Dynamic Holding Co., Ltd.

The Information Security Management

A. Information Security Management Strategies and Frameworks

1. The Definition of Information Security

Information security management is a management issue that cannot be ignored nowadays. Its main spirit is to identify the organization's important information assets and the threats they face, and to plan reasonable control measures under the effective allocation of resources to reduce risks to the acceptable level of the enterprise.

This is a risk management process. The focus of management should be on the protection of the organization's confidential information, rather than the access to all information assets as this will increase the company's cost and sidetrack the main purpose. In recent years, the endless information security incidents worldwide are mostly caused by the lack of the above-mentioned information security risk management mechanism.

2. Information Security Risks

The main information security risks we face are as follows:

- Virus/worm/ransomware attack: caused by accidental or malicious click on unknown files or links.
- Natural disasters: typhoons, floods, etc. that cause power outages and indirectly interrupt the operation and maintenance service of the system/equipment.
- Man-made disasters: carrying or sending confidential information, improper destruction process etc.
- Recovery plan: The likelihood of the backup data being completely recovered to use.

The company will plan response plans for the above-mentioned information security issues, and perform drills for different information security situations to strengthen the response capabilities of the processing personnel, so as to detect and block in the first time; in addition, Dynamic conducts security audits regularly, such as vulnerability scanning or penetration testing to ensure that the information system and network environment meet security standards.

