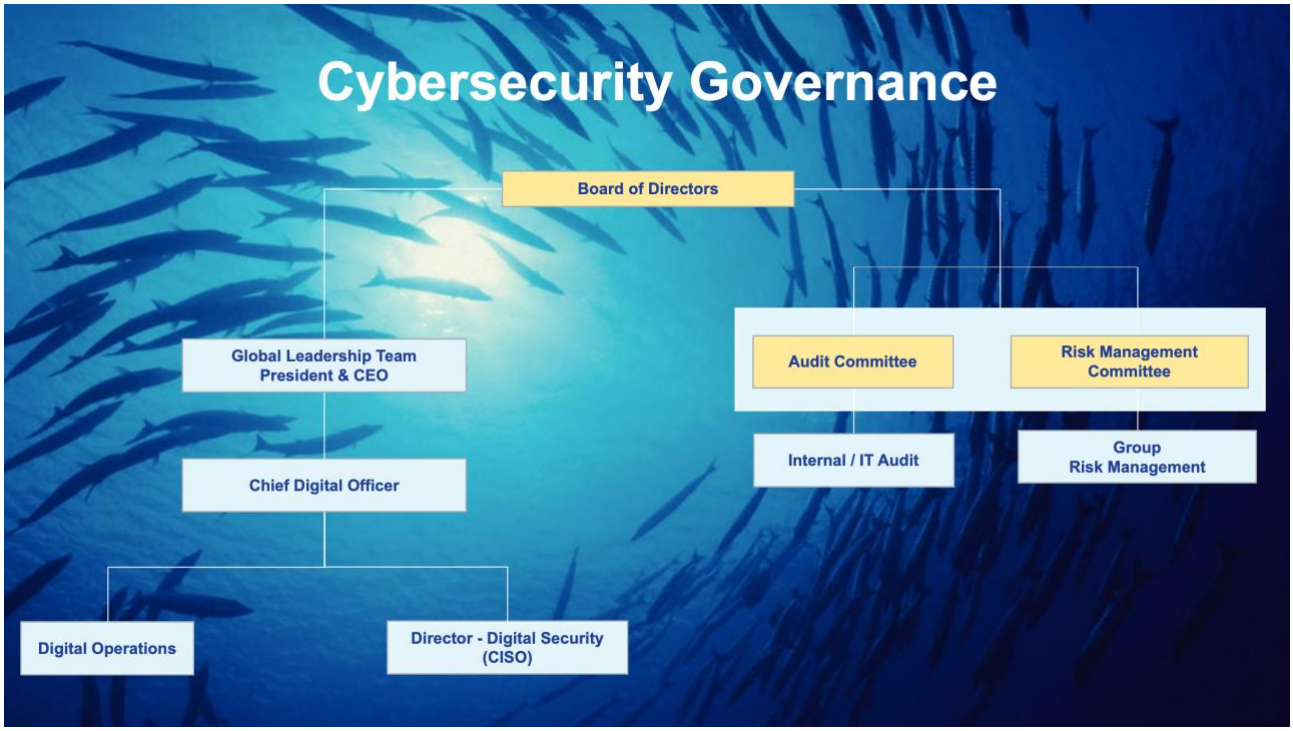
Cybersecurity Governance

With a drive towards more efficiency and automation, we are increasingly reliant on digital technology solutions to support our business. With this increased reliance on technology, our exposure to cyber threats also increases proportionally. Thai Union Group tackles cybersecurity threats and risks with support from the Board of Directors, Audit Committee, Risk Management Committee, and members of the Global Leadership team. In governing digital security, Thai Union Group has developed a Cybersecurity Governance framework with the express purpose of ensuring that we design and develop resilient digital systems according to local regulation and international standards.



