

Information Security Policy

Information security is a critical aspect in supporting the Company's business operation to achieve efficiency and reliability, as well as to foster trust. Therefore, the Company is dedicated to developing an information security system based on the fundamental principles of Confidentiality, Integrity, and Availability (CIA). This is aimed at ensuring that.

1. Access to the system data or information storage locations is restricted to authorized individuals only.
2. Adequate encryption controls are in place to uphold the confidentiality of critical information.
3. Physical security and environmental safeguards are implemented to ensure the constant readiness and security of the information system for use.
4. The information system ensures accuracy and reliability.
5. Regular audit, monitoring, and evaluation of information security measures are conducted.
6. A comprehensive process has been established for managing information security incidents, which includes developing plans, conducting drills, and continuously improving efforts to ensure preparedness for emergencies.
7. Employees are encouraged to have knowledge, suitable abilities and have awareness about related information security.

Furthermore, Information security is a collective responsibility. Therefore, both employees and external parties granted access to the Company's information system are obligated to exert every effort to uphold the Company's information security standards.