Cyber Security Policy

Wyncoast Industrial Park Public Company Limited and subsidiary

Cyber Security Policy

Wyncoast Industrial Park Public Company Limited

Wyncoast Industrial Park Public Company Limited and Subsidiary company can manage their operations efficiently with the information technology system. The company therefore gives importance and is aware of the security risk management of cyber threats. The company has established a cyber security policy to manage risks that may occur effectively.

Risk oversight cyber threats

1. The company defines the roles, duties and responsibilities of information officers in risk oversight cyber threats. The company has security standards that can be identified, prevented, detected, dealt with, and able to recover to return to normal and supporting the company to have adequate and appropriate capabilities with the volume and complexity of the company's work systems.

2. The company has designated responsible persons to be responsible for monitoring, preventing, and dealing with cyber threats and report cyber threat risk information to the Board of Directors. Audit and Risk Management Committees have been informed that the company may consider appointing specific officers to be responsible for responding to and dealing with abnormal cyber incidents in a timely manner to reduce the impact that occurs.

3. The company will provide knowledge about potential cyber threats that employees will have a better understanding and awareness of the need for security and understand the consequences that will occur as a result. If an incident occurs, including communicating guidelines for prevention and response to cyber threat incidents

4. The company has clearly established contact channels for coordination between internal and external departments in order to determine guidelines for dealing with and resolving safety incidents effectively.

Cyber Security Risk Management

The Company has an information technology system that covers cyber threat risk identification, prevention, detection, response, and recovery, as well as reviews and updates cyber threat information to keep up with changes that occur as follows:

1. The Company assigns information staff to identify which information assets are at risk of cyber-attack and must be secured in order to manage the risk of cyber threats affecting the system, assets, and company information appropriately.

2. The Company has appropriate preventive measures to limit the impact of cyber threat incidents, which includes training and awareness raising for employees and those involved in information security and various security measures. In addition, the company will regularly maintain equipment and software related to electronic systems in order to support continuous operations.

3. The company provides notification of abnormalities related to cyber threats that occur both internally and externally in order to prevent risks and impacts that will occur in the future.

4. The company has a plan to deal with cyber threat incidents and solutions in the case that damage from cyber threats causes operations to be disrupted. The company will analyze the cause and detect evidence of threats that have occurred. Including a communication process with customers and stakeholders for a correct understanding of the company's situation.

5. The company restores the system to return to normal operations. Including reviewing and updating the plan to keep up with the situation and taking lessons learned from the threat incident as part of reviewing the plan and system recovery process to be more effective in order to prevent problems and Impacts that will be repeated in the future.

Announced on 29 February B.E. 2024

Mr. Jak Chamikorn
Chairman of the Board
Wyncoast Industrial Park Public Company Limited

This Cyber Security Policy
was approved by the Nominating of Committees Meeting No. 2/2024 on February 29, 2024.
was approved by the Board of Directors Meeting No. 2/2024 on February 29, 2024