Data and Cybersecurity

In an era where data plays a crucial role in business operations, information and technology security form the foundation of corporate governance. Sun Vending Technology Public Company Limited (“SVT”) places great importance on comprehensive data protection and information system security to safeguard the privacy of customers, employees, and stakeholders, while supporting business continuity and sustainable operational efficiency.

Supporting Sustainable Development Goals

Peace, Justice, and Strong Institutions

Partnerships for the Goals

Management Approach

The Information Technology Security Policy has been established in alignment with the company’s objectives and strategies to define a governance framework and guidelines for maintaining information security within Sun Vending Technology Public Company Limited. The policy ensures clarity, consistency, and compliance with relevant laws, policies, and regulations through four key areas

1. Organizational Controls

   - Policy and Structure: The company must establish a clear information security policy, reviewed and updated annually in accordance with applicable laws. Roles and responsibilities of employees regarding the use of portable computing devices and must be defined.
   - Asset Management: Information assets must have designated custodians, with data classified by confidentiality level and storage media properly managed.
   - Access Control: Access and modification rights must be defined to prevent unauthorized individuals from accessing systems or applications.

2. People Controls

   - Employee Responsibilities: Security responsibilities must be communicated to employees and external parties before employment, during employment, and upon termination.

- Disciplinary Actions: Clear disciplinary measures must be in place for violations of security rules or regulations.

3. Physical Controls

   - Facility and Equipment Protection: Measures must be implemented to prevent unauthorized access to areas housing IT equipment, protecting against damage, interference, or theft of company assets.

4. Technological Controls

   - Data and System Protection: Encryption (cryptography) is used to maintain confidentiality and prevent data leaks. Backup systems and malware protection are also implemented.
   - Vulnerability Assessment: Regular vulnerability scans (VA Scans) and penetration tests (Pentests) are conducted to minimize the risk of cyberattacks.
   - Communication and External Providers: Network and data exchange security are maintained, and external service providers (suppliers) are required to strictly comply with security agreements.
   - Incident Response and Continuity**:** A response plan is in place to handle security breaches without disrupting services, ensuring equipment readiness and business continuity.
   - Legal Compliance: Regular reviews are conducted to ensure compliance with legal and contractual requirements.

<u>Relevant Stakeholders</u>

1. Employees/Management

   - Strictly comply with the company's information and technology security policies.

2. Shareholders

   - Benefit from secure systems and transparency in IT data management.

3. Business Partners

   - Benefit from secure systems and transparency in IT data management.

4. Government Agencies

   - Supervise, regulate, and establish laws related to information and technology security.

Related Document Link

- Information Technology Security Policy https://www.sunvending.co.th/storage/downloads/corporate-governance/corporate-policies/svt-it-security-policy-th.pdf