2. 4. 2Information Security Management and Personal Information Protection

(1) Policies/Commitments

•Catcher is dedicated to robust information security management to safeguard our products and services against unauthorized access, alteration, misuse, or disclosure, while also minimizing risks from natural disasters. Our goal is to deliver accurate and accessible information promptly, ensuring the confidentiality, integrity, and availability of critical information assets in compliance with applicable laws and regulations. Through these efforts, we strive to build customer trust, uphold our commitments to shareholders, and maintain the uninterrupted operation of our core business activities.

Information Security and Personal Information Protection Policies		
Full Participation Enhanced Awareness	Proactive Prevention Effective Management	Customer Trust Sustainable Operations
Foster employee awareness and cultivate a shared responsibility for information security across the organization.	Deploy comprehensive security technologies and maintain an information security management system, driving continuous improvement through the Plan–Do–Check–Act (PDCA) cycle.	Ensure a secure and reliable manufacturing environment that supports the long-term sustainability of business operations.

(2) Targets: Safeguarding information confidentiality

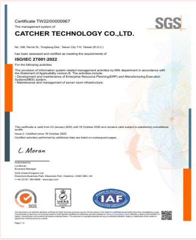
✧ **Promotion of Information Security**

1. Implement appropriate protective and preventive measures for all information stored or transmitted by the Company.
2. Minimize the impact of potential data security incidents, including destruction, theft, leakage, alteration, misuse, or infringement.
3. Continuously strengthen the confidentiality, integrity, and availability of operations within the information service system.

✧ **Promotion of Personal Data Protection**

Comply with the Personal Data Protection Act and applicable personal information protection regulations in all operating regions. Collect, process, and use personal information in accordance with legal requirements, while implementing appropriate security measures to ensure compliance. By doing so, we safeguard personal information security and protect the rights of data subjects.

Target	2024 Goal and Actual Performance	Short-term Goal (1~3years)	Mid-term Goal (3-10 years, till 2030)	Long-term Goal (>10 years, till 2050)
Annual average click-through rate of social engineering emails	Group average 0.6%	The annual average click-through rate is below 10%. In the mid- to long term, Catcher will continue to expand the application markets of its core products and technologies, while safeguarding the Company's critical assets and customers' confidential information.		
Number of complaints related to personal data protection	0	None		



Certificate TW22/00000967

The management system of

CATCHER TECHNOLOGY CO.,LTD.

No. 398, Ren'ai St., Yongkang Dist., Tainan City 710, Taiwan (R.O.C.)

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

The provision of information system related management activities by MIS department in accordance with the Statement of Applicability version B. The activities include:
- Development and maintenance of Enterprise Resource Planning(ERP) and Manufacturing Execution System(MES) system.
- Maintenance and management of server room infrastructure.

This certificate is valid from 03 January 2025 until 18 October 2025 and remains valid subject to satisfactory surveillance audits.

Issue 2. Certified since 18 October 2022

Certified activities performed by additional sites are listed on subsequent pages.

L. Moran

Authorised by
Liz Moran
Business Manager

SGS United Kingdom Ltd
Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK
t +44 (0)151 350-6666 - www.sgs.com

Page 1 / 2

▲ISO 27001
(valid from 2022 to 2025)

(3) Responsibilities

- According to the internal Information Security Management System Manual and Personal Information Protection Management Procedures, the scope of application covers the Company's operations, customers, suppliers, and all personnel involved in the personal information protection system. The Sales and Marketing Department is responsible for new project development, production schedule control, delivery, and pricing. The Quality Assurance Department ensures product quality, the Cybersecurity Office is responsible for formulating and promoting the protection of confidential information, and the Information Unit executes various tasks related to the information security management system. All employees are required to comply with the Company's confidentiality policy.

(4)Resources

- Appoint dedicated information security personnel to oversee and coordinate policy supervision, audits, training, and awareness enhancement activities. Information staff are responsible for implementing various information security systems and measures, as well as maintaining hardware and software operations.

