WHA GROUP

Policy

Cybersecurity and Information Security Management Policy

Document Properties	
Document Number	WHACG-ICT-PLCY-0001
Softcopy Location	CDMS / WHA SharePoint
Owner Division	IT Department
Owner Department	IT Department
Version Number	v5.0.0 (Approved Final)
Release Date	01 Aug 2024
Review/Update Due Date	01 Aug 2027

Document Approval	
Approver	Jareeporn Jarukornsakul (Chairman and Group Chief Executive Officer)
	Somkiat Masunthasuwun (Chief Executive Officer - WHAUP)
Reviewer	Nunsilp Janvarin (VP – IT Department)
Owner	Soros Sottitavorn (Infrastructure and Cybersecurity Senior Manager – IT Department)

Document Control

Document changes:

The following table presents the change record of this document.

Version	Approval date	Document owner	Change(s)
v5.0.0	01 Aug 2024	Soros Sottitavorn - Infrastructure and Cybersecurity Senior Manager - IT Department	Change working group to committee
v4.0.0	01 Jul 2023	Soros Sottitavorn - Infrastructure and Cybersecurity Senior Manager - IT Department	Change format and content to comply with ISO/IEC 27001 version 2022
v3.0.0	01 Jul 2021	Soros Sottitavorn - Cybersecurity Senior Manager - IT Department	Change format and contents
v2.0.0	01 Aug 2020	Nunsilp Janvarin - VP - IT Department	Add personal data
v1.0.0	20 Nov 2015	Apichat Thongsuksan - IT Department	First version

Author:

The following persons are the authors who drafted this document.

Name - Surname	Position
Soros Sottitavorn	Infrastructure and Cybersecurity Senior Manager - IT Department

Reviewer:

In addition to the main reviewers, the following persons have also reviewed this document.

Name - Surname	Position
Nunsilp Janvarin	VP – IT Department

Approver:

In addition to the main approvers, the following persons have also approved this document.

Name - Surname	Position
Jareeporn Jarukornsakul	Chairman and Group Chief Executive Officer
Somkiat Masunthasuwun	Chief Executive Officer - WHAUP

Table of Contents

1) Introduction

At present, the Company has a wide use of information technology. Therefore, the Company places importance on protecting information systems as well as implementing policies to prepare for cyber threats. The policy is aimed at complying with the Cybersecurity Act, B.E. 2019 ("Cybersecurity Act"). In addition, the Company attaches importance to the protection and respect of your privacy rights under the Personal Data Protection Act B.E. 2019 ("Personal Data Protection Act") including those amended from time to time, and other applicable laws and regulations in Thailand. And we intend to protect your personal data collected by the Company, use, and disclose for the Company's business operations. The Company has duties as stipulated in the subjects of Personal Data Protection, Privacy, or data security applicable and in effect in Thailand.

To explain the purpose and scope of the information security policy as a whole and to show the directions of the organization director on information security which aims at persons concerning the organization's information to adhere to and implement. The goal is to ensure that employees' operations related to information including data-related systems have sufficient information security to support the organization's current and future business operations.

This information security policy covers the protection of the organization data as well as personal data. This is because data is regarded as a vital asset that in the business operation of the organization. In cases where an organization's critical data is not secure, cannot maintain its confidentiality, integrity, and availability, it will have an impact on the organization; whether financially, credibly, or reputationally. The information mentioned in this policy is not limited to electronic form only, but can also be in other forms, such as documents, publications, film, or even in the form of conversations. However, the protection of electronic data will be largely discussed because most corporate data is in electronic form and is likely to increase in the future.

In order to ensure that the Company's information security measures are in comply with the international standard ISO/IEC 27001 version 2022, the Company divides information security control measures into 4 groups as follows:

1. Organizational controls
2. People controls
3. Physical controls
4. Technological controls

2) Information Security Objectives

2.1) To stabilize the information technology system and secure from cyber threats and make it ready for use and fit the business needs of the organization.

2.2) To ensure that the organization has systematically implemented information security in the same direction.

2.3) To ensure that the accurate information and its use by authorized persons.

2.4) To prevent information from misuse, destruction, or unauthorized disclosure.

2.5) To determine information security responsibilities and raise awareness of information security to relevant departments and personnel.

3) Organizational controls

Policy content and actions

3.1) Policies for information security

3.1.1) Policies for Cybersecurity and Information Security

1) This Cybersecurity and Information Security Management Policy is prepared in writing according to its purpose and scope and approved by the management or the Board of Directors. It shall apply to personnel at all levels of the organization, from executives, employees, as well as third parties involved in the use of information, assets, and media of the organization.

2) Executives, employees, and third parties involved in the use of information assets of the organization have a direct duty to support and comply with the regulations on the safe use of the organization's information systems and cooperate in the strict implementation of the policy. Violation of this policy is considered a serious offense with maximum penalties according to the organization's regulations.

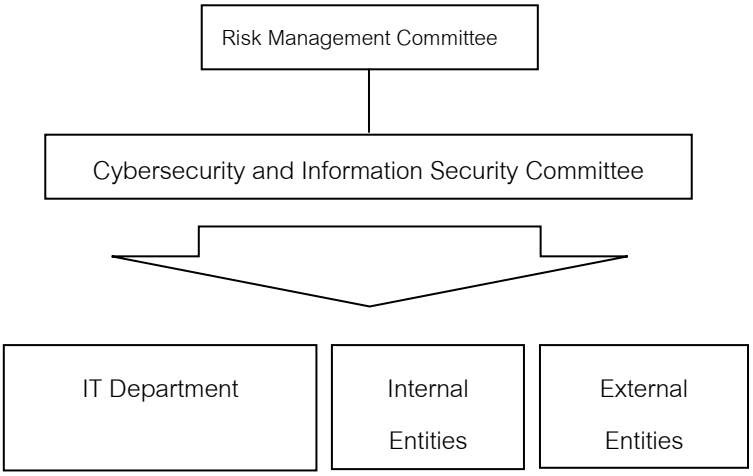
3.1.2) Review of The Policies for Information Security

The Cybersecurity and Information Security Committee may review and update this Policy from time to time to reflect changes and trends in future risks that may affect the organization's information security, such as amendments to laws including laws on personal data protection, changes in information technology strategies or directions, or significant changes such as changes in organizational structure or technology structure, etc. Meanwhile, when this Policy is updated, the Company will notify Users by displaying a "Updated version" message at the link of the Cybersecurity and Information Security Management Policy.

3.2) Information security roles and responsibilities

The Management Team gives importance to and supports the cybersecurity and information security management by approving the establishment of the Cybersecurity and Information Security Committee as follows:

1) The structure of the Cybersecurity and Information Security Committee is shown in the picture below.



Picture 1 shows the organizational structure of the Cyber Security and Information Committee.

2) The Cybersecurity and Information Security Committee consists of executives of the following departments:

(1) Vice President - IT	Chairman of the Committee and Chief Information Security Officer (CISO)
(2) Information Security Manager	Working Team and Secretary
(3) Operations Specialist	Working Team
(4) Human Resources Specialist	Working Team
(5) Business Development Specialist	Working Team
(6) Finance Specialist	Working Team
(7) Data Protection Officer	Working Team

3) The Cybersecurity and Information Security Committee has the following duties:

(1) Review, approve, and update the Information Security Policy as required or according to the situation.

(2) Plan public relations and train personnel in all entities about information security.

(3) Review and endorse information security-related projects.

(4) Plan, monitor, and manage risks arising from system limitations.

(5) Verify, review, and evaluate the continuity plan for security in case of an emergency.

3.3) Segregation of duties

The Risk Management Committee determine the roles, duties, and responsibilities of relevant persons according to the structure of the Cybersecurity and Information Security Working Team as follows:

1. Information Technology Department

Established to prevent organization damage caused by data threats such as data loss or data breach, etc., and ensure that data related operations are secured at a level consistent with the organization's business goals.

