.
  2.3.3 Propose correction, corrective actions and/or improvements and implementation plan.
  2.3.4 Pass the original CAR to the requestor and copy of CAR to ISMR/ISMA.
2.4 Responsible Person (nominated in CAR) implements the proposed actions and monitor the effectiveness of actions within the defined plan.
2.5 Requestor follows up monitoring or audits to verify that the correction, corrective actions, and/or improvements are properly and effectively implemented. If the correction, corrective actions and/or improvements are unsatisfactory, requestor will repeat step 2.1-2.4.
2.6 Requestor sign-off the CAR and send to filing with ISMR/ISMA.
2.7 Document controller updates the status in CAR log and maintain all CAR records.

Remark:

- ISMR/ISMA shall follow up all CAR and update the status in CAR log for reporting to Lead ISMR on a weekly basis.
- Corrective actions taken shall be appropriate to the impact of the potential problems.
- In case of customer or third-party complaints, the concerned personnel, when and where necessary, shall reply to the customer/third party the investigation results and corrective/preventive measures taken to eliminate the cause of nonconformities.

3. Correction and corrective action reporting

ISMR/ISMA shall monitor and review the results to ensure that the corrective actions are conducted effectively, especially on the CARs which are delayed or rejected by the requestor. All corrective action results shall be summarized for input into the management review meeting.

Supporting documents

1. Corrective Action
2. Corrective Log

13. Statement of applicability (SoA)

Statement of applicability (SoA) is a documented statement describing the controls that are relevant and applicable to the organization's ISMS along with the explanation and/or reference document for controls application. The document also describes the controls not implemented (exclusions) with justification/reasons why controls have not been implemented.

Refer to *Statement of Applicability (SoA)*

14. ISMS improvement

Organization will continually review and improve the ISMS in order to maintain the effectiveness of information security management and to protect the information assets and critical systems of Organization from new threats.

15. Risk exception management

Risk exception management shall be applied when a particular information security policy, security program requirements cannot be implemented and might be major or critical impact. There are two Risk exception may be granted in such following situations:

- Temporary exception, where immediate compliance would disrupt critical operations.
- Another acceptable solution with equivalent protection is available.
- A legacy system is being retired and compliance is not possible (risks must be managed).
- Compliance would cause a major adverse business impact that would not be offset by the reduced risk occasioned by compliance (e.g., the cost to comply offsets the risk of non-compliance).

The risk exception shall be reported into 2 levels of acceptance as follows.

1. Risk acknowledgement

   Risk acknowledgement shall involve the risks associated with non-compliance and deemed acceptable by the organization or customers. It requires to inform the associated risks for their acknowledgement if the security requirements cannot be implemented.

   This typically occurs when the organization has conducted some security improvements involving the client's corporation, but the client is not ready to apply that. For example, if a particular security control cannot be implemented due to customers' technical constraints, it's required to remind the associated risks for their acknowledgement.

2. Risk acceptance

   Risk acceptance shall involve a conscious decision by the organization to accept a certain level of risk due to factors such as cost, operational requirements, or other business considerations. In case, compliance with a specific security policy or standard may cause a major adverse business impact that outweighs the reduced risk achieved through compliance.

   The risk acceptance request shall identify:

   - The specific policy, standard for which an exception is being requested.
   - The specific device, application, or service for which the exception is being requested.

- The nature of the non-compliance, e.g., specific deviation from the policy, standard.
- Why an exception is required, e.g., what business need or situation exists, what alternatives were considered, and why are they not appropriate.
- Assessment of the potential risk posed by non-compliance, e.g., if the exception is granted, the consequences that will be affected, either directly or indirectly, by the exception.
- Plan for managing or mitigating those risks, e.g., compensating controls, alternative approaches.

The requests for acceptance must be signed by the person responsible for implementing the standards or controls. The requests for acceptance must be reviewed and approved by management of that services or business unit owner, and the information security coordinator for their area.

End of document