Roles and functions responsible for cybersecurity governance:

- Mr. Nart Liucharoen, Independent Director and Chairman of the Audit Committee
- Ms. Parnsiree Amatayakul, Independent Director, Chairman of the Risk Management Committee and Member of Audit Committee
- Mr. Thiraphong Chansiri, President and CEO and Member of the Risk Management Committee
- David Llamas, Chief Digital Officer
- Group Risk Management Department
- Virag Thakkar, Director - Digital Security (Chief Information Security Officer)

The Audit Committee and the Risk Management Committee, established by the Board of Directors, have direct roles and responsibilities related to cybersecurity as defined by their respective Charters:

Audit Committee Responsibilities include : (URL : Thai Union Group Public Company Limited)

- Review the correctness and effectiveness of the Digital systems relating to internal controls, financial reports, risk management and data & network security together with suggested updates and improvements as needed.

- Conduct site visits to business units of the Company which includes domestic and foreign subsidiary companies to review the risk management and internal control systems, information systems including cyber security, the important operational systems and regulations as well as problems and comments of the external auditors and the internal audit team
- Oversees and monitors risk management by means of independent reviews, in order to ensure that risk management is implemented according to the policy and effectively throughout the organization

Risk Management Committee Responsibilities : (URL : Thai Union Group Public Company Limited)

- Oversees risk management implementation and reports the Company's significant risks, mitigations and improvements to the Board
- Cybersecurity has been identified as one of the key risks that requires a mitigation plan (For more detail, please see our Annual Report)

The Group Digital and Group Risk Management functions work together to manage cybersecurity risks and report to Thai Union's Global Leadership Team. In addition, the following Digital related roles and functions have direct roles and responsibilities in addressing cybersecurity risks.

Chief Digital Officer (CDO) is responsible for the digital strategy and roadmap that support the growth objectives of the company and is accountable for digital transformation, and all aspects of digital technology to meet the company's short and long-term needs. This includes:

- Develop technical aspects of the company's strategy to ensure alignment with its business goals
- Discover and implement new technologies that yield competitive advantage
- Monitor KPIs and technology budgets to ensure the investments meet business expectations
- Use stakeholders feedback to inform necessary improvements and adjustments to technology
- Overall accountability for cybersecurity strategy and implementation

Director - Digital Security (CISO) Responsible for governing and providing digital security strategic decision-making, system and data protection, digital technology risk management program, and improving Thai Union Group's overall security and robustness of infrastructure. This role also supports operation teams and relevant functions to implement cyber security activities, as well as promote awareness and preventive measures to reduce risks in cyber threats.

Cybersecurity Measures:

To meet the enterprise business objectives and ensure continuity of its operations, Thai Union Group has defined a set of policies and relevant documents to ensure integrity, availability, confidentiality, and protection of all information and to commit of the continuously improving of our information security systems.

A set of baseline digital controls and security requirements are defined in compliance with industry best practice, as well as applicable local law and regulations and technical benchmarks. These measures are designed to secure and protect the following, but not limited to

- relevant, personal data and information collected and/processed by Thai Union Group;

- Thai Union Group's information resources and assets;
- Thai Union's assets against theft, fraud, malicious or accidental damage, breach of privacy or confidentiality.

The above and other measures are designed to enhance digital security, cloud security, data security, cybersecurity security awareness training, and other digital programs for better future service enablement to support business objectives and growing needs. We also monitor Information security trends and emerging security threats on a global digital system landscape.

Thai Union Group Information Security Policy


Thai Union

Thai Union Group

Information Security Policy

Approved by: Thiraphong Chansiri (President & CEO)

Approved by: Shue Chung Chan (Group Director)

Signed by: David Florijn (Group Director Information Technology - CIO)

Version: 3.0

Revised Date: 16-Oct-2024

Disclaimer: This document is the property of Thai Union Group PCL. Any modification to the entire document or any part of its content must be done by authorized individuals or parties with appropriate approval from the document issuer only. Duplication, copy, or distribution of this document or its content must be carried out in accordance with Thai Union Group PCL.'s Information Handling Guideline.

1 / 12

Information Security Policy at Thai Union

Thai Union is committed to safeguarding the confidentiality, integrity, and availability of its digital systems, data, and personal information. To ensure robust protection against threats such as theft, fraud, malicious or accidental damage, and breaches of privacy or confidentiality, Thai Union has implemented a comprehensive Group Information Security Policy.

