(Translation)

Cyber and Information Security Policies

The Board of Directors of I.C.C. International Public Company Limited recognizes the importance of the cyber and information security which is an important factor in supporting the Company's business operations; therefore, the efficient cyber and information security management is stipulated in compliance with the Computer-related Crime Act B.E. 2560, and Personal Data Protection Act B.E. 2562, including other relevant laws and international practices.

To make the personnel of the Company aware of their duties and practices related to the information technology systems which are the shared responsibilities of the board of directors, management, employees and all involved parties; the following practice guidelines are established:

1. Assign the management direction and support on cyber security in compliance with the laws, rules and regulations; disseminate information to people involved both inside and outside the Company; and conduct a regular review.
2. Establish a company structure for managing cyber and information security in all processes and projects of the Company by assigning duties and responsibilities, contact channels of personnel as well as departments both inside and outside the Company to exercise the right to supervise remote working and mobile device.
3. Have a background check and describe the duties and responsibilities in the contract for the employees and contractual parties prior to the employment. Raise awareness of cyber threats and disciplinary action in case of a failure or violation during the employment. Upon the termination of employment, the Company shall have to revoke access to applications; however, the employees and contractual parties shall continue to have duties and responsibilities for cyber and information security as stated by the Company.
4. Classify asset and information resources. Make labels according to the legal requirements, usefulness, value, worth, or importance. Create an asset list that classifies the assets, persons in charge and users; and conduct a regular review in order to manage and handle the storage media in an appropriate manner such as reclaiming assets upon termination of employment or contract, and method of destruction suitable for degree of data protection when no longer in use.

Certified Correct Translation

(Banyat Vongklednak)
Licensed Qualified Lawyer LL.B.
World Translation Center
Tel. 08 1929 2144, 08 1556 6441

5. Create a user registration, supervise users as well as people with privileged access rights to some information and network services and conduct a regular review. System administrators and developers are responsible for maintaining confidentiality and controlling access to information systems. The users are responsible for maintaining confidential information for authentication.
6. Have data encrypted by taking consideration of the degree of protection according to the specified policy and timeframe, and create a list of active and encrypted accounts.
7. Establish procedures for controlling entry-exit area for the controlled area, office and others, in order to prevent damages, espionage and hazard which may interfere with the operation of the Company; develop, install, prevent and maintain information systems in good working condition.
8. Establish procedures for predicting the resources required by the systems, separating program development from service implementation, protecting from malware, backing up data, recording event logs, managing technical vulnerabilities, checking systems, monitoring software installation controls on the service system, reviewing when there are important workflow changes or according to the period specified by the policy.
9. Separate networks according to user groups and information systems by identifying the security tools of each network group. Exchange of information requires a secure information exchange agreement and appropriate confidentiality or non-disclosure agreement according to the degree of protection requirements.
10. Define cyber security as part of system requirements. Establish safe procedures for custom system development. Purchase, procurement, or use of public networks shall cover procurement, development, acceptance and maintenance processes.
11. Establish a cyber and information security agreement with partners involved in the supply chain of services and products by taking consideration of the access requirements, operation, storage and communication or provision of information infrastructure components. Regularly monitor, inspect, review and assess the risks of the partners' services.

Certified Correct Translation

(Banyat Vongkllednak)
Licensed Qualified Lawyer LL.B.
World Translation Center
Tel. 08 1929 2144, 08 1556 6441

12. Determine the duties and procedures for cyber and information security personnel including relevant management, users, system administrators, system developers, contractual parties and people who shall record and report any cyber and information security vulnerabilities in their systems or services and report an incident immediately. Study, analyze and use the acquired knowledge to prevent future events after the incident. Identify, collect, obtain and store information assets that can be used as evidence.
13. Establish cyber security response requirements and management plan to create business continuity. Prepare documents, work processes and work systems including emergency backup system in order to control damages within the specified extent in a crisis or disaster situation. Upgrade and test operations regularly.
14. Specify conditions, rules, regulations, standards, laws, and technical requirements for protecting data, especially about an individual, from loss, destruction, falsification, unauthorized access and disclosure in the written procedures for the related information systems which shall always be updated to encompass the requirements of the law.

The cyber and information security policies have been approved at the Board of Directors' Meeting No. 10, on 13th January, 2023, and shall become effective from 15th February, 2023.

(Mr. Thamarat Chokwatana)
Chairman

Certified Correct Translation

(Banyat Vongklednak)
Licensed Qualified Lawyer LL.B.
World Translation Center
Tel. 08 1929 2144, 08 1556 6441