Information Technology Management and Cybersecurity

The Board of Directors has assigned the Risk Management, Corporate Governance, and Sustainability Committee to oversee and provide guidance on information technology and cybersecurity operations through the Managing Director, ensuring maximum agility and efficiency in the organization's IT and cybersecurity management.

Policy

The Company recognizes the importance of information technology and cybersecurity management and has therefore established a written Information and Information System Security Policy as a guideline for the effective management of the organization's IT and cybersecurity operations.

Information and Information System Security Policy

Details are available on the Company's website.
https://www.ttwplc.com/en/about-ttw/company-policy#tab-governance-7

Targets for 2025

Targets	Key Performance Indicators (KPIs)
1. All employees and executives have been communicated with and acknowledged the Information and Information System Security Policy.	100%
2. All employees and executives have received training on information and information system security.	100%
3. Breach or leakage of the organization's business data	0 Case
4. Complaints regarding breaches or leakage of the organization's business data.	0 Case

Note: Stakeholders include employees, shareholders/investors, customers, business partners/suppliers/contractors, communities, and government agencies/environmental sectors.

Long-term Targets

Targets	Key Performance Indicators (KPIs)
1. All employees and executives have been communicated with and acknowledged the Information and Information System Security Policy.	100%
2. All employees and executives have received training on information and information system security.	100%
3. Breach or leakage of the organization's business data	0 Case
4. Complaints regarding breaches or leakage of the organization's business data.	0 Case

Note: Stakeholders include employees, shareholders/investors, customers, business partners/suppliers/contractors, communities, and government agencies/environmental sectors.

Performance Results

การดำเนินงาน	Results		
	2023	2024	2025
1. All employees and executives have been communicated with and acknowledged the Information and Information System Security Policy.	100%	100%	100%
2. All employees and executives have received training on information and information system security.	100%	100%	100%
3. Breach or leakage of the organization's business data	0 Case	0 Case	0 Case
4. Complaints regarding breaches or leakage of the organization's business data.	0 Case	0 Case	0 Case

Note: Stakeholders include employees, shareholders/investors, customers, business partners/suppliers/contractors, communities, and government agencies/environmental sectors.

Significant Changes and Developments in the Review of the Information Technology Management and Cybersecurity Policy and Operational Guidelines over the Past Year

In 2025, the Company implemented significant changes and developments in its information technology management and cybersecurity operations as follows:

1. Updated the Password Policy and Multi-Factor Authentication (MFA) requirements to cover all users across the Company.
2. Updated the IT operations manual to reflect current practices and strengthen cybersecurity controls for greater security.
3. Cybersecurity Awareness Raised cybersecurity awareness among users by collaborating with the Human Resources department to provide Cybersecurity Awareness training.
4. Deployed Microsoft Defender EDR to detect and respond to security threats.

Operational Approach

Cybersecurity is a critical issue for the organization that may impact both internal and external stakeholders, including operational safety risks, system disruptions, and potential personal data breaches affecting employees, customers, and business partners/suppliers/contractors.

The Company therefore utilizes information technology systems as a key tool to meet the expectations and needs of stakeholders by adopting modern, efficient practices, tools, frameworks, and standards. The Company emphasizes risk management and information security in alignment with international standards and applicable regulatory requirements, including the Computer Crime Act B.E. 2560, the Cybersecurity Act B.E. 2562, and the Personal Data Protection Act B.E. 2562. This approach supports business expansion in line with the corporate strategy while preventing violations of stakeholders' rights arising from the misuse of personal data.

Information Security Management System (ISMS) in Accordance with International Standards

1. The Company evaluates the effectiveness of its Information Technology Security Policy at least once a year as part of the ISO 9001 audit system, conducted by both internal auditors and external auditors, in order to identify and address weaknesses in the Company's IT security controls.

2. The Company engages external system specialists to review, maintain, and improve its systems at least twice a year, in accordance with system maintenance agreements.

Information Security Controls and Practices

1. Business Continuity Plan for Cyber Threats

The Company prioritizes cybersecurity risk management to ensure business continuity even in the event of cyber threats or attacks. The Company has established a comprehensive Business Continuity Plan (BCP), which is integrated with the Disaster Recovery Plan (DRP) and the Incident Response Plan (IRP).

