INFORMATION TECHNOLOGY POLICY
SIAM STEEL INTERNATIONAL COMPANY LIMITED

To ensure that all information technology activities and operations across Siam Steel International Public Company Limited and its subsidiaries remain secure and reliable, the Company's information and IT assets must be systematically and appropriately safeguarded. This framework carefully accounts for potential cybersecurity threats and mandates the use of information systems that uphold confidentiality, integrity, and availability, in strict compliance with applicable information security rules, regulations, and legal frameworks. Consequently, the Company hereby establishes the Information Technology Policy as follows:

Information Technology Policy

The Company shall:

- **Conduct business under the principles of good corporate governance**, ensuring that all information technology operations comply with applicable IT laws and regulations.
- **Establish and maintain a standardized Information Security Management System (ISMS)** in alignment with recognized international frameworks.
- **Enforce appropriate access controls for data and systems to maintain robust security standards**, while developing proactive plans and measures to prevent and mitigate cybersecurity impacts based on comprehensive risk assessments.
- **Promote IT literacy and regulatory awareness among executives and employees** to ensure correct system utilization and compliance with information technology policies.
- **Perform regular audits and continuous monitoring** of all information technology system utilization.

Guidelines

1. IT Audit and Risk Assessment

The designated department responsible for information systems shall conduct information technology risk assessments and implement controls to maintain risks within the Company's acceptable risk appetite. This is to ensure that the Company's information technology risk management is executed and managed appropriately.

2. Information Asset Security

The designated department responsible for information systems shall define security standards to regulate and control access to, as well as the usage of, the Company's information systems. These controls must align with the specific data classification, criticality, and confidentiality levels, alongside user access clearances, and permissible access times and channels. Additionally, robust network intrusion prevention measures must be established to safeguard against unauthorized access and malicious software (malware) that could compromise or damage the Company's data, as specified below:

2.1 Information Asset Classification

Guidelines shall be established for categorizing information assets and defining confidentiality classifications, ensuring full compliance with relevant laws and regulatory requirements applicable to the Company.

2.2 Backup Systems and Emergency Contingency Planning

Appropriate backup information systems shall be established and maintained in a constant state of operational readiness. Comprehensive emergency contingency plans must be formulated to ensure the uninterrupted and normal utilization of information in the event of electronic operation failures. Additionally, the roles and responsibilities of personnel managing these information systems must be explicitly defined. Both the backup systems and the emergency contingency plans shall be subject to routine readiness testing to ensure their ongoing effectiveness.

2.3 Cryptographic and Encryption Controls

The Company shall establish data encryption guidelines tailored to the potential risks associated with each defined confidentiality classification. Additionally, continuous monitoring shall be enforced to ensure strict adherence and ongoing compliance with the aforementioned policies and procedures.

2.4 Personnel Supervision and Oversight

The designated department responsible for information systems shall execute the following actions:

(A) User Access and Activity Controls

- Users shall be required to undergo password authentication to access computers or information technology systems, and must log out of the systems immediately upon completing their tasks. Furthermore, computers and critical devices must be screen-locked when left unattended or remaining idle for an appropriately designated period of inactivity.
- Security control measures for portable and mobile communication devices shall be established, evaluating the inherent risks of connecting such devices to the Company's internal network. Furthermore, regulatory measures must be defined to govern the off-site utilization and transport of these devices outside the Company's premises.
- **Software Installation Controls:** Standard operating procedures and control measures shall be established to restrict user-driven software installations and prevent the deployment of unauthorized software on operational systems. An authorized software master list approved for installation on the Company's computers must be formally documented in writing, continually updated, and effectively communicated to internal users to ensure strict awareness and compliance.
- **Acceptable Use Controls:** Personnel shall be strictly supervised to prevent the utilization of information, electronic data, or other digital assets in an inappropriate, unethical, or unauthorized manner that could compromise or cause damage to the Company's information systems and data.
- **Proprietary Technology and Intellectual Property:** All information technology systems developed internally within the Company shall be deemed the sole and exclusive property of

the Company. Users are strictly prohibited from replicating, modifying, adapting, or otherwise exploiting these systems for the personal gain of themselves or any third party without prior written authorization from the Company.

(B) Vendor and IT Outsourcing Management

- Comprehensive requirements and operational frameworks for third-party IT service providers shall be established and enforced to ensure operational efficiency and robust information security compliance.

2.5 Information and Data Transfer Controls

Regulatory controls shall be established to govern the exchange of information and data between internal departments, across group companies, and between the Company and external entities. These transfer mechanisms must comply with the following criteria:

(A) Electronic Messaging Controls

- Control procedures shall be established to govern electronic messaging communications, including electronic mail (e-mail). Critical electronic messages must be adequately safeguarded against unauthorized access, modification, or disruption by unauthorized individuals.

(B) Confidentiality and Non-Disclosure Requirements

- All personnel and external entities performing work for the Company shall be strictly required to execute formal confidentiality or non-disclosure agreements in writing.

2.6 Protection Against Information System Threats

Measures shall be established for the detection, prevention, and system recovery to safeguard assets from malicious software (malware). Concurrently, appropriate user security awareness programs must be implemented to ensure ongoing compliance and vigilance.

3. Compliance and Incident Reporting

The designated department responsible for information systems shall submit operational reports regarding adherence to this Information Technology Policy, specifically in the event of any incidents that could significantly impact compliance with the established policies, rules, and regulations. This includes scenarios where computer systems or information assets are damaged, compromised, or exposed to hazards due to negligence, omissions, or breaches of the Information Technology Policy, as well as any other rules and regulatory requirements prescribed by the Company.

Announced on October 10, 2024

(Surapol Kunanantakul)

President