4.4 Information Security

4.4.1 Information security management

In order to coordinate information development and information security management matters, and reduce information security risks, Mega Securities has established the "Information Security Policy" and "Information Security Policy - System Access Control" approved by the Board of Directors; in 2023, the Company continuously introduced and obtained the international information security certification ISO 27001 Information Security Management System, and the ISO 22301 certification in the same year. By operating the information security governance, legal compliance, risk control and audit review mechanisms, and in conjunction with the application of technology, we comprehensively enhance the information security protection capabilities. In addition, we have established the "Operating Regulations of Information Security Reporting and Response" to manage information security incidents at different levels (Level 1 to 4). When emergencies such as the information and communication systems compromised by various factors or inappropriate use, the required reporting and responses may be taken to reduce the probability of possible damage, and ensure the normal operation of the Company's information and communication systems.

Mega Securities Co., Ltd.
Information Security Policy

Information Security Team

I. Mega Securities has an information security team (the "information security team") composed of personnel from various departments to coordinate and discuss information security policies, plans, resource allocation, and other matters, as well as reporting and response of information security incidents. The information security meetings are held every six months.

II. The members of the information security team and the division of their responsibilities are as follows:

1. Person in charge of the information security team: the head of Information Department, responsible for the promotion of information security management affairs and resource allocation, and notifying the General Manager of the Level 3 or Level 4 information security incidents if occur.
2. Information security team convener: the person in charge of the information security team assigns a personnel of the Information Department to act as the convener, to assist person in charge of the information security team in implementing information security management affairs.
3. Members of the information security team from each department: The head of each department appoints one person to be a team member (in the case of a business unit, appointed by the head of the business group) to be responsible for various internal affairs to be cooperate d by the department.

◆ Management Structure Chart

Organizational Structure of the Information Security Team

- Approval of Information Security Policy | Board of Directors
- Information Team Leader | Head of Information Department
- Information Team Convener | Information Department Personnel
- Member of Information Team | Appointed by the head of each department

Information security incident reporting process and information security incidents

Where and information security incident falls into the cybersecurity incident defined in Subparagraph 6, Paragraph 1, Article 2 of the "Procedures for Major Incidental Events of Mega Securities," or the types of material information security incidents specified in Paragraph 3, Article 3 of the Regulations, it is deemed as a material information security incident with the following operations performed:

1. After reporting a material accident, the executive secretary of the Group's Information Security Incident Response Team ("the CSIRT team") shall be notified by phone or other means. Since the next day of reporting, complete the "Guidelines of Group Information Security Incident Response Form" based on "Guidelines of CSIRT Organization Establishment" and send it to the CSIRT Team Executive Secretary.
2. Fill in the "Material Incident Reporting Form" and report it to Mega Holdings before 17:00 on the next working day to the date of occurrence.
3. Information security incidents shall be reported through the securities and futures market information security incident reporting system (https://sfevents.twse.com.tw/) based on the "Notes for Report and Response of Information Security Incident in the Securities and Futures Markets." These deemed as the material information security incidents specified in Paragraph 3, Article 3 of the Regulations shall perform the following operations pursuant to the "Reporting Procedures to Report Scopes of Material Information Security Incidents by Securities Firms and Other Compliance Required:"
   (1) Fill out the "Material Information Security Incident Reporting Form for Securities Firms - Preliminary (Formal) Notification" within 30 minutes.
   (2) After reporting a material information security incident, the detailed information shall be reported to TWSE or TPEx within seven business days in letters, and fill out the "Material Information Security Incident Reporting Form for Securities Firms - Case Closing Notification," including time of occurrence, cause of incident, incident category, impact on securities firm and investors, whether sensitive data has been leaked, handling measures, recovery status, follow-up handling progress of the incident, handling of investor disputes, improvements, and preventive measures.
   (3) If reporting via letter within seven business days is impossible due to force majeure, the deadline for letter reporting may be postponed after being notified to TWSE or TPEx for record.

In 2023, Mega Securities had no data (including personal data) leakage incidents, and no customer or employee was affected by the information leakage incident, so no fines were paid.

