Circular No. 112/2025

Cyber Security Policy

In order for the information systems of Thai Oil Public Company Limited (the "Company") and its subsidiaries whose shares are both directly and indirectly held more than 50% of shares ("Thaioil and Subsidiaries"), to prevent threats and provide efficient risk management on cyber security and to be in line with the Cyber Security Framework and international-standard practices, the Company deems it appropriate to adopt the Cyber Security Policy (the "Policy") All executives, staff, and contractors shall comply with this policy with the summarized essence as follows:

1. Responsible for cyber security and shall regularly report to executives and directors any relevant information.

2. Improve and keep the Cyber Security Framework or practices in line with international standards, with continuous improvement to effectively prevent threats to information systems.

3. Establish, oversee, and define security requirement practices for information systems for third parties (e.g., suppliers) to follow.

4. Determine control measures and risk management regarding cyber security covering information systems that are vulnerable to cyber threats.

5. Set up and operate Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) to cover all information systems. Ensure continuous monitoring, regular reporting of security events, and timely response to information system security threats.

6. Ensure the integrity and protection of data to prevent unauthorized access, modification, or deletion.

7. Ensure a test run of security system for information systems as well as information infrastructure and applications before the launch of actual service.

Upon this Policy, the Circular No. 92/2563 on Cyber Security Policy, dated July 15, 2020, is hereby cancelled.

8. Vulnerability Assessment or Penetration Testing must be executed at least on an annual basis, covering information infrastructure and applications that are vulnerable to cyber threats.

9. Communicate and provide trainings on potential cyber threats on a regular basis to create Cyber Security Awareness and understanding in dealing with cyber threats.

10. All departments shall establish a sense of responsibility and awareness of cyber security on a regular basis. Roles and responsibilities for information system security are defined at the individual level and cover the entire organization.

This Policy is enforced on all departments and units throughout Thaioil and subsidiaries. All executives, staffs, and contractors are to understand and comply with this Policy. executives at all levels shall be role models, supporting the determining implementation of the Policy.

(Mr. Bandhit Thamprajamchit)

Chief Executive Officer and President

1st July 2025

Upon this Policy, the Circular No. 92/2563 on Cyber Security Policy, dated July 15, 2020, is hereby cancelled.