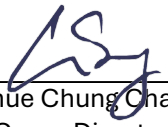
Thai Union Group

Information Security Policy

Approved by:

Thiraphong Chansiri
(President & CEO)



Shue Chung Chan
(Group Director)

Version:	4.0
Published Date:	07-Nov -2025

Document Control

Document	Name-Surname	Position
Owner	David Llamas	Chief Digital Officer
Preparer & Reviewer	Virag Thakkar	Director, Digital Security

Document Change Record

Date	Author	Version	Change Description
15-Jul-2019	Radhakrishnan Selvarangan Nuttawuth Swangpol	v1.0	Initial version.
12-Jul-2023	Radhakrishnan Selvarangan David Florijn	v2.0	Controls updated to align with best practices.
15-Jul-2024	Radhakrishnan Selvarangan	V3.0	Annual review
22-Oct-2025	Virag Thakkar	V4.0	Annual review (Inc. of Shadow IT & AI)

<table>
<tr><td colspan="2">Internal Use</td></tr>
<tr><td colspan="2">Policy</td></tr>
<tr><td rowspan="3">Information Security Policy</td><td>Creation Date: 15-Jul-2019</td></tr>
<tr><td>Version: 4.0</td></tr>
<tr><td>Latest Revision Date: 22-Oct-2025</td></tr>
<tr><td colspan="2">Issued by: Mr. Virag Thakkar</td></tr>
<tr><td colspan="2">Verified by: Mr. David Llamas and Mr. Virag Thakkar</td></tr>
<tr><td colspan="2">Approved by: Mr. Thiraphong Chansiri and Mr. Shue Chung Chan</td></tr>
<tr><td colspan="2">Distribution List: All Thai Union Colleagues</td></tr>
<tr><td colspan="2">Targeted Group: All Thai Union Colleagues</td></tr>
<tr><td colspan="2">Distribution Method: Online Communication</td></tr>
</table>

Table of Contents

1. Introduction

1.1 Purpose

This policy sets out mandatory requirements for companies belonging to the Thai Union Group. The purpose of this document is to ensure that:

1. All appropriate controls and security measures are put in place, to secure and protect
   a. Thai Union Group Digital systems and data;
   b. Personal data collected and/processed by Thai Union Group companies (e.g., in relation to employees, consumers, third parties etc.);

   against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality.
2. Management and Users (as defined below) are made aware that they must ensure the confidentiality, integrity and availability of all systems and data, as required.

1.2 Scope

This policy applies to Thai Union Group PCL and all its subsidiaries and affiliates around the world, in which Thai Union Group PCL holds 50% or more of the share capital and/or voting rights (hereinafter, all together referred to as "**Thai Union Group**" – each company being referred to as a "**Thai Union Group company**").

This policy applies to all Thai Union Group employees, contractors, consultants, and other individuals, including third parties who access or utilize Thai Union Group Digital systems and data with respect to the security and privacy of information (hereinafter referred to as a "**User**" or "**Users**").

This Policy and the related documents shall be reviewed annually, or whenever the business environment of Thai Union Group changes in a way that affects the current policy.

1.3 Owner

The document is owned by the Group Director Digital of Thai Union Group.

2. Information Security Policy

Objective

To provide direction and support for information security considering business requirements and relevant laws and regulations.

Policy Statement

1. The Policy shall be communicated to all relevant stakeholders and Users.
2. The Digital Security Head of Thai Union Group shall review the provisions of this Policy and, when and where required:
   a. Liaise/inform relevant other local Departments (e.g., technology, human resources, legal etc.).
   b. Review applicable local policies to reflect the provisions hereof and have them implemented within each Thai Union Group company. For the avoidance of doubt, Thai Union Group companies are allowed to create, implement, and enforce any additional policies and procedures to comply with local laws and regulatory requirements.

3. Changes to the policy shall be reviewed by the Digital Security Head and approved by the Group Director Digital.
4. Supporting documents such as standards, procedures, or guidelines for use within Thai Union Group must not conflict with this Group Information Security Policy. In case of conflict, this Group Information Security Policy shall prevail each time possible.
5. Records for management review and approval will be maintained.

3. Organization Security

3.1 Internal Organization

Objective

To designate the roles and responsibilities for managing information.

Policy Statement

The Digital Security Head of Thai Union Group is responsible for implementing and maintaining the information security policies and procedures across Thai Union Group.