(5) Grievance Mechanism

- Contact information and customer complaint handling procedures are provided on the official website.

(6) Specific Action in this year

❖ To demonstrate its commitment to information security management and to ensure that all information and information systems are properly protected, Catcher has established, documented, implemented, and maintained an Information Security Management System (ISMS) in accordance with the requirements of ISO/IEC 27001:2022. The system has been externally certified and will remain valid until October 18, 2025, with ongoing efforts to continuously improve its effectiveness.

Privacy Protection

To ensure robust personal data protection and management, Catcher has established the Regulations Governing the Collection, Processing, and Utilization of Personal Data in compliance with ISO 27001 and applicable local regulations. These regulations apply to all Catcher Group employees, suppliers, customers, and other personnel involved in the personal information protection system, and provide clear standards for the collection, processing, and use of personal data. The Company also delivers regular training and awareness programs to strengthen employee understanding and compliance with privacy protection requirements. Periodic internal audits are conducted to ensure that data handling practices conform to local laws and the Company's internal codes of conduct.

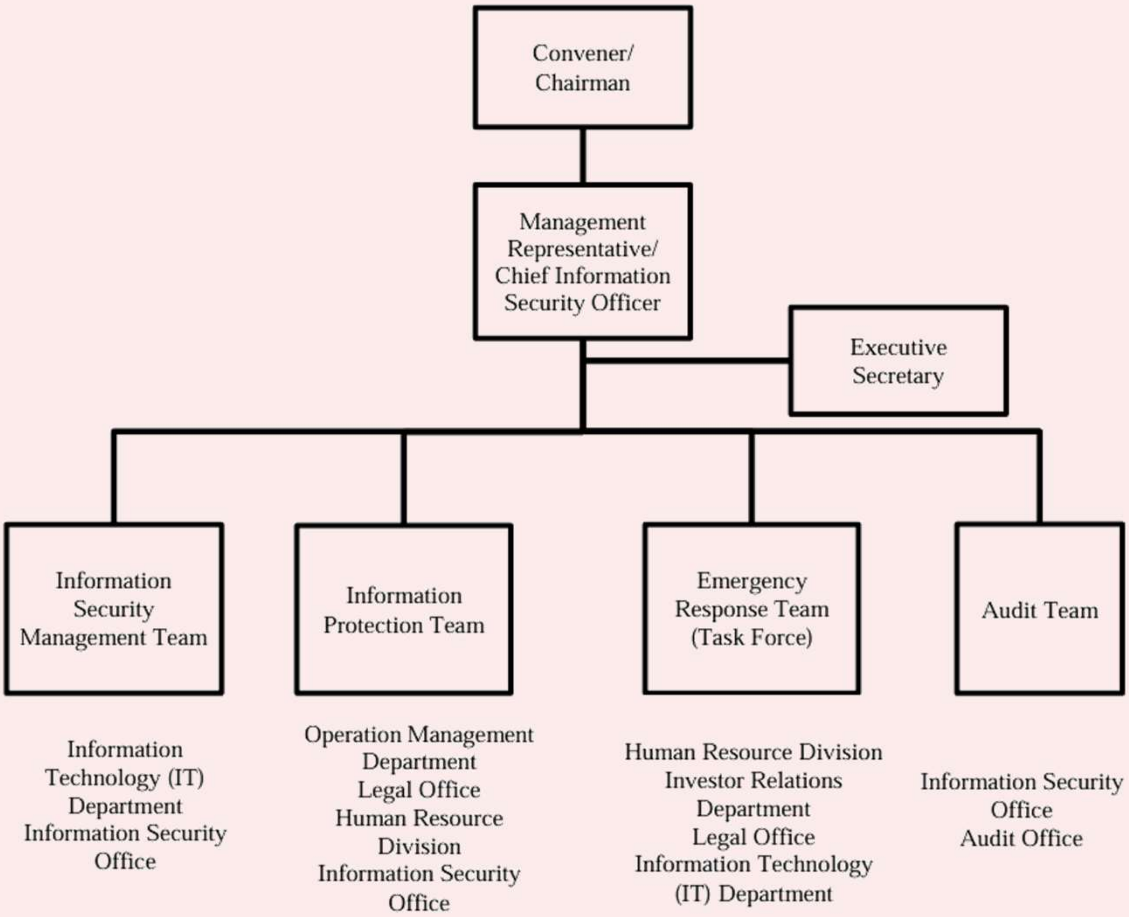
Catcher recognizes that safeguarding confidential information is critical to both the Company and its customers, as corporate reputation and customer trust depend heavily on it. Any mismanagement could result in penalties or legal consequences; therefore, Catcher is firmly committed to upholding the highest standards of privacy and confidentiality. Externally, the Company requires customers, suppliers, contractors, verification agencies, and other relevant parties to sign non-disclosure agreements to prevent potential losses arising from the unauthorized disclosure of confidential information.