3. Information Security Policy

- The information security policy of Dynamic Holding Co., Ltd. covers the company and its domestic and international subsidiaries.
- Establish the concept of "Everyone is responsible for information security", enhance the colleagues' awareness of information security, and guide them to implement information security protection work.
- To comply with international information security standards and local information security laws and regulations.
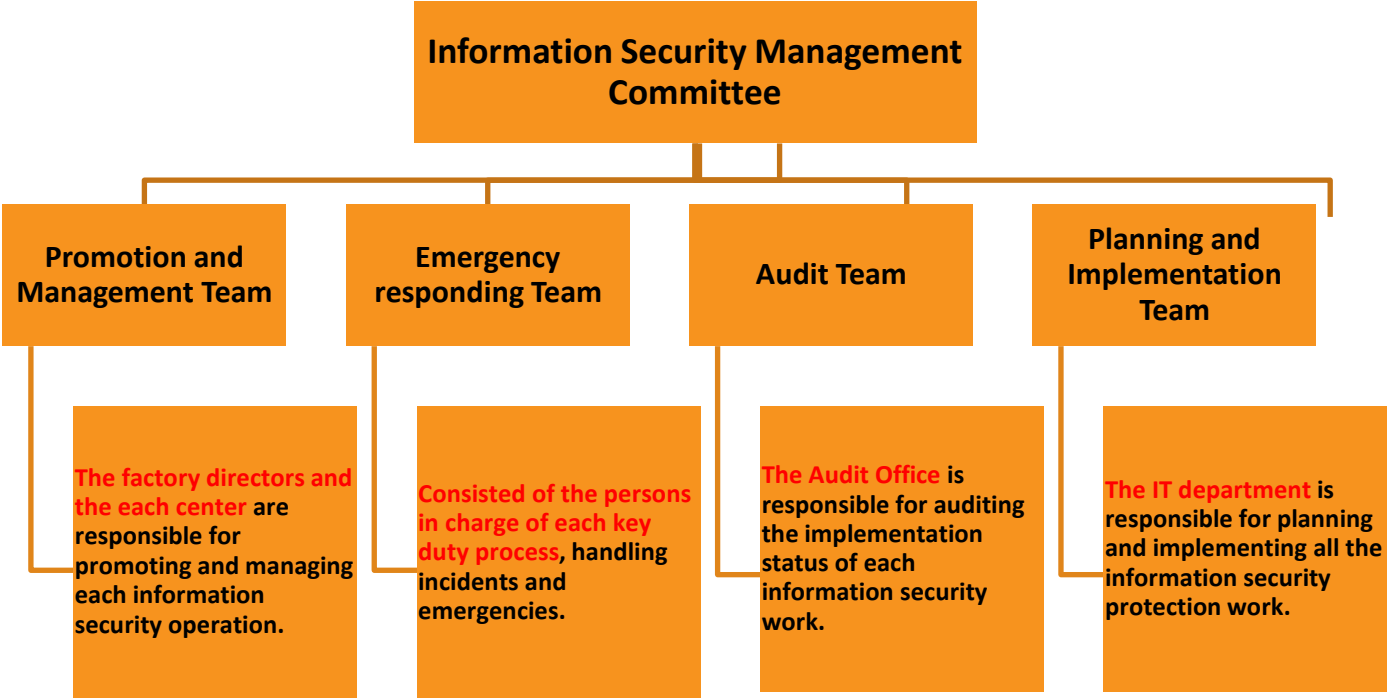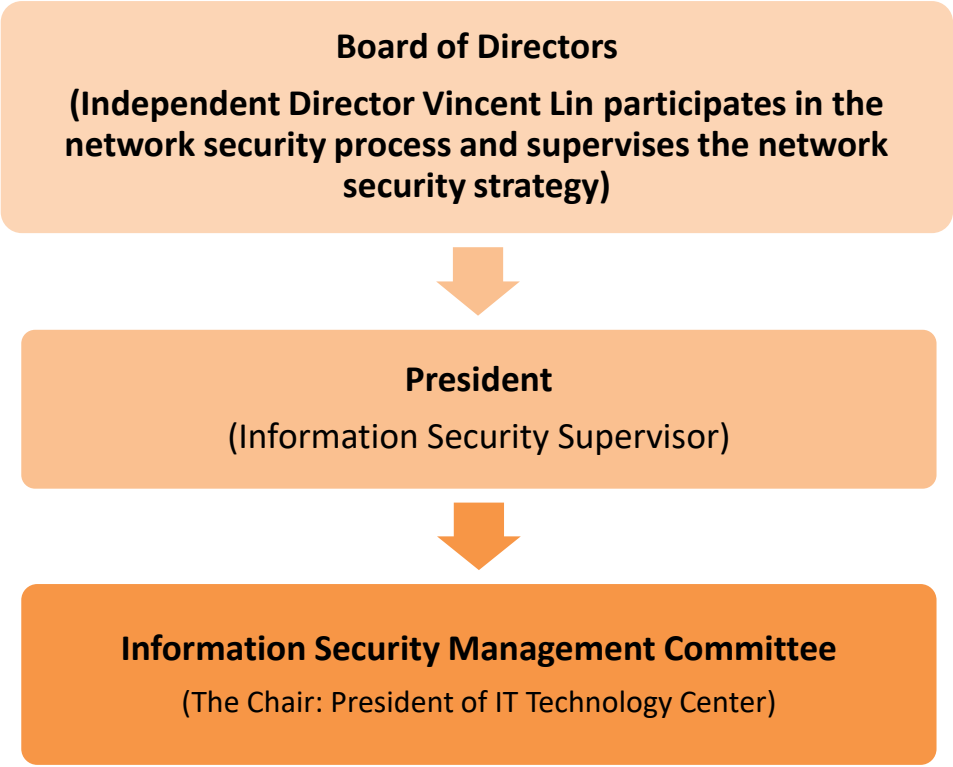
- Establish information security management standards that comply with regulations and meet customer requirements.
- Carry out appropriate protection measures for customer information and the company's important information assets to maintain the company's normal and continuous operations.
- Continue to pay attention to changes in the information environment and conduct related risk assessments.
- With the three core pillars of information security protection—antivirus, anti-hacking, and anti-leakage—as objectives, we have implemented firewalls, intrusion detection systems, antivirus solutions, and various internal control systems to enhance the company's ability to defend against external attacks and safeguard internal confidential information.