1. Establish an Information Security Program.
2. Develop controls to comply with all applicable statutory and regulatory requirements.
3. Monitor the effectiveness of the implementation of the Group Information Security Policy by random/sample check and audits.
4. Develop programs to maintain information security awareness within Thai Union Group.
5. Document and maintain a risk register.
6. Monitor Information security trends and emerging security threats on a global Digital system landscape.
7. Ensure compliance with the Group Information Security Policy and communicate any non-compliance to Thai Union Group management for corrective actions.

3.2 External Parties

Objective

To maintain security and privacy when external parties are involved.

Policy Statement

1. A formal written Non-Disclosure Agreement (NDA) must be established, or equivalent provisions included in a formal contract or agreement when sourcing Digital systems or services or when exchanging sensitive information with third parties. Thai Union Group companies shall maintain effective vendor or third-party management processes or procedures for the following:
   a. Vendor or third-party selection.
   b. Identify risk involved by risk assessment (questionnaire or review of configurations) to avoid as much as possible any security incidents.
   c. Performance monitoring, assessment and examination.
2. Vendors or third parties delivering Digital systems and services shall provide adequate security measures and processes.
3. Security requirements shall include, as a minimum: maintaining confidentiality and privacy of data, shared on behalf of Thai Union Group or residing on Thai Union Group systems.
4. Security requirements must be included in the signed contracts/agreements and shall address how the vendor / third party guarantees that adequate security, privacy, availability

will be implemented maintained and managed, and how security management will adapt to changing security landscape and fraud risk.

5. Third Party Security Assessment (TPSA) and updating the policy/process/SOP as and when required.

4. Human Resources and Personal Data Information Security

Objective

To ensure that Users understand their responsibilities and liabilities, notably in case of collection and/or processing of personal data, as well as to reduce the risk of theft, fraud, human error, or misuse of facilities.

Policy Statement

1. There shall be a defined process to manage Users access privileges during employment, transfer, and termination.
2. There shall be security awareness training as part of the induction process for new Users as well as an ongoing process for existing Users.

5. Asset Management

Objective

To achieve and maintain appropriate protection of Digital assets owned by Thai Union Group by ensuring all assets are accounted for and have a nominated owner.

Policy Statement

1. Develop and maintain an inventory of Digital assets and ensure the inventory is kept up to date.
2. Categorize and classify Digital assets based on their impact to the organization, in terms of confidentiality, availability and integrity.
3. Each asset owner shall be responsible for implementing appropriate controls and ensuring the protection of the assets under his/her authority including the secure disposal of media (physical or electronic).
4. All relevant purchasing records should be maintained with supporting documentation (agreements, warranties etc.).

6. Data Classification, Labelling and Disposal

Objective

To ensure that data is subject to an appropriate level of protection, handled and disposed appropriately.

Policy Statement

1. Classification guideline
    a. Data shall be classified in accordance with Thai Union Group's data classification scheme [Refer 6.1] considering its value, legal requirements, sensitivity, and criticality to the organization.
    b. Each data owner is responsible for defining the classification level of data under his/her responsibility and to ensure that the receivers are aware of the classification level (e.g. by means of labelling, email, etc.).
2. Data labelling and handling

a. Data shall be securely processed, stored, transmitted, disposed, and destroyed in accordance with its classification level.
b. Data shall be protected and handled in accordance with its data classification schema.

3. Data Disposal
   a. If data is no longer required, the same shall be disposed of in a secure manner.

6.1 Data Classification Scheme:

Level	Description	Examples
Restricted	Data that is highly sensitive and is available only to specific / named individuals or position only.	✓ Trade secrets ✓ Intellectual Property ✓ Strategic business plans ✓ Mergers and Acquisitions data
Confidential	Data that is sensitive within the Thai Union Group, and available only to a specific function / department / project group or role.	✓ Personal data ✓ HR, Payroll data ✓ Financial and accounting data ✓ Sales data and opportunities ✓ Contracts / Proposals ✓ Financial results ✓ Client's confidential data (as specified in the contractual agreement)
Internal	Data that is sensitive outside the Thai Union Group. Only authorized Users with a legitimate business need can access and handle the data.	✓ Thai Union Intranet / Portal site content / Internal Memos ✓ Member directory / Organizational Chart ✓ Policies, standards, and procedures ✓ Company-wide internal communications / announcements
Public	Public data (including data deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors, and agents.	✓ Published Annual Report ✓ Thai Union Group Website content ✓ Marketing Materials ✓ Marketing brochures ✓ Contact Information

7. Communications and Operations Management

7.1 Change Management

Objective

Define formal requirements to manage changes of Digital systems, to protect data and ensure availability of systems.