This policy outlines mandatory requirements for all companies within the Thai Union Group, applying globally to Thai Union Group PCL and all subsidiaries and affiliates in which the Group holds 50 percent or more of the share capital and/or voting rights. It applies to all employees, contractors, consultants, and third parties who access or use the Group's digital systems and data. The Information Security Policy emphasizes that both management and users are responsible for maintaining the confidentiality, integrity, and availability of all systems and information. To ensure ongoing relevance and effectiveness, the policy and its related documents are reviewed annually or whenever significant changes occur in the business environment.

Thai Union's Group Information Security Policy covers 17 sections, ensuring comprehensive protection across our operations. We publicly disclose the key principles and frameworks underpinning our policy while detailed technical and operational procedures are maintained internally to safeguard security effectiveness.

Organization Security

Thai Union has designated the Group Information Security Head to oversee the implementation and maintenance of information security policies and procedures. Responsibilities include establishing an Information Security Program, developing controls to ensure compliance with statutory and regulatory requirements, monitoring policy implementation effectiveness, promoting information security awareness, maintaining a risk register, and continuously monitoring global information security trends and emerging threats. Implementation of the program is supported by regular internal audits and external assessments against recognized standards.

Thai Union conducted a review of the internal IT control system at least on an annual basis by regularly evaluating the internal audit and IT audit work plans and reports. This included assessments based on the Securities and Exchange Commission (SEC) internal control checklist. The review concluded that Thai Union's IT control environment is adequate and appropriate to support its business operations. This conclusion aligns with the external auditor's opinion, which found no material deficiencies that could impact the consolidated financial statements of Thai Union Group and its subsidiaries, or the separate financial statements of the Company.

Third-Party Security Management

All third-party engagements involving digital systems or sensitive information require formal Non-Disclosure Agreements (NDAs) or equivalent security provisions within contracts. Thai Union maintains effective vendor and third-party management processes, including risk assessments, performance monitoring, and ensuring that all vendors implement appropriate security measures. Security requirements are contractually enforced, covering confidentiality, privacy, availability, and adaptability to the evolving cybersecurity landscape and fraud risks.

Business Continuity Management

To ensure operational resilience, each company within the Group is required to establish, document, implement, and maintain business continuity plans for digital systems. The effectiveness of these plans is regularly validated through testing and crisis simulation exercises.

Thai Union has implemented a comprehensive Disaster Recovery and Incident Response action. The company has enhanced its Disaster Recovery Plan (DRP) for key applications to ensure seamless continuity of operations during cyber emergencies.

Vulnerability Management

Thai Union conducts regular vulnerability scans. Critical environments are subject to periodic penetration testing, with identified vulnerabilities promptly remediated based on severity and impact. Findings are documented and used to update security controls, with results reported to management for review and action.

Thai Union, using external attack surface management technology, conducts real time 24x7 Vulnerability Assessment of its external facing infrastructures, along with periodic reviews to ensure ongoing security. Additionally, Thai Union carried out a Tabletop Exercise simulating hacker attacks. This exercise assessed Thai Union's response processes by evaluating their effectiveness against the scenario, existing documentation, and industry best practices.