4. Information Security Implementation Plan

- Establish a compliance cycle mechanism, regularly review and revise internal operating regulations to conform to the international information security standards and local information security laws and regulations.
- Well equipped with all relevant information security norms and train excellent information security personnel.
- Keep the colleagues well informed of the risks of using e-mail, Internet and daily file access, and improve colleagues' crisis awareness of preventing attacks to reduce risks, so as to achieve the purpose of protecting customer data and important company operating information and services.
- Formulate disaster prevention countermeasures and disaster recovery plans for the company's important information assets.
- Review the information security policy regularly and report to the board of directors regularly (at least once a year).

5. Information Security Management Committee

On August 5, 2020, the company established the "Information Security Management Committee," dedicated to the governance and planning of the group's information security management. The committee is responsible for developing and maintaining the information security management system, as well as coordinating, implementing, and promoting related policies. With the goals of enhancing the company's comprehensive cybersecurity defense capabilities and strengthening employees' awareness of information security, the committee is chaired by the General Manager of the Information Technology Center. Regular progress updates are reported to the General Manager, along with assessments of information security risks, and the results are presented to the Board of Directors.

Board of Directors

(Independent Director Vincent Lin participates in the network security process and supervises the network security strategy)

↓

President

(Information Security Supervisor)

↓

Information Security Management Committee

(The Chair: President of IT Technology Center)

Information Security Management Committee

Promotion and Management Team	Emergency responding Team	Audit Team	Planning and Implementation Team
The factory directors and the each center are responsible for promoting and managing each information security operation.	Consisted of the persons in charge of each key duty process, handling incidents and emergencies.	The Audit Office is responsible for auditing the implementation status of each information security work.	The IT department is responsible for planning and implementing all the information security protection work.

6. Information Security Accountabilities

Company employees, contracted personnel and outsourced personnel are required to comply with the relevant provisions of the information security policy to ensure the safety of the company's production area, office area and information assets and equipment.

- All units: The operation content of all the equipment in the work area must comply with the company's information security policy.
- Information unit: Advocate information security risks and put forward risk issues and improvement measures.
- Subcontractor: Must follow the company's information security policy and adapt to the mechanism of necessary inspection.
- Information Security Committee: The increase, revision and abolishment of management measures, and the approval of major information security incident losses.

7. ISO27001 Certificate

- Huangshi Plant ISO 27001 Certificate (Valid: 2024.09.13~2027.09.12)
- Thailand Plant ISO 27001 Certificate (Valid: 2024.09.13~2027.09.12)

8. Concrete Management Solution

- Automatically perform website and system vulnerability scans on a regular basis.
- Sign regular contracts with external security companies to ensure that all software services installed on end systems, including IT and OT equipment, are kept up to date and all vulnerabilities have been patched.
- Manage and monitor movable company equipment.
- Import the bastion host and perform multi-factor authentication for maintenance personnel.
- Firewall integration and replacement to improve protection.
- Information security management system certification ISO 27001:2013 has been revised to ISO 27001:2022.
- Daily tape offline backup, weekly cloud offline backup; regular restore drills every six months to avoid blackmail.
- Regularly review the legality of account permissions, remove account permissions of resigned employees, and regularly change internal passwords.
- Provide regular information security training to senior managers and lower-level employees to effectively establish information security defense lines.
- Regularly conduct information security incident response drills.
- Use Sangfor Internet Behavior Management System for web page filtering, behavior control, traffic management, prevention of intranet leaks, prevention of regulatory risks, Internet security, etc.; set up firewalls and anti-virus walls to block malicious attacks and viruses from spreading to the internal network, and prevent Unauthorized users enter the system; use the WhatsUp system to monitor the network status of servers, switches and other equipment.
- In 2024, the company joined the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT) as a member and began sharing cybersecurity intelligence with other members.

