

Information Security Management System Policy

AIRA Property Public Company Limited

Approved by the Board of Directors at Meeting No. 4/2025, held on 7 November 2025.

1. Purpose

This policy serves as the primary guideline for activities under the Information Security Management System (ISMS) of AIRA Property Public Company Limited. It defines high-level policies, responsibilities, and operational activities.

2. ISMS Policy

2.1 Information Security Requirements

- KPIs: ISMS performance shall be measured at least annually, reported to management, and communicated to all relevant departments.
- Legal requirements: Compliance is required with the following laws:
 - Computer Crime Act and its amendments
 - Copyright Act and its amendments
 - Cybersecurity Act B.E. 2562 (2019)
 - Personal Data Protection Act B.E. 2562 (2019)
 - International standards: The ISMS shall comply with ISO/IEC 27001:2022.

2.2 Information Security Principles

- Confidentiality: Information must be protected from unauthorized access.
- Integrity: Information must remain accurate, complete, and reliable.
- Availability: Information must be accessible in a timely manner when required.
- Risk-based approach: The value of assets, threats, and vulnerabilities shall be assessed to manage information security risks.

2.3 Objectives

To minimize and prevent information security incidents, maintain the Company's reputation and the confidence of its business partners, and sustain international information security certification.

2.4 Strategy

- Flexibility: The ISMS shall be adaptable to the Company's operational environment.
- Risk-based approach: Data-related risks shall be prioritized when selecting policies and security controls.
- Personnel competency: Personnel shall possess appropriate competencies in technical areas, IT infrastructure, security management, business continuity management (BCM), and ISMS processes.

2.5 Roles and Responsibilities

- ISMS Committee: Approves policies, allocates resources, approves risk assessment methodologies, and conducts management reviews.
- ISMS Management Representative (ISMR): Reports to the ISMS Committee, monitors ISMS effectiveness, and coordinates with internal auditors and certification bodies.
- ISMS Working Team: Implements policies, conducts risk assessments, provides training, and maintains performance indicators.

- Internal Auditor: Performs internal audits to verify compliance with Company policies, ISO standards, and applicable requirements.
- System Owner: Manages information within assigned systems and approves access rights.
- Custodian: Administers systems in accordance with information security policies and standard operating procedures.
- User: Is responsible for safeguarding information and reporting suspected information security incidents.

3. ISMS Framework (PDCA)

3.1 Plan

1. Define the ISMS scope and objectives, and appoint the ISMS Committee.
2. Establish the document structure and information security policies.
3. Define the ISMS operational scope and information assets.
4. Establish the risk assessment and risk management methodology.
5. Set measurable key performance indicators (KPIs).

3.2 Do

1. Risk Assessment and Management: Identify assets, assess risks, and implement appropriate treatment for overexposed assets.
2. Statement of Applicability (SOA): Document control objectives and selected information security controls.
3. Risk Treatment Plan: Implement and monitor risk treatment activities.
4. Training: Provide general information security awareness training and specialized skills training.
5. Operational Management: Maintain records in accordance with the Record Control Procedure.

3.3 Check

1. Performance Reporting: Summarize operational data and significant events.
2. Internal Audit: Verify compliance with Company policies, ISO/IEC 27001:2022, and applicable legal requirements.
3. Performance Measurement: Analyze performance data to identify deficiencies and opportunities for improvement.
4. Management Review: Conduct at least annually to review audit results, risk status, incidents, and improvement opportunities.

3.4 Act

1. Corrective Actions: Address, monitor, and track nonconformities.
2. Continuous Improvement: Continually enhance the effectiveness of the ISMS.

3.5 Support

1. Document Control: Manage documented evidence and external documents according to classification and retention requirements.
2. Competency Development: Develop personnel competencies to ensure they can fulfill their assigned responsibilities.

Announced on 7 November 2025