Information Security Management Policy:

All employees of the company are required to strictly adhere to the requirements of the ISO/IEC 27001 standard to establish, implement, maintain, and improve the company's information security management system. This includes continuously enhancing information security awareness, standardizing the management of information lifecycle processes, persistently identifying and controlling information security risks, and ensuring the security of all company information. The company will continually increase investment in information equipment and enhance information technology levels to provide efficient, convenient, and secure services for business operations, ensuring the continuous and reliable operation of overall business systems.

Information Security Objectives:

a. Zero incidents of leakage of important information pertaining to the company and its clients;
b. Zero complaints from clients regarding information security;
c. No major information security incidents occurring throughout the year;
d. 100% coverage of annual information security training personnel;
e. Data collection, provision, statistics, and analysis.

The number of information leakage incidents will be reported by each department to the leader of the information security working group, who will compile the statistics; the system and key network equipment downtime rates will be collected and compiled by the network management team of the Product Technology Center.

For any unmet information security objectives, the relevant departments must conduct a root cause analysis and propose solutions. For objectives that are continuously unmet, the information security working group will issue a "Corrective and Preventive Action Tracking Record" to the relevant departments for further action.

CEO:

Date: September 21, 2022