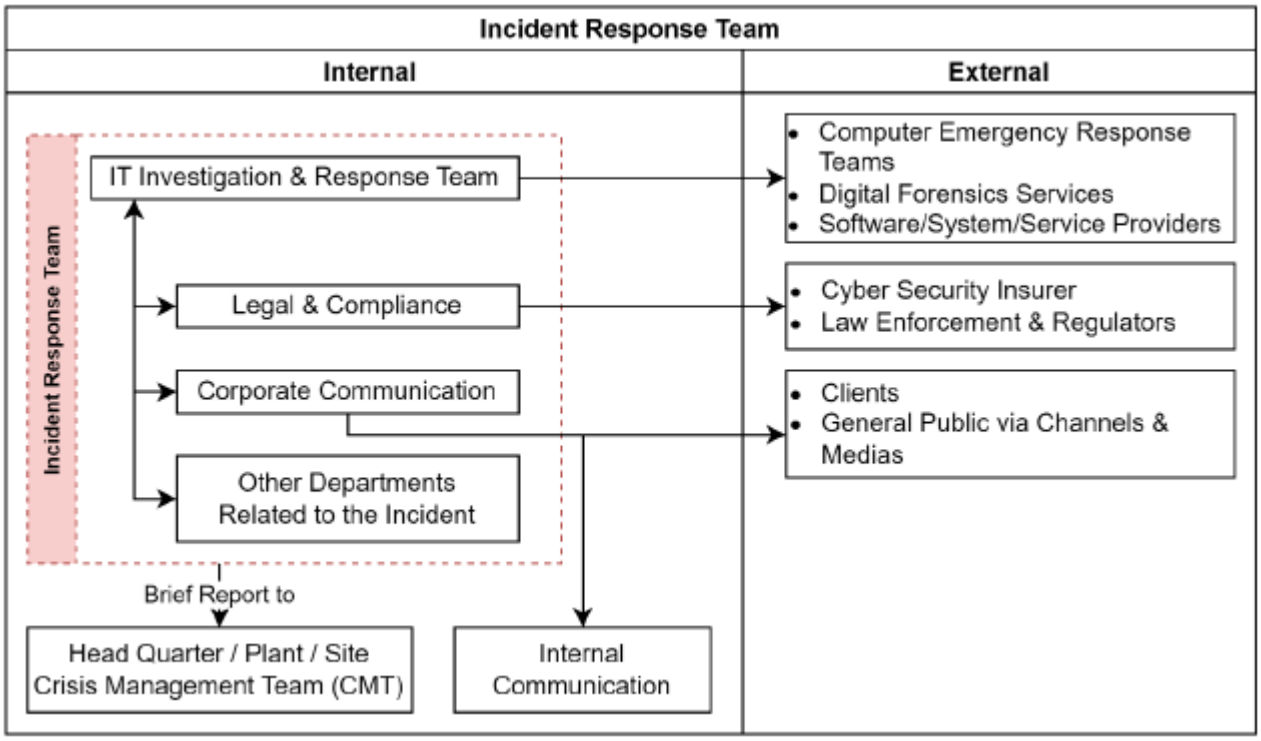
Logs and Monitoring

Audit logs of user activities and data processing are maintained and regularly monitored to detect irregularities or vulnerabilities. Strict measures are in place to protect logs from tampering and unauthorized access, supporting the Group's capacity to investigate and respond effectively to any irregularities.

Cybersecurity Incident Management

A formal cybersecurity incident management procedure is established to ensure that security incidents are promptly detected, reported, handled, and communicated. Monitoring mechanisms are deployed to identify security events, and incidents are recorded, analyzed, and escalated to the Director – Digital Security and/or Chief Digital Officer and relevant management levels. Employees are required to report any suspected breaches immediately, and disciplinary actions are applied in accordance with local regulations if misconduct is found. A structured escalation process ensures prompt reporting and resolution of security issues.

Thai Union has conducted the Incident Response Plan, which aims to establish a clear and standardized approach to incident response, ensuring a quick and effective response during incidents. We have an Incident Response Team (IRT), a cross-functional team, responsible for coordinating and promptly responding to reported incidents, conducting thorough investigations, and reporting findings to management and relevant authorities to ensure appropriate actions are taken.



The process of Incident Responding comprises four main stages: Preparation, Detection & Analysis, Response & Recovery, and Post Incident.

