# Symtek Automation Asia Co., Ltd.

# Cyber Security Management Act

Board Report - November 12, 2024

## I. Cybersecurity Policy

1. Purpose

   Cybersecurity is the foundation of all information and communication services. In order to maintain the secure operation of all personnel, information systems, stored d13ata, equipment, and networks of Symtek Automation Asia Co., Ltd. (Short as SAA), this Cybersecurity Policy is formulated as the guiding principle.

2. Scope

   All employees, customers, outsourced or collaborative partners, suppliers, thirdparty personnel, and the security management of all relevant information and communication assets of the company shall be handled in accordance with the Cybersecurity Policy.

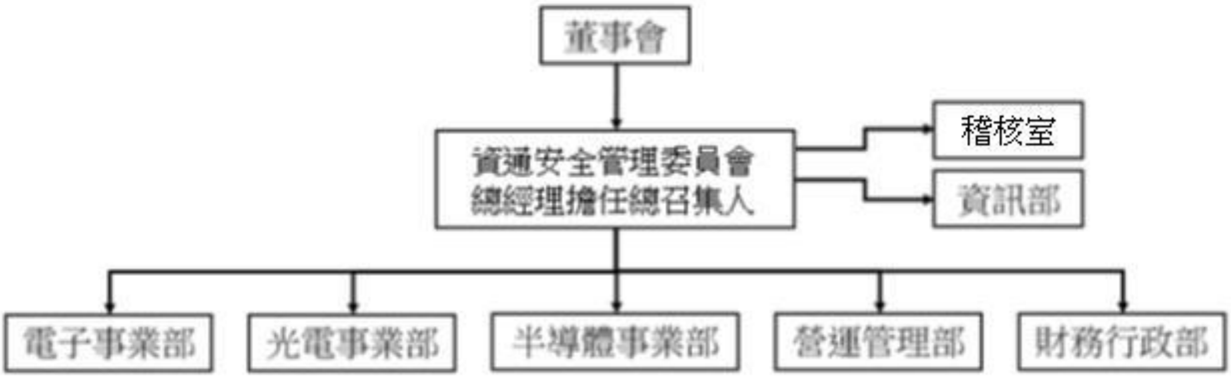
3. Content

   SAA with an attitude of sincere service, provides high-quality services to achieve customer satisfaction. With a proactive and innovative approach, prioritizing quality, and aligning with market growth and customer requirements, the company establishes the Cybersecurity Policy to protect the information and communication security and rights of stakeholders. To ensure the effective operation of information and communication systems, the organizational structure and responsibilities for cybersecurity are defined to promote and maintain various management, execution, and auditing activities. The Cybersecurity Management System is implemented based on the PDCA model, ensuring the effectiveness and continuity of information and communication service operations. To reflect changes in relevant laws and regulations, technological advancements, customer expectations, business activities, internal environments, and resources, the Cybersecurity Management Committee regularly reviews the Cybersecurity Policy and reports on the implementation to the board at least once a year.

II. Cybersecurity Management Framework

1. SAA establishes the Cybersecurity Management Committee, which oversees information and communication technology-related matters necessary for operations. The General Manager serves as the chairman (convener), and the highest executive of the information unit serves as the Information Security Officer. The committee is composed of the highest executives of various business units, information, audit units, etc., and holds periodic meetings to make decisions, manage, and promote cybersecurity affairs, fulfilling the responsibility of corporate operators, safeguarding the legitimate rights and interests of shareholders, and balancing the interests of other stakeholders.

2. Cybersecurity Management Framework:



3. Implement control from the perspective of "risk management," regularly selfcybersecurity audits, form a cycle of improvement and strengthening management, and ensure the smooth operation of various business operations.

4. Establish a threat intelligence analysis and warning mechanism. Through the sharing of intelligence with group companies, subsidiaries, and external units, provide information on cybersecurity events, reports, and other information to assist the company in enhancing the cybersecurity management system.

5. Conduct reporting procedures and response measures to enhance the ability of internal personnel to respond to sudden situations caused by cybersecurity events, minimizing the damage caused by cybersecurity incidents and thereby enhancing the company's resilience.

III. Specific Cybersecurity Management Plans

1. Strictly require the quality of various services, pass ISO 9001 management standards, and formulate relevant specifications in accordance with international cybersecurity standards.

2. Establish information management policies and follow the SAA's internal control system for information security, combining the PDCA method to gradually improve, aiming to protect the confidentiality, integrity, availability, and compliance of personnel, data, information and communication systems, equipment, and networks.

3. Senior executives actively participate in cybersecurity management activities, providing support and commitment.

4. Regularly convene cybersecurity management meetings to reflect the latest

developments in laws and regulations, internal and external risks, technological advancements, and business requirements, meeting the expectations of stakeholders.

5. Initiate from the perspective of risk management, assess and reduce risks to ensure the confidentiality, integrity, availability, and compliance of information and communication assets.

6. Introduce new technologies, deploy real-time monitoring equipment and protective systems, actively deepen mechanisms for protecting confidential information and communication, enhance the overall cybersecurity environment's security, reduce the incidence of various risks, and safeguard the interests of customers, partners, and stakeholders.

7. Continuously conduct various operational exercises to ensure that SAA can respond quickly when services face external threats, demonstrating the company's resilience.

