CENTRALPATTANA

Information Security and Responsible Artificial Intelligence Development Policy

Central Pattana Public Company Limited

1. Introduction

In an era where information technology and artificial intelligence (AI) are integral to business operations and competitiveness, information security management and the safe use of AI are critical to maintaining the trust of all stakeholders, including customers, suppliers, shareholders and employees. Misuse or errors in the application of technology and AI can cause serious harm to the Company's financial stability, reputation and critical information. Central Pattana Public Company Limited and its subsidiaries (the "Company") recognize the importance of managing information security and developing AI responsibly to meet the challenges of digital transformation and to deliver long-term value for business and society. The Company is committed to operating in alignment with highest international standards by aligning with key regulatory and governance frameworks, including relevant Thai laws such as the Personal Data Protection Act (PDPA), ISO/IEC 27001 and good governance practices established by the IOD.

The Company emphasizes the ethical and secure use of AI, by establishing safeguards against potential risks, such as data leaks, unfair decision-making and AI-related cyberthreats. These measures ensure that AI adoption enhances business performance while maintaining stakeholder trust.

To support this commitment and reinforce stakeholder confidence, the Company continuously strengthens its information security and AI measures and practices to ensure the highest standards of effectiveness. These efforts help prevent data leaks, unauthorized access and potential cybersecurity threats. The Company also reviews and updates its policies and guidelines regularly to reflect the rapidly evolving technology and business environments. Guided by principles of transparency, integrity and sustainable management, this Information Security and Responsible Artificial Intelligence Development Policy and related practices serves as a framework for all employees and stakeholders to uphold the Company's standards and international best practices in information security and responsible AI use.

2. Scope

This Policy applies to all Company personnel at all levels, including permanent and temporary employees, executives, suppliers and relevant third parties who are assigned or granted access to the Company's data or technology systems. It covers the collection, use and protection of all types of Company data, including financial information, operational data, and the personal data of customers, suppliers, employees and other stakeholders. The Policy also governs the ethical and secure development and use of artificial intelligence (AI).

3. Objectives

- To prevent data leaks, unauthorized access and cyberattacks that could compromise the Company's data or technology systems
- To ensure that the Company's development and use of AI are safe, transparent and fair, and do not negatively impact any stakeholder group
- To ensure that information security and AI practices comply with applicable laws, regulations and standards, including the Personal Data Protection Act (PDPA), ISO/IEC 27001 and the good governance principles defined in the Company's Code of Conduct and Corporate Governance
- To build stakeholder confidence in the Company's transparency and accountability in responsible management of information and technology
- To align the Company's information security and AI management with the UN Sustainable Development Goals (SDGs), and strengthen long-term competitiveness

4. Roles and Responsibilities

To ensure the effective management of information security and responsible AI development across all levels of the organization and alignment with the Company's strategic direction, the roles and responsibilities of relevant functions and individuals have been defined as follows:

4.1 Board of Directors

- Approve and oversee this Policy to ensure alignment with the Company's strategic objectives and governance principles

- Review the Policy to