Cybersecurity Policy

To ensure efficient administration compliance with the information technology policy, Cybersecurity Act B.E. 2562 (2020), Personal Data Protection Act B.E. 2562 (2020), Computer Crime Act B.E.2550 (2007), Electronic Transactions Act B.E. 2544 (2001), including other relevant laws, regulations, and rules, Mitr Phol Group has determined the Cybersecurity Policy for the Group as follows:

1. Objectives

Cybersecurity for the internal information technology system is a vital part to be considered, taking into account that there are many potential factors for threats where criminals could attack from any source. For instance, the vulnerabilities in connections between IT systems, the ability to seal and improve the complex IT system. Such a threat could negatively impact our business operation or the rights and freedom of data owners, including employees, customers, and related parties to whom Mitr Phol Group has processed their personal data. For this reason, compliance with this policy is a vital part of mitigating cyber threat risks.

This policy consists of IT assets protection, monitoring, and supervising the IT department regarding IT system management and data processing protection against cyber threats. The policy also covers our business units, which run their own IT system management and data processing without supervision from the IT Department, which requires strict compliance.

2. Definitions

Information System means a computer system, communication system, or system that contains data processing, retrieving, or transferring between systems, including programs, requirements, and procedures used in operation and system maintenance.

Cybersecurity means measures or an operation determined to prevent, manage, and mitigate cyber threats from internal and external scales.

Cyber Threat means any wrongful acts or operation using a computer or computer system or any program with malicious intention to cause harm to a computer system, computer data, or other related data.

Confidentiality means keeping or maintaining the computer network system, computer system, computer work system, information system, information, electronic data, or computer data by accessing, using, or disclosing without permission from an owner.

Preserving Integrity means any act conducted to maintain the completeness of information, electronic data, or computer data while using, processing, transferring, or storing to prevent any changes, loss, damage, or destruction without permission or in an illegal manner.

Preserving Availability means an act conducted to ensure the availability of IT assets or technology for access or usage at the time required.

Standard means the norms applied for actual practice to achieve the objectives or goals.

Procedures means the procedures determined for operation or in response to the situation required to achieve the work management objective and the policy implementation to initiate the enforcement. The mentioned procedure is effective unless written approval for an exception.

The Cybersecurity Management Framework means the framework established for managing and controlling cyber work by the National Institute of Standards and Technology (NIST), referring to version 1.1 (NIST Cybersecurity Framework v1.1).

Personal Data Management Framework means the framework established to manage and control personal data information by the National Institute of Standards and Technology (NIST), referring to version 1.0 (NIST Privacy Framework v1.0)

Control Measure means the risk management approach, which includes policy, operating procedures, operating guidelines, work procedures, or Company construction, whether under supervision, management technique, or law.

Risk Assessment means the procedures implemented to identify the severity and priority of risk factors based on the likelihood and potential impacts.

Authentication means data processing using a computer system to verify and confirm user identity by checking the user account code and password before allowing access to resources in the system, for instance, key card, password or PINS, fingerprint, etc.

Physical Security means the physical control of data access, which affects the continuity of working in the Company's computer system or valuable IT assets.

External Party Services means the service used or received from an external party, for instance, data storage service, data processing service, hardware and software distributors, business and security consultant, including other services that are not provided the services in the Company, i.e., internet and system network linked around the globe.

Information means the data in document format and facts contained in various forms, for instance, company data, IT system, network system, computer hardware, or corporate data storage, regardless of the formats, i.e., publication, microfiche, or online data, etc.

Data Controller means executives of business units who are responsible for data creation, usage, or data credibility.

Data Processor means executives of business units who are responsible for data processing. The data is under supervision and management by the data controller.

Data Subject means an owner of personal data, not the party processing the data or creating or collecting the data. The personal data owner is an individual and does not include a juristic person.

Information Asset means valuable items to the Company. Such an asset could be an IT asset related to information processing of the owner company, for instance, employment, development, or procurement for benefits of business operation or operation of the Company. Information assets are in several formats, as follows:

- Tangible Information Assets include computer hardware, communication devices, data record media, and other related equipment for information processing, etc.

- Intangible Information Asset
  - Information includes databases and files, contracts and agreements, system manuals, research data, user guidelines, training material files, work procedures, business continuity plans (BCP plans), Fallback Arrangements, documents or records for audit trails, and permanent data storage, etc.
  - Software Assets include application software, operating systems, and Software Development Tools, etc.

Encryption means encrypting data to prevent illegal access. Those who can open encrypted data files must have a decryption program to ensure data resumes normal use.

Remote Working means connecting to the company network using a device connected out of the Company's network.

Vulnerability means the weakness of information security, which can be exploited and cause damage to information systems, data, and personal data, including the Company's business operations.

3. Roles and responsibilities

3.1 The Board of Directors determines the direction and supports implementing the Cybersecurity policy for Mitr Phol Group through the Cybersecurity Committee and Chief Executive Officer.

