

4.6 Cyber Security

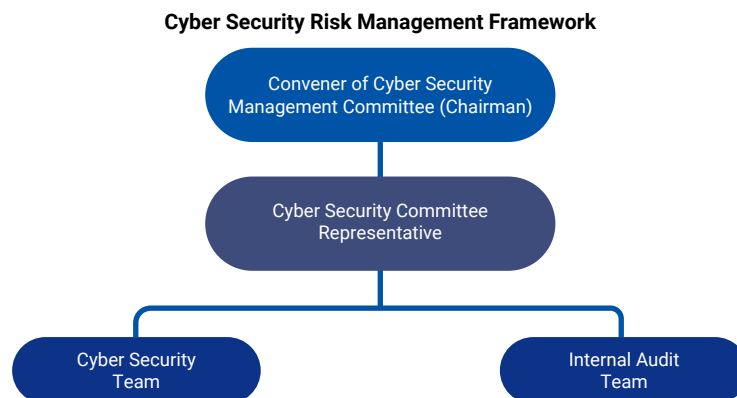
Cyber security is crucial for the protection of a company's trade secrets. Our IT Department formulates and implements the cyber security policy and execution plans, and drives their implementation and review for continuous improvement. Additionally, the Audit Office has established an internal audit team responsible for conducting audits at least once a year. This team reviews the effectiveness of the controls related to cyber security and tracks the progress of improvement plans

• Cyber Security Risk Management Framework

With regard to cyber security, the IT Department is responsible to form the Cyber Security Management Committee, which is convened by the Chairman and appointed the cyber security management representative. The Cyber Security Team and the Internal Audit Team under the committee are responsible for setting the Cyber Security Policy (hereafter "the Policy") and the action plans.

The Cyber Security Team reports the Company's cyber security management status to the cyber security management representative each quarter and reviews the Policy every year. The Internal Audit Team (Audit Office) is responsible for conducting audits, regularly performing annual spot checks on the implementation of the Policy and tracking the effectiveness of corrective action plans.

In 2024, the Cyber Security Team was composed of 2 personnel and the Internal Audit Team was composed of 2 personnel, with 1 cyber security meeting held. No major cyber security violations occurred during the year.



• **Cyber Security Policy and Guidelines**

The Cyber Security Policy of Microbio includes the following four guidelines:

- 1. Formulate management rules**
Standardize of the code of conduct for employees.
- 2. Information technology**
Introduce advanced software and hardware to effectively prevent cyber security incidents.
- 3. Promotion and improvement**
Raise employees' awareness of cyber security and strengthen self-protection, and constantly revise the ever-changing cyber security policies.
- 4. Join the cyber security organization**
Participate in official or private information and communication security organizations to strengthen the ability to search for cyber security and improve the proactive defense mechanism.

In addition, Microbio's "Cyber Security Policy" also specifies the applicable subjects, scope, and principles of information security management, covering all employees, external contractors, information assets, systems and application services. The core policy content focuses on strengthening the Company's overall information security governance capabilities and implementing the following key management commitments:

- 1. Continuous improvement of the information security management system:**The Company has established an Information Security Management System (ISMS) and regularly conducts management reviews and internal audits to continuously enhance its information security system and adjust its practices, in order to comply with laws and regulations and business needs.
- 2. Integrity and protection of information assets:** The policy explicitly specifies that information classification, access control, data backup, and restoration mechanisms must be implemented properly, in order to prevent unauthorized access and data loss, thereby ensuring the accuracy and reliability of information assets.
- 3. Strengthening of threat monitoring and response capabilities:** The Company has established an information security incident reporting and response process, and regularly conducts drills and reporting education, in order to strengthen the ability of identifying, responding to and handling potential threats.
- 4. Enhancement employee awareness on information security responsibilities:** Personnel who use information systems must comply with this policy and regularly participate in information security education and training, in order to enhance overall information security awareness.
- 5. Implementation of information security management for third parties:** Corresponding information security terms and control measures are established for suppliers and outsourcing

units involved in information processing, and such terms and measures are also incorporated into contracts, risk assessments, and audit management, in order to reduce external information security risks.

• **Cyber Security Goals**

In order to maintain the confidentiality, integrity, and availability of the information assets of the Company, the Cyber Security Policy has been implemented to achieve the following goals:

1. Establish a safe and reliable information-based operating environment to ensure the security of the Company's data, systems, equipment, and network, protecting the sustainable operation of the Company's business.
2. Protect the security of the Company's business services and ensure that only authorized personnel can access information to ensure its confidentiality.
3. Protect the security of the Company's business services and prevent unauthorized modification to ensure their correctness and completeness.
4. Establish the Company's business continuity plan to ensure the continuous operation of the Company's information services.
5. Ensure that the implementation of the Company's business services must meet the requirements of relevant government laws and regulations (such as: Cyber Security Management Act, Criminal Code, Classified National Security Information Protection Act, Patent Act, Trademark Act, Copyright Act, Personal Data Protection Act, etc.).
6. Protect the security of the personal information related to the Company's business activities from external threats or improper management and use by internal personnel that may result in theft, tampering, destruction, loss, or leakage.
7. Improve the protection and management of information assets and reduce operational risks.



• **Cyber Security Management Measures**

The specific management measures of Microbio are as follows:

1. Formulate management rules

In order to improve the information and communication security management system, Microbio passed ISO 27001 certification in October 2022, and obtained the certificate at the end of 2022. In order to implement the relevant management system through the international cyber security management standard, to enhance the awareness of cyber security among employees, and to establish the correct guidelines for the use of computer network, we have formulated the information policy and related management procedures as follows: Cyber Security Policy, Cyber Security Organization and Target Management Procedures, Information Asset Management Procedure, Procedures and Instructions for Cyber Security Risk Evaluation. As well as Physical Security, Operational Security, Access Control, and Cyber Security Incident Management-Related procedures and instructions.

2. Information technology

In terms of information security protection, the Company has strengthened its multi-layered protection of its software and hardware , including complex password verification, antivirus protection for servers and clients, web behavior management/malicious site protection, firewall blocking, host data backup, data encryption, network IP management, and Endpoint Detection and Response (EDR), etc. The scope of EDR deployment in 2023 was approximately 30%. Currently, core server EDR deployment has been completed to prevent malicious attacks.

Business Continuity Plan (BCP): The BCP is activated when disaster events disrupt business operations. The Information Security Team is responsible for coordinating the response to ensure that critical information services are restored to minimum operational levels as quickly as possible, minimizing potential losses. To ensure the effectiveness of the plan and enhance personnel readiness, at least one drill is conducted annually. On April 9, 2024, a disaster recovery drill was carried out, and both the system and database were successfully restored to normal operation.

3. Promotion and improvement

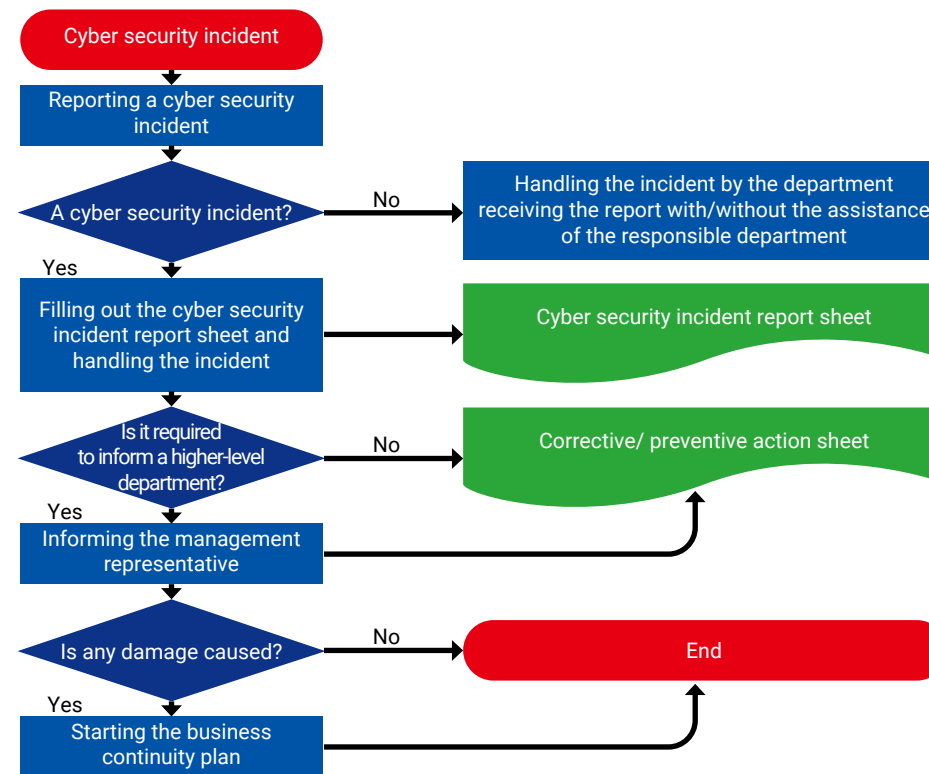
To enhance information security knowledge and to strengthen self-protection awareness of employees, at least one information security management review meeting is held annually to supervise and control relevant information security systems and events throughout the year. Additionally, at least three hours of information security training, one information security incident reporting drill, and continuous online information security promotion are conducted annually. In 2024, a total of 3 employee cybersecurity education and training sessions were organized, and 14 online email security training sessions were completed. In 2024, a total of 4 email social engineering drills were conducted to enhance the information security awareness of the Company's personnel.

4. Join Cyber Security Alliance for joint-defense mechanism

Microbio joined the TWCERT/CC Cyber Security Alliance in September 2022 and the Cyber Security Executive Association of the Information Service Industry Association (CISA) of the Republic of China in August 2023. Through these platforms, the company conducts periodic exchange of cybersecurity intelligence to enhance its defense breadth and strengthen cybersecurity resilience through collaborative defense mechanisms and shared information.

Vulnerability Analysis: The Information Security Team conducts annual vulnerability assessments to ensure robust cybersecurity management across the Company's data centers, internet infrastructure, EIP system, and office environment. On October 1, 2024, a system vulnerability scan was carried out, followed by an in-depth analysis of the identified risks. Based on the results, targeted remediation measures were implemented to mitigate potential threats and strengthen overall system security.

Flowchart of Reporting and Responding a Cyber Security Incident



Preface

1. Sustainability Performance

2. ESG Overview

3. Health Care

4. Corporate Governance

5. Safe Workplace

6. Social Inclusion

7. Environmental Protection

Appendix

2024 Microbio Cyber Security Training Statistics

Title of the Cyber Security -Related Training Course	Target Participants	Number of Actual Participants	Training Hours of the Course	Coverage Rate
IoT security and recent information security case study	All employees	124	3	91%
Job division and precautions of different units during an information security incident (unit heads and auditors)	Department Head	13	1	100%
Corporate anti-corruption and information security educational promotion	Designated personnel	9	1	100%

2024 Cotton Field Organic Cyber Security Training Statistics

Title of the Cyber Security -Related Training Course	Target Participants	Number of Actual Participants	Training Hours of the Course	Coverage Rate
ISO 27001 information security course	All employees at headquarters	44	2.5	75%
IoT security and recent information security case study	All employees at headquarters	49	3	83%

2024 Microbio (Shanghai) Cyber Security Training Statistics

Title of the Cyber Security -Related Training Course	Target Participants	Number of Actual Participants	Training Hours of the Course	Coverage Rate
Information security	All employees at headquarters	46	1	71%

Note: Coverage Rate = Number of Actual Participants / Target Participants

Microbio (including subsidiaries) Cyber Security Management Result

Classification	2021	2022	2023	2024
Total Number of Major Cyber Security Breaches	0	0	0	0
Total Number of Data Breaches	0	0	0	0
Total Number of Employees or Customers Affected by the Company's Data Breach	0	0	0	0
Total Amount of Fines/Penalties Paid in Relation to Information Security Breaches or Other Cyber Security Incidents	0	0	0	0

Note: Major cyber security incidents are defined in accordance with the Company's Information Security Incident Management Procedure.

• Introduction of ISO 27001 ISMS

To demonstrate the importance we place on cyber security and to align with international cyber security standards, we implemented ISO 27001 Information Security Management System (ISMS) in 2022 Q2, and established the Cyber Security Management Committee at the beginning of August 2022. The Chairman serves as the convener of the Committee, and the management representative is authorized to promote the management and operation of information and communication security, important information protection measures, and disaster drills and execution plans.

The ISO certification introduced covers system and management aspects. The implementation items include risk assessment, vulnerability repair, security protection, risk verification, asset inventory and risk assessment, and personnel education and training, in order to comply with international cyber security management standards. In October 2022, ISO 27001 Information Security Management certification was completed, and the certificate was obtained in December 2022. In 2023, the annual surveillance audit was completed by a third-party verification unit, and the certificate is valid until December 2025.