1.1 Chief Information Security Officer : CISO

(1) Being the Chairman of the Cybersecurity and Information Security Committee and is responsible for information security and leads all operations related to information security in the organization.

(2) Set goals and information security policy to be in line with the organization's strategic plan.

(3) Present operational plans, policies, budgets, manpower, as well as operational plans on information security for approval from senior executives and to raise senior executives' awareness of the importance of information security.

(4) Analyze and manage risks related to information security, as well as assess options for appropriate response to information security risks.

(5) Develop information security policies to ensure the organization’s system stability, accuracy, and confidentiality of data.

(6) Manage and monitor information attacks with an intruder prevention system, implementing intruder detection and warning systems or virus removal management systems, as well as making long-term business plans or disaster recovery plans to recover systems in times of emergency.

(7) Contact and maintain relationships with business partners, organizations, or third parties related to information security matters in both the public and private sectors.

(8) Review and approve information security policies, procedures and organizational guidelines to suit the importance of business processes.

(9) Establish an information security team to work in times of emergency in the organization.

1.2 Information Security Manager

(1) Report directly to the CISO on all operations related to information, including regularly reporting progress in information security to the CISO.

(2) Design information security policies, including organizational procedures and practices, to suit business process priorities.

(3) Review all policies and procedures related to information security.

(4) Act as an information security consultant to CISO to help analyze and properly manage information security related risks, as well as provide information security knowledge to other departments.

(5) Ensure that the processes and controls described in this Policy are implemented sustainably.

(6) Manage and monitor information attacks by employing an intruder prevention system to detect and notify of intruders, or antiviral software, as well as developing business continuity or disaster recovery plans to recover the system in the event of an emergency.

(7) Examine and monitor information security communications.

(8) Be prepared for situations and constantly learn new things about information.

(9) Control and manage the Information Security Team to be able to work in the event of an emergency in the organization, such as a computer virus outbreak.

1.3 IT Infrastructure Team

(1) Maintain the IT infrastructure to ensure smooth operation.

(2) Protect, inspect, and monitor the IT infrastructure to ensure information security.

(3) Perform duties in the event of an emergency in the organization, such as recovering system from emergency, troubleshooting computer virus outbreaks, etc.

(4) Consult and assist in the development of systems, as well as in the organization of educational activities and training, and raise user awareness of information security in business applications.

1.4 IT Business Application Development Team

(1) Maintain business application systems to ensure smooth operation.

(2) Protect, inspect, and monitor the information security of business applications to ensure information security.

(3) Perform duties in the event of an emergency in the organization, such as recovering the business applications system from emergencies, etc.

(4) Consult and assist in the development of business applications, as well as in the organization of educational activities and training, and raise user awareness of information security in business applications.

2. **Internal entities** are all employees of the organization who are involved in information in any way and can be divided as follows:

2.1 Human Resources Department has the following duties:

(1) Provide advice on employment policies, performance evaluation, and other HR-related issues, including advice on personal information.

(2) Provide administrative support to recordkeeping required to comply with laws, regulations and

internal policies related to human resources, which may be necessary to control access to the system and verify access to the information system for IT Department.

2.2 **Legal Department** is an entity that conducts legal activities for the organization and provides expert legal advice to its management and employees. It is responsible for the followings:

(1) Conduct business activities in accordance with current laws/regulations.

(2) Investigate crimes against organizations and prevent legal action.

(3) Protect properties, assets, and employees of the organization from legal risks.

2.3 **Head of division/Head of department** has the following responsibilities:

(1) Advise and emphasize to subordinates the importance of information security and the need for appropriate data protection for business operations.

(2) Make business decisions in line with Cybersecurity and Information Security Management Policy.

2.4 **Data/Information owner** has the following responsibilities:

(1) Own and fully control their data/information in accordance with the law and other related operational requirements.

(2) Define, manage, control, create, process, dissemination and dispose of data/information.

2.5 **Data Protection Officer: DPO** is a controller or processor who is required to demonstrate compliance and has the following responsibilities:

(1) Provide advice and knowledge on compliance with important requirements related to the Personal Data Protection Act: PDPA to data controllers, data processors, and other relevant parties.

(2) Examine the organization’s access to and management of personal data to ensure compliance with the requirements of the PDPA and the organization's data protection policy.

(3) Evaluate and specify the purpose of the use or dissemination of personal information and clarify the data subject's rights and the organization's protection measures for personal information.

(4) Coordinate with the Personal Data Protection Committee in case of issues arise regarding the application of the Personal Data Protection Act inside the organization.

(5) Maintain the confidentiality of the personal data known or acquired in the course of performing duty.

2.6 **Employees** are all employees of the organization, who are involved in information in any way and are responsible for the followings:

(1) Strictly comply with Cybersecurity and Information Security Management Policy.

(2) Maintain the confidentiality of corporate information and not revealing the password to access their own system.

(3) Maintain the confidentiality of personal data and consent of the data subjects.

(4) Report cybersecurity and information security incidents and safety issues when an incident occurs.

(5) Use corporate information and information assets responsibly and only for tasks for which they are responsible or authorized.

External entities are outsiders who work in an organization or work for an organization and are involved in the use of information or other information assets of the organization, such as service providers/vendors, contractors, or authorized persons with the same responsibilities as employees of the organization.

3.4) Management responsibilities

Executives of all levels, department heads, and supervisors of all departments must supervise personnel, temporary personnel, and contractors (individuals) to ensure compliance with the organization's policies, standards, and procedures, including being aware of their Cybersecurity and Information Security responsibilities.

3.5) Contact with authorities

IT Department must create a contact with authorities, which includes external parties which related to cybersecurity and information security and must review and update this contact with authorities at least once a year.

3.6) Contact with special interest groups

1) IT Department must coordinate with specific groups which related to cybersecurity and information security to bring their experience and knowledge to improve the information security of the organization.

2) IT Department must liaise with external agencies to receive intrusion warnings and incident reports, as well as to exchange information on intrusion incidents and prevention methods.

3) IT Department is responsible for coordinating internal and external information security function.

4) Each entity must designate at least one representative to be responsible for the information security function.

3.7) Threat intelligence

Data related to cybersecurity and information security threats must be collected and analyzed to produce cybersecurity and information security data or intelligence.

3.8) Information security in project management

Cybersecurity and information security must be integrated into project management, with the project manager in charge of all matter.

3.9) Asset Management

Asset means property related to data, such as software data or equipment involved in the processing. More than that, the organization should fix the asset owner to supervise and control such property. The asset owner may assign a third party to take care and control of the asset on his behalf. However, the asset owner remains the most responsible person for such assets in order to properly identify the organization's assets and properly determine their responsibilities for asset protection.

3.9.1) Inventory of Assets

The Information Technology Department must register the assets account in the information system. In case of inability to so, it must follow the form related to the organization's information and personal information by specifying details in the information system.; or follow the form of an authorized officer. The Information Technology Department will investigate the asset with the asset owners in every entity to improve the asset account regularly at least once a year.

3.9.2) Ownership of Assets

In the registration of assets, each agency must designate an asset owner who is responsible for the preservation of that property. The asset owner must verify the accuracy of the details of the asset in the asset register as well as inform the asset administrator of any changes made to the asset.

3.10) Acceptable Use of Assets

Rules for the proper use of information, assets concerning information, and information processing equipment must be specified in writing. Users, employees, or external entities must agree to the terms of use of data and information assets.

3.11) Return of Assets

Staff and employees of all external entities must return all corporate assets held by them. Upon termination of employment, termination of contract, or termination of employment agreement, assets related to information technology must be inspected by the Information Technology Department first. Or, in case of inability to register in the information system, it must register with the asset return form if the inspection results show that there is damage or some information is missing, the asset owner is responsible according to the agreed terms.

