



Information Security Policy

Krungthai Card Public Company Limited

(Public Version)

Information Security Policy

Krungthai Card Public Company Limited

Krungthai Card Public Company Limited and its subsidiaries (“the Company” or “KTC”) recognize that information security is fundamental to sustainable business operations and plays a critical role in building and maintaining the trust of its stakeholders. This commitment is reflected in KTC’s Information Security Policy, which sets out the Company’s approach to protecting the confidentiality, integrity, and availability of its information, information systems, and related assets.

Objective

To establish a framework for information security and privacy management to protect the Company’s information, systems, and services, support secure and resilient business operations, promote awareness among relevant stakeholders, and build and maintain trust among all stakeholders.

Scope

This Policy applies to all information assets, information systems, and business processes under the ownership or management of the Company, including the storage, processing, transmission, retention, and disposal of all types of information. The Company shall communicate this Policy to employees, outsourced personnel, customers, suppliers, business partners, and external parties authorized to access or use the Company's information systems.

Guidelines

1. Continually Strengthening Our Information Security Management System

- Regularly reviewing and updating information security policies, standards, and procedures, at least annually or whenever significant changes occur, to ensure alignment with applicable laws, regulations, and relevant international standards, including ISO/IEC 27001.
- Conducting ongoing risk assessments and updating security controls to address changes in the threat landscape, business environment, and technology, with reference to internationally recognized frameworks such as the NIST Cybersecurity Framework (CSF).
- Monitoring the performance and effectiveness of information security operations to drive continual improvement.

2. Protecting the Integrity and Confidentiality of Data

- Committed to safeguarding data throughout its entire lifecycle to prevent unauthorized access, alteration, disclosure, or destruction.
- Classifying information assets according to their sensitivity, criticality, and business impact.
- Restricting access to information on a need-to-know basis through clearly defined and appropriate access controls.
- Applying technical safeguards, such as encryption and Data Loss Prevention (DLP), to protect data at rest, in transit, and during processing, with cardholder data protected in line with the Payment Card Industry Data Security Standard (PCI DSS).

3. Monitoring and Responding to Cybersecurity Threats

- Continuously monitoring cyber threat intelligence from multiple sources to detect and anticipate emerging risks, consistent with the Identify and Detect functions of the NIST Cybersecurity Framework (CSF).
- Maintaining a dedicated incident response capability to contain, investigate, and remediate information security incidents in a timely manner.
- Reviewing incidents to identify root causes and lessons learned to strengthen KTC's information security and prevent recurrence.

4. Fostering a Culture of Security Awareness and Accountability

- Requiring all employees, contractors, and trainees to comply with information security requirements and to immediately report suspected incidents or vulnerabilities that may affect information security.
- Providing regular information security training and awareness programs throughout the organization.
- Monitoring compliance and addressing violations through established disciplinary and governance processes.

5. Establishing Information Security Requirements for Third Parties

- The Company applies its information security standards to third-party relationships to manage risks arising from suppliers, vendors, and service providers with access to the Company's systems, infrastructure, or data.
- Assessing the information security practices of critical suppliers, vendors, and service providers and establishing and maintaining risk profiles to support ongoing oversight and risk monitoring.
- Embedding information security requirements into contracts and service agreements, requiring third parties to implement controls consistent with the Company's standards, including PCI DSS requirements for third parties with access to cardholder data.
- Monitoring and controlling third-party access to the Company's information and systems and conducting periodic reviews of third-party information security performance to ensure that shared systems, infrastructure, and data are appropriately and securely protected.

These practices reflect the Company's ongoing commitment to building and maintaining the trust of customers and stakeholders, as well as supporting secure and sustainable business operations in an increasingly digital and interconnected environment.

Policy Review

This Policy shall be reviewed at least annually or whenever significant events occur that may affect its implementation, to ensure that it remains responsive to significant changes in legal and regulatory requirements, business operations, technology, and emerging risks.

This Policy has been approved by the Board of Directors and shall be effective from the date of approval.