Policy Statement

1. There shall be a documented Change Management Process to control and monitor changes to Thai Union Group's Digital systems.
2. All changes to Thai Union Group's Digital systems shall undergo formal change management approval.
3. All changes shall be verified to confirm that security requirements have been met.
4. All change requests shall be formally recorded and submitted via standard change management tools.
5. Change management logs shall be maintained for review and audit purposes.

7.2 Segregation of Duties

Objective

To reduce the opportunities of unauthorized or unintentional modification or misuse of Digital assets and data.

Policy Statement

1. Roles and responsibilities should be clearly defined and separated to prevent conflicts of interest and promote accountability.
2. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
3. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

7.3 Protection against Malicious Code

Objective

To protect the integrity of Digital data and systems from damage that may have occurred by malicious code.

Policy Statement

1. Ensure the installation and setup of Thai Union Group's standard malicious code protection software (e.g., Anti-virus and Anti-spyware) on all Digital devices, including but not limited to workstations, laptops, servers, and network equipment, with regular scanning for new or existing malicious code.
2. Establish and maintain a list of blocked websites, blocked network ports, and blocked email attachments file types.
3. Installation of unauthorized software on any Thai Union Group companies' Digital devices shall be prohibited.

7.4 Logs and Monitoring

Objective

To detect unauthorized data processing activities that may have occurred within systems.

Policy Statement

1. Audit log of user activities and data processing to Thai Union Group's systems by a Thai Union Group's employee, contractor, consultant, third-party or customers shall be sufficiently produced and maintained for future investigation of irregularities.
2. Regular monitoring shall be conducted to examine and detect any irregularities or vulnerabilities of Digital systems.
3. Logs shall be protected against tampering and unauthorized access.

7.5 Back-up

Objective

To maintain the integrity and availability of data and data processing facilities.

Policy Statement

1. Critical data and systems necessary for Thai Union Group's business operations shall be regularly backed up to ensure availability.

2. There shall be a formal backup and restoration procedure outlining the necessary requirement.
3. Test backup arrangements as necessary to recover the complete system in the event of failure or disaster.
4. Backup data and storage media shall receive sufficient level of protection against unauthorized modification and physical/environmental damages.

7.6 Media Handling

Objective

To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

Policy Statement

1. Management of media devices:
   a. All media devices using or connecting to Thai Union systems may be monitored.
   b. The use of removable media shall be restricted for business purposes only and only used following explicit approval of the Information Security Head. Media drive or connection ports that are not required for business purposes may be disabled.
2. Disposal of media:
   a. Media containing sensitive data shall be disposed or destroyed securely and safely when no longer required.
3. Data handling procedure:
   a. Media containing sensitive data shall be protected from unauthorized disclosure or misuse.
4. Security of system documentation:
   a. All Thai Union Group companies' documentation whether hard copy document or electronic document shall receive sufficient protection during its use, transmission, and in storage. The level of protection shall be in accordance with its classification [Refer 6.1].

7.7 Systems Security

Objective

To protect Digital systems and data from unauthorized access, modification and emerging threats.

Policy Statement

1. Digital systems include but are not limited to servers, platforms, networks, communications, databases and software applications.
2. Ensure all Digital systems are configured to the approved standard baseline set by Thai Union Group in accordance with business and security requirements.
3. All changes related to the Digital systems shall be strictly controlled and monitored.

8. Artifical Intelligence (AI) Usage & Governance

Objective

To ensure the responsible, secure, and compliant use of Artificial Intelligence (AI) systems within Thai Union Group.

Policy Statement

1. The design, development, procurement, and use of AI systems must comply with applicable laws and Thai Union's security and privacy requirements.
2. AI systems that impact safety, personal data, HR decisions, customer or consumer interactions must be assessed for fairness, accuracy, transparency, and ethical use.
3. Only approved AI tools and platforms are permitted. The use of public generative AI tools (e.g., ChatGPT, deepseek etc) with company or personal data is restricted unless specifically approved by Digital Security.
4. AI systems must incorporate appropriate human oversight, especially in high-risk use cases (e.g., hiring, financial decisions, surveillance).
5. AI vendors must undergo the Third Party Risk Management (TPRM) process and disclose how AI is integrated, including data usage, bias mitigation, and human override capabilities.

