Information Security and Cybersecurity

Information Security and Cybersecurity Guidelines

To ensure that the practice of information security management is in accordance with the objectives and processes of the Company business and has established this Information Security Standard to be strictly enforced, including all employee and all units within the Company and external parties given access to the Company's information assets. The policy state as follows:

1. Assign the Information Technology Department to annually propose reviews or revisions of this policy and its related practices. It should also develop and maintain the framework and guidelines for information security management in alignment with international standards. In addition, the department must monitor relevant laws and regulations and ensure full compliance. The department is also responsible for managing cybersecurity to prevent threats originating from business processes and production activities.

2. Establish guidelines for the use of information technology services that align with user requirements and international standards, aiming to prevent cyberattacks and manage cybersecurity risks in accordance with Enterprise Risk Management. The scope of cybersecurity risk management practices shall cover all assets and human resources, as well as external parties.

Information Security and Cybersecurity

Information Security and Cybersecurity Guidelines

3. Implement cybersecurity prevention and intrusion detection systems that comprehensively cover the Company's information systems, including access control, data exchange, backup, and secure data destruction. The cybersecurity responsible unit shall continuously monitor for threats and report cybersecurity threat information to the executive management.

4. Establish a cybersecurity incident response plan to ensure prompt and effective management of security incidents. This includes monitoring incidents, developing incident recovery plans to reduce business disruptions, as well as arranging rehearsals to assess its accuracy and effectiveness.

5. Promote cybersecurity awareness and provide training through effective communication and education on cyber threats. Employees shall be made aware of their roles and responsibilities, understand how to respond to cyber threats, and be able to apply the knowledge effectively. All employees are accountable for the security of information within their responsibilities and must stay vigilant against behaviors or activities that may pose cybersecurity risks.

Information Security and Cybersecurity

Cybersecurity risk management structure

TVO has adopted the risk management principles by having the Audit and Risk Management Committee is responsible for setting policies and frameworks for enterprise risk management. Risk management is carried out by the Risk Management Working Group, while the Information Technology Department acts as the operational risk owner, responsible for managing and to assess IT-related risks. Risk mitigation measures are then implemented by the relevant departments. Cyber threats are recognized as one of the risks that could impact information and IT systems, with the potential to cause harm to customers, stakeholders, and business partners.

Objectives

TVO is committed to developing and adopting information technology systems in alignment with key IT legal requirements, such as the Personal Data Protection Act B.E. 2562 (2019). The objectives of this commitment are:

- To safeguard critical information from leakage or destruction caused by ransomware or viruses, including personal data.
- To establish effective cyber risk management by ensuring the ability to identify, protect, detect, and respond to cyber threats.
- To recover systems to normal operations and maintain business continuity.

Information Security and Cybersecurity

Risk management measures

To strengthen confidence in the Company's capability to prevent potential cybersecurity threats in the future, the Company has established the following risk management measures:

- Enhance the data backup system to cover all of the Company's core information systems, such as the ERP system and other IT systems, in order to prevent potential issues in data recovery arising from cybersecurity risks.
- Require regular testing of the emergency backup and data recovery plan in the event of a cyber-attack, at least once per year.
- Perform penetration testing and vulnerability analysis at least once every two years by an independent third party with specialized expertise.
- Provide a channel for reporting suspicious incidents or information security issues via MIS@tvothai.com.

Information Security and Cybersecurity

Performance results in 2024

- Installed ransomware protection software and performed full scans on all servers and client machines to ensure that no ransomware exists within the system.
- Conduct testing of the emergency backup and data recovery plan.
- Implemented additional authentication processes for accessing the computer systems.
- Blocked internet access and data transmission to and from high-risk countries identified on the ransomware risk list via the Company's firewall system.
- Conduct employee training to provide knowledge on the Personal Data Protection Act (PDPA) and proper practices in handling personal data, as well as to enhance awareness of cybersecurity threats. The program also includes assessments on cybersecurity knowledge and phishing email awareness.

Related Document

- Regulations for the use of computers and computer networks of the company