Information leakage incidents	2021	2022	2023
Complaints from external parties that have been substantiated by the organization	0	0	0
Complaints from regulatory authorities	0	0	0
Number of information leakage incidents	0	0	0
Percentage of personal data-related leakage incidents (%)	0	0	0
Number of customers affected by information leakage incidents	0	0	0

Information Security Improvement Measures

1. The chief information security officer is appointed to oversee information security policy promotion and resource allocation. A Information Security Department has been established under the Information Department, with one information security officer and three information security specialists. Information security meetings are held on a regular basis for planning of the information security system, and monitoring and implementation of information security management.
2. The information security management system is introduced in the core system, certified by an impartial third party (SGS) for ISO 27001, and the validity of the certification is maintained constantly (valid until October 31, 2025).
3. Establish the Data Loss Prevention (DLP) system to monitor and block personal data to reduce the risk of personal data leakage.
4. Automatically compare the program versions of all external trading systems of Mega Securities daily. If there are any abnormalities, the relevant personnel will be notified to take action.
5. Dedicated personnel check regularly whether there are external websites are phishing websites illegally forging the official website of Mega Securities, or counterfeiting apps of Mega Securities. Investors will be reminded of any discovery, and reported to the Financial Information Sharing and Analysis Center (F-ISAC).
6. The information security promotion, education and training are regularly conducted for all employees of the Company, to enhance their information security awareness, including the awareness of in-depth forgery and prevention issues.

7. The social engineering drills are conducted for all employees on a regular basis to improve their information security awareness.
8. The vulnerability of systems and webpages are scanned, and intrusion and penetration testing are conducted on a regular basis to strengthen the security of the Company's information system.
9. The remote backup market simulation tests are conducted regularly to ensure the effectiveness of the backup system.
10. The third-party laboratory information security testing are conducted for the Mega Securities mobile app (Mega Mobile VIP) every year to strengthen the app's information security.
11. The email filtering system (Softnext SPAM SQR) is constructed to strengthen the Company's email information security.
12. The automated management system for endpoint equipment (Security Intelligence Portal; SIP) is established to prevent unauthorized equipment from using the intranet.
13. The personal computer highest permission management system is constructed to centrally manage the highest permission of personal computers at the client end company-wide, to strengthen the Company's information security.
14. The web application firewall (WAF) is constructed to enhance the information security of Mega Securities.
15. The IDS/IPS-intrusion detection and prevention mechanism system is constructed to strengthen the Company's information security.
16. The host privileged account management system is constructed to centrally manage the privileged accounts of each system, for enhancing the Company's information security.
17. The source code security testing tools and third-party component testing tools are purchased to test the applications developed and maintained by the Company. These tools are able to identify potential risks in advance and fix them in a timely manner to strengthen the Company's information security.
18. Every two years, an information vendor is commissioned to conduct a cyber security checkup service, the checkup results help Mega Securities to understand the information security vulnerabilities hidden, and serve as a reference for planning and strengthening information security control in the future.
19. The main information security equipment are introduced into the information security monitoring center (SOC), to strengthen the Company's information security monitoring and defense.
20. The business continuity management system is introduced in the core system, certified by an impartial third party (BSI) for SO 22301, and the validity of the certification is maintained constantly (valid until December 27, 2026).
21. In order to maintain the system stability, the upgrade of the middle office operating system and database (APGW) of the trading system is completed.
22. The construction of a log server is completed for centralized log control.

Information security management mechanisms and measures

For the cyber threats and risk changes brought by technological developments, Mega Securities continuously reviews the adequacy of relevant regulations and measures, and has established a comprehensive network and computer security protection system. The system vulnerability scanning and patching,

penetration testing, social engineering drills, cybersecurity education and trainings are conducted from time to time every year. Furthermore, through the introduction of ISO 27001 information security management system to verify and establish an SOC (information security monitoring center), ensuring the appropriateness and effectiveness of information security and network risk control. The actual expenditure on information security in 2023 (including hardware, software, and licensing-related expenses) accounted for 5% of the 2023 budget; of which Mega Securities' actual expenditure on the operation of the core operating system and equipment in 2023 accounted for 82.63% of the budget of core operating system and equipment operations.

Information security management measures	Mega Securities' information security management measures in 2023 and their implementation
Information Security Monitoring Center (SOC)	The information security monitoring center (SOC) is established to implement the data protection mechanism, the storage media control mechanism, and IDS information security protection to strengthen information security monitoring and defense.
Vulnerability scanning	The vulnerabilities are scanned regularly every year, and the vulnerabilities are continuously improved and tracked to identify potential cybersecurity threats and vulnerabilities in advance, to strengthen the security protection capability of the cyber system.
Penetration testing	The Company commissions a third-party agency to complete the penetration testing of all external services on a regular basis every year, and no major risks were found after the test.
Social engineering drill	The email social engineering drills are conducted regularly every year, with information security education and training for employees and promotion of information security-related issues, to enhance employees' information security awareness and make them more alert to phishing emails.
Business continuity testing	The business continuity drills are conducted every year, to ensure that critical systems and backup systems can continuously provide key services, and the test results are verified to ensure that the backup mechanism is implemented to ensure normal and continuous system services.
Information security management system	To standardize and internationalize the information security system, Mega Securities has completed the introduction of ISO 27001:2013 information security management systems and third-party verification, with continuous third-party re-certification to maintain the validity of the certificates (please refer to Appendix 8.3 External Independent Assurance Statement)