All plans are designed to operate together under the Incident Management Process to respond to and mitigate the impact of system attacks or IT disruptions. The Company conducts Disaster Recovery Plan (DRP) testing at least once a year and continuously reviews and updates the BCP and IRP.

In addition, the Company has implemented strict security measures and risk controls to ensure business continuity and compliance with relevant laws and regulations, including the Personal Data Protection Act (PDPA), as well as international cybersecurity standards and frameworks such as the NIST Cybersecurity Framework (NIST CSF).

The Company places the highest importance on its ability to maintain business continuity even in unforeseen circumstances. It has developed a comprehensive Business Continuity Plan (BCP) that covers various critical events that may impact operations and information security, both physically and in cyberspace, as follows:

Scenarios / Events	Measures
1.1 In the event of a power outage or fire incident (blackout or fire), the Company has clear guidelines and procedures in place to respond to emergencies such as power failures or fires, which may affect service delivery or critical systems of the organization.	▪ Switching to backup power sources or emergency electrical systems in the data center. ▪ Automatic activation of the Disaster Recovery Site when the primary system is unavailable. ▪ Procedures for safely evacuating personnel from the affected area. ▪ Coordination with building management and external emergency response agencies. ▪ Regular evacuation drills and routine safety readiness checks.
1.2 In the event of information security threats, the Company has established an Incident Response Plan (IRP), which is systematically integrated with the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), to address threats related to information systems, such as ransomware attacks, data breaches, unauthorized access, or service disruptions.	▪ **Incident management through the Security Operations Center (SOC), in collaboration with the IT team and relevant departments.** ▪ **Rapid detection, containment, and recovery of affected systems.** ▪ **Internal communication for coordination and stakeholder notification in accordance with established plans.** ▪ **Compliance with applicable laws and regulations, such as breach notification requirements under the Personal Data Protection Act (PDPA).** ▪ **Regular updates and improvements to the BCP, DRP, and IRP plans.**

2. Vulnerability Analysis of Information Security.

Scenarios / Events	Measures
2.1 General system vulnerability assessment (Vulnerability Assessment)	▪ **The Company's information technology systems utilize the Vulnerability Management feature, an automated vulnerability detection function of Microsoft Defender.**
2.2 Security testing of critical systems (Penetration Testing)	▪ Penetration testing conducted by external specialists has not been performed in 2025 and is scheduled to be carried out in accordance with the plan in 2027.
2.3 Website security rating (Security Rating)	▪ **The Company regularly conducts website security assessments in coordination with its hosting provider to identify risks and enhance the system in line with the Company's security policies and standards.**

3. Internal Audit

The Company places strong emphasis on the management of information technology and information security across all related processes, in accordance with internationally recognized standards. This is to enhance confidence in both internal and external services and to ensure compliance with applicable standards, policies, and laws. Accordingly, internal audits are conducted regularly. Internal audits are performed once in January, while external audits are conducted in July. These audits are carried out under the scope of the ISO 9001 standard, covering all three IT services: Microsoft 365, Business Plus, and the information technology infrastructure.

4. External Independent Audit

The Company places strong emphasis on the management of information technology and information security across all related processes, in accordance with internationally recognized standards, to enhance confidence in both internal and external services.

The Company has assigned external expert consultants and independent audit bodies to conduct reviews, assessments, and provide continuous improvement recommendations, resulting in certification of the following standards:

4.1 ISO 9001 Standard

4.2 ISO 14001 Standard

5. Incident Reporting and Escalation Process

Employees and users can report suspicious incidents or information security issues through the Company's designated channels, including Hotline Call 02-0199490 ext. 3142–3144, or by email to the Data Protection Officer at ttw_pdpa@ttwplc.com, or to the cybersecurity system administrators at support@ttwplc.com.

All received information is recorded in the Incident Management System and escalated to the relevant responsible units, including the information security management team, for prompt investigation, analysis, and remediation. Once the incident has been resolved, post-incident procedures are carried out in accordance with established plans, such as preparing follow-up reports and conducting lessons-learned meetings to prevent recurrence.

Protection Against Threats to Assets, Data, and Information Systems

The Company has implemented its Information and Information System Security Policy, which provides comprehensive governance as follows:

1. Security Responsibilities: The Company shall ensure clearly defined responsibilities for the development, implementation, and monitoring of information security, as well as continuous improvement of its operations.