- In 2025, a disaster recovery (DR) host was introduced to perform full system backups. In the event of server failures, systems can be fully restored—either as virtual machines or physical machines—using the DR host, significantly reducing service downtime.
- No data breach incidents occurred during the period from 2023 to 2025.
- Reports were presented to the Board of Directors on December 16, 2024, and December 15, 2025, respectively.

9. Invest resources in information security management
- There are currently 11 people in charge of information security, and we are continuing to add more people.
- The current construction cost of information security software and hardware equipment is approximately NT$44.95 million.
- The budget for information security in 2026 is approximately NT$13.63 million.

10. Number of personnel receiving information security education and training, and their hours:
- Course name: Information security and confidentiality awareness training, Email Security Awareness
- In 2025, 1812 people received information security education and training, with a total of 1339 hours.

B. Major Information Security Incidents:

1. In 2025, Dynamic did not experience any major information security incidents.
2. Security protection is established with a FortiGate firewall as the first line of defense, while Trend Micro antivirus and NOD32 provide malware protection for all servers, computers, and production-line equipment.
3. The company's firewall subscriptions are renewed annually and the system is regularly updated. Antivirus software is configured for daily automatic updates, and the bringing in of information equipment is strictly controlled.

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2022

This is to certify that: **Dynamic Electronics Co., Ltd.**
Factory P1, P2, No. 88 Daqi Avenue
Wangren Town, Economic and
Technological Development Zone
Huangshi
Hubei
435000
China

Holds Certificate No: **IS 746762**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2022 for the following scope:

> Provide printed circuit boards (including high-density interconnect multilayer printed circuit boards, high layer count printed circuit boards, high frequency and high speed printed circuit board) manufacturing and sales services. This is in accordance with the Statement of Applicability version 1.4 issued on April 8, 2024.
> Registration address: No.88 Daqi Avenue, Wangren Town, Economic and Technological Development Zone, Huangshi, Hubei

For and on behalf of BSI:

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2022-01-24
Latest Revision Date: 2024-09-13

Effective Date: 2024-09-13
Expiry Date: 2027-09-12

Page: 1 of 2

...making excellence a habit.™

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM

This is to certify that: Dynamic Technology Manufacturing
(Thailand) Co., Ltd.
99 Village No. 6
Si Maha Phot Subdistrict
Si Maha Phot District Prachin Buri
25140
Thailand

Is included as a location on Certificate number: **IS 746762**

And BSI location is: 0047694932-003

Operates an Information Security Management System
which complies with the requirements of
ISO/IEC 27001:2022
for the activities detailed in the scope of registration.

For and on behalf of BSI

Michael Lam - Managing Director Assurance, APAC

Original Registration Date: 2022-01-24   Expiry Date: 2027-09-12

...making excellence a habit.™

Certificate No: **IS 746762**

Location	Registered Activities
Dynamic Electronics Co., Ltd. Factory P1, P2, No. 88 Daqi Avenue Wangren Town, Economic and Technological Development Zone Huangshi Hubei 435000 China	Provide printed circuit boards (including high-density interconnect multilayer printed circuit boards, high layer count printed circuit boards, high frequency and high speed printed circuit board) manufacturing and sales services.
Dynamic Technology Manufacturing (Thailand) Co., Ltd. 99 Village No. 6 Si Maha Phot Subdistrict Si Maha Phot District Prachin Buri 25140 Thailand	Provide printed circuit boards (including high-density interconnect multilayer printed circuit boards, high layer count printed circuit boards, high frequency and high speed printed circuit board) manufacturing and sales services. Registration address: 99 Village No.6, Si Maha Phot Subdistrict, Si Maha Phot District Prachin Buri Thailand 25140

Original Registration Date: 2022-01-24
Latest Revision Date: 2024-09-13

Effective Date: 2024-09-13
Expiry Date: 2027-09-12

Page: 2 of 2