SinoPac Holdings Co., Ltd.
Information Security Management Guidelines

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

Formulating Unit: Information Division　　Approval Level: President

Article 1. Purpose

To strengthen the overall information operations of the Company and its subsidiaries, ensure the smooth operation of information security management, comply with relevant information security regulations, and establish a secure and reliable information security management system, the information security system and management mechanisms shall be continuously optimized and enhanced to ensure security in the face of constantly changing threats. Accordingly, these guidelines are hereby established.

Article 2. Scope of Application

1. The term "subsidiary" as referred to in the Guideline shall be determined in accordance with Article 4 of the Financial Holding Company Act.
2. The Guideline is applicable to the management of all employees, contract personnel, and vendors and its personnel of the Company and its subsidiaries.

Article 3. To ensure the implementation of the information security management system, the information security plan pertaining to the following is established in accordance with the "Information Security Policy":

1. Separation of powers and responsibilities in information security
   (1) Department in charge of information security shall plan, monitor and implement the operations of information security management.
   (2) Shall base on information security management requirements, set up information security unit or allocate appropriate manpower resources and equipment.
   (3) Separation of information security powers and responsibilities shall comply with the relevant laws and regulations of the Financial Supervisory Commission.

2. Information Security Training
   (1) To meet operational requirements or to raise employees' work capabilities, information security training shall take into consideration employees' roles and functions and cater to different job categories.
   (2) The content of information security training shall take into consideration information security related topics, such as information security management system implementation specification, information security laws and regulations, information operating procedures, information security incidents or cases, information security technologies,

and other relevant knowledge.

(3) Departments of the Company and its subsidiaries in charge of information security shall regularly conduct information security training and comply with the relevant laws and regulations of the "Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries."

3. Information System Security Management

(1) Relevant control process shall be established for all operating system environment configuration, database management, information resource control, version control management, and system architecture change management, etc., based on the system characteristics.

(2) To ensure the normal operation of information system or equipment, shall establish preventive and control measures against other malware such as computer virus, mining, etc.

(3) Shall obtain technical vulnerability information of the information system or that published by the equipment supplier, or regularly execute server vulnerability scan, to evaluate whether appropriate control measures shall be adopted to handle the risk faced.

(4) Shall evaluate information security and carefully assess the vendors before handling any information operations. Vendors' information security responsibilities and confidentiality regulations shall be clearly specified and included in the contract requirements for the vendors to comply with.

(5) Shall consider ensuring the availability, integrity, confidentiality, source identification, non-repeatability, and non-reputability of audit trail information, with inspections being conducted and relevant records being retained.

(6) Usage of cloud service shall comply with the relevant laws and regulations or operational specifications, such as "Operational Standards on the use of Emerging Technologies by Financial Institutions."

4. Network security management

(1) During network planning or adjustment, the Company shall take into consideration whether the network architecture meets the operational needs and information security.

(2) Addition of equipment due to business or operational requirements shall abide by the purpose of usage of the network segment, and no unauthorized mixing or linking of equipment is allowed. For important network segments, appropriate protection and monitoring mechanism shall be applied, including the installation of firewall and intrusion detection system, regular inspection of the audit record, etc. The audit records shall not be added, deleted, or amended.

(3) The terms of use of email shall be clearly stated. Documents containing customer particulars or involving confidential business information that needs to be sent to external parties through email or other electronic means shall be protected with security

technologies such as encryption or electronic signature.

(4) Information system management for external website i. Shall use appropriate and effective encryption technologies based on the importance of data and system to ensure data confidentiality, authentication, and integrity. ii. Prevent data and system from intrusion, damage, tampering, deletion, and unauthorized access. iii. Addition, change, and deletion of information published on the external website have to be officially authorized to ensure the confidentiality and integrity of the published information. iv. Security protection measures for the website containing personal data and files shall be enhanced to prevent personal data from theft or improper or illegal use.

(5) Shall build a firewall and other necessary security facilities to enhance network security management, to ensure the security of data transmission and data access through the network.

(6) All employees shall not connect the external network to the internal network without permission, and necessary security facilities shall be set up to protect the internal and external network.

(7) When using a public network to transmit confidential level information, data shall be encrypted to ensure the integrity and confidentiality of the data during transmission over the public network, as well as ensure the security of the system connected to prevent unauthorized access.

(8) Control shall be enhanced on users or vendors who access the internal network 3 through remote login. Special security control mechanism such as logging in with account and password or other certification mechanisms shall be adopted.

(9) To ensure data integrity and protection, a commitment is made to continuously strengthen information security-related internal control mechanisms and to prevent unauthorized access, alteration, or destruction.

(10) Network security risks shall be continuously monitored, incidents shall be responded to in a timely manner, and mitigation strategies shall be implemented to ensure information security. In the event of major contingencies or emergencies, each unit shall immediately act in accordance with the “Guidelines for Emergency Incident Response.” If an incident is determined to be an information and communication security event, it shall be handled in accordance with the Company’s “Information Security Policy.” In this case, The Information Security Division shall assess the scope of impact, formulate a response plan, and report to the convener of the Information Security Committee for necessary decision-making and task coordination. If an incident is determined to be a personal data security event, the convener and executive secretary of the Personal Data Protection Management Task Force shall be notified immediately upon discovery of the incident, and a report shall be completed within two days, including the cause of the incident, response measures, methods for controlling damage to the data subjects, notification mechanisms, and notification content. Such incidents shall be handled in accordance with the Company’s “Personal Data Protection Policy and File Security Maintenance

Procedures," and, for material information as defined by the Taiwan Stock Exchange regulations, in accordance with the Company's "Material Information Announcement Guidelines."