3.12) Information Classification Policy

In defining criteria for data classification so that data is classified and properly protected according to data management guidelines in each layer. In addition, the policy defines the roles of data subjects and data administrator in relation to the management of data class. This is to provide information with an appropriate level of protection and align with the importance of that information to the organization.

Information must be classified as confidential based on legal needs, values, priorities, and sensitivity levels. If the information is disclosed or altered without permission, the Cybersecurity and Information Security Committee prepares a Class of Confidential Information Document for entities to register documents according to the specified class as follows:

1. Level 1 Public

   Data that can be known in general without blocking or data that is required by law to be disclosed.

2. Level 2 Internal

   Data that the data subject sees that it can be disclosed to all employees within the organization or can be disclosed to people outside the organization who is listed in the registration of persons entitled to receive the data only.

3. Level 3 Restricted

   Data that the data subject considers that cannot be disclosed to all employees. This type of data will only be provided to those who are involved and need to perform the work. It is the use of privileges that need to be sufficiently known for the performance of tasks, whether it is limiting permissions to employees within the business group's organization (HUB), departments, division, groups of related parties. For people outside the organization, it can be disclosed to only those who is listed in the registration of persons entitled to receive the information.

4. Level 4 Confidential

   Data that has a business effect of the Company, which is used only by certain groups of users of the organization (mainly executives). It cannot be disclosed to all employees or people outside the organization. This type of data needs to be encrypted and must be accessed only by the persons listed in the data acquisition grantee registration. For people outside the organization, it can be disclosed to only those who is listed in the registration of persons entitled to receive the information and receive approval of the use by management.

5. Level 5 Personal

   Data that can identify the identity of the data subject (Personal Identifiable Information) or link to that person, both directly or indirectly. It will be used within the organization only with the consent of the data subject. It cannot be disclosed to third parties before obtaining consent from the data subject.

3.13) Labeling of information

Organizations must determine how to label data appropriately, in accordance with the class of confidentiality of the data.

3.14) Information transfer

The organization requires the security of information transferred within the organization and/or transferred with external organizations.

3.14.1) Information transfer policies and procedures

Entities wishing to exchange information with external entities or business partners must comply with the standards and relevant legal requirements and regulations.

3.14.2) Agreements on information transfer

1) Entities wishing to exchange information and/or software programs in the confidential level upwards must check the rights concerning exchange information and/or software programs with external persons or entities by coordinating with legal entities to check legal restrictions. The corporate regulations and must be approved by the data subject before exchanging information and/or software programs with external persons or entities.

2) Legal entities must prepare/update confidential agreements or contracts to comply with specified standards.

3.14.3) Electronic Messaging

Information related to electronic messaging must be properly protected by

1) The system administrative entities must improve a secure system for transmission of electronic information to prevent unauthorized access, alteration, and modification of electronic messages.

2) The administrative entities must manage and control the electronic mail system in accordance with the standards and related laws.

3) Users of electronic mail must use electronic mail in accordance with specified standards.

3.15) Access Control

To limit access to information and information processing equipment in order to reduce the risk of inappropriate use, it is necessary to control access to the information system by considering the appropriateness of system access based on necessity. Information technology units must compile an access log into the information system, or in cases where it is not possible to register in the information system, they should record using form that complies with the information security policy. Such registration should then be reviewed in accordance with business requirements and information security needs.

To prevent unauthorized access to the system and to prevent the use of people who do not have access rights to the operating system.

3.16) Identity management

The lifecycle of identity data, which is a part of the authentication process for system access, must be managed throughout its entire lifecycle.

3.17) Authentication information

The allocation and management of data related to authentication must be controlled through management processes, which include providing guidance to personnel on appropriate handling of such identity verification data.

This is to prevent unauthorized access to the system and to emphasize that system users are aware of the security in using the data system. Users must cooperate in using passwords and must know the procedure when finishing tasks on the computer.

3.17.1) Use of Secret Authentication Information

Users must comply with corporate practices for data usage. Authentication of confidential information are as follows:

1) Login passwords are confidential, and users must not share or disclose their passwords to anyone else.

2) The user must set up and use the password that contains combination of at least 8 characters of numbers, symbols, and letters (for information system administrators, a secure password must be set with a minimum length of 14 characters).

3) Users must regularly change their passwords every 90 days whether or not the system prompts them to do so. And the users must not set up same the password with the original one at least 12 times (except password for user ID used for information system).

4) Users must check whether their rights they have to access the system are appropriate to their responsibilities. If they find that the rights granted are inappropriate, they must notify their supervisor to consider and make the necessary adjustments.

3.18) User Access Management Policy

To control access for only authorized users and prevent unauthorized access to the system and services, records should be made in the information system. In cases where it is not possible to record in the information system, registration should be done using the 'User Registration and De-registration Form'. The control of users' rights in processes related to system users starts from the registration request up to the revocation of rights when certain users no longer need access. This also includes controlling of the rights of users with special permissions who can modify various system rights.

3.18.1) Account Registration and Deregistration

The official registration and de-registration processes must be followed to ensure proper access rights.

1) All employees who have access to the data system must have a specific user ID to log in.

2) User ID is an individual ID, not Shared User Account in case of employee resignation. If employees resign, that user IDs must not be reused.

3) User accounts that are used for monitoring or maintaining the system at all times is required to have Shared User Account which must be assigned the lowest access right i.e., Read Only.

4) Passwords for users of information systems that must always be active, and password changes that affect the use of a system/service account, must be set to the bare minimum privileges necessary. The access log must be logged every time a password is used to access the system.

3.18.2) Access Right Change

1) The request for access to any system must be considered and approved by the supervisor in the department.

2) The department of data ownership and IT department must immediately remove the rights of users whose access to the system is no longer required.

3.18.3) Review of User Access Rights

The Cybersecurity and Information Security Committee must review the general user access rights every six months and the administrator access rights at least once a year. IT Department provides the system owner with a list of user information and access permissions to verify and sign off. If an abnormality is found that requires correction, IT Department should be notified so that it can be fixed.

3.19) Information Security in Supplier Relationship Policy

The organization must have established processes and procedures to manage information security risks associated with the use of the products and/or services of third party service providers, to protect corporate assets accessed by third party service providers, to maintain the level of security and service level as agreed in the third-party service agreement, and to establish and maintain the level of security of the third party's performance in accordance with the agreement.

3.19.1) Cybersecurity and Information Security Policy for Supplier Relationships

Cybersecurity and information security requirements for mitigating risks associated with outsourced access to corporate assets must be defined, agreed upon with the service recipient, and documented in writing.

3.20) Addressing information security within supplier agreements

Entities employing the supplier who has access to processing, communications, management of information, and/or information systems are required to have the supplier who is an outsourced service provider sign a confidentiality agreement or non-disclosure agreement in accordance with the Policy, which includes a clause on the liability of the supplier if damages occur.

3.21) Managing information security in the information and communication technology (ICT) supply chain

Entities employing the supplier who has access to processing, communications, management of information, and/or information systems are required to establish an agreement with the supplier to outline the responsibility of the supplier in all cases when the supplier subcontracts to other suppliers (supply chain).

3.22) Monitoring and Review of Supplier Services

Organizations must regularly monitor, review, and assess the services provided by suppliers. In cases where the company hires an external entity related to the operation of storing documents containing employees' personal data, such as a document storage company, the company will require the hired agency to keep the data confidential for the security of employees' personal data and not to use such documents for purposes other than the company's operations, and

1) Service must be audited by external entities. The person in charge of the inspection must have knowledge and understanding of information security and personal data as well as terms and conditions.

2) In the event of an incident caused by a third party which affects safety, procedures must be taken to maintain the accuracy of evidence and legal action, if necessary, such as non-disclosure agreements, etc.