In 2024, there were no complaints or incidents related to breaches of customer privacy, loss or disclosure of customer information, or violations of personal data protection. This outcome reflects the effectiveness of Catcher's internal management systems and its commitment to information security.

Information security management structure

The Company has established an Information Security Steering Committee, composed of a convener, management representative, executive secretary, Information Security Management Team, Information Protection Team, Emergency Response Team (task-based), and Audit Team. This committee is responsible for defining the direction and strategies for information security development, promoting and implementing various information security management tasks, and ensuring healthy operations of the information security management system.

- **Information Security Steering Committee**: The company's decision-making body for information security, responsible for overseeing and promoting all related initiatives.
- **Management Representative**: Oversees the planning of systems, resource coordination, and implementation of projects related to information security.
- **Executive Secretary**: Assists the management representative and convener in executing information security management tasks.
- **Information Security Management Team**: Responsible for the planning, establishment, implementation, maintenance, review, and continuous improvement of the information security management system for IT systems. It reports information security issues to the Steering Committee, coordinates audit schedules, oversees execution, and follows up on preventive and corrective measures.
- **Information Protection Team**: Promotes the management system for data and personal information protection.
- **Emergency Response Team**: A task-based team responsible for monitoring and tracking the development of major information security incidents, maintaining, updating, and executing disaster recovery procedures.
- **Audit Team**: Develops audit plans related to information security, conducts audits, and continuously monitors corrective and preventive actions for issues that do not comply with audit standards.


Convener/ Chairman
Management Representative/ Chief Information Security Officer
Executive Secretary
Information Security Management Team
Information Protection Team
Emergency Response Team (Task Force)
Audit Team
Information Technology (IT) Department
Information Security Office
Operation Management Department
Legal Office
Human Resource Division
Information Security Office
Human Resource Division
Investor Relations Department
Legal Office
Information Technology (IT) Department
Information Security Office
Audit Office

Three Major Safeguards for Personal Data Security Management

Information Security Management

Conduct inventory and classification of personal data files, and establish separate control mechanisms for data access, system access, and network access.

Personnel Management

Manage all personnel involved in the personal information protection system, and require them to sign confidentiality agreements to fulfill their obligation to protect personal data.

Environment and Equipment Management

Equipment and peripheral environments used for processing personal data files shall be subject to control and protection mechanisms to ensure file security. Protective and monitoring software shall also be applied to safeguard personal data and maintain relevant records.

Corresponding Information Security Mechanisms

To safeguard the confidentiality, integrity, and availability of its critical information assets, Catcher has established a comprehensive framework of network and IT security measures. The Company acknowledges, however, that it cannot fully guarantee absolute protection or uninterrupted operation of key corporate systems under its management—such as those supporting manufacturing, operations, and accounting—against potential cyberattacks by third parties.