2. Asset Classification and Control: The Company shall maintain an inventory of all assets, including both tangible and intangible assets, and assign ownership to the relevant responsible units. Asset owners are responsible for complying with security guidelines to ensure appropriate control over the use of the Company's assets.

3. The Company shall implement appropriate controls to ensure that employees, contractors, and consultants working for the Company are aware of and adhere to information security requirements and practices.

4. Physical and Environmental Security: The Company shall implement appropriate controls for physical and environmental security in accordance with the value and criticality of its assets.

5. Communications and Operations Management: The Company shall implement information systems and network infrastructure to ensure adherence to the following three key principles:

5.1 The system is available and ready for use when needed.

5.2 The system is accessible only to authorized users.

5.3 The system is accurate and reliable, and operates in accordance with recognized standards, best practices, and the Company's requirements.

6. Access Controls: The Company shall implement secure access controls across all systems and networks. Asset owners are responsible for authorizing access to information and ensuring appropriate access permissions.

7. Systems Development and Management: The Company shall conduct risk assessments for newly acquired systems and network infrastructure, as well as for any significant changes to existing systems. Security requirements shall be integrated as part of the system and network development lifecycle.

8. Information Security Incident Management: The Company shall ensure that information security incidents and related vulnerabilities are reported to the relevant parties and addressed promptly. Additionally, incidents shall be monitored and reviewed to ensure effective risk management and to minimize potential impacts arising from information security breaches.

9. IT Outsourcing) IT Outsourcing Controls: The Company establishes appropriate standards for the use of IT services from external providers, including formal written agreements that specify minimum operational standards and information security requirements (IT Outsourcing control procedures).

Cybersecurity Threat Response Measures

The Company has established an Incident Management Plan, in which the IT department focuses on managing information technology issues to ensure that problems are resolved efficiently and systems are restored to normal operations as quickly as possible.

Cybersecurity Threat Protection

Currently, information technology and systems are key tools for driving business and organizational growth, accelerating progress, and enabling digital transformation. However, this also exposes businesses and organizations to increasing cyber threats. As a result, cybersecurity plays a critical role in protecting operations. Implementing robust cybersecurity measures aligned with risk levels ensures preparedness against cyber threats and supports comprehensive risk management across personnel, processes, and IT tools. This, in turn, enhances confidence and trust for both public and private service users.

Information and IT Systems Risk Management

The Company's information and IT systems risk management encompasses both preventive and corrective measures. Preventive Maintenance (PM): This includes intrusion prevention systems (firewalls), antivirus programs, and policies controlling access to critical company data. Corrective Maintenance: This includes data backup solutions for recovery, as well as insurance for critical equipment, ensuring replacement or repair within 24 hours if damaged.

The Company places great importance on IT security and cybersecurity threat prevention. Accordingly, emerging risks from evolving cyber attacks are recognized as new risk areas. These include detailed information on risk factors, potential impacts on the organization and stakeholders, and corresponding risk mitigation measures, all documented under the sustainability topic of Sustainability Risk Management (ESG).

Internal Awareness and Communication

The Company places great importance on enhancing the knowledge and skills of employees and personnel in using information technology and digital tools through the following activities:

1. The Company produces cybersecurity knowledge materials and distributes monthly email updates to keep employees informed. Additionally, the IT staff provide guidance and answer questions while performing preventive maintenance (PM) on employees' computers, ensuring systems and software are up to date.
2. Employees and supervisors are notified according to their departments whenever inappropriate usage is detected, such as unauthorized software or access to high-risk websites.

Information Technology Security Management Program

1. Independent external audit of the infrastructure and/or information security management system, including the name of the audit and the standards applied (e.g., ISO 27001, ISO 9001).
2. IT Security Awareness Training in 2025 – Please specify (e.g., course examples).
   - 2.1 Cyber Security Awareness Course – The course aims to provide basic cybersecurity awareness to all users of the Company's computer systems.
   - 2.2 Fortinet Certified Fundamentals in Cyber Security – This course aims to equip system administrators with the knowledge and skills to manage basic cybersecurity threats.
   - 2.3 Introduction & Requirements for ISO/IEC 27001:2022 – This course aims to provide an understanding of the concepts and principles of the ISO/IEC 27001:2022 standard, enabling the Company to apply them in developing information management practices under cybersecurity protection.