3.) An evaluation of suppliers is conducted annually. The results will be recorded in the supplier evaluation report in the information system. In cases where it is not possible to record in the information system, the process should be carried out using the form.

3.23) Information security for use of cloud services

The processes for procuring, using, managing, and terminating Cloud services must be defined in accordance with the organization's needs on information security.

3.24) Information security incident management planning and preparation

To provide a consistent and effective approach to information security management, including reporting situations and weaknesses in information security and personal data in order to have a consistent and effective approach to incident management related to cybersecurity and information and personal data.

3.24.1) Responsibilities and Procedures

It is necessary to define roles, responsibilities, and operational procedures for effective management to ensure a swift, efficient, and prioritized response to information security incidents. This should be recorded in the information system. In cases where it is not possible to record in the information system, documentation should be prepared for incident reporting using the incident report form or reporting violations related to the protection of personal data (Internal Privacy Policy).

3.24.2) Reporting Information Security Events

Any issues that have been notified and resolved within a timely manner will be processed to summarize it into a report. This is to show that in the past period, in order to summarize into a report, it is to demonstrate what issues were most prevalent during the past period, what caused these problems, and what measures can be taken to prevent

these issues from occurring in the future. Meanwhile, the Information Technology Authority will submit a summary report to the Cybersecurity and Information Security Committee every 6 months to jointly consider problems and formulate solutions to prevent problems that arise in the future.

3.24.3) Breach Management

As the security and protection of your personal data is the Company's top priority, if there is a breach, the Company will notify you of the incident that may cause your personal data to be compromised, as detailed below.

- [Specify the date and place where the event occurred]
- [Company details – Details of the types of data that may be affected.]
- [Measures that the company has already taken and are going to take to mitigate the impact]
- [Other details if applicable]

In addition, the Company will notify such incident to the Personal Data Protection Committee to comply with its duties under the Personal Data Protection Act B.E. 2562

3.25) Assessment and decision on information security events

1) The Incident Response Team (IRT) must define an information security incident category.

2) The Incident Response Team (IRT) must define the severity level of an information security incident.

3) The Incident Response Team (IRT) must assess a preliminary situation by analyzing the extent, severity, impact, and damage caused by an information security incident.

3.26) Response to information security incidents

1) Incident Response Team must take control of the incident as quickly as possible so that the information security incidents have the least impact on the organization.

2) Incident Response Team (IRT) is responsible for resolving information security incidents by identifying the causes and taking corrective action to eliminate information security incidents as quickly as possible.

3.27) Learning from information security incidents

Incident Response Team (IRT) must present statistical data, overview, trends, root cause of information security incidents, guidelines on supervision and/or other necessary information related to information security incidents to the IT Department for acknowledgement and support the planning of corrective actions and/or establishing guidelines on supervision and/or auditing to prevent repeat information security incidents.

3.28) Collection of evidence

The Incident Response Team (IRT) must gather preliminary evidence for information security incidents that is sufficiently reliable to ascertain the cause of information security incidents and can be used as evidence in court.

3.29) Information security during disruption

To prevent and cope with business disruptions caused by threats to the operation of the system, such as accidents, natural disasters, or unforeseen events that causes damage to the organization, a Business Continuity Management Plan (BCP) as documented (P-ISP-1301) should be developed to reduce the severity of the impact of such incidents to an acceptable level and to be able to continue the core business of the organization.

3.29.1) Planning Cybersecurity and Information Security Continuity

The organization must determine the needs of information security and continuity of the disaster that happens, such as in the event of a disaster, executives or related entities must manage processes to develop and maintain business continuity. To do so, the followings must be taken into account:

1) Analysis and assessment of risks affecting the business operations of the organization.

2) Organizing strategic documents to create business continuity and to be in line with the business goals of the organization.

3) Training for employees to be aware of security and understand the plans to follow.

4) Assignment of responsibilities for coordination, developing, reviewing, and updating plans.

3.30) ICT readiness for business continuity

3.30.1) Implementing Cybersecurity and Information Security Continuity

Organizations must establish, document, execute, and update processes, procedures, and measures to ensure the desired level of information security continuity in the event of a damaging incident.

1) Communicate to all employees about the emergency action plan.

2) Test and practice plans to create business continuity to a set schedule.

3) The owner of the plans and guidelines for which the plan owner is responsible for maintaining, testing, developing, criteria, requirements, and conditions for the implementation of the plan.

3.30.2) Verify, Review, and Evaluate Cybersecurity and Information Security Continuity

Organizations must periodically review the prepared continuity measures to ensure that they are still appropriate and effective in case of adverse events or disruptions. The foundation of business continuity management is understanding the processes and the events that can lead to business operation disruptions. Therefore, the process owner entities including those in charge of business systems that support those processes, must participate in identifying events that could impact business operations as well as in risk assessment. This ensures accurate and comprehensive data for the subsequent development of a business continuity management plan.

3.31) Compliance With Legal and Contractual Requirements Policy

To avoid violation of legal obligations, regulations, or employment contracts related to information security, including personal data protection, and security needs.

3.31.1) Identification of Applicable Legislation and Contractual Requirements

All requirements related to the law, regulations, and employment contracts, including organizational procedures to comply with such requirements must be clearly stated, made in writing, and updated.

3.32) Intellectual property rights

For each system and for entities, organizations require that contractual documents related to software copyright law and intellectual property rights be stored at the information entities which will be recorded in the information system. In case of inability to record in the information system, it will be stored in the contract form to control the number of users not to exceed the number of licenses. Plus, users are required to use only authorized software.

3.33) Protection of records

Those who have record data related to laws and business requirements must manage, store, and destroy record data, including protecting record data from loss, destruction, falsification, and misuse of log data.

3.34) Privacy and protection of personally identifiable information

Personal data of users and employees, both in hard copy and electronic form, is considered confidential information which requires prior approval from the data subject only.

3.35) Independent review of information security

Independent entity must review compliance with the policy at least once a year to support the development of information security and report the results of the review to the IT Department.

3.36) Compliance with policies, rules and standards for information security

To ensure that cybersecurity and information security practices are in line with the organization's policies and procedures.

3.36.1) Compliance with Security Policies and Standards

Heads of departments are obliged to review the conformity of procedures under their own responsibility by comparing with standard policies and relevant security requirements. The Cybersecurity and Information Security Committee requires the Information Security Entities to present the information structure systems, main security systems, new technologies, and technical data to the Cybersecurity and Information Security Committee once a year. This is to determine the compliance with the organization's information security policies and standards. The Cybersecurity and Information Security Committee has prepared a list of tasks that need to be performed in the information system. In case of inability to record in the information system, they will be documented in the Cybersecurity and Information Security Review Form. This form serves as a medium to check if all the review procedures have been fully implemented.

3.36.2) Compliance with Personal Data Protection Act and Standards

Heads of departments are obliged to review the conformity of procedures under their own responsibility by comparing with standard policies and relevant personal data protection regulations. The Cybersecurity and Information Security Committee requires the Information Security Entities to present the information structure systems, main security systems, new technologies, and technical data to the Working Team once a year. This is to determine the compliance with the organization's information security policies and standards. This is to determine the compliance with the organization's information security policies and standards of personal data protection. The Cybersecurity and Information Security Committee has prepared a list of tasks that need to be performed in the information system. In case of inability to record in the information system, they will be documented in the Cybersecurity and Information Security Review Form. This form serves as a medium to check if all the review procedures have been fully implemented.

3.37) Documented operating procedures

To ensure that the operation of information processing equipment is accurate and secure in order to ensure safe and accurate operations in the processing system; roles and responsibilities, as well as management and operational procedures for the system, should be clearly defined. These responsibilities should consider appropriate separation of duties. In addition to standard operating procedures, there should be specific steps in place to respond to security incidents within the processing system, to address such situations.