9. Shadow IT

Objective

The objective of this policy is to establish guidelines for the use of technology, software, and cloud-based services within the organization to reduce risks associated with unauthorized tools (commonly referred to as "Shadow IT"). This ensures that technology use aligns with the company's security, compliance, and operational standards.

Definition of Shadow IT

Shadow IT refers to any hardware, software, or service used within the organization without the knowledge, approval, or oversight of the Digital function. Examples include:

1. Using personal email accounts for business purposes.
2. Storing company files in unauthorized cloud storage (e.g., Dropbox, Google Drive, iCloud).
3. Installing any unapproved collaboration or productivity tools.
4. Connecting personal devices to corporate networks without approval.
5. Implementing any type of technology, software, cloud-based services not formally authorized by Thai Union Group's Digital function.
6. The use of external technology suppliers or vendors for the development of technology solutions (including AI) whether hosted at Thai Union Goup technology infrastructure or otherwise.

Policy Statement

1. All technology and software and technology vendors used for business purposes must be reviewed and approved by Thai Union Group's Digital function before deployment.
2. Employees are prohibited from using unapproved services for storing, transmitting, or processing company data.
3. Employees must report the use of any external or unauthorized tools to Thai Union Group's Digital function for assessment.
4. Personal devices used for work must meet security requirements (e.g., encryption, strong authentication) and be registered with Thai Union Group's Digital function.
5. Employment or engagement (directly or indirectly) of any technology professionals (including, but not limited to, software developers, system administrators, infrastructure engineers, or consultants) for performing Digital-related work outside of the Digital function is strictly prohibited across all business units

Risks of Shadow IT

1. Data breaches and information leakage.

2. Non-compliance with industry regulations (e.g., PDPA, GDPR, HIPAA).
3. Increased likelihood of malware and ransomware.
4. Operational inefficiencies due to incompatible systems.
5. Additional cost for Thai Union organization, lack of synergies or economies of scale.
6. Lack of overall Thai Union Digital and Enterprise Risk Management strategy alignment.
7. Risk of systems service failure resulting in business disruption an/ or financial loss.

10. Access Control

Objective

To control and ensure that only authorized personnel have access to Thai Union Group's systems and data.

Policy Statement

The identification and authorization process shall comply with the following principles:

1. Where technically viable, all systems should leverage the standard Thai Union identity platform and activate single-sign-on and multi-factor authentication.
2. All subjects (users or systems) should have a unique ID and password or other authentication mechanisms.
3. Access to any data, information processing facilities or physical location operated or controlled by a Thai Union Group company shall be granted only by authorized owner.
4. Multi-level authorization shall be used for granting all access rights.
5. Access rights shall be reviewed at regular intervals.
6. Password requirements set by the Group Digital department as follows:

No	Password Control	Suggested Setting
1	Minimum password length	8 characters
2	Password expiration interval	90 days (maximum)
3	Required password complexity	Combination of alphabetic character, numeric, and special character, small letters capital letters (No sequential numbers or letters are permitted).
4	Number of previous password usage prohibition	10 previous passwords
5	Number of failed sign-on attempt	3 times before account lockout
6	Forced password changed at first log-on	Enable
7	Session timeout	30 minutes (maximum)

The selection and use of password shall follow good security practices, such as (but not limited to):

a. Password shall not be created based upon anything that somebody else could easily guess or obtain using personal data.
b. Password shall be changed whenever there is any indication of possible system or password compromise.
c. Password shall be kept confidential and shall not be shared among Users or any third party.
d. Password shall not be recorded in any form (e.g., paper, software file, hand-held device, automated log-on process).

Privileges shall be revoked without delay for Users who have changed roles or left any Thai Union Group company organization. To ensure accountability for subjects and authorizers, a valid audit trail should be enabled.

11. System Acquisition, Development and Maintenance

Objective

To ensure that Information Security is an integral part of Digital systems across the entire lifecycle including those which provide services over public networks.

