Information and Communication Security Management Policy

1. Purpose

The Company is committed to protecting its information and communication assets and maintaining a secure and resilient operating environment. This Policy outlines the governance framework for managing information security risks, enhancing organizational resilience, and supporting responsible and sustainable business operations. The framework references ISO 27001, domestic regulations, and recognized international practices.

2. Scope

This Policy applies to all information and communication assets managed by the Company, including hardware, software applications, network infrastructure, cloud services, and outsourced operations. All users and authorized personnel are expected to comply with this Policy.

3. Governance Structure

The Company has established a top-down governance framework to oversee information security management and ensure accountability, transparency, and effective risk oversight.

3.1 Information Security Committee

Chaired by the President and composed of senior leaders from relevant departments, the Committee meets annually to review strategy, assess risk posture, and monitor the effectiveness of security initiatives.

3.2 Chief Information Security Officer (CISO)

Held by the Head of the IT Department, the CISO is responsible for coordinating information security management, reporting on risk conditions, and supporting continuous improvement efforts.

3.3 Supporting Teams

- Cyber Incident Response Team: Handles incident reporting, containment, investigation, and recovery, and conducts periodic exercises.
- Security Management Team: Oversees daily security operations, training, policy implementation, and audit follow-up.
- Internal Audit Team: Conducts audits, evaluates compliance, and provides recommendations for improvement.

4. Core Principles of Information Security Management

The Company follows the Plan–Do–Check–Act (PDCA) cycle to support continuous enhancement of cybersecurity maturity. Key areas include:

- Continuous Improvement: Regular review of risks, controls, and policy relevance.
- Security Policy Compliance: Alignment with ISO 27001 and applicable laws.
- Risk Management: Identification and assessment of threats, vulnerabilities, and control effectiveness.
- Access Governance: Application of least-privilege principles, multi-factor authentication, and periodic access reviews.
- Incident Management: Real-time reporting and coordinated response and recovery mechanisms.
- Business Continuity & Disaster Recovery: Ensuring timely restoration of services in the event of disruptions.
- Third-Party Management: Requiring suppliers to comply with security standards and contractual obligations.
- Regulatory Compliance: Ensuring adherence to personal data protection and information security requirements.

5. Operational Security Practices

- Critical Operations Identification: Classify key business functions and systems based on risk levels.
- Asset Inventory & Risk Assessment: Maintain an updated inventory and conduct assessments in accordance with international standards.
- Secure System Development: Apply standardized SDLC practices, including security testing and code reviews.
- Access Control: Enforce least-privilege access and review account permissions periodically.
- Logging & Monitoring: Retain logs per legal requirements and implement monitoring to enhance detection and response capabilities.

6. Outsourcing and Vendor Management

- Vendor Standards: Vendors must demonstrate adequate security competence, such as holding ISO 27001 certification.
- Assessment & Contract Requirements: Conduct pre-engagement reviews and include security requirements, reporting obligations, audit rights, and service-level expectations in contracts.
- Access Oversight: Grant access based on least-privilege principles and audit access logs periodically.
- Incident Handling: Require immediate reporting of security incidents and impact assessments. Significant incidents may affect service scope or contractual terms.

7. Business Continuity and Disaster Recovery

- Risk Assessment & BIA: Identify business risks and define recovery objectives.
- Recovery Strategy: Maintain off-site backups and adopt resilient infrastructure to ensure continuity.
- Emergency Response: Establish structured communication and coordination procedures for emergencies.
- Testing & Drills: Conduct at least one disaster recovery drill annually to validate readiness.

8. Incident Reporting and Response

- Reporting Mechanism: Implement a tiered reporting structure based on severity.
- Response Execution: Isolate affected systems, assess root causes, and implement corrective actions.
- Post-incident Learning: Update risk assessments and controls based on incident reviews.

9. Audit and Review

The Company conducts periodic internal audits, risk assessments, and required training to ensure ongoing compliance and capability improvement.

10. Policy Management

This Policy becomes effective upon approval by the Chairperson, and any revisions shall follow the same approval process.