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 information security policy of AMICCOM Electronics Co., Ltd. covers the company and its subsidiaries both domestically and internationally. It is guided by the following principles: 1. Establishing information security management standards that comply with regulations; 2. Achieving a consensus that everyone is responsible for information security through awareness among all employees; 3. Protecting the confidentiality, integrity, and availability of company information; 4. Providing a secure production environment to ensure the sustainable operation of the company's business. The policy focuses on three main security protection areas: antivirus, anti-hacking, and data leakage prevention. It establishes 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.

AMICCOM Electronics Co., Ltd. has implemented and established a complete Information Security Management System (ISMS) to reduce enterprise information security threats from the system, technical, and procedural aspects. The company has created an information security protection environment that meets customer needs and continuously conducts the "Plan-Do-Check-Act" (PDCA) cycle for ongoing improvement.

The "Planning Phase" focuses on information security risk management. To strengthen information security, AMICCOM Electronics Co., Ltd. has implemented the ISO 27001 Information Security Management System since the year 112 of the Republic of China. This allows information systems to operate under standardized management regulations, reducing security vulnerabilities and production anomalies caused by human errors. Additionally, through annual review processes, continuous improvement is pursued.

In the "execution phase," a multi-layered cybersecurity protection mechanism is constructed, continuously introducing new cybersecurity risk management technologies. The efficiency of detection and response procedures for various cybersecurity incidents is enhanced through intelligent/automated mechanisms, while strengthening the processes for information security and network security protection to safeguard the company's critical assets.

The "Audit Phase" involves regular monitoring of the effectiveness of cybersecurity management indicators, as well as annual third-party review audits of the aforementioned management system. Additionally, a well-known cybersecurity vendor is commissioned to
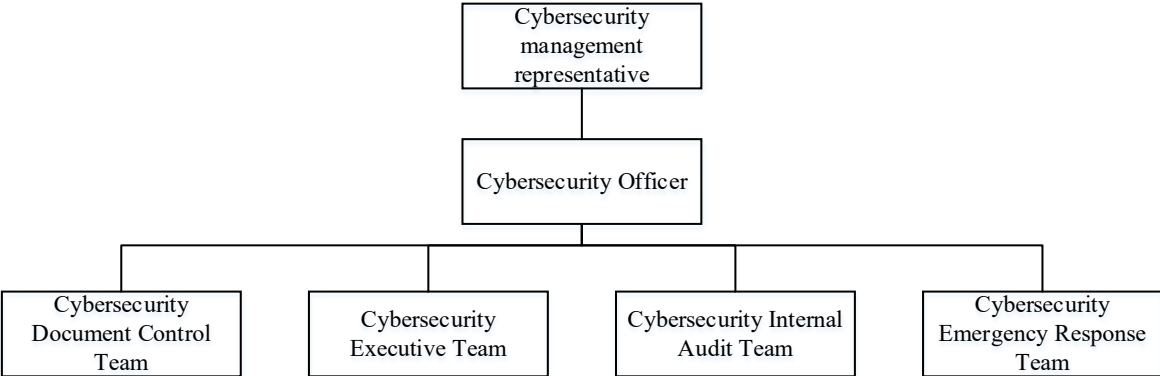
conduct penetration testing to ensure continuous improvement of cybersecurity management and defense capabilities.

"Action phase" review and continuous improvement, through annual review processes, continuously enhance and improve information security management and defense capabilities.

1.2 Information and Communication Technology Security Risk Management Framework

AMICCOM Electronics Co., Ltd. established the "Information Security Management Committee" in the year 2023 of the Republic of China, 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 │ │Cybersecurity │ │Cybersecurity │ │ Cybersecurity│
│Document      │ │ Executive    │ │ Internal     │ │ Emergency    │
│Control Team  │ │ Team         │ │ Audit Team   │ │ 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:

Compliance with laws and the introduction of international cybersecurity certification standards: AMICCOM Electronics Co., Ltd. implements ISO 27001 certification standards and regulations related to information security as a method and basis for achieving various risk management goals. The company has also established a corresponding "Information and Communication Security Management Committee" to specifically promote standardized operations and reduce operational risks.

Enhancing 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.

Enhancing Cybersecurity: Overall optimization of the information system's network security area, increasing multi-factor authentication protection for privileged account logins on critical servers.

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 at every employee level with the support of senior management and various departments.

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:

Item No.	Audit items	Discovery and Risk	Suggestion	Improvement Strategy
(1)	System Change Control	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.	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.	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.
(2)	Access Security Control	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: 	account number	Date of last password changed
---	---
sa	2022/03/17	 Risk: If the password strength is insufficient, system accounts may be more susceptible to theft, thereby increasing the risk of data tampering.	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.	It is recommended to change the password manually every year. (Password updated on 12/5)

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.