# Mega International Commercial Bank Information Security Policy

Approved on November 24, 2010 in 16th meeting of 13th board of directors
Approved on October 18, 2018 in 15th meeting of 16th board of directors
Approved on June 10, 2022 in 7th meeting of 17th board of directors
Approved on October 17, 2025 in 8th meeting of 18th board of directors

**Article 1 (Purpose and Basis)**

To reinforce management of information and network security, establish a secure and reliable operating environment, ensure data, system, equipment and network security, and protect the interests of our clients, this policy is made as a basis of implementing all information security measures, in accordance with the Cyber Security Management Act, Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries, and Mega Holdings Information Security Policy.

**Article 2 (Responsible Unit)**

The Information Security Dept. is responsible for this policy.

**Article 3 (Definition of Information Security)**

The term “Information Security” in this policy refers to the protection for information systems and data from unauthorized access, use, control, transmission, damage, change, destruction, or other violation, to ensure their confidentiality, integrity and availability.

**Article 4 (Scope)**

This policy applies to all employees (including service staff and contractors), consultants, cooperative vendors and outsourcing personnel.

**Article 5 (Organization and Responsibilities)**

The Bank shall assign a manager ranked senior executive vice president or above or an individual with equivalent powers to serve concurrently as the

chief information security officer, who shall oversee the implementation and coordination of the information security policy and resource allocation.

The Information Security Dept. is set up as a dedicated unit responsible for planning, monitoring, and implementing the management processes of information security.

**Article 5-1 (Operation Mechanism of Information Security Management)**

To manage information security management matters the Bank shall regularly hold information security management meetings, the chief information security officer is the convener, and the Information Security Dept. is responsible for executing and coordinating determined resolutions.

Executive management shall support and provide necessary resources for the information security management to continuously enhance the information security management capabilities.

The Information Security Dept. shall report annually by the end of Q1 overall information security status of the Bank in the previous year to the Board of Directors, and in accordance with the regulations Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries in Paragraph 1, Article 27, the chief information security officer shall jointly sign and issue the internal control system statement.

**Article 6 (Information and Network Security Management Scope)**

Information and network security management shall include at least the following:

(1) Formulation and maintenance of information security policies

(2) Organizations and responsibilities of information security

(3) Employee management and information security awareness training

(4) Information system operation security management

(5) Network security plans and risk assessment management

(6) System access control management

(7) System / application development and maintenance security management

(8) Information asset security management

(9) Physical and environment security management

(10) Business continuity planning management

(11) Information operations supply chain security management

(12) Other information security management

**Article 7 (Information Security Principles)**

In accordance of the following principles, the Bank will strive for operation safety to achieve objectives of reducing the impact of information security risks, avoiding internal error to damage our reputation and images, insisting on high quality information security protections, and maintaining the trust and interests of our clients.

(1) All operations must be in accordance with the regulations of governing authorities and the Bank.

(2) Work assignment should refer to the segregation of duties. Proper duty segregation should be implemented to prevent information or service from being tampered or misused.

(3) According to business needs, proper background checks should be performed on all employees hired by our hiring methodologies. To enforce confidentiality of information kept or used by all employees and required to sign non-disclosure agreements.

(4) The qualifications of third-party vendors, outsourcing providers, and consultants involved in information operations shall be reviewed to ensure that the technologies, products, or services they provide meet contractual service levels and comply with the Bank's information security and confidentiality requirements. Where the nature of the

business necessitates, the Bank may require such parties to sign a non-disclosure agreement.

(5) All employees are obligated to protect our sensitive data and client data. Unauthorized access, disclosure or informing other colleagues, vendors, consultants or other clients about those data is prohibited.

(6) All employees should remain alert to abnormal events or violation of security policies or processes. If abnormal events or violation of security policies or processes take place, the event should be reported by predefined procedures.

(7) Emergency Response and reporting mechanism for information security incidents shall be established. In case of information security incidents, procedures shall be followed, and competent authorities shall be informed.

(8) Network security risk assessments, penetration tests, and vulnerability assessments shall be conducted periodically, in order to monitor vulnerabilities in data processing environments.

(9) According to business needs, business continuity plan should be established and tested and drilled periodically to maintain its adequacy.

(10) All changes made to critical information equipment (including software and hardware) should be evaluated by Data Processing & Information Dept. in terms of technical and specification aspects. If the assessment indicates involvement of information security risks, the Information Security Dept. shall be invited to participate.

(11) Continuous monitoring of threat intelligence shall be maintained, and mechanisms for antivirus and anti-hacking protection shall be established to safeguard information operations and related assets, prevent intentional misuse or unlawful activities, and deter intrusions and destructive actions by hackers, viruses.

(12) Information security awareness trainings shall take place to improve all

employees' knowledge on information security, and the Bank's overall information security robustness and management capabilities.

(13) All employees shall follow the relevant operating procedures and obtain proper authorization before accessing and utilizing any information assets (including data and documents). They are responsible for safeguarding and safekeeping of these assets to ensure the confidentiality, integrity, and availability of important information assets, and to prevent unauthorized access, alteration, destruction, improper disclosure, or loss, in order to align with the Bank's operational interests and comply with applicable legal and regulatory requirements.

(14) In consideration of current business development and prevailing network threats, necessary resources shall be continuously invested in information security management.

**Article 8 (Operating Standard)**

Information Security Dept. and Data Processing & Information Dept. should follow policy requires, and stipulate an information security operating standard. All units should follow the standard to secure our operating environment, and to enhance confidentiality, integrity and availability of our services.

**Article 9 (Policy Assessment)**

This policy shall be assessed annually, and shall be re-assessed upon any significant changes in the organization to reflect the development of government regulations, technologies and business operations.

**Article 10 (Unspecified Matters)**

All matters not covered by this policy should comply with relevant regulations and relevant rules of our banks.

**Article 11 (Approval Level)**

The policy will be effective upon approval of the board, also for amendment and abolishment.