3.2 The Cybersecurity Committee considers and advises about the risks and adequacy of cyber security measures by coordinating with the Risk Management Committee and periodically reports to the Board of Directors.

3.3 The Management

3.3.1 **Other Departments** shall control and supervise to ensure the policy implemented, announce and communicate the policy to relevant parties, and monitor the continuous practices, with support from the Cybersecurity Committee and Cybersecurity Department.

3.3.2 **The Cybersecurity** Department applies the policy for implementation, announces and communicates the policy to related parties, and supervises and monitors the risks and adequacy of the cybersecurity measures to ensure compliance with corporate risk management. The Cybersecurity Committee supports the Cybersecurity Department.

3.3.3 **All Employees** must comply with the Cybersecurity policy, including relevant practice guidelines and work procedures that have been strictly approved.

4. Important Principles

4.1 Cybersecurity Supervision and Management: The Company has in place measures or operating procedures to ensure that the supervision and management of cybersecurity is effective, comprehensive, covering the entire organization, and in compliance with relevant laws.

4.2 Cybersecurity Management Framework: The Company has in place measures or operating procedures to ensure that there is a practice guideline in managing cybersecurity and personal data adhering to the National Institute of Standards and Technology (NIST), which include the NIST Cybersecurity Framework and NIST Privacy Framework

4.3 Cybersecurity Risk Management: The Company has established measures or operating procedures to ensure that risks are assessed, and cybersecurity and personal data are controlled. Moreover, risk management is maintained within an acceptable range. Risk matters are monitored and reported periodically with conformity to corporate and international risk management.

4.4 Information Asset Management: The Company has established measures or operating procedures to ensure the adequate preparation of the information asset register and control for availability and compatibility to serve or proceed with business operations constantly. The management also covers the control to ensure proper usage of information assets in line with the copyright.

4.5 Human Resource Management for Cybersecurity: The Company has measures or operating procedures to ensure the communication to executives, employees, and those performing duties for the Company for their acknowledgment and understanding of roles and responsibilities, including compliance with the Cybersecurity policy and relevant practices.

4.6 **Physical and Environment Security Management:** The Company has established measures or operating procedures to ensure the security and availability of computer centers and major areas related to information assets and continuous support business demand.

4.7 **Information Security:** The Company has measures or operating procedures to ensure the security of information in hard copy and electronic format, covering the transferring of data through the communication system, storage, data usage on the work system, data recording, storing, and destruction.

4.8 **Access Management:** The Company has measures or operating procedures to ensure the control to access the operating system, network system, information technology system, and database system by implementing the proper management and identity verification to be consistent with the figuration based on the necessity of usage and risk level to prevent the access and changes of the system or data by an unauthorized person, ensuring the accuracy, consistency, and safeguarding of information to support the Integrity of Information, or the third party according to the Least Privilege concept and consistent to the Segregation of Duties.

4.9 **Procurement, Development, and System Maintenance:** The Company has measures or operating procedures to ensure the procurement, development, and system maintenance are under stringent security control and consistent with the international control principle.

4.10 **Vulnerability Inspection and Penetration Testing:** The Company has measures or operating procedures to ensure the operation to identify security vulnerabilities of the system to be able to take necessary actions to prevent emerging risks in a timely manner.

4.11 **Surveillance of unusual cyber security events:** The Company has measures or operating procedures to identify, prevent, and manage any incident promptly with monitoring procedures on system security, including constant monitoring or threat.

4.12 **Management of Unusual Cyber Security Incidents:** The Company has measures or operating procedures to ensure prompt management as a result of cyber threats, including unusual events of information technology, to resume the situation to normal condition in a timely manner and to minimize the potential damage that may affect business operation of the Company.

4.13 Third-Party Management: The Company has measures or operating procedures to ensure the risk management implemented to any services, connection, or access by the third party to maintain risk level within an acceptable range of the Company.

4.14 Business Continuity Management: The Company has measures or operating procedures to cope with incidents that may cause disruption or damage to the business, ensure business continuity, and resume the system to normal condition within an acceptable time frame.

4.15 Related Laws and Regulations: The Company has measures or operating procedures to ensure the operation conducted to prevent the violations of legal obligations, regulations, rules, or employment contracts related to the Cybersecurity Act, Computer Crime Act, Electronic Transaction Act, Personal Data Protection Act, including other relevant laws, regulations, and rules, which are currently enforced and hereafter.

5. Policy Review

5.1 In the event the Management considers that this Cybersecurity policy is not suitable for the business context, or significant changes related to criteria, laws, and technology that may affect the Company, must be report to the Board of Directors through the Cybersecurity Committee for approval to revise the policy.

5.2 The Cybersecurity Committee will review this Cybersecurity policy every year and reports to the Board of Directors to ensure the suitability with Mitr Phol Group business context.