AMICCOM Electronics Corporation **(The “Company”)**

Information Security Management Implementation Status for the Year 2025

Information Disclosure in Information Security Management

Board report date：December 24, 2025

Contents

1 Information Security Management Strategy and Framework…………………….………… 3
1.1 Information Security Policy ……………………………………………………………3
1.2 Information and Communication Technology Security Risk Management Framework ...3
1.3 Specific Management Plan ……………………………………………………….…4
1.3.1 Review Results of the Information Security Management Review Meeting …………..4
1.3.2 Annual Information Operations Audit………………………………………………… 5
1.4 Resources Invested in Information Security Management……………………………… 5
2 Significant Information Security Incident ……………………………………………………7

1. Information Security Management Strategy and Framework

Describe the information security policy, information security risk management framework, specific management plans, and resources invested in information security management, etc. (Regulatory basis: Article 18, Item 6, Sub-item 1 of the Annual Report Standards)

1.1 Information Security Policy

The company's information security policy guidelines are 1. Establish information security management standards that comply with regulations; 2. Achieve a consensus that everyone is responsible for information security through awareness among all employees; 3. Protect the confidentiality, integrity, and availability of company information; 4. Provide a secure production environment to ensure the sustainable operation of the company's business, with the main goals of preventing viruses, hacking, and data leaks. This includes establishing firewalls, intrusion detection systems, antivirus systems, and various internal control systems to enhance the company's ability to defend against external attacks and ensure the protection of internal confidential information.

The company has introduced and established a complete Information Security Management System (ISMS) to reduce corporate information security threats from the system, technology, and procedures aspects, establish an information security protection environment that meets customer needs, and continuously conduct a "Plan-Do-Check-Act" (PDCA) cycle for continuous improvement.

The "Planning Phase" focuses on information security risk management. In order to strengthen information security, the ISO27001 information security management system has been introduced since 2023, so that all information systems can operate under standard management specifications, reducing security loopholes and production anomalies caused by human negligence. Through annual review operations, continuous improvement is also achieved.

In the "Execution Phase", the company builds a multi-layered information security protection mechanism, continuously introduce new information security risk control technologies, use intelligent/automated mechanisms to improve the efficiency of the detection and response procedures for various information security incidents, and strengthen the information security and network security protection processes to maintain the protection of the company's important assets.

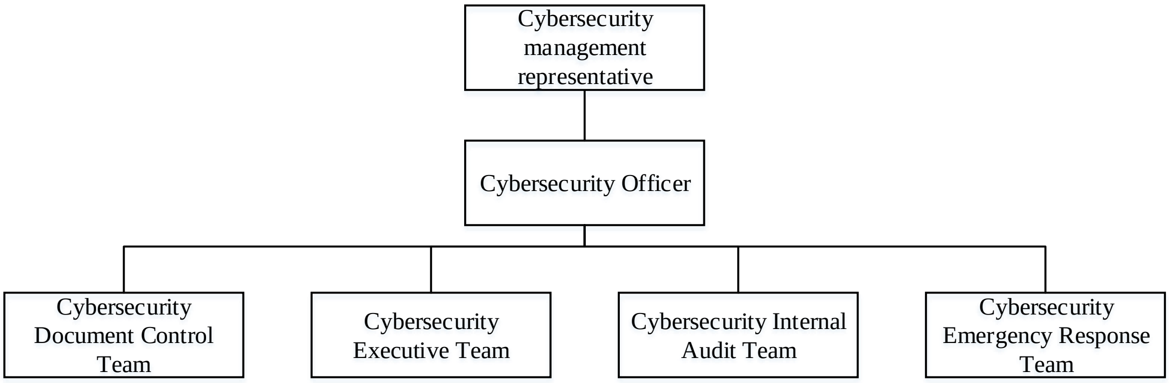
The "Audit Phase" regularly monitors the effectiveness of information security management indicators, and the above-mentioned management system is audited by a third party every year. In addition, a well-known information security vendor is commissioned to conduct penetration testing to ensure continuous improvement of information security management and defense capabilities.

The "Action Phase" review and continuous improvement: Through annual review operations, continuous improvement is made to enhance information security management and defense capabilities.

1.2 Information and Communication Technology Security Risk Management Framework

The company established the "Information Security Management Committee" in the year 2023, responsible for implementing information operation security management plans, building and maintaining an information security management system, and coordinating the formulation, execution, risk management, and compliance auditing of information security and protection-related policies.

Organizational Chart of the Information Security Management Committee:


Cybersecurity management representative
Cybersecurity Officer
Cybersecurity Document Control Team
Cybersecurity Executive Team
Cybersecurity Internal Audit Team
Cybersecurity Emergency Response Team

Cybersecurity management representative: served by the "Executive Vice President."

Cybersecurity Officer: Held by the "Head of Information Services Department."

Cybersecurity Emergency Response Team: Composed of "Information Services Department staff."

The committee reports the results of the information security management review meeting to the board of directors every year.