The system administrative entities and information systems and network processing entities must always make/improve operating procedure documents to be accurate, complete, and up to date.

3.38) Document Management Policy

To ensure that employees can manage the company's documents, which are considered important information, they should be properly controlled and managed.

3.38.1) Document management procedures and division of authority in document management.

There are 3 steps to document management. The first is the document owner prepare the draft document and send it to the document reviewer. After the review, it will be presented to a document approver to approve. Then, the approved document can be used in communication or published internally and externally.

Document Accountability List

(1) The document owner must not be a document reviewer or document approver.

(2) The document reviewer must not be a document owner but can be a document approver.

(3) The document approver must not be a document owner but can be a document reviewer.

Rights to process documents

- The document owner has the right to define or modify the Information Classification Level: (ICL) of the document.

- Only the document owner has the right to bring or allow the approved documents to be communicated or published, both inside and outside the Company. According to the requirements of the documents in each confidentiality class.

3.38.2) Document confidentiality classification

(1) The classification of confidentiality must be defined and embedded in the document body in a prominent area, such as the header, footer, either in paper or electronic file format.

(2) Documents that are removed from computer systems must be correctly assigned a confidentiality class.

(3) Documents in paper form must be define a class of confidentiality and stored in a secure and protected location.

(4) Documents for which no confidentiality class is defined is automatically assigned an "internal use only" class of confidentiality.

3.38.3) Approved Document Management

Approved controlled documents or documents with an Information Classification Level (ICL) as confidential or personal information must comply with the following requirements:

- Documents are reviewed, updated (if necessary), changed-controlled, version-controlled, approved, and electronically documented to be stored in the WHA Document Management System (WHA-DMS) before being communicated or published.
- Documents are clearly assigned an Information Classification Level (ICL) and are protected according to the requirements of each class.
- Documents in electronic format must be stored in WHA-DMS only to ensure availability of access by authorized persons. Document access rights must be set correctly and appropriately.
- Documents may not be copied or published without obtaining permission from document owner.
- Pre-update versions of documents must be marked as deprecated and must not be used.

3.38.4) Types of Control Documents

The Company's control documents are as follows:

(1) Organization policy

(2) Organization procedure

(3) Contract / Agreement

(4) Letter of engagement

(5) Land deed)

(6) Permit

(7) certificate / license)

(8) Drawing

(9) Work instruction

(10) Form template

3.38.5) Draft Document Management

All draft documents will be treated as follows:

- Do not need to be archive in WHA-DMS
- Are invalid and not implemented.
- Are clearly assigned a confidentiality class and are protected according to the requirements of each class of confidentiality.

3.39) Cybersecurity and Information Security Risk Management

Cybersecurity and information security risk management are not solely the responsibility of the Information Technology Department. Personnel at all levels and departments in the organization must be aware of and have guidelines for risk management arising from information technology covering both policies and practices for the organization to be able to prevent, detect, and respond to potential risks. The Cybersecurity and Information Security Committee has designed cybersecurity and information security risk assessments and risk mitigation processes as follows:

3.39.1) Cybersecurity and Information Security Risk Assessment

- The Company should design and perform cybersecurity and information security risk assessments as follows:
  - Define risk acceptance criteria and criteria for assessing cybersecurity and information security risks.
  - Ensure that cybersecurity and information security risk assessments produce valid results.
  - Identify risks:
    - Implement a risk assessment process associated with the loss of confidentiality, integrity, and availability for data and information system.
    - Identify the risk owner.
  - Risk analysis:
    - Assess the potential consequences that would occur if the risks listed above actually occur.
    - Assess the actual possibility of the risks listed above, and
    - Determine the level of risk
  - Risk assessment:
    - Compare the results of the risk analysis with the risk criteria set above; and
    - Prioritize risks
- The Company should perform cybersecurity and information security risk assessments at planned

intervals or when significant changes are proposed or occur, taking into account the above-defined risk criteria established.

- Risk assessments shall take into account vulnerabilities, threat sources, and planned or in place security controls to determine the resulting level of residual risk posed to the organization's operations, assets, or individuals that support business functions.

3.39.2) Cybersecurity and Information Security Risk Treatment

- The Company should design and implement the following treatments to reduce cybersecurity and information security risks:
  - Set appropriate cybersecurity and information security treatments, taking into account the risk assessment results, for example,
    - Establish appropriate control systems or processes to mitigate risks.
    - Minimize risks by avoiding, preventing, or disallowing actions and situations that may pose a risk.
    - Transfer or diversify risks to others such as insurance or business partners (in contracts).
    - Implement a process for risk acceptance if the risk is clearly acceptable to the organization.
  - Establish a cybersecurity and information security plan and implement it accordingly.

A cybersecurity and information security plan should be formally approved by the Cybersecurity and Information Security Working Team.

4) People controls

To provide security guidelines related to human resource management processes from the step of admission until termination of employment. This is because the human resources process is necessary to help keeping the organization's information secure.

To reduce information risks caused by personnel, either from intentional and unintentional information security breaches, or from neglect to perform duties related to information security.

To increase the safety associated with the management process for employees that will be terminated by identifying the responsibilities and roles of those involved in the process. It also provides better control over information security, and to protect the interests of the organization as part of the process of changing or termination of employment.

Policy and Action

4.1) Screening

Background checks of job applicants must be carried out in accordance with laws and regulations. The human resources department should review an individual's history before hiring them; for example, education proof, reference persons, work history from a previous workplace, and official documents issued by government agencies, etc. Especially, the positions concerning vital data of the organization are required special investigation.

4.2) Terms and Conditions of Employment

Terms and conditions in employment contracts is clearly specified duties and responsibilities (job description), and also identify information security responsibilities. Violation or neglect of the duties and policies is considered an offense. The penalty is determined according to the penalties of the organization, which depends on the severity of the impact on the organization.

4.3) Cybersecurity and Information Security Awareness, Education and Training

The human resource department provides all employees trainings by information technology entities or external entities at least once a year to raise awareness of cybersecurity and information. Moreover, this is to conduct an assessment at least once a year to acknowledge the organization's additional security policy, security breach incidents, and new case studies, while IT agencies must be trained by external agencies at least once a year.

4.4) Disciplinary Process

Disciplinary procedures must be formally established, and all employees should be informed about these procedures through the company's trustworthy information system. In cases where it's not possible to proceed through the information system, employees can be informed either through information system or by signing a receipt acknowledging the guidelines on securely using the organization's information system available at the human resources department. The set disciplinary procedures aim to address employees who violate the organization's

information security. The human resources and legal entities should stipulate penalties for employees violating information security policies and related practices.

4.5) Responsibilities after termination or change of employment

Human resources departments and entities jointly determine the procedures for employees who leave the organization at the termination of their employment, or when employment is changed as follows:

1) Related entities have the duty to inform the Human Resources Department about the resignation or change of position of the employees.

2) Human Resources Department complies with user access management policies, Article 3.18. In case of inability to record in the information system, action should be taken according to the form by notifying IT entities immediately after transferring, resigning, or terminating the employment of the organization's employees. So, the rights and access to work systems and the organization's area will be revoked.

3) The Information Technology Department complies with the article of returning Assets, article 3.11. and record in the information system. In case of inability to record in the Information System, action should be taken according to the form by inspecting the employees' assets and reporting the inspection results to the Human Resources Department.

4) Information Technology Entities makes necessary data backups of such employees for a period of 1 year and inform the heads of relevant departments how to access such data.

4.6) Confidentiality or nondisclosure agreements

Organizations must prepare and review to improve confidentiality agreements or non-disclosure agreements to align with the organization's policies, in compliance with relevant laws and best practices.

4.7) Remote working

It is a supportive measure for remote work from a particular location. It must be implemented to protect data accessed, processed, or stored from such a place.

1) It is clearly specified who is allowed to work remotely.

