- English Translation -

Data Classification Policy and Guidelines

Pinthong Industrial Park Public Company Limited

14 November 2025

Approved on 14 November 2025 (BOD 4/2025)

Data Classification Policy and Guidelines

Pinthong Industrial Park Public Company Limited and its subsidiaries (the "Company") recognize that information in all forms is a critical resource for operations, administration, and management at all levels of the organization. Proper information management is therefore essential to ensure that the Company's business operations are conducted efficiently, transparently, and securely.

In determining whether any information should be classified as confidential, the Company shall consider key factors, including the importance and value of the information, applicable laws, source of the information, methods of utilization, the number of persons who have access, as well as the potential impact in the event that such information is disclosed or altered without authorization. In this regard, such information shall be controlled and approved by the data owner or authorized persons as designated by the Company.

In order to protect the Company's information from damage, unauthorized access, disclosure, alteration, or use, the Company has established a Data Classification Policy and Guidelines to prescribe clear criteria and practices for classifying information according to levels of confidentiality and for determining appropriate access control measures in accordance with the level of importance of such information.

Definitions

"Company" means Pinthong Industrial Park Public Company Limited and its subsidiaries.

"Information" means any facts, details, or symbols, whether in the form of text, numbers, images, sounds, or any other media, which can be recorded, stored, processed, analyzed, or utilized, including general information or information that can be disclosed to the public, or information that requires access control, such as personal data, business information, or confidential information of the organization.

"Personal Data" means any information relating to an individual, which enables the identification of such individual, whether directly or indirectly, as defined under the Personal Data Protection Act B.E. 2562 (2019).

"Public Information (Public)" means general information that the Company is required to disclose to the public, customers, or external parties, or information that is generally accessible to the public without restriction, or information required by law to be disclosed.

"Internal Information (Internal)" means information prepared for internal use only, whereby employees are authorized to use such information for the performance of their assigned duties. Disclosure of such information to external parties shall only be made with approval from the data owner or authorized persons as designated by the Company.

"Restricted Information (Restricted)" means information that the Company cannot disclose to all employees, being highly critical information accessible only to relevant persons who have a need to know for the performance of their duties. Disclosure of such information to external parties shall only be made with approval from the data owner or authorized persons as designated by the Company.

"Confidential Information (Confidential)" means information that is important and has an impact on the Company's business, with access restricted only to designated employees or users (primarily executives or directly related persons). Such information shall be encrypted. Disclosure to external parties shall only be made upon approval from the relevant executives.

The classification of confidentiality levels shall comprise three (3) categories, as follows:

1. **Top Secret** means information or data which, if disclosed in whole or in part, may cause the most severe damage to the Company.

2. **Highly Confidential** means information or data which, if disclosed in whole or in part, may cause severe damage to the Company.

3. **Confidential** means information or data which, if disclosed in whole or in part, may cause damage to the Company.

Data Classification Practices

1. Determination of Data Classification Levels

Executives, department heads, data owners, and the information technology function shall jointly be responsible for considering and determining the classification of information within information systems, including assigning appropriate levels of data classification in accordance with the nature and importance of such information. Such determination shall take into account the level of importance of the information, security risks, impact on business operations or market value, as well as potential impacts in the event that the information is disclosed, altered, lost, or accessed without authorization. Internal information shall be used jointly with integrity, due care, and prudence.

2. Criteria for Determining Data Classification Levels

The determination of data classification levels shall take into account the level of information security risk, the impact on value, and potential damage that service users or personal data owners may incur, as well as potential impacts on the Company's assets, business reputation, and operations.

3. Authority and Responsibility for Data Classification and Retention

The management of the data owner (Data Owner) shall have the authority and responsibility to determine data classification levels and data retention periods, and shall ensure strict compliance with the Company's Information Security Policy and Personal Data Protection Notice. The management may delegate such authority to department heads as appropriate. In urgent cases, the assigned department heads shall have the authority to determine temporary data classification levels.

4. Storage of Information with Multiple Classification Levels

In cases where information with multiple classification levels is stored together (e.g., within the same sub-folder), the highest classification level shall apply. Department managers shall exercise the utmost care to prevent any leakage of information with higher classification levels.

5. Access Control

All information shall be subject to access control based on the "need-to-know" principle, whereby access shall be granted only to personnel whose duties require such information.

For information within information systems, any modification or change to access rights shall require a formal request and prior approval from a department manager or above through the Company's IT system before implementation. Upon approval, the information technology function shall assign access rights in accordance with such approval.

6. Changes to Data Classification Levels

Any change to data classification levels, whether an increase, decrease, or revocation, shall be supported by clear reasons and necessity. In particular, in cases of downgrading the classification level, the reasons shall be documented in all cases.

7. Data Protection & Storage

Information with high classification levels shall be stored in specially controlled environments, such as locked cabinets or information systems with encryption and restricted access rights. The transmission of such information through unsecured channels, such as personal email or unauthorized applications, is strictly prohibited.

8. Data Disposal

When information is no longer required, it shall be disposed of appropriately in accordance with its classification level, such as shredding physical documents or permanently deleting electronic data in a manner that prevents recovery.

9. Training & Awareness

The Company shall regularly provide training and communicate guidelines on data confidentiality to employees in order to promote understanding and ensure that employees at all levels recognize the importance of information security.

10. Whistleblowing

Any employee or person who becomes aware of or suspects any act that may constitute a violation of this policy may submit a complaint or report such matter to the Company in accordance with the procedures prescribed in the Company's Whistleblowing Policy. In this regard, the Company shall provide protection to whistleblowers or complainants. The information and identity of the whistleblower shall be kept confidential, and such reporting shall not affect the employment status, position, or remuneration of the whistleblower, both during the investigation process and after the completion of such process.

11. Disciplinary Actions

This Data Classification Policy and Guidelines shall form part of the Company's code of conduct. All directors, executives, and employees shall strictly comply with this policy. In the event of any violation or non-compliance, the Company shall conduct an investigation and impose disciplinary actions in accordance with the Company's rules and regulations, charters, and applicable laws, which may include termination of employment. In this regard, during any investigation, all employees shall fully cooperate with the relevant internal and external parties.

This Data Classification Policy and Guidelines shall be effective from 14 November 2025, by the approval of the Board of Directors at its Meeting No. 4/2025.

- Mr. Prasan Tanprasert -
Chairman of the Board of Directors
Pinthong Industrial Park Public Company Limited