Mega Financial Holding Company Ltd., Information Security Policy

Formulated by the 10th meeting of the 7th Board of Directors on March 26, 2019
114.6.24 First amendment adopted at the 15th meeting of the 9th Board of Directors

Article 1 (Definition and purpose)

In order to strengthen information security management, establish secure and reliable information operations, ensure the confidentiality, integrity and availability of data, systems, equipment and networks, and protect the interests of customers, this policy is formulated as the basis for the company and its subsidiaries to implement various information security measures.

Article 2 (Scope of application)

This policy sets out the information security policies to be followed by the employees of the company and its subsidiaries, as well as their roles, rights and responsibilities in the process of information security work planning, practice and continuous improvement. The scope includes:

I. Organization and personnel: All employees, contractor workers, third parties and consultants, etc.

II. Documents: All materials, documents, official papers and reports, etc.

III. Software information assets: All application systems, utilities, software packages, databases, operating systems, etc.

IV. Hardware information assets: All servers, personal computers, storage media, terminal devices, communication lines, etc.

Article 3 (Management scope)

The scope of information security management shall at least cover the following items:

I. Information security management organization and responsibilities.

II. Personnel security management, education and training.

III. Information system security management.

IV. Network security management.

V. System access control.

VI. Security management of system development and maintenance.

VII. Security management of information assets.

VIII. Physical environment and environmental safety management.

IX. Continuous management of operation.

X. Security management of the information operations supply chain.

XI. Other information security management matters.

Article 4 (Information security management operation system)

In order to coordinate the Group’s information security management matters, an Information Security Management Meeting will be convened. The Chief Information Security Officer shall serve as the convener and designate appropriate staff units to execute and coordinate decisions related to information security meetings.

Management should support and provide the necessary resources for information security management, ensuring continuous enhancement of information security capabilities.

Article 5 (Compliance items)

The company and its subsidiaries should adhere to the following information security requirements:

I. It is necessary to continuously invest the required resources for information security management, considering current business development and network environment threats.

II. The information assets possessed should be properly protected. All information processed, stored, or transmitted and exchanged within the company’s internal information systems, equipment, and network resources belongs to the company as property, and the company has the right to view, copy, or access such information.

III. All employees, contractor workers, partner suppliers and consultants of the company and its subsidiaries who use the company’s information to provide information services or perform project work shall have the responsibility and obligation to protect the information assets(including data and documents) acquired or used by them, so as to prevent unauthorized access, alteration, destruction or improper disclosure.

IV. The qualifications of relevant third-party vendors and consultants involved in information operations should be reviewed to ensure that the technology, products, or services they provide meet contractual service levels and comply with the company's information security

and confidentiality requirements.

V. All employees shall be responsible for the custody of the information assets(including data and documents) held by the business they are responsible for, ensure the confidentiality, integrity and availability of important information assets, and prevent them from accidental or deliberate destruction, unauthorized alteration, improper disclosure or loss (including physical or electronic theft), so as to meet the operational interests of the company and comply with the requirements of relevant laws and regulations.

VI. It is everyone's duty to maintain and protect information security. When somebody knows that there is any violation of information security, he or she shall immediately prevent and report it.

VII. Information security needs shall be considered in the development, formulation and change of all types of management, administrative and technical operations.

VIII. The responsibility of information protection and confidentiality of the information obtained in each operation shall not be lost due to work change.

IX. The access and utilization of various information assets, including the installation, construction, development, use and maintenance of software and hardware such as computers, network facilities and information systems, shall refer to the relevant operating procedures and be authorized before implementation.

X. According to the needs of different types of work, such as management, business and information, information security education, training and publicity shall be conducted on a regular basis, so as to build employees' awareness of information security and improve the company's information security level and information security management ability.

XI. Anti-virus and anti-hacker systems shall be established to protect information operations and related assets, prevent improper or illegal use by people, and prevent hackers, viruses and other intrusion and destruction.

XII. In order to maintain network security and prevent the invasion of computer viruses, purchase legal anti-virus software or shut down

unnecessary network connections and services, and regularly update the relevant virus code and anti-virus engine. Additionally, maintaining awareness of current threat intelligence is essential.

XIII. An emergency notification system shall be established for information security incidents. When an information security incident occurs, it shall be reported to the competent authority immediately according to the handling procedures. According to the business needs, a business continuity operation plan shall be formulated and regular tests and drills shall be conducted.

XIV. The information security measures established shall comply with applicable legal regulations and the requirements of this policy.

Article 6 (Policy evaluation)

This policy is evaluated at least once a year, or reevaluated in case of major changes, to meet the latest development of relevant laws, technologies, organizations and operations.

Article 7 (Provisions on matters not covered)

Matters not covered in this policy shall be subject to the laws and regulations of the competent authority and the relevant provisions of the company.

Article 8 (Implementation and Amendment)

This policy will be implemented and will be amended after being approved by the Board of Directors.