Information security education and training

In recent years, the information security has become an ESG focus of the financial industry, and the customer information security protection is a core item in Mega Securities. To ensure that employees are equipped with information security knowledge and raise their awareness, the information security-related education and training are held every six months, and online courses are provided for employees to enhance the information security knowledge for coping with changing information

security issues. In 2023, two sessions of education and training were conducted, with 3,033 person times completing the training, and 9,099 hours of education and training in total, or an three hours of training per employee in average.

Other highlights of information security management in 2023	
Case descriptions	Mega Securities has completed the international information security certifications: 1. The core system for brokerage business passed ISO 22301 (Business continuity management system) certification (valid from 2023.12.28 to 2026.12.27) 2. ISO/IEC 27001:2013 continuous verification (valid from July 12, 2023 to October 31, 2025)
Key Performance Outcomes	1. On December 28, 2023, the core system for broker business passed (ISO 22301 Business continuity management system) certification 2. ISO 27001:2013 continuous verification (information security-related management activities, including data center management, network management, and development, maintenance, and management of securities trading middle office system, back office system, front office system, mobile VIP, e-Netcom, Global Money Management, HTS (Home Trading System), Mega Winner, Mega API, Sysjust API, Multi Chart, E Radar, and wealth management systems) (valid from July 12, 2023 to October 31, 2025)
Public links to press release/ relevant information)	For details, refer to ISO 22301 and ISO 27001 certifications, and refer to Appendix 8.3 External Independent Assurance Statement for certifications.

4.4.2 Customer privacy and personal data protection

Mega Securities has fulfilled its duty to maintain the confidentiality of personal data and customer privacy information, and established the “Personal Data File Security Safeguard Plan and Personal Data Processing Methods after Business Termination,” specifying that the Company collects, processes, and utilize customers’ information, and establishes the measures for customers’ information security management pursuant to the “Personal Data Protection Act,” the “ Enforcement Rules of the Data Protection Act,” and the “Regulations Governing Security Measures of the Personal Information File for Non-government Agencies Designated by Financial Supervisory Commission,” among other regulations, while implementing the customer privacy and personal data protection through incorporation of customers’ personal data into the internal control system, conducting employee education and training, as well as regular personal data status inventory, risk assessment, and security maintenance self-assessments.

In addition, in order to become the most trusted partner of customers, Mega Securities has established the "Employee Code of Conduct," "Employee Reward and Punishment Procedures," and "Customer Information Confidentiality Measures of Mega Financial Holding Co., Ltd. and its Subsidiaries" to regulate employees' respect for company information and customer privacy. Information shall be kept confidential and shall not be disclosed except by law or with approval, even after resignation.

If employees violate the provisions of the Principles and the confidentiality measures, their permission to use the Company's information will be terminated immediately. Based on the severity of the violation, such employees will be penalized according to the Company's relevant punishment regulations and held accountable for legal responsibility, to demonstrate the emphasis of Mega Securities on personal data protection and customer privacy.

Mega Securities only allows the government to request customer privacy-related information under lawful circumstances. No other illegal requests for data, no customer data are used for secondary marketing, nor violation incidents of customer privacy rights or loss of customer data.

Customer Data Used for Secondary Marketing Purpose	2021	2022	2023
Number of customers whose data are used for secondary marketing (may be the number of accounts)	0	0	0
Total number of customers (may be the number of accounts)	384,996	408,600	434,115
Percentage of customers whose data were used for secondary marketing (%)	0	0	0

Information security incidents	2021	2022	2023
Total number of information security incidents	0	0	0
Number of customer data loss due to information security incidents	0	0	0
Number of customers affected by information security incidents	0	0	0

Implementation of the "Personal Data Protection Education and Training Course" in 2023

Description of the Related Education and Training Courses	Number of courses (sessions)	Number of people trained(person-time)	Total course hours (=number of trainees x number of hours per course)
1. 2023 Online courses on Ethical Corporate Management Best Practice Principles, Personal Data Protection Act, whistleblowing system, and Sexual Harassment Prevention Regulations 2. 2023 Legal Compliance Seminar_Handling Whistle-Blowing Case and Personal Data Protection 3. In 2023, the era of strong personal data supervision came. 4. The value of personal data is maximized through de-identification	4	1,671	3,479