Capital Layer Information Security Policy (Public Website Version)

1. The Company's information security objectives are to ensure the confidentiality, integrity, and availability of critical and core systems. **Quantitative** indicators for information security performance shall be defined and measured across all levels and functions to **verify** the implementation status of the information security management system and achievement of information security objectives.
2. To accomplish the Company's mission objectives and fulfill top management's expectations and requirements for information security, and to ensure the security of the Company's information assets, the information security policy is established as follows:

   a. Ensure the confidentiality of the Company's business-related information and prevent the leakage and loss of confidential information and personal data.

   b. Ensure the integrity and availability of the Company's business-related information **to ensure proper execution** of the Company's operations and **various** business activities.

3. To ensure effective operation of the information security management system, the Company has established an Information Security Committee to oversee the planning and implementation of the information security management system. Its organizational structure is **set forth** in the Company's "Information Security Policy" and "Information Security Organization and Management Review **Operational Procedures**."
4. Human Resources Security Control: To mitigate human factors affecting the Company's information security, the Company implements appropriate information security education, training, and awareness programs to enhance personnel awareness of information security.
5. Asset Management: To protect the security of the Company's information assets, the Company establishes an information asset inventory in accordance with **established standards** and defines principles for information asset classification, grading, and control measures.
6. Access Control:

a. To ensure authorized access to information processing equipment, user password, registration, modification, deletion, and periodic review mechanisms are established, along with clear desk and clear screen policies.

b. To maintain network security, network service mechanisms are established to segregate internal networks from **external access** and control the use of remote work and mobile devices.

7. Cryptographic Controls: Appropriate and effective **cryptographic usage** policies are established to protect the confidentiality, **authenticity**, and integrity of information.
8. Physical and Environmental Security Control: To ensure the security of **server rooms**, office premises, and related equipment, the Company establishes access control principles for **server rooms**, equipment inspection and management principles, and usage, management, and disposal principles for general office information equipment.
9. Operations and Communications Security:

   a. To ensure correct and secure operation of information equipment, regulations for proper use of information are established to prevent confidential information leakage, and mechanisms for preventing **malicious software** and mobile code are implemented.

   b. To ensure the integrity and availability of information assets, backup procedures for information processing facilities and control principles for using external information processing facility services are established.

   c. To maintain network security, network security control mechanisms and principles for protecting **system usage logs and audit trails** are established.

10. System Acquisition, Development, and Maintenance: To ensure the security of application system development management, testing, acceptance, deployment, maintenance, and outsourcing management operations, the Company has established standard control procedures.
11. Supplier Relationships: Supplier relationships and management are defined to ensure the security of suppliers' access to, processing of, and management of the Company's information and information processing facilities.

12. Information Security Incident Management: To minimize damage caused by information security incidents, the Company has established information security reporting and handling procedures and maintains records thereof.
13. Cloud Usage Security: When using cloud services, ensure the security of data, applications, and infrastructure to prevent unauthorized access, data breaches, and other security risks.
14. Threat Intelligence: Through the collection, analysis, and interpretation of cybersecurity threat-related information, assist the organization in predicting, identifying, and responding to various security threats to reduce potential risks and strengthen defensive measures.
15. Configuration Management: Manage and maintain the **configurations** of systems, **network devices**, software, and cloud environments to ensure their security, consistency, and predictability.
16. Business Continuity Management: To ensure the Company's continuous business operations, the Company has established information security control principles for business continuity management, established business continuity management processes and frameworks, and developed and implemented business continuity plans.
17. Compliance: To ensure that the implementation of the information security management system complies with relevant laws and regulations, security policies, and **current technological developments**, the Company has established compliance verification principles.
18. Employees who violate information security regulations shall be subject to disciplinary procedures for their information security responsibilities.
19. This policy shall be reviewed by the Company's top information security **executive** at least **once annually** to ensure compliance with current developments in relevant laws, technologies, and business operations, and to ensure the effectiveness of information security practices.
20. Matters not covered by this policy shall be handled in accordance with relevant laws and regulations and the Company's related provisions.
21. This policy shall be implemented upon approval by the Company's top information security management; the same applies to amendments.