IRPC Public Company Limited
Announcement No. 028/2562

Cyber Security Policy

The Company places great importance on cyber security to prevent potential threats from cybercrime, unauthorized access, theft, and data breaches that may cause damage or disruption to the Company's computer systems, internet networks, computer data communication, and computer systems. The Company emphasizes the protection, monitoring, and control of risks by establishing appropriate tools, policies, and security measures (Security Concepts, Security Safeguards, and Security Tools Technologies) to prevent cyber incidents that may impact the Company's operations. The objective is to ensure the confidentiality, integrity, and availability of information and systems.

The Company assigns relevant departments to establish strategies, missions, policies, and work plans to serve as guidelines for implementing cyber security. This includes risk assessments, security plan preparation, system recovery measures, and ongoing system maintenance to ensure that the Company can manage cyber security risks effectively. The Cyber Security Policy is outlined as follows:

1. Departments responsible for cyber security must establish strategies, missions, policies, and work plans as guidelines for implementing cyber security, including risk assessments, planning, and reporting cyber security risks to the management regularly.

2. Develop and maintain operational manuals and practices that meet organizational cyber security standards.

3. Manage and control risks of computer systems and networks by assessing threats and implementing appropriate security measures.

4. Review cyber security measures periodically and continuously to ensure their effectiveness, and recommend improvements or updates to enhance security protection.

5. Establish backup systems and data recovery plans to ensure continuity of operations when cyber incidents occur, and ensure that information and systems can be recovered quickly and accurately.

6. Ensure that all employees, contractors, and related parties understand and comply with the Company's cyber security policies, practices, and measures to prevent incidents or

minimize damage from cyber threats.

7. Monitor and assess emerging cyber threats regularly, and provide training and awareness to all employees to strengthen their knowledge and readiness to respond to cyber incidents effectively.

8. Executives, employees, contractors, and outsourced personnel must comply with this policy, relevant regulations, royal decrees, and cyber security-related laws as prescribed by the government.

This announcement is made for acknowledgement and compliance by all concerned.

Announced on 30 December 2019

(Signed)
(Mr. Pongpol Pinsupa)
Chairman of the Executive Board