Human Resources and Personal Data Information Security

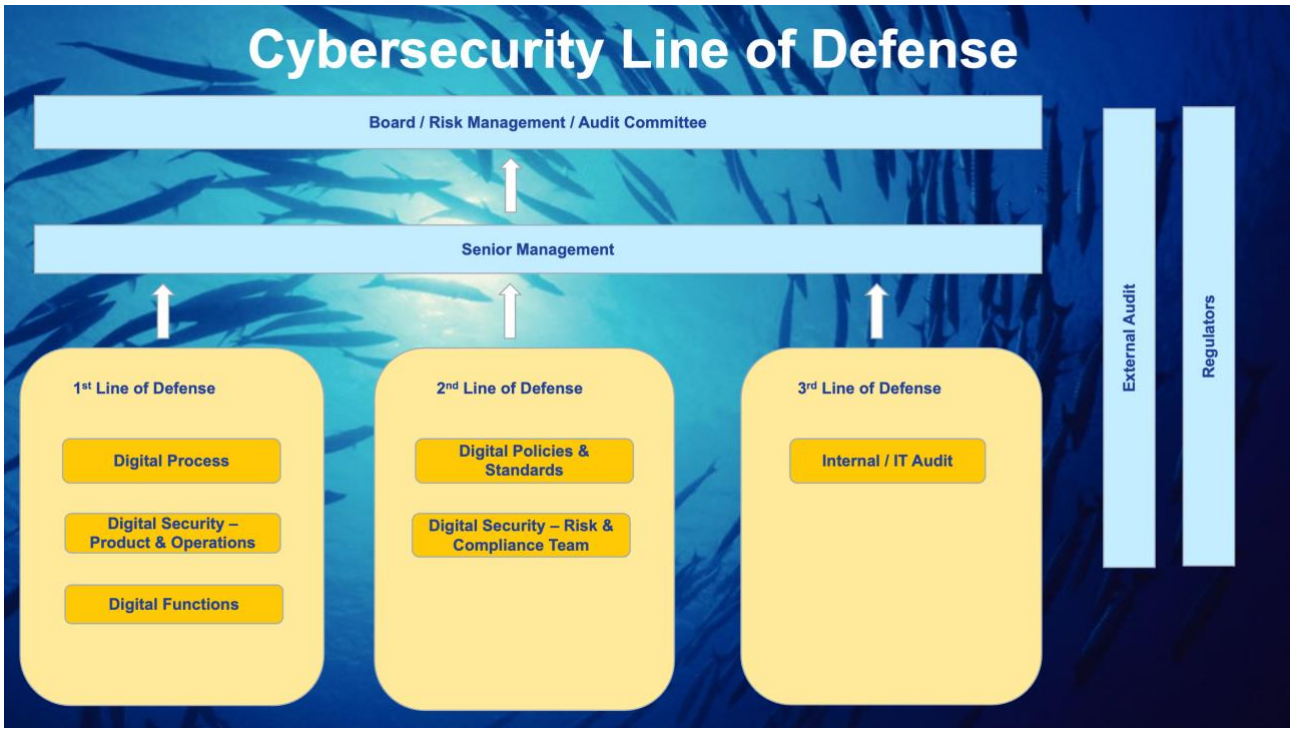
Processes are in place to manage user access privileges throughout employment, transfer, and termination. Thai Union integrates security awareness training into the onboarding process for all new employees and conducts ongoing training programs to reinforce information security responsibilities and reduce risks such as theft, fraud, human error, or misuse of facilities. The training program is reviewed regularly to ensure it addresses emerging risks and best practices.

Thai Union integrates its Personal Data Information Security program into Human Capital Development by continuously raising employee awareness about responsible technology use. This is achieved through regular training sessions and initiatives such as Cybersecurity Awareness Month, led by the Chief Executive Officer. The program aims to equip both executives and employees with the knowledge and understanding necessary for safe and effective technology usage. It also helps safeguard against cyber threats, reduce associated risks, and foster a safety-first mindset. These efforts are designed to protect both business and personal data.

Policy Governance and Performance

Future changes to Thai Union's digital security standards are approved by the Director – Digital Security (CISO) and are communicated to relevant parties across the organization. Compliance with policy controls is continuously monitored and reported to Digital Management.

For the year 2024, Thai Union recorded zero incidents related to breaches in cybersecurity, reflecting the effectiveness of its comprehensive information security framework.



<u>Reference Policies, Documents, and Topics:</u>

Group Digital Security Policy

- Human Resources
- Communications and Operations Management

- Access Control Management
- System Acquisition, Development and Maintenance
- Vulnerability and Patch Management
- Security Incident Management
- Business Continuity Management
- Physical and Environmental Security

Risk Management Framework

Data Protection Agreement / Privacy Policy

Acceptable Usage Policy