



Information Security Policy

Thai Vegetable Oil Public Company Limited

Information Security Policy

1. Introduction

Information technology has come to play an important role in the business operations of Thai Vegetable Oil Public Company Limited (the “Company”), including in management, data storage, and data processing, contributing to convenience, speed, and efficiency in operations and increasing the Company’s competitive opportunities.

However, the adoption of technology may introduce risks from various forms of threats. Without appropriate and sufficiently rigorous information security management, such information may be disclosed, altered, destroyed, or lost, which could affect the Company’s business operations, image, and reputation.

The Company’s top management has therefore established this Information Security Policy to serve as the principal framework for managing information security in a manner consistent with the Company’s operations and business objectives, and has developed information security operating standards, requiring all employees of the Group of Companies to comply strictly.

2. Scope of Policy

The information security operating standards cover the protection and maintenance of the security of the Company’s information, both within the premises of internal units and of relevant external parties, covering:

1. All employees and departments of the Company
2. Employees and external parties granted rights to access assets related to the Company’s information

3. Definitions

Information Security: The protection of information from various threats to ensure the continuity of business operations, reduce business risk, and increase the return on investment and business opportunities of the Group of Companies.

Company: Thai Vegetable Oil Public Company Limited.

Alert (Information Security Alert): An alert relating to information security from various sources, including personnel, systems, and information disclosed to the public.

Attack: An authorized or unauthorized attempt, whether successful or not, to destroy, alter, disable, access assets, or to attempt to disclose, steal, or use assets without authorization.

Weakness or Vulnerability: A cause or defect that provides an avenue giving rise to a threat.

Information Security Incident Response Team: A team appointed by top management, comprising personnel with sufficient skills and experience and provided with appropriate resources and facilities, responsible for handling matters related to information security, whether information security events, information security incidents, or vulnerabilities.

Operational Technology: Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Internet of Things (IoT), Robotics and Automation Systems, and other systems relating to Industrial Control.

Recovery Point Objective (RPO): The most recent point of data that must be recoverable in the event of damage to the information system.

Recovery Time Objective (RTO): The maximum acceptable period of time for restoring business operations, services, or information systems to normal service following a point of damage or disruption arising from an emergency or disaster.

Malicious Software: A program or set of programs that intentionally causes damage to information or information systems, such as a Virus, Worm, Trojan, Adware, or Spyware.

Threat: An event or occurrence, whether internal or external, that adversely affects the Company's assets.

Information Security Event: An event occurring in a system, Service, or network that indicates a possible breach of the information security operating policy, a control failure, or a previously unknown situation that may be related to security. Such an event may or may not have an impact on the Company.

Information Security Incident: A single event, or a series of unwanted and unexpected events, that has the potential to affect business operations and endanger information security. In other words, an event with the potential to affect the Group of Companies will be considered in order to confirm whether it constitutes an information security incident.

External Party: An external organization or individual conducting business or providing services who may be granted rights to access the assets of the Group of Companies.

External parties include:

1. Outsourcers performing work for the Company (Outsourcer), such as component manufacturers, advertising producers, or packaging manufacturers
2. Developers of operating systems or suppliers of materials and equipment (Supplier), such as developers of production control systems or computer equipment vendors
3. Service Providers, such as those installing and maintaining assets, network service providers, or internet service providers
4. Consultants, such as ERP system consultants
5. Business Partners
6. Any other external party granted rights to access the organization's assets or information

4. Information Security Policy

The Information Security Policy is established in accordance with ISO/IEC 27001:2022, which provides a comprehensive framework for managing information security risk across all dimensions, from Organizational Controls, People Controls, and Physical Controls, to Technological Controls.

These measures strengthen the organization's information security posture, enabling it to respond effectively to evolving cyber threats while maintaining compliance with relevant standards.

The Information Security Policy comprises the following four areas:

4.1 Organizational Controls

The Company maintains policies and guidelines for managing information security, establishing strategies, risk management processes, and appropriate control measures to ensure that information security management is carried out efficiently and supports continuous business operations.

The Company clearly defines roles and responsibilities for information security and promotes an information-security-aware culture across the organization, including establishing information security requirements for service providers, suppliers, and other

external parties who access the Company's data or information systems, to ensure that information security risk is managed throughout the business relationship, in addition to complying with applicable laws, regulations, and recognized standards.

The Company is committed to continuously reviewing, assessing, and improving its information security management system, so as to respond to evolving risks, threats, technologies, and requirements, while continually enhancing the effectiveness of information security controls in line with recognized standards and best practices.

4.2 People Controls

The Company maintains a policy for managing personnel to support information security, covering the recruitment and selection of personnel with qualifications suitable for positions involving critical data, the assignment of information security duties and responsibilities, and training and awareness-building on information security, so that personnel can perform their duties appropriately and reduce potential risk.

The Company requires personnel at all levels to have roles, duties, and responsibilities for complying with information security policies and measures, including the protection of the Company's data and information systems, and provides appropriate access control and privilege management measures for employees from onboarding, through role changes, to termination of employment, in order to prevent unauthorized access to data and reduce the risk of intentional or unintentional information security breaches.

4.3 Physical Controls

The Company maintains policies and physical security measures to protect data, assets, and information systems from unauthorized access, theft, damage, or natural disasters that may affect business operations, by providing appropriate access controls for areas of importance or containing critical information, such as access cards, fingerprint or facial recognition systems, closed-circuit television (CCTV), and other appropriate security measures to prevent unauthorized access to such areas.

In addition, the Company shall establish security measures for equipment used outside the organization, including guidelines for the appropriate storage, disposal, or destruction of data and equipment no longer in use, in order to prevent data leakage and to ensure that operations are consistent with the Company's Information Security Policy.

4.4 Technological Controls

The Company maintains a policy for applying technological control measures to protect data and information systems from cyber threats, by establishing appropriate security measures to support stable and continuous business operations. Accordingly, the Company provides for access control of information systems, encryption of critical data, security of networks and communication channels, vulnerability management, software updates, and appropriate data backup, in order to preserve the Confidentiality, Integrity, and Availability of data and information systems throughout the data lifecycle, and to reduce the risk from information security threats.

In addition, the Company provides for continuous monitoring, inspection, and logging of information security events, as well as processes for detecting, reporting, responding to, and recovering from information security incidents in an appropriate and timely manner, in order to minimize the impact of potential incidents and maintain business continuity.

This policy will be effective as of 14 August 2026, and thereafter.

- Signature -

(Dr. Suvit Maesincee)
Chairman of the Board