2) In cases where external units need to remotely access, there must be logging and continuous monitoring of their activities. The password for external units should be changed after each use, or there should be a set expiration for user/password credentials, depending on the job's requirements.

3) Session Timeout is set in case the remote person leaves the screen behind.

4) Record remote connections in the information system. In cases where this cannot be done, record the remote connections in the information system. If it's not possible to record in the information system, action should be taken according to the form.

4.8) Information security event reporting

In the event that employees encounter weaknesses or information security incidents, the employees are obliged to notify the entities responsible for reporting unusual events to be aware and take preventive measures before such anomalies occur.

5) Physical controls

This is to prevent unauthorized physical access, damage, and interference with the organization's information and information processing equipment in order to establish security control areas within the organization and to determine appropriate preventive measures according to the level of risk in each area. Such controls protect basic information and information processing systems from unauthorized access, damage from threats, and interference, regardless it is intentional or natural disasters.

To prevent loss, damage, theft, or harm to assets and to prevent disruption to the organization's operations, computer equipment and network devices are considered crucial for information and business operations. Therefore, these devices should be protected from environmental hazards, and there should be restrictions on using such equipment outside the designated locations.

Policy content and actions

5.1) Physical Security Perimeter

The entities provide a server room with an external environment safe from external threats, i.e., the location is in a place that is difficult to access from outsiders, a high-rise building that can prevent water incidents, the surrounding area is open and can be seen clearly if the server room is accessed.

5.2) Physical entry

Area administrative entities must control the physical access of areas designated as special control areas, such as server rooms by allowing only authorized persons to enter and exit special controlled areas.

Security equipment must be provided in order to access the server room as follows:

1) CCTV cameras are installed and inside the room is recorded at all times, which can be viewed retrospectively for 60 days.

2) The Computer System Room and Computer Center (Server or Data Center Room) are rooms with a key lock or a key card system or a system that can verify identification which the access is restricted to only those who have been granted permission.

5.3) Securing Office, Room and Facilities

Organizations must design and implement physical security measures for the office, operation rooms, and equipment rooms in order to provide concrete protection of these areas from various threats, such as assigning entry and exit rights to only authorized persons, installing air conditioning, lighting system, fire extinguishing system, etc.

5.4) Physical security monitoring

Computer centers, office spaces, offices, and equipment rooms should be monitored by surveillance systems. This may include the use of security personnel, an alarm system to alert in case of intrusions, and the installation of CCTV cameras to prevent unauthorized physical access.

5.5) Protecting against External and Environmental Threats

Physical protection against natural disasters, attacks or raids, or accidents must be designed and implemented as follows:

1) Computer centers must have a fire protection system, air conditioning and humidity system, and electrical system.

2) 2 air conditioning units that alternate in operation, set to a temperature of 20-23 degrees Celsius, and maintaining a humidity level of 40-50%.

3) Fuel or hazardous materials should not be stored in a computer center.

4) Water leakage detection devices must be installed for high-risk areas in computer centers.

5) Protective devices against threats from animals must be installed, such as birds, rodents, insects, or crawling creatures in areas at risk of these issues.

5.6) Working in secure areas

1) Entities responsible for specific areas should prepare a manual and/or display security control measures for operations within those secured areas. Furthermore, they should publicize these security control measures to ensure that relevant individuals can perform their tasks correctly within those secured zones.

2) Those who work in areas that require security control are required to have authorization and/or employee card clearly visible at all times when in the area.

3) Those who work in areas that require security control are required to record entry and exit information every time entering and exiting the area.

4) Those who work in areas that require security control must not bring non-operational persons into the area.

5) Those who work in areas that require security control must not have non-corporate network or computer equipment connected to the organization's information system without permission.

5.7) Clear desk and clear screen

1) Users must not leave important documents on their desks without close supervision.

2) Users must securely store important documents whenever they are not in use to prevent loss or unauthorized access. For instance, important documents should be kept in a lockable cabinet every time they are not being used.

3) Users must log out and lock the computer monitor with a password every time whenever they are not in use to prevent use by unauthorized persons.

5.8) Equipment siting and protection

1) The entities in charge of specific area must supervise and ensure that important information equipment is installed in a place that can prevent access to information equipment from unauthorized persons.

2) The entities in charge of specific area must supervise and ensure that important information equipment is installed in a place that can prevent damage from natural disasters, theft, power outages, fire, and harm caused by human.

5.9) Security of assets off-premises

Assets owners must have measures to protect the equipment before taking off-premises. Those devices must be approved before being installed and/or used outside the organization.

5.10) Media Handling Policy

To prevent damage to business operations from unauthorized disclosure, modification, removal, or destruction of information stored on media (Hard Copy and Electronics), media must be properly controlled and managed.

5.10.1) Management of Media

Procedures must be put in place for the management of media in accordance with the information classification scheme set by the organization.

1) The storage media must be named according to the criteria and have a control register.
2) The disbursement and distribution of storage media must be approved by the authorized person of the user entity.
3) Storage media must be counted at least once a year.

5.10.2) Physical Media Transfer

Any media containing information needs to be protected against unauthorized access, misuse, or corruption during transportation.

5.11) Supporting Utilities

Equipment needs to be protected from power failures and other disruptions caused by failures in supporting systems and utilities.

1) Critical computer and network equipment must have an uninterruptible power supply (UPS) to keep the system running or properly shut down when there is a power failure.

2) Uninterruptible power supplies must be regularly inspected according to the manufacturer's procedures to ensure that they can support operation in the event of a power failure.

5.12) Cabling security

The organization must control the electrical wiring and signal cable in accordance with the specified standards. The power and signal cables should be separated in an orderly way to prevent signal interference.

5.13) Equipment maintenance

The asset owner must maintain the equipment so that it is available for use for a specified period of time.

5.14) Secure disposal or re-use of equipment

To ensure that the information and copyrighted software stored on such devices are permanently destroyed before reuse, disposal, or donation, the equipment and storage media must be securely disposed of or destroyed in accordance with officially established destruction procedures when they are no longer in use.

1) Confidential or personal data in the form of a document must be destroyed by shredding, burning, or by other means so that the data cannot be reused.

2) Destruction of equipment and storage media that record confidential or personal data must be approved by an authorized person, and every destruction must be recorded as evidence for future investigations.

6) Technological controls

Policy and Action

6.1) User end point devices

Data that is stored, processed, or accessed by the end device of several users must be protected (this user's end device is generally includes computers, laptops, mobile phones, tablets, and other device capable of data processing. These devices can communicate and transfer data over a network.)

6.1.1) Mobile Device

The organization has established measures to securely control the use of mobile devices related to the organization's information. Users of mobile devices have the following responsibilities:

1) Users can register their mobile devices using their user ID and password to register their access. Information Technology (IT) entities must define permissions and patterns of access to data to ensure cybersecurity and personal data.

2) The IT entities must install the program as necessary to access the data or work systems approved by the supervisor under the user's affiliation taking into account of cybersecurity and personal data.

3) Officers of information entities must have a system to monitor registered mobile devices and a system to prevent intrusion and attacks from outsiders.

6.2) Privileged access rights

The administrators or users with special rights, such as "administrator" or "root", must have controlled access. The use of these privileged accounts on the operating system requires prior request and approval before accessing. And there must be a review of the event logs after the use to ensure that the use of these privileged accounts was strictly in line with approved activities only.

6.3) Information Access Restriction

Access to information and functions in work systems must be restricted in accordance with access control policies. Administrators must ensure that the system displays a warning message, "**Only relevant person is allowed to access**" before connecting to the organization's computer system. Plus, the system must allow users to disconnect from the system if the system is known It is not related to oneself.

1) Every user must have an individual user account to be able to identify and track the usage of each user.

2) User ID for monitoring or administering the system at all times must have a shared user account. The shared user account must have the lowest permissions such as Read Only. And specify only specific groups of users.

