Information Technology Security Statement

In order to ensure the information technology systems of PTT Global Chemical Public Company Limited (GC) and its affiliates are secure, operate efficiently, and align with the Information Security Management System Standard (ISO/IEC 27001) or other internationally recognized frameworks, the company has established guidelines to raise awareness and implement preventive measures against potential threats and improper use of information systems. These efforts also aim to ensure compliance with relevant laws, including: The Computer Crime Act B.E. 2550 (2007), The Cybersecurity Act B.E. 2562 (2019), The Personal Data Protection Act B.E. 2562 (2019), and other applicable regulations related to the Chief Executive Officer's responsibilities.

1. Assign the Cyber Security Department to annually propose reviews or revisions of this policy and its related practices. It should also develop and maintain the framework and guidelines for information security management in alignment with international standards. In addition, the department must monitor relevant laws and regulations at least once a year and ensure full compliance. The department is also responsible for managing cybersecurity to prevent threats originating from business processes and production activities across all plant sites.
2. Establish guidelines for the use of information technology services that align with user requirements and international standards, aiming to prevent cyberattacks and manage cybersecurity risks in accordance with Enterprise Risk Management. The scope of cybersecurity risk management practices shall cover all assets and human resources, as well as relevant third parties.
3. Implement cybersecurity prevention and intrusion detection systems that comprehensively cover the company’s information systems, including access control, data exchange, backup, and secure data destruction. The cybersecurity responsible unit shall continuously monitor for threats and report cybersecurity threat information to the executive management at least once per quarter.
4. Establish a cybersecurity incident response plan to ensure prompt and effective management of security incidents. This includes monitoring incidents, developing incident recovery plans to reduce business disruptions, as well as arranging rehearsals to assess its accuracy and effectiveness.
5. Promote cybersecurity awareness and provide training through effective communication and education on cyber threats. Employees shall be made aware of their roles and responsibilities, understand how to respond

to cyber threats, and be able to apply the knowledge effectively. All employees are accountable for the security of information within their responsibilities and must stay vigilant against behaviors or activities that may pose cybersecurity risks.

In addition, GC established and announced the Information Technology Security Policy, endorsed by Chief Executive Officer (CEO) and this policy applies to all GC businesses and operations across the supply chains. GC promotes the adoption of Information Technology Security policy by suppliers, contractors, and other key business partners (e.g. non-managed operations, joint venture partners, licensees, outsourcing partners). All managements shall be good role models and are accountable for policy alignment. All workforces shall understand and continually comply with the policy throughout their activities.