The Announcement of Board of Directors,
Ratch Pathana Energy Public Company Limited
No. 10/2024
Cyber Security Policy
.....

To ensure the information system of Ratch Pathana Energy Public Limited Company ("the Company") are secure and continually supportive to the Company's operations, and measures are in place to prevent potential problems arising from various threats and non-compliance of Information Technology system usage which may cause any damage to the overall company, and to prevent violations of relevant laws and regulations. The Board of Directors' meeting of the Company No. 5/2024, held on June 26, 2024, resolved to establish a Personal Data Protection Policy for the Company and subsidiaries, and to revoke the announcement of Cyber Security Policy on June 20, 2022, The policy details are mentioned as follows.

No. 1 in the announcement

"Users" means employees, full-time employees, temporary employees who work on the Company's information system, external users and organizations authorized to access the Company's information system.

"User Permission" means general rights, specific rights, privileges and other rights to access the Company's information system and property.

"Property" means data, hardware, software, and other assets applied for information system operation.

"Identity Management and Access Control" means the permission, determination of access rights or the access of computer device, network system, and information system, both logical and physical.

"Cyber Security" means confidentiality, integrity, and availability of the Company's Information system, along with the authenticity, accountability, non-repudiation and reliability.

"Cyber Security incident" means incidents that involve with the Company's network and information system, or be suspected to be vulnerable or potentially damaging, which may interrupt the process or procedure of the Company's network and information system. The mentioned incidents may demonstrate that the Cyber Security policy has been breached, or preventive measures have failed; or an event that could not be identified to have concerned the security.

"Undesirable or unexpected Cyber security incident" means defective or breached situation of the security which may cause unconscious information system processes, along with losing some or all services which indicate that the security has been attacked or breached.

"Computer devices" means any device or computer device sets, which have been set instructions, sets of instructions or any other directives, and the working principles to enable the duty of processing data automatically.

"Information system" means data of the Company that utilize the technology of the computer and network system to create the Company information, and then use the information for planning, managing, developing, controlling, supporting company's operations and device usage policies or guidelines.

"Administrator" means officers who designated by Information Technology Division Manager to administrate, manage, and maintain the Company's properties, network and information system.

"External organizations" means external organizations authorized to access the Company's data or assets under their authority and responsibility for the confidentiality.

No. 2 The Cyber Security guideline has been established to regulate access and usage of the computer device, network operation system, and information system. Users who work on the company's information system must be authenticated to access the system, be approved strictly following the instructions, and be limited their access to the system in accordance with their roles and responsibilities to raise the reliability and prevent damage from any misbehavior, in compliance with the Cyber Security guidelines.

No. 3 Administrator must provide access control of the company's information system by always requiring authentication whenever the users access the system and considering the user's access as necessary. The administrator is responsible for carrying out each step of the procedure, including determining the registration method, managing passwords, controlling access to the information system securely, and establishing regulations regarding access permission to the information system, data types, priority, and access rights revision.

No. 4 Administrator is responsible for managing company computer devices, computer access, and computer usage, along with maintaining unused computer devices, managing the procedure of media and electronic data destruction, determining the procedure of server room access control, and managing network access. Different network access control processes are established to prevent unauthorized users from accessing the network and damaging the information technology system and data, to avoid network intrusions and system disruption, and to identify the access users.

No. 5 Administrator must have Information Security Awareness and must comply with Cyber Security guidelines strictly. Authentication is required every time before using any assets or accessing the company's information system, and the administrator must understand the access rights of their own position in accordance with their role and responsibility.

No. 6 Preparing a manual of backup plan and Information Technology Contingency Plan to enable the proper system backup and restoration within a specific period as well as developing a plan to solve problems from uncertainties and disasters that may occur with the

system, and constantly updating the system to keep operating continuously in accordance with the Cyber Security guidelines.

No. 7 The manuals about the Cyber Security and risk assessment should be constantly reviewed at least once a year, to prevent and decrease the risk level which may occur with the information system in accordance with the Cyber Security guidelines.

No. 8 Information Technology Division Manager is responsible for maintaining and managing information systems, network, and IT Asset as well as assigning the administrator to do so in accordance with the policy.

No. 9 Cyber Security policy and guideline have been reviewed and improved regularly at least once a year or in the case of changes that affect the security.

No. 10 In the case of the computer system or information receive any damage or harm in any way, whether to the company or any individual, due to negligence, omission, or violation of the policy and guideline for cyber security, the Information Technology Division Manager shall be responsible for the associated risks, damages, or harm.

Announced on 26 June 2024

Sujarit Patchimnan
(Mr. Sujarit Patchimnan)
Chairman