5. Application system access management
   (1) Application for access shall be raised based on job duties, which will be used as the basis of the authorization. Access to network, system, and service is only granted to users for which they have been specifically authorized to use, to prevent unauthorized access.
   (2) Personnel granted the highest permission of system administration and designated personnel handling important technologies and operational control, shall be carefully assessed.
   (3) If the special permission account has information equipment management permission, special information access permission, other system resource control permission, and access to the audit trail, its usage shall be restricted to the items it is authorized to, and appropriate audit trail has to be retained.
   (4) When a user leaves or is transferred, shall ensure that all of his or her task permission have been canceled or changed.
   (5) To enhance user control, besides restricted by system characteristics, all user accounts are required to enter the password for user identification and authentication.
   (6) Shall establish password management such as password policy and changing cycle.
   (7) To ensure effective control on data access and information service, shall regularly review the permissions of the authorized accounts.

6. Application system development and maintenance management
   (1) The self-developed or outsourced system shall during the planning and analysis stage, taking information security into consideration. Security control shall be applied on system maintenance, update, implementation, and version change to prevent improper software, backdoor, computer virus, and malware from threatening the system security.
   (2) During programming stage, common vulnerabilities such as OWASP shall be included into security consideration to prevent similar vulnerabilities from occurring, and security inspection on the program codes shall be conducted to reduce security loophole in the program.
   (3) Application source codes shall be properly managed.
   (4) Shall specify and restrict the scope of system and data which the vendor can access.
   (5) Proper testing shall be carried out before launching the application after development, maintenance, or the purchasing of the software. Real data shall not be used in system development and testing. If real data is required for testing, control measures shall be assessed to protect the confidentiality of the data.
   (6) When using a key as the security protection mechanism in developing an information

system for external service, the Company shall take into consideration the management and protection of the key.

(7) E-commerce service shall comply with the regulations of the competent authority, and application developer shall adopt relevant protective measures after taking into consideration the transactions' characteristics and requirements.

(8) Relevant application development for mobile device programs provided for customers shall comply with the operating standards published by the Financial Supervisory Commission or the association, such as "Operational Standards 4 for Mobile Device Applications provided by Financial Institutions," etc.

(9) Application development and maintenance management shall comply with the relevant laws and regulations or operational standards.

7. Computer asset management

(1) Appropriate protection shall be implemented for each equipment to prevent damage which will affect the continued operation of the business.

(2) Shall adopt mobile device security measures to manage the risk of using a mobile device.

(3) Regularly execute necessary data and software backup and recovery operation so as to enable quick reversion to normal operation in times of disaster or storage medium failure. (4) Personal data file shall be regularly reviewed to determine the need for its existence and be regularly deleted. When transferring or replacing information equipment, ensure that personal data files not required for business needs, confidential data and authorized software have been deleted.

(5) Outsourced computer equipment, information gathered from media, and outsourced data processing shall be outsourced to organizations with sufficient security management capability and experience.

(6) Shall conduct regular checks on the software installed in the computers to ensure the compliance on regulations regarding intellectual property.3

8. System environment security management

(1) Servers and network equipment shall be placed within control zones with access control, air-conditioning, and stable power supply, and are fireproof, and earthquake and flood resistant, to prevent illegal access or sabotage.

(2) For unattended information equipment, shall consider using video surveillance or other remote monitoring equipment for control.

9. Information system disaster recovery management

(1) Information system disaster recovery plan shall be established to evaluate the impact of man-made and natural disasters on normal business operation; regular drills shall be conducted and the plan shall be regularly updated.

(2) Information security event emergency handling mechanism shall be established. Information security incident shall be handled in accordance with “Outline of Emergency Response” and reported in accordance with the relevant procedures of internal and external regulations immediately.

10. Other information security management matters
    (1) Shall ensure that all internal information operations outsourced to third parties comply with the requirements of information security.
    (2) Comply with relevant internal and external laws and regulations, and establish corresponding control procedures.
    (3) All employees shall comply with information security-related regulations, and any information security responsibilities shall be handled in accordance with disciplinary procedures.
    (4) A supply chain risk management mechanism shall be established to ensure consistent information security risk management for outsourced information and communication systems.

Article 4. Matters not mentioned in the Guideline shall be handled in accordance with the relevant laws and regulations of the competent authority and the Company’s relevant regulations.

Article 5. This Guideline is effective upon approval by the President, the same applies in the event of amendments.

Approved by the President on December 17, 2018
Amended on July 23, 2020 (formulated in accordance with internal regulations and Article 3 of Announcement Rules and amended in the 3rd meeting in 2020 by the 7th Board of Directors)
Approved for the amendment by the President on July 25, 2025