

Cybersecurity Policy

Sabina Public Company Limited and its subsidiaries.

Sabina Public Company Limited effectively manages cybersecurity and cyber risk in alignment with internationally recognized best practices, a Cybersecurity Policy has been established with the following key points.

1. Develop and maintain a framework or cybersecurity practices that align with international standards. Monitor laws and regulations related to cybersecurity at least once a year and ensure compliance accordingly.
2. Implement cybersecurity risk management by assessing threats, vulnerabilities, likelihoods, and impacts on the business. Ensure risk management aligns with enterprise-level risk management practices. The scope of cybersecurity risk management should encompass all organizational assets and personnel, as well as related external entities.
3. Communicate and conduct training on cybersecurity threats (Cybersecurity Awareness) to enhance employees' awareness, responsibility, and understanding of how to address cyber threats, at least once a year.
4. Implement cybersecurity protection and intrusion detection systems to cover the company's information systems. Ensure ongoing monitoring, and require the department responsible for cybersecurity to report cyber threat information to the management at least once per quarter or immediately when a cyber threat occurs.



(Miss Duangdao Mahanavanont)

Chief Executive Officer