SinoPac Holdings Co., Ltd.
Information Security Policy

■ Not formulated in accordance with external regulations
□ Formulated in accordance with external regulations

Formulating Unit: President's Office　　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, with its main objectives being:

Confidentiality: Ensure only authorized personnel can access information.

Integrity: Ensure the correctness and completeness of data and processing method.

Availability: Ensure authorized users are able to access information and relevant assets when needed.

Article 4. To effectively implement information security, an information security committee shall be set up, with its rules being set separately.

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.

Subparagraphs 3 to 9 of the preceding paragraph are to be handled in accordance with the Company's "Information Management Guidelines" and "Information Equipment and Resources User Guidelines."

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 are to be conducted by personnel delegated by the convener of the information security committee.
2. The departments in charge of the applications are responsible for security requirements discussion, usage management and security of the information and information systems.
3. Risk Management Division is in charge of the review and assessment of information security risk management.
4. Review and assessment of the legality of information security policies and management system are to be in charge of personnel designated by the convener of the information security committee.

Article 7. Information security training and promotion shall be based on the requirements of different job categories, such as management, business, and information, to build employees' information security awareness and information security management capabilities, raising the Company's information security standard.

Article 8. Information security incidents shall be handled in accordance with "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 decision and work schedule.

Article 9. The subsidiaries may base on actual management requirements, establish relevant regulations for information security based on the Policy, and submit to the information security committee for future reference.

Article 10. 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.

Article 11. 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.