SinoPac Holdings Co., Ltd.
Information Security Policy

■ Not formulated in accordance with external regulations

□ Formulated in accordance with external regulations

Formulating Unit: Information Security Division Approval Level: Board of Directors

Article 1. The Policy is formulated to enhance information security management by the Company and its subsidiaries, establish a secure and reliable information system, ensure the security of data, system, equipment, and network, raise employees' awareness on information security, protect customer rights, and be in compliance with information security related regulations.

Article 2. The term "subsidiary," as referred to in the Policy, shall be determined in accordance with Article 4 of the Financial Holding Company Act.

Article 3. Information security in the Policy refers to ensuring the confidentiality, integrity, and availability of information processing by the Company and its subsidiaries.

Article 4. An information security committee shall be set up to implement information security, with its rules set separately effectively.

Article 5. The scope of information security is as follows:

1. Separation of powers and responsibilities in information security.
2. Information security training.
3. Information system security management.
4. Network security management.
5. Application access management.
6. Application development and maintenance management.
7. Computer asset management.
8. System environment security management.
9. Information system disaster recovery management.
10. Other information security management matters.

Article 6. The principles of separation of powers and responsibilities for information security are as follows:

1. The discussion, establishment, and assessment of directions for information security policies, plans, and technologies will be conducted by personnel delegated by the convener of the Information Security Division.
2. The applications departments are responsible for discussing security requirements, usage management, and security of the data and information systems.
3. The Risk Management Division is in charge of reviewing and assessing

information security risk management.

4. The Compliance Division should formulate and revise information security policies and management systems.

Article 7. The information security training is as follows:

1. To address the needs of different work types, such as management, business, and information technology, to provide information security training and promotion to build employees' information security awareness and management capabilities.
2. Enhance training for information security personnel to improve information security management capabilities.

The Information Security Division shall handle information security training-related matters.

The information security responsibilities of employees who violate related regulations shall be handled per the "Employee Reward and Punishment Rules."

Article 8. Information security incidents shall be handled in accordance with the "Outline of Emergency Response" and reported to personnel designated by the convener of the information security committee immediately. The designated personnel shall evaluate the scope of impact, establish a response plan, and report to the convener for necessary decisions and work schedules.

Article 9. When outsourcing the information technology operation, the information security requirements should be studied in advance, and the vendor's information security responsibilities and confidentiality regulations should be clearly defined and included in the contract for compliance.

Article 10. Depending on its actual management needs, each subsidiary may establish information security-related rules and regulations to be followed by the subsidiary per this Policy and report to the Information Security Committee for review.

Article 11. Matters not mentioned in the Policy shall be handled in accordance with the relevant laws and regulations of the competent authority and the Company's relevant regulations.

This Policy shall be reviewed at least annually to see if it needs to be revised or updated based on actual business needs or changes in the law.

Article 12. This Policy is effective upon approval by the board of directors; the same applies in the event of amendments.

Approved in the 6th meeting by the 4th Board of Directors on June 22, 2012.

Amended in the 12th meeting by the 4th Board of Directors on December 21, 2012.

Amended in the 6th meeting by the 4th Board of Directors on June 21, 2013
Amended on April 17, 2018 (formulated in accordance with internal regulations and Article 3 of Announcement Rules and amended in the 3rd meeting in 2018 by the 6th Board of Directors)
Amended in the 9th meeting by the 6th Board of Directors on September 21, 2018.
Amended in the 3rd meeting by the 7th Board of Directors on June 19, 2020.
Amended in the 3rd meeting by the 7th Board of Directors on March 15, 2022.