



Information Technology Security Guideline

Our organization is committed to protecting the confidentiality, integrity, and availability of all information assets under our care. We recognize that effective information security is essential to maintaining trust, ensuring operational continuity, and meeting regulatory and stakeholder expectations.

To this end, we commit to the following 5 principles:

- 1. Continuous Improvement:** We will continuously enhance our information security management systems to adapt to evolving threats, technologies, and business needs.

Scope:

- All components of the Information Security Management System (ISMS), including policies, procedures, technologies, risk assessments, incident handling, and stakeholder feedback mechanisms across the organization.

Approach:

- Establish a formal review process for regularly assessing and updating security controls, policies, and procedures.
- Integrate feedback from audits, incidents, threat intelligence, and user experience to guide improvements.
- Promote a culture of continual learning through updated training, knowledge sharing, and industry benchmarking.
- Leverage automation and analytics to measure effectiveness and detect areas for optimization.

Impact:

- Improved resilience against evolving cyber threats and emerging risks.
- Better alignment of security practices with current business objectives and regulatory requirements.
- Enhanced adaptability and agility in security governance and operational response.
- Ongoing compliance with ISO/IEC 27001 and continuous readiness for audits.

- 2. Integrity and Data Protection:** We will ensure the integrity, accuracy, and protection of organizational and customer data, applying appropriate controls to prevent unauthorized access, alteration, or destruction.

Scope:

All organizational and customer data that is stored, processed, or transmitted through the organization's information systems, including both digital and physical records.

Approach:

- Implement security controls such as data encryption, access control, and audit logging to protect data integrity and confidentiality.
- Enforce role-based access control (RBAC) and conduct regular access reviews to prevent unauthorized data access.
- Maintain robust data backup and recovery procedures to ensure data availability and resilience against loss or corruption.

- Provide awareness and training programs to staff on best practices for data handling and protection.

Impact:

- Reduced risk of unauthorized access, alteration, or destruction of critical data.
- Increased trust from customers and stakeholders in the organization's data management practices.
- Enhanced compliance with data protection laws and regulations (e.g., PDPA, GDPR).
- Improved data accuracy, reliability, and continuity of business operations.

- 3. Threat Monitoring and Response:** We will actively monitor for information security threats and take prompt, appropriate actions to detect, mitigate, and respond to any incidents or vulnerabilities.

Scope:

- All organizational information systems, networks, endpoints, applications, and data flows that may be subject to internal or external security threats, including third-party service integrations.

Approach:

- Implement continuous monitoring systems (e.g., SIEM, IDS/IPS, endpoint detection) to detect anomalies and threats in real time.
- Define and maintain an incident response plan (IRP) with clear roles, escalation paths, and communication protocols.
- Conduct regular vulnerability assessments and penetration testing to proactively identify and remediate weaknesses.
- Collaborate with external partners and threat intelligence sources to stay updated on emerging risks and indicators of compromise.
- Perform periodic incident response drills and post-incident reviews to strengthen response capabilities.

Impact:

- Faster detection and containment of security incidents, reducing potential damage.
- Minimized downtime and impact on business operations due to proactive threat response.
- Improved organizational readiness and resilience against evolving cyber threats.
- Enhanced stakeholder confidence in the organization's ability to protect information assets.

- 4. Individual Responsibility:** We will define and communicate clear roles and responsibilities for information security across all levels of the organization. All employees, contractors, and relevant stakeholders are expected to understand and fulfill their security obligations.

Scope:

- All employees, contractors, temporary staff, and relevant stakeholders who interact with the organization's information systems or data.

Approach:

- Clearly define and document information security roles and responsibilities within job descriptions and contractual agreements.
- Deliver role-specific training to ensure personnel understand their responsibilities and follow security best practices.
- Promote a security-conscious culture through leadership support and continuous communication.
- Conduct periodic security awareness assessments, such as simulated phishing tests, to reinforce learning and identify areas for improvement.

- Encourage reporting of suspicious activities or potential security incidents by all individuals.

Impact:

- Increased accountability across all levels of the organization regarding information security.
- Reduced likelihood of security incidents caused by human error, such as phishing or social engineering attacks.
- Enhanced collaboration and alignment with organizational security objectives and standards.

5. **Third-Party Requirements:** We will establish and enforce information security requirements for all third parties who access, process, or store our data, including suppliers, contractors, and service providers, to ensure alignment with our security standards.

Scope:

- All external parties who access, process, or store organizational data, including suppliers, contractors, business partners, and service providers (e.g., IT vendors, cloud platforms).

Approach:

- Define and include information security requirements in contracts, service level agreements (SLAs), and security agreements with third parties.
- Conduct risk assessments on third parties before engagement and at regular intervals during the relationship.
- Perform third-party audits or reviews to evaluate compliance with organizational security policies.
- Provide guidance and support to ensure third parties understand and align with the organization's security standards.
- Establish incident management procedures to address breaches or security risks originating from third parties.

Impact:

- Reduced exposure to risks from third-party security gaps or negligence.
- Strengthened end-to-end data protection across the supply chain and service ecosystem.
- Clear accountability and mutual understanding of security responsibilities.
- Improved compliance with legal, regulatory, and internal security requirements.

This guideline will be reviewed periodically and updated as necessary to ensure its continued relevance and effectiveness.

บริษัท ไทยเบฟเวอเรจ จำกัด (มหาชน)

14 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กทม.10900

โทรศัพท์ (662) 1276555, โทรสาร (662) 2722