Policy Statement

1. For a project relating to Digital systems, the project or service owner is responsible for integrating Information Security Requirements in the project scope and invite the Digtial function to review completeness and compliance.
2. There shall be a documented procedure for system development within Thai Union Group to ensure it follows industry best practices.
3. Information security standards must be incorporated in new information systems or enhancements to existing information systems.
4. Data involved in application service transactions and passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
5. Supervise and monitor the activity of outsourced system development.
6. Where AI capabilities are included in system development or procurement, they must be reviewed by the Digital Security and architecture teams.

12. Patch Management

Objective

To reduce the risks resulting from exploitation of technical vulnerabilities.

Policy Statement

1. All vendor patches shall be applied as per Thai Union Group standards.
2. Digital devices that do not comply with such standards must be registered in the risk register.

13. Vulnerability Management

Objective

To identify and address vulnerabilities in order to enhance the overall security posture of the organization.

Policy Statement

1. Regular vulnerability scans are conducted on all systems before deployment and periodically thereafter.
2. Critical environments and systems undergo periodic penetration testing to identify any vulnerabilities.
3. Identified vulnerabilities are promptly addressed and remediated based on severity and impact.
4. Results of vulnerability assessments are documented for audit and compliance purposes, with regular reports for management visibility.
5. AI systems must be tested for adversarial attacks, data poisoning risks, and model drift as part of ongoing vulnerability management.

14. Cryptographic Controls

Objective

To safeguard information and network by deploying essential encryption and other cryptographic techniques.

Policy Statement

1. Encryption shall be adopted for Information Assets based on the criticality of information. Standard encryption technology would be deployed for encryption and required by regulatory requirements.
2. Encryption shall be applied for remote connectivity services such as links between offices sites or with customers over the Internet or service providers.
3. A key management system shall be used to securely store and manage the keys used by the business.

15. Cyber Security Incident Management

Objective

To ensure security incidents are timely and efficiently detected, reported, handled, and communicated.

Policy Statement

1. There shall be a formal cyber security incident management procedure to ensure security incidents being detected or reported are timely and efficiently handled and communicated to relevant personnel as well as management.
2. There shall be appropriate monitoring mechanism to monitor and detect security events or weaknesses associated with Thai Union Group's Digital systems and processing facilities.
3. Security events being detected and reported shall be properly recorded.
4. Security incidents shall be reviewed, analyzed, documented, and communicated to Group Director Digital function and appropriate level of management on a regular basis.
5. Employees are responsible to report suspected breaches of security policy without delay to their line manager, and the Digital function helpdesk/support.
6. In the event of any incidents involving misconduct, appropriate disciplinary action may be taken in accordance with local disciplinary rules.

16. Business Continuity Management

Objective

To ensure business continuity in the event of a crisis or disaster.

Policy Statement

1. Thai Union Group shall determine its requirements for continuity of Digital systems in adverse situations, such as a crisis or disaster.
2. Each Thai Union Group company should establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity during an adverse situation.

3. Each Thai Union Group company should verify the established and implemented continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

17. Physical and Environmental Security

Objective

To prevent potential physical or environmental damage to Digital systems.

Policy Statement

1. There shall be adequate physical safeguards and control mechanisms to protect all area, offices, and location that host, own, or maintain Thai Union Group's systems against internal and external threat.
2. Physical access to Thai Union Group's information processing facilities shall be restricted to authorized Users only.
3. There shall be formal physical access control procedure to ensure appropriate granting, controlling, and monitoring of physical access to Thai Union Group information processing facilities.
4. The environmental conditions within the information processing facilities such as temperature and humidity level shall be carefully monitored and kept at a level where the equipment can operate safely.
5. All equipment in the information processing facilities shall be routinely maintained in accordance with manufacturer's recommended service interval and specifications.
6. All visitors shall be escorted by Thai Union Group staff with appropriate approval.

18. Compliance

1. This Information Security Policy shall take effect upon publication and be complied with by all Users.
2. In cases where compliance with this Information Security Policy is not feasible or technically possible, or when deviation is necessary to support a business function, Users must request exception approval from the Director, Digtial Security of Thai Union Group, the Managing Director of the affected Operating Company or Department, and the Chief Digital Officer of Thai Union Group.
3. All approved deviations will be recorded in the risk register.

19. Changes and Updates

The Director – Digital Security is responsible for maintaining and updating this Information Security Policy.