3) For user ID used for the information system which needs to be activated all the time, and changing of the password affects the System/Service Account, the system owner must set a strong password after the information system is successfully installed. Plus, for using a password to access the system, there must be a check and log every time it is used.

4) Users should log out of the network (Log-off) immediately when it is finished or no demand to use again.

5) The user has installed a screen saver with a password on the computer. These programs start after a specified amount of time on the computer has been idle.

6) If the computer will be idle for a long period of time, the user must turn off the computer or the end device.

6.4) Access to source code

1) The system administrative entities must determine access rights to the original program (Source code) by allowing access only as necessary for those responsible for their duties. This includes updating user names and user rights to ensure they are correct and always up-to-date.

2) The system administrative entities responsible for storing the source program must have log data stored that sufficiently shows access to the source program for investigate the access, change, and edit occurred to source programs.

6.5) Secure authentication

Organizations must use technology and operational procedures for secure identity verification to limit access to data in accordance with policies related to access control.

In the case of critical information systems, the organizations should consider upgrading authentication to a higher level of security by using multi-factor authentication. The multi-factor authentication is a multi-step information technology login process that requires users to enter additional information in addition to a password.

6.6) Capacity Management

The use of system resources requires communicating, improving, and anticipating of future needs in order to have desired systems. Therefore, the Information Technology Entity has prepared an IT Master Plan into the information system. In case of inability to record in the information system, action should be taken according to the form to ensure the security, easy access, and application according to the rights of organization's information and personal data. Computer software and equipment are prepared to support the work of various entities according to the organizational strategic plan.

6.7) Protection from Malware Policy

To ensure that information, information processing equipment, and personal data are protected from malicious software to control and protect them against unwanted and harmful software.

6.7.1) Controls against Malware

Measures to detect, protect against, and recover from malicious software must be implemented in conjunction with raising awareness among appropriate users.

1) The information technology entities must ensure that the latest version of the virus protection software is installed at the operating system level on every computer and server, and it should be updated to stay current at all times.

2) The information technology unit must specify that the virus detection program runs concurrently with the startup of the processing system and system is using.

3) Files attached to electronic mail or files downloaded from the Internet are detected for viruses before use.

4) Employees are prohibited from taking any action related to the development of viruses or malicious software or keeping them as owners.

5) In the case of importing data storage media from external authorized entities, the person using that data medium must check for computer viruses before using it every time.

6.8) Technical Vulnerability Management Policy

To prevent exploitation of technical vulnerabilities

6.8.1) Management of Technical Vulnerabilities

Information related to technical vulnerabilities and the organization's vulnerability points are collected, assessed, and prepared with appropriate measures. They must be used to manage related risks. All vulnerabilities are stored in technical vulnerability documentation within the information system. In cases where it is not possible to record in the information system, action should be taken according to the form. All vulnerabilities will be reviewed by the Cybersecurity and Information Security Committee at least once a year.

6.9) Configuration Management

This ensures that hardware, software, services, and networks work accurately with the necessary security settings. The settings must not be modified unauthorizedly or incorrectly. The organizations should define processes and tools to enforce the configuring security settings.

6.10) Information deletion

The organization requires that data stored in information systems, devices, or other storage media must be deleted by secure delete means when that data is no longer needed.

6.11) Data masking

To reduce the disclosure of sensitive information, including personal data, in compliance with laws, regulations, rules, and related contractual agreements.

Organizations must employ data masking techniques to ensure that information stored in information systems is not visible or used without authorization. This must be in line with business requirements and consistent with the organization's information system access control policies and relevant laws.

6.12) Data Leakage Prevention

Organizations must apply data leakage prevention measures to systems, networks, and various devices that process, store, or transmit important data.

6.13) Backup Policy

To prevent data loss so that the information processing equipment is accurate, complete, and always ready for use.

6.13.1) Information Backup

Data for information, personal data, software, and system images must be backed up and regularly tested for readiness and usability, in accordance with the agreed-upon data backup policy.

1) There is a preparation of a data backup plan and a system/data recovery test in the data backup plan and recovery test plan, which are recorded in the information system. In case of inability to record in the information system, action should be taken according to the form, the plans are reviewed every year.

2) Prepare manual for data backup and data recovery with all important systems by making the backup and recovery manual in the information system. In case of inability to record in the information system, proceed according to the form.

3) The information technology unit checks the backup status in the system every day that there's a backup, noting its status and updating the backup situation promptly. This is recorded in the information system or, in case of inability to record in the information system, action should be taken according to the form. In cases where the services are utilized from external entities and the information technology unit cannot verify the data backup in the system, the external entities must provide the report of the backup situation every day the backup is carried out to the information technology entities. Additionally, the external entities must summarize the backup situation and send it to the information technology unit at least once a month.

4) The information technology entities is responsible for testing the backup data recovery in all critical systems. The critical systems must be tested according to the recovery plan, and a report should be summarized to inform the Cybersecurity and Information Security Committee at planned interval .

5) Personal computer: Users are responsible for backing up important files.

6.14) Redundancies Policy

To ensure the availability of information processing facilities

6.14.1) Availability of Information Processing Facilities

Information processing facilities must be sufficiently redundant to meet required availability requirements.

6.15) Logging and Monitoring Policy

To provide incident records and evidence

6.15.1) Event Logging

[An event log, which records user activities such as access to information about non-procedural system operations, system failures, and security events, must be recorded, stored, and regularly reviewed. Log storage devices are protected against unauthorized modification and access.

6.16) Monitoring Activities

The organization needs to monitor the operation of networks, systems and applications to detect abnormal behavior and to assess the likelihood of potential information security incidents.

6.16.1) Server Monitor

A report on the working status of servers, including the necessary peripheral equipment should be conducted on a daily basis. Operators will record working status in the information system. If it cannot be recorded in the information system, it must be recorded in the server status log, and a report summarizing the server's working status must be prepared for the Management every 6 months.

6.16.2) Network Monitoring

The information entity has monitored the organization's network usage and has prepared a report summarizing the network usage into the information system. If it cannot be recorded in the information system, action should be taken according to the form to submit to the Cybersecurity and Information Security Committee at planned interval.

6.17) Clock Synchronization

The system administrator must control and synchronize the clocks of information systems in accordance with the specified standards and the requirements of laws or relevant regulations.

6.18) Use of privileged utility programs

1) The system administrator should restrict the number of authorized users and access to system utilities on the computer server and use them only when necessary.

2) The entity that takes care of the clients' computers should restrict the number of authorized users and access to utility programs on their computers to be used only as needed.

6.19) Control of Operational Software Policy

To ensure that the system is working correctly

6.19.1) Installation of Software on Operational Systems

All computer software will be installed by IT Department only, with audits in accordance with IT Asset Management Procedure.

6.20) Network Security Management Policy

To protect information and information processing equipment, to make the network system secure and usable as a medium for transmitting data efficiently.

6.20.1) Network Controls

Networks must be managed and controlled to protect information across systems. The head of the network control entity is responsible for providing network controls, as follows:

1) Define and create a network configuration diagram that clearly displays information about equipment and cable lines used in the communication of all networks by creating and revising a network diagram in the information system to always be up to date. If it cannot be recorded in the information system, action should be taken according to the form.

2) Control the installation of communication equipment in accordance with the network configuration diagram.

3) Implement measures to control the condition and evaluate the efficiency of cable lines, communication cables, and equipment in the communication network to ensure they are always ready for use.

4) Maintain equipment regularly

5) Evaluate the efficiency of the network system at least once a year and develop a plan to improve the network system to support the workload that will expand in the future.

6.21) Security of Network Services

Security mechanisms, service levels, and management requirements of all network services need to be identified and included in network services agreements, whether these services are provided in-house or outsourced. Network service providers must be audited and analyzed for service levels, network security models, and enterprise requirements management.