8. Handle personal information and related system security with caution in accordance with relevant regulations such as the Personal Data Protection Act and the Cybersecurity Management Act.

9. Implement cybersecurity audits to ensure that SAA’s various businesses adhere to relevant policies and that the cybersecurity management system continues to operate normally.

# 2024 Cybersecurity Implementation Status

I. To strengthen SAA cybersecurity management and ensure the security of data, systems, equipment, and networks, create a healthy information and communication environment, deploy innovative cybersecurity protection technologies, and promote cybersecurity management operations. In October of 2021, the company established the Cybersecurity Management Policy and Framework, formed the Cybersecurity Committee, and formulated relevant cybersecurity specifications to confirm the effectiveness of cybersecurity management operations. The company reports the implementation status to the board once a year.

II. Conducted one remote backup drill in 2024:

1. Simulation scenario: In the event of a disaster, rapidly transfer system environment data to another system host.
2. Recovery time: From June 8, 2024, to June 11, 2024, the formal zone host data of SPA (Production).
3. Restoration environment: SQA (Test) zone host.
4. Relevant departments are requested to confirm whether the test area environment data is correct - June 17, 2024.

III. Conducted a cybersecurity equipment update report in 2024:

Year Company Project Completion 2023 Group Group VPN Equipment Replacement In progress Asset Management System In progress SAA SSL VPN Equipment Replacement Completed Core Switch Replacement SAC Branch Office Firewall Completed

| Year | Company | Project | Completion |
|---|---|---|---|
| 2024 | Group | Asset Management System | In progress |
| | | Social Engineering Simulation | In progress |
| | SAA | Cybersecurity Vulnerability Detection | In progress |
| | SAC | VMware Server Replacement | Completed |

IV. Post-update effectiveness:

1. Cybersecurity Vulnerability Detection
In response to TSMC's supply chain cybersecurity requirements, an external cybersecurity vulnerability detection system was introduced to enhance information security. (Total cost: NTD 59,850)

2. SAC VMWare Server Replacement
The original VMWare hardware reached the end of its service life and could no longer be expanded or updated. Therefore, the system was replaced to improve system stability and operational efficiency. (Total cost: RMB 1,136,900)

3. Social Engineering Drills
On 8/20 (Tuesday), the first social engineering training session was held for participants from SAA, SAC, SAE, and SAH. (Total cost: NTD 150,000)

V. Planned cybersecurity equipment update projects for 2025:

| Year | Company | Project | Completion |
|---|---|---|---|
| 2025 | Group | Group Point-to-Point VPN Equipment Replacement | In progress |
| | | Endpoint Management System | TBD |
| | SAA | Cybersecurity Vulnerability Detection | In progress |
| | | Social Engineering Simulation | |

VI. Expected post-update effectiveness:

1. The VPN load balancer will be replaced due to the inability to renew the maintenance contract. This is to ensure more stable data exchange and traffic between the various plants within the group.

2. Build an endpoint management system to enhance the security protection of user computer devices.

3. Conduct security vulnerability detection to strengthen the protection of information equipment vulnerabilities.

4. Perform social engineering drills to raise users' awareness of network and information security.

VII. Conducted five cybersecurity awareness campaigns in 2024.

1. Cybersecurity Alert: Recently, hacker groups have become more active. The ransomware group Red CryptoApp claims to have breached over 10 corporate organizations. For detailed information, please refer to the description in the text - May 3, 2024.

2. Cybersecurity Alert: A hacker group exploited system vulnerabilities to successfully breach the Ministry of Education, resulting in data leakage. For detailed information, please refer to the description in the text - May 15, 2024.

3. Cybersecurity Alert: Phoenix UEFI firmware has a high-risk vulnerability - July 1, 2024.

4. Cybersecurity Alert: VMWare ESXi is being exploited by ransomware hacker groups - July 31, 2024.

5. Cybersecurity Alert: Chinese hacker group TIDrone has targeted Taiwan's satellite and military industries, with three listed companies experiencing DDoS attacks - September 13, 2024.

VIII. Information Security Education and Training

In the 2024, Information Security Training Class List:

| Department | NAME | Position | Course Dates | Remarks |
|---|---|---|---|---|
| Information Security | Li, Hsin-Chung | Manager | 5/4 ~ 5/18 | CISSP, Course Completion Certificate |
| Information Technology | Hong, You-Wen | Assistant Manager | 5/4 ~ 5/18 | CISSP, Course Completion Certificate |
| Information Security | Li, Hsin-Chung | Manager | 6/28 | TSMC Supplier Information Security Conference |
| Information Security | Lü, Kun-Yan | Senior Engineer | 6/28 | TSMC Supplier Information Security Conference |

IX. **Implementation of ISO/IEC 27001:2022 Edition**

In order to maintain the secure operation of all personnel, information systems, stored data, equipment, and networks within the company, we have adopted the ISO/IEC 27001:2022 edition as the highest guiding principle.

| Information Security Committee | Personnel and Contact Information (Extension or Mobile) |
|---|---|
| Convener | Huang, Fa-Bao (General Manager) #508 |
| Management Representative | Lin, Chao-De (Deputy General Manager) #128 |
| IT Team | Hong, You-Wen #355<br>Zeng, Yi-Lun #391<br>Tsai, Cheng-Hsun #357 |
| Information Security Team | Li, Hsin-Chung #370<br>Lü, Kun-Yan #356 |