

Announcement No. 009/2024

Information Security Management System Policy

(Revised Version)

Ichitan Group Public Company Limited (the “Company”) would like to apprise that in accordance with the resolution of the Executive Board Meeting No. 4/2024 on April 17, 2024, the Board of Directors have considered and approved the Information Security Management System Policy (revised version). The Company is committed to protecting information assets related to the provision of technology and information systems in the host computer room (Server) from internal and external threats that may occur, whether intentionally or unintentionally, in order for the information security management to be in line with the revised international standards as follows:

“Ichitan Group Public Company Limited is committed to information security management to ensure that the data center’s technology and information systems are stable, secure, safe and in accordance with ISO/IEC 27001 standards, as well as to continuously develop them.”

To achieve the Company’s policies as follows:

1. Establish information security management system policies and provide support in terms of policies, budgets, resources, and other matters necessary to enable the information security management system to be continuously developed and improved.
2. Appoint an information security management system executive and an information security management system team to be responsible for driving and maintaining the information security management system.
3. Information security management system policy must ensure the following:
 - 3.1 Information and communication technology security policies, procedures and practices must be defined and strictly implemented.
 - 3.2 The information security management system is integrated into the organization's procedures and practices.
 - 3.3 Information assets must be maintained in terms of confidentiality, integrity and availability.
 - 3.4 Information assets must be protected from unauthorized access.
 - 3.5 Compliance with orders, regulations, rules, laws and agreements affecting security.
 - 3.6 Events that affect information security must be recorded, monitored, managed and reported.
 - 3.7 Business continuity plans must be developed, updated and tested.
 - 3.8 Information security management systems must be continuously reviewed, evaluated and improved to suit changing circumstances.

In this regard, Announcement No. 022/2021 is hereby cancelled and this announcement is replaced to be served instead.

For your acknowledgment.

Announced on April 17, 2024



(Tan Passakornnatee)
Chief Executive Officer