6.22) Segregation in networks

The entity that administers the network system must divide the network based on the specified groups, such as the information services group, the user group, the executive group, the administrator group, etc.

6.23) Web filtering

The organization requires that access to external websites be managed to reduce the likelihood of access to malicious content, such as malicious programs and malicious software that can in any way damage corporate data and computers.

6.24) Cryptographic Controls Policy

To ensure the proper and effective use of cryptography, to protect the confidentiality, integrity, and accuracy of information and to protect data and sensitive personal data in terms of confidentiality and integrity, it is necessary to consider the introduction of software and techniques to encrypt high-risk and highly-protection-required data.

6.24.1) Use of Cryptographic Controls

A cryptographic controls policy to protect information must be established and followed.

1) All passwords stored in the database are encrypted. Only the owner of the password and the data owner software know such a password.

2) All passwords stored in the personal database are encrypted. Only the owner of the password and the data owner software know such a password.

3) Enable encryption as needed for sending and receiving Email.

6.25) Secure development life cycle

To ensure information security is designed and carried out throughout the system development life cycle:

1) Security must be embedded into the SDLC by defining activities to analyze, plan, and/or create security measures for each phase of the information system development cycle.

2) Security requirements must be defined for the information system that needs to be developed, including

2.1) Input data validation

The system owner entity must develop an information system with an input verification function according to the specified standards to ensure that the data is complete and accurate before importing it to the information system.

2.2) Control of internal processing

The system owner must develop the information system to control the processing according to the specified standards in order to prevent the modification and/or change of information from unauthorized persons.

2.3) Message integrity

System owner entity has a duty to develop the information system to verify the accuracy of messages sent and received in the information system or between information systems. This is to be able to verify that the original message is correct, as well as to control and prevent changes or corrections of messages/information by unauthorized persons.

2.4) Output data validation

System owner entity has a duty to develop information system to control and verify the accuracy of the result logging in accordance with the specified standards. This is to ensure that the results of the processing. It should also sufficiently store result logging for the investigation in case of incidents that affect information security.

3) For information systems that provide services through public networks (e.g., the Internet), the system owner entity should assess risks and plan for risk mitigation.

4) Secure software development principles should be applied.

5) Software development requires a secure approach.

6) During the design and development of the information system, security checkpoints must be defined to ensure that security controls will be developed to meet the specified security requirements, such as conducting a source code review (Security Code Review) before proceeding to software testing.

7) Any issues discovered during the development phase that may affect security must be reported to the project manager or team leader. Every issue must be addressed and documented.

8) The system owner entity and information system developers should receive training on information system development to ensure security and/or knowledge of information security threats annually.

6.26) Application security requirements

To ensure that information security and privacy are integral parts of information systems across the entire lifecycle, including the requirements for information systems that provide services over public networks, and to ensure that the development of the system takes into account safety and adequate control, the organization must consider the security and privacy requirements of the system as well as internal controls before system development.

6.26.1) Information Security Requirements Analysis and Specification

Information security related requirements need to be included in any requirements for new information systems or enhancements to existing information systems.

1) The system owner must specify the information security requirements before developing or procuring a system. This should be documented in the information system. In cases where it's impossible to record it in the information system, it should be prepared as a document in the form of a software development request form within the information system. If it's impossible to record it in the information system, actions should be taken according to the form, which is considered a part of the documentation requirements for system development or procurement.

2) The arising requirement must be approved by the requester's supervisor before being submitted to IT Department to consider the feasibility of its development.

6.27) Secure system architecture and engineering principles

The organization must establish the secure system engineering principles for its information systems to be reliable, have an adequate level of security, and be able to meet its business requirements.

The principles must be applied to the organization's information systems development life cycle (SDLC) and comprise the following fundamental issues that must be considered during the design, construction and/or development of an information system:

1) Security by design

Security measures must be considered and defined early in requirements development phase and is considered a part of the overall information system design. If the requirements of the information system are changed, there must be consideration to adjust or add security measures to always be in line with the changing requirements.

2) Balance risk and control

The chosen security measures must be proportional to risks, costs, business objectives, and the effectiveness of the use of information systems to prevent the problem of selecting ineffective security measures, such as those that are less stringent or more stringent than necessary, resulting in higher costs than benefits received.

3) Usability and manageability

Security measures must be user-friendly and not overburden users. Management of security measures (for example, modifying configuration) should not be unnecessarily complicated to avoid human errors.

4) Defense-in-depth

There should be multi-layered information security measures covering physical and logical security measures at the operating system, database, application, and network levels so that they can work synchronously and replace each other if any of the measures fail or are bypassed.

5) Simplicity

Information systems should be designed to minimize complexity, unnecessary elements, potential errors, and the likelihood of attack by malicious actors.

6) Resilience and Recoverability

Systems should be designed to withstand threats. For example, when security measures fail or are bypassed, the system must restrict or deny access and have recoverability (automatically or by establishing a recovery process) within a timeframe appropriate to business requirements.

7) Confidentiality and integrity

Security measures should be established to protect the confidentiality, accuracy, and completeness of information during processing, sending - receiving, and storage.

8) Enforced policy

Security measures should be designed to enforce information security policies as well as operational procedures, standards, or practices related to the security of the organization.

9) Design for malicious actor/environment

Preventative, detectable, and recoverable security measures should be designed from the perspective of malicious actors who are not within the framework of an organization's information security policy or who attempt to bypass existing security measures. If the information system must be used in an adverse environment, such as during an emergency or natural disaster, additional security measures must be established.

10) Mobility

Security measures should be designed or modified appropriately for operational information systems with mobile devices, taking into account the related information security risks, such as physical security controls, the use of personal mobile devices, network usage, the use of mobile applications, information exchange, and GPS tracking.

6.28) Secure Coding

The organization must apply processes for secure coding to software development.

6.29) Security testing in development and acceptance

Test plans and relevant criteria for system acceptance must be established for new systems, improved systems, and new versions of systems.

1) Determine the accuracy of the result data obtained from the computer system to ensure that the data is accurate and complete.

2) The requester must test and inspect the system in the information system. If it cannot be recorded in the information system, it must be recorded in the Development Request Form.

6.30) Outsourced development

The team using outsourcing must determine the software security requirements and ensure that the outsourced software development adheres to the specified criteria.

6.31) Separation of development, testing and operational environments

Separation of development, testing, and operational environments is needed to reduce the risk of unauthorized access or changes to the operational environment.

1) In system development, there must be a separate environment for the development and production systems.

2) Personal data cannot be used for system testing without the data owner's consent.

3) No confidential or sensitive data may be used during system testing. Data must, if necessary, be masked before being used in system testing.

4) Compilers or other development programs must not be installed on the production system.

6.32) Change management

System changes in the system development life cycle are controlled by following a formally defined IT Change Management Procedure. The Information Technology Department will record changes in the information system. If it cannot be recorded in the information system, it will update the version control documents of the system in the information system, or if it cannot be recorded in the information system, action should be taken according to the form.

6.33) Test information

To provide protection of test data.

6.33.1) Protection of test data

1) System testing and system development teams must obtain approval from the data owner before using production data for information system testing.

2) System testing and system development teams must convert confidential information from the production system before testing and destroy the test information after the test is complete to prevent confidential information from the operation system from leaking during information system testing.

3) The system administrator team should control test system access to ensure the same level of security as the production system.

6.34) Protection of information systems during audit testing

To minimize the impacts of audit activities on information systems.

6.34.1) Information Systems Audit Controls

Audit requirements and activities involving verification of operational systems need to be carefully planned and agreed on to minimize disruptions to the business processes. The Information Technology Department will set a key system audit plan for system audit controls in the information system. If it cannot be recorded in the information system, action should be taken according to the form and submit the assessment results to the Cybersecurity and Information Security Committee at planned interval.

- END OF DOCUMENT -