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

Information Security Management Implementation Status for the Year 2024

Information Disclosure in Information Security Management

Board report date：December 25, 2024

Contents

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.

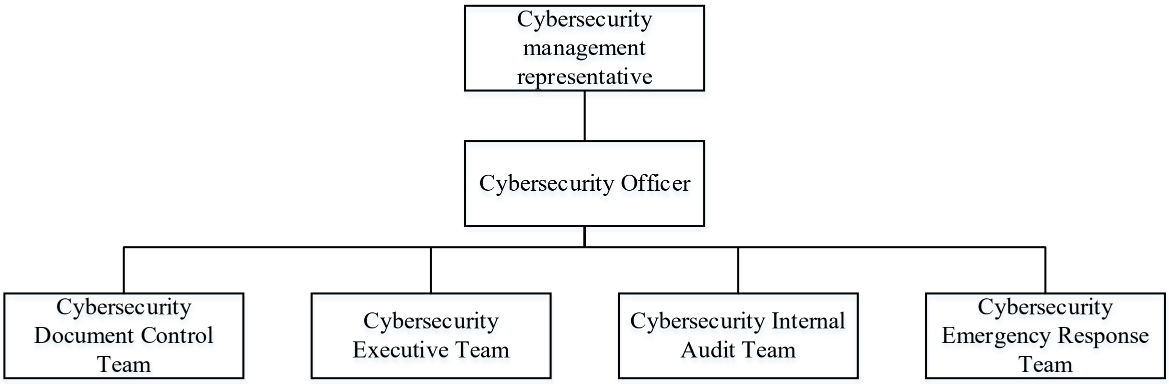
The "Audit Phase" regularly monitors the effectiveness of information security management indicators, and the above-mentioned management system is audited by a third party every year. In addition, a well-known information security vendor is commissioned to conduct penetration testing to ensure continuous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

Item NO.	Audit items	Audit Findings	Improvement Strategy
4	Other	Windows 7 operating system is too outdated, and Microsoft no longer provides security patches, raising concerns about cybersecurity.	Updating the Windows operating system of computers with Internet capabilities to Windows 10 and 11 has been completed in 2024.

1.3.2 Annual Information Operations Audit

In November 2024, Deloitte & Touche conducted an information operations audit on our company. The audit results are as follows:

<table>
<tr><th>Item No.</th><th>Audit items</th><th>Discovery and Risk</th><th>Suggestion</th><th>Improvement Strategy</th></tr>
<tr><td>(1)</td><td>System Change Control</td><td>Findings:
After inspection, it was found that the Windows operating system where your company's Workflow ERP host (CORPAP03) and AD host (CORPDC01) are located has not installed the major updates released by Microsoft this year, and has not regularly evaluated whether updates are needed.

Risk:
If security updates are not carried out in a timely manner and the system status is not assessed, vulnerabilities may not be patched immediately and the system may be vulnerable to external attacks/threats.</td><td>Suggestion for your company

It should be regularly evaluated whether major updates released by Microsoft require updating. If the evaluation does not require installation, evaluation records and supervisor approval records must be kept.</td><td>The current plan is to use the patch update system (Ivanti), which will be updated once a month. The system is scheduled to go online at the end of December 2024.</td></tr>
<tr><td>(2)</td><td>Access Security Control</td><td>Findings:
After inspection, it was found that the following accounts in the MS SQL database linked to your company's Workflow ERP system did not apply the Windows password validity period setting, and there were no manual changes to the passwords on a regular basis:
<table>
<tr><th>account number</th><th>Date of last password changed</th></tr>
<tr><td>sa</td><td>2022/03/17</td></tr>
</table>
Risk:
If the password strength is insufficient, system accounts may be more susceptible to theft, thereby increasing the risk of data tampering.</td><td>Suggestion for your company:

In order to strengthen information security, it should be evaluated to manually change the password regularly (at least once a year) without affecting the operation of the system.</td><td>It is recommended to change the password manually every year.

(Password updated on 12/5)</td></tr>
</table>

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: 5 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 2024 Taiwan Cybersecurity Conference.
- Protecting the completeness and availability of company information.
  - Establish a software patch system to manage and update software patches.
    Investment amount: NT$320,000.
  - Update the disk host (store all virtual machines, M data, ERP data, electronic sign-off system data...).
    Investment amount: NT$700,000.
- Provide a safe production environment.
  - Expand the UPS (uninterruptible power supply system) in the computer room and add a power circuit.
    Investment amount: NT$69,720.
  - Computer room UPS (uninterruptible power supply system) battery pack replacement.
    Investment amount: NT$65,000.
  - Computer room UPS (uninterruptible power supply system) reinforcement project.
    Investment amount: NT$35,175.
- Antivirus, anti-hacking.
  - Anti-virus software authorization.
    Investment amount: NT$630,000
  - Update Windows operating system.
    - Update Windows operating system, Investment amount:NT$448,000.
  - Perform all server vulnerability scans - penetration testing.
    Investment amount NT$138,000
  - Perform social engineering drills to increase employee security awareness and avoid executing malicious emails.
    Investment amount NT$138,600

2. Major cybersecurity incident

This year, no major information security incidents occurred.