Information Security Policy

1. Purpose

Acter recognizes information security as fundamental to its operations and sustainable development. To preserve the confidentiality, integrity, and availability of information, reduce information security risks, and ensure business continuity, Acter has established an Information Security Management System (ISMS) in line with business needs, applicable laws and regulations, and ISO/IEC 27001. Through the ISMS, Acter continually strengthens information security governance and protects the information of the Company and its stakeholders.

2. Scope

This policy applies to the Company's information assets, information systems, networks, and related information security management activities. It also covers internal and external personnel involved in relevant business operations.

3. Information Security Governance and Responsibilities

The Company has established an information security management organization with clearly defined roles and responsibilities. The Information Security Committee oversees the implementation of the ISMS and regularly holds Information Security Management Review Meetings to review information security performance, risks, and improvement actions, thereby continuously enhancing the effectiveness of information security management.

4. Core Management Principles

The Company continuously promotes information security management in accordance with business needs and information security risks, following the principles below:

- **Information Protection:** Safeguard the confidentiality, integrity, and availability of information belonging to the Company and its stakeholders while reducing information security risks.
- **Risk Management:** Continuously identify and assess information security risks and implement appropriate management and protection measures based on risk levels.
- **Incident Response:** Establish mechanisms for reporting and responding to information security incidents to minimize their impact on business operations and stakeholders.
- **Business Continuity:** Establish business continuity and recovery mechanisms to reduce the risk of business disruption and enhance operational resilience.
- **Third-Party Management:** Manage information security risks associated with suppliers and third parties to reduce supply chain security risks.
- **Emerging Technologies:** Monitor risks associated with emerging technologies, including artificial intelligence (AI), while balancing innovation and information security.
- **Security Awareness:** Continuously promote information security education, training, and awareness programs to strengthen security awareness and responsibility among all personnel.

- **Regulatory Compliance:** Comply with applicable laws, regulations, contractual obligations, and information security requirements.
- **Continual Improvement:** Regularly review information security management performance, risks, and changes in the operating environment to continually improve the ISMS.

5. Information Security Objectives

The Company establishes information security objectives based on business needs and information security risks, allocates appropriate resources, and regularly monitors and evaluates the achievement of these objectives to continuously enhance the effectiveness of information security management.

6. Policy Establishment and Revision

This policy shall be reviewed at least once a year and revised when necessary. Any revisions shall be reviewed and approved by the appropriate management level before implementation.