1.3 Specific Management Plan

To achieve information security policies and objectives, a comprehensive information security protection system will be established. The management matters and specific management plans to be implemented are as follows:

1. Compliance with laws and the introduction of international cybersecurity certification standards: The company implements information security-related ISO 27001 certification standards and regulations as a method and basis for achieving various risk management goals. An internal " Information Security Management Committee " has also been established to promote standardized operations and reduce operational risks.

2. Enhance cybersecurity defense capabilities: Regularly conduct vulnerability assessments and penetration testing of cybersecurity systems, and reinforce and repair them to reduce cybersecurity risks. Establish a network security incident response plan, assess the impact and losses based on the severity of incidents, and take corresponding reporting and recovery actions.

3. Enhance network security: Optimize the overall information system network security area and increase multi-factor authentication protection for privileged account logins on important servers.

4. Education and Training: Conduct comprehensive cybersecurity education and training for all employees, along with periodic social engineering phishing email tests, to enhance cybersecurity awareness. This ensures that cybersecurity operations are implemented with the support of senior management and all departments, reaching every employee.

1.3.1 Results of the Information Security Management Review Meeting

No major issues.

1.3.2 Annual Information Operations Audit

In October 2025, Deloitte & Touche conducted an information operations audit on our company. The audit results are as follows:

Item No.	Audit items	Discovery and Risk	Suggestion	Improvement Strategy
(1)	System Change Control	Findings: Upon investigation, it was found that your company: 1. While the Windows operating systems hosting the Workflow ERP host (CORPAP03) and AD host (CORPDC01) have undergone operating system patch updates, the "Information Service Request Form" has not been completed. 2. The Windows operating system hosting the AD host (CORPDC01) has not installed the major updates released by Microsoft this year, and no evaluation records have been kept. Risks: 1. Failure to implement patch update requests and testing acceptance procedures may result in improper system changes that go undetected by administrators, potentially affecting the accuracy of system data. 2. Failure to perform timely security updates and assess the system's condition may lead to vulnerabilities not being patched promptly, increasing vulnerability to external attacks/threats.	Suggestion for your company 1. When updating or upgrading the Windows operating system via patch, an "Information Service Request Form" should be completed to maintain application and testing records, and approved by supervisor. 2. Regular assessments should be made to determine if major updates released by Microsoft are necessary. If an update is deemed necessary, application, testing, and supervisor approval records should be maintained; if an update is deemed unnecessary, relevant assessment records should be maintained. Note: Official patch information can be found at: https://portal.msrc.microsoft.com/en-us/security-guidance	1. The process will now require filling out the form first, followed by updating, to avoid situations where the form is not filled out after updating. 2. Information service application forms will be completed after assessments in March and September each year, and the assessment results will be listed on the application form.

Item No.	Audit items	Discovery and Risk	Suggestion	Improvement Strategy
(2)	Access Security Control	Findings: Upon inspection, it was found that your company's Check Point firewall authentication method: Check Point Password password policy is not fully configured as follows: Password expiration time: never expires Minimum password length: 6 characters Risk: If the system's passwords are not strong enough and are not changed regularly, the system account may be more easily stolen, which could lead to the risk of data tampering.	Suggestion for your company: It is advisable to assess whether, without affecting normal system operation, the Check Point firewall password policy should be adjusted according to the S2-I-13 Access Control Management Procedure Specification, with the following recommended values: Password expiration period: 90~180 days Minimum password length: 8 characters	The password is updated and changed to 8 characters every 180 days.

1.4 Resources Invested in Information Security Management

- Establish information security management standards that comply with regulations.
  - Implementing the ISO 27001 Information Security Management System.
    - Number of related meetings held: 6 times.
  - Establishment of the "Information Security Management Committee".
    - Total number of personnel in the Information Security Management Committee: 20 people.
    - Cybersecurity Executive Team External Training Course.
      IT Home's CYBERSEC 2025 Taiwan Cybersecurity Conference.
      Online Information Security Course Hosted by Taiwan Academy of Banking and Finance.
- Protecting the completeness and availability of company information.

  - ■ Update the HR system mainframe (store all virtual machines, M data, ERP data, electronic sign-off system data...).
    Investment amount: NT$255,000
  - ■ Update backup host and storage space (store all virtual machines, M data, ERP data, electronic sign-off system data...).
    Investment amount: NT$390,000
- Antivirus, anti-hacking.
  - ■ Update endpoint security software.
    Investment amount: NT$360,000
  - ■ Update your Windows operating system (Win7 -> Win11).
    Investment amount: NT$93,000
  - ■ Perform all server vulnerability scans - penetration testing.
    Investment amount: NT$150,000
  - ■ Perform social engineering drills to increase employee security awareness and avoid executing malicious emails.
    Investment amount: NT$180,000

The total amount invested in ICT security management hardware and software is: NT$1,428,000

2. Major cybersecurity incident

This year, no major information security incidents occurred.