(Translation)

Information Technology Security Policy
Saha Pathana Inter-Holding Public Company Limited
(2nd Revised Edition)

The Company has recognized the significance of information and communication technology which is the key factor in supporting and promoting the Company business operations. Therefore, to ensure that Company personnel are aware of their duties and practices pertaining to information technology, as well as to control and prevent problems which may arise as a consequence of improper use of information technology and potential threats, being within the collective responsibility of the Board of Directors, Executives, Company employees and all relevant personnel, the following guidelines are provided in writing:

1. Information technology risk assessments and procedures in response to any potential security infringements are prepared.
2. Manage information technology resources in accordance with the Company's strategic plans also by covering human resource management and information technology systems that are sufficient for information technology operations.
3. Regular monitor and review are implemented to minimize risks of damage, irregularities or inoperability of the information technology system. In addition, procedures for improvements, changes and alterations of the information technology system are prescribed.
4. Access control and use of information technology system of executives, employees or relevant persons are carried out to ensure appropriateness and prevent unauthorised access to the Company information which could lead to risks pertaining to information and processing of the information technology system.
5. Restricted access of computer control room and to prevented physical damage from unauthorised persons, which could lead to damage to information stored in the computer systems.
6. Communication of the term of use of information technology system to executives, employees and relevant personnel to ensure a proper and appropriate use.
7. Implement data encryption measures in accordance with relevant agreements, laws, and regulations to ensure appropriate and effective encryption, preventing the leakage of confidential information, forgery, and ensuring the integrity of information within the Company's information technology and communication systems.
8. Determine the practice of sequencing information technology tasks and dealing with problems from information technology systems to reduce the impact on the work processes. Able to fix the issue to be able to return to normal as soon as possible through proper backup and information system recovery which will prevent permanent loss caused by any emergencies or disaster events.
9. Set requirements to review the information technology system security policy at least 1 time a year or whenever there are material significant changes.
10. Every agency has a responsibility to make an announcement and publish these policies including supporting and responding to the Company's policies.
11. Control the use of information technology systems to be in accordance with the Computer-related Crime Act and to comply with the laws and regulations related to information technology systems.

This Information Technology Security Policy (2nd Revised Edition) has been approved by the Board of Directors Meeting No. 3 (Board #31) on August 14, 2024 and effective from August 15, 2024 onwards by cancelling the policy of Information Technology Security 1st Revised Edition) which came into effect on December 17, 2021 and approved by the Board of Directors Meeting No. 9 (Board #28) on December 16, 2021.

Mr. Somkid Jatusripitak
(Mr. Somkid Jatusripitak)
Chairman of the Board of Directors