Information and Cybersecurity Management

1. Cybersecurity Risk Management Framework

1-1. Personnel Allocation

1-1-1. Dual Chief Information Security Officers (CISOs)

Ampoc has appointed two Deputy General Managers, one from the Business Operations Division and the other from the Manufacturing Division, to serve jointly as Chief Information Security Officers. Their responsibilities include:

- Approving and overseeing cybersecurity management policies and objectives.
- Approving cybersecurity-related regulations, procedures, and system documentation.
- Coordinating the assignment of responsibilities, resource allocation, and implementation of cybersecurity measures.
- Supervising and reviewing cybersecurity incidents.
- Approving other cybersecurity-related matters.

1-1-2. Dedicated Cybersecurity Officer

Key responsibilities (1 position):

- Promoting information system classification, implementing cybersecurity management systems, conducting internal audits, and organizing training programs.
- Managing system classification and security standards, performing security assessments, ensuring business continuity drills, monitoring cybersecurity mechanisms, building protective infrastructure, reporting and responding to incidents, and ensuring legal compliance.

1-2. Cybersecurity Task Force

1-2-1. Composition

Convened by the CISOs, this cross-functional team comprises department heads or designated representatives. Member roles and responsibilities are documented in the “Cybersecurity Task Force Roles and Responsibilities Matrix” and updated as necessary.

1-2-2. Responsibilities

Coordinating inter-departmental roles and responsibilities for cybersecurity-related matters.

Evaluating and recommending cybersecurity technologies, methods, and procedures.

Coordinating and reviewing overall cybersecurity measures and plans.

Formulating and promoting cybersecurity policies and objectives.

Establishing cybersecurity regulations and procedures, ensuring compliance with laws and contracts.

Developing annual work plans aligned with cybersecurity objectives.

Communicating cybersecurity policies and goals throughout the organization.

Researching and evaluating cybersecurity technologies.

Overseeing the implementation of cybersecurity rules and procedures.

Conducting system and data asset inventories and risk assessments.

Implementing data and information system protection measures.

Executing incident reporting and response mechanisms.

Conducting internal cybersecurity audits.

Reporting annual cybersecurity implementation status.

2. Cybersecurity Policy

2-1. Cybersecurity Objectives and Policy

This policy aims to prevent unauthorized access, use, control, disclosure, destruction, modification, or other forms of compromise to information or IT systems, ensuring confidentiality, integrity, and availability. Key principles:

Employees must undergo training to raise awareness in response to evolving cybersecurity threats.

Confidential and sensitive data must be protected against unauthorized access or tampering.

Internal audits shall be conducted regularly to ensure policy adherence.

3. Specific Cybersecurity Measures

Ampoc has adopted comprehensive measures to ensure the confidentiality, integrity, and availability of its information assets and to support business continuity:

3-1. Network and System Security Enhancements

Periodic asset inventories and risk assessments to guide risk control actions.

Designated system administrators perform routine security checks based on system classification.

Engage third-party IT service providers for system maintenance.

3-2. Host Security Classification & Internal Auditing

Cybersecurity and data protection are included in annual audit plans.

Internal control reviews are reported to the Board of Directors with statements of compliance.

3-3. Vulnerability Assessments and Penetration Testing

Biannual vulnerability scans, phishing simulations, and penetration tests.

High-risk vulnerabilities are scanned and mitigated as needed.

3-4. Cybersecurity Awareness

Periodic employee training on cybersecurity and data protection.

New employees must sign confidentiality agreements and adhere to company security policies.

Antivirus software is mandatory on all personal computers; unauthorized software is prohibited.

3-5. IT Administrator Capability Building

System audit logs are maintained to detect unauthorized modifications.

OS and application patches are promptly applied.

Administrators monitor online threats and review system logs routinely.

Training is provided to enhance administrators' log analysis skills.

3-6. Network Security Management

Firewalls isolate internal networks from external access.

Critical systems are isolated from the internet; external access may be routed through proxy servers.

3-7. Access Control Measures

System access rights are strictly controlled.

Passwords are regularly updated and must follow security standards.

Remote maintenance access is restricted to specific access lists.

Vendors and contractors must comply with the company's cybersecurity protocols.

3-8. Backup and Redundancy

Critical systems and data are backed up and equipped with redundancy mechanisms.

4. Resource Allocation for Cybersecurity Management

4-1. Organizational Structure

A dedicated “Cybersecurity Task Force” includes dual CISOs, one cybersecurity officer, and two full-time cybersecurity staff responsible for formulating policies, planning, coordinating, and executing protection measures.

4-2. Management Review

The Task Force reports annually to senior management on implementation outcomes, reviews policies for effectiveness and relevance, and ensures compliance with laws and regulatory standards.

4-3. Incident Record

No significant cybersecurity incidents or confidential data breaches were reported in 2024. No losses occurred to the company or its clients.

4-4. Awareness and Training

Annual cybersecurity awareness and training programs are conducted for all system users through workshops, internal meetings, and bulletin postings. Key personnel receive professional training. Vendors and service providers are also informed of company cybersecurity goals and monitored for compliance.

4-5. Policy Compliance

The cybersecurity policy and its implementation guidelines were updated in 2024 to comply with local and international regulations and to reflect changes in the external environment.

4-6. External Security Assessments

Third-party cybersecurity risk assessments were completed in 2024.