To mitigate these risks, Catcher proactively develops and enforces information security measures, continuously strengthens its IT security environment, and reduces exposure to cyber threats. Furthermore, the Company has implemented multi-layered mechanisms to prevent, detect, and mitigate the impact of information security incidents. These initiatives provide a systematic and resilient approach to managing information security risks across the organization.

Category	Description	Measures
Management System	Establish information security management system	• Establish an Information Security Management System (ISMS) in accordance with ISO 27001:2022 international standards.
Network Security	Potential vulnerabilities & anti-malware / anti-intrusion measures	• Deploy next-generation firewalls to protect the internal network environment. • Establish spam email filtering and blocking systems. • Implement antivirus and endpoint protection mechanisms, conduct regular virus scans, and actively detect malicious programs. • Perform regular vulnerability scans on software and hardware, applying necessary patches and updates. • Conduct virus scans on incoming machines and enforce application whitelisting controls to prevent devices with malicious software from entering the Company. • Implement DDoS protection and network traffic scrubbing services. • Continuously strengthen the execution of network segmentation strategies.
Application System	System availability and response to service interruptions	• Establish system and network monitoring and reporting mechanisms. • Implement data backup and off-site disaster recovery solutions for systems and data. • Formulate contingency measures to address potential service interruptions. • Develop and maintain business continuity plans, conducting regular drills to ensure effectiveness.
Access Control	Control measures for personnel access to internal/external systems and data transmission channels	• Establish account authorization management and review mechanisms, with regular audits. • Monitor and analyze internal and external data access and operation logs. • Provide a zero-trust VPN channel to enable secure remote work for employees. • Implement a mobile device management (MDM) system. • Deploy multi-factor authentication (MFA) mechanisms.
Employee Training	Continuously develop and promote employee awareness programs on information security, thereby strengthening the Company's overall security posture	• Conduct regular and ad-hoc information security awareness campaigns. • Provide information security education and training for all new employees. • Deliver ongoing information security awareness training for employees. • Conduct quarterly social engineering drills.

Information Security Management and Personal Data Protection Achievements of the Year

Enhance Information Security Management System

1. Successfully completed the transition certification to ISO/IEC 27001:2022, with certification valid until October 18, 2025. Both the Company and its overseas subsidiaries established and implemented an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022, applying the Plan–Do–Check–Act (PDCA) cycle to ensure certification validity and drive continuous improvement.
2. Convened 12 information security management meetings throughout the year.
3. Revised 57 documents in alignment with operational procedures and ISMS requirements.
4. Strengthened data protection measures across both management and technical dimensions.
5. Initiated a personal data protection project to comply with the Personal Data Protection Act and relevant regulatory requirements.
6. Conducted information security audits of suppliers to reinforce the integrity of the supply chain.

Strengthen Information Security Protection Measures

1. Conducted 10 operational drills for critical information systems to strengthen business continuity and emergency response capabilities.
2. Completed 3 information security incident response drills to enhance the Company's ability to respond effectively to security incidents.
3. Performed 6 system vulnerability scans and risk assessments on a regular basis; all high-risk improvement projects achieved a 100% completion rate during the year.
4. Carried out external website penetration testing in 2024 to identify and reduce vulnerabilities, thereby improving website security and defense capabilities.
5. Continued to receive threat intelligence updates from the Taiwan Computer Emergency Response Team (TWCERT) and applied them to internal security management practices. The Company also actively participated in related industry and community activities.
6. Recorded zero complaints unrelated to personal data protection during the year.

Improve Employee Cybersecurity Literacy

1. Developed 30 information security awareness materials based on risk assessments and current events, continuously promoting key information security regulations and related topics. Over the year, more than 60,000 security awareness messages were delivered to employees.
2. Achieved a 100% completion rate for the general information security training, with all employees completing the annual information security and data protection program.
3. Conducted 4 social engineering drills across the Group, achieving an average annual click-through rate of 0.6%.

Information Security & Data Protection Education and Training Results (Group)

Number of Participants	Training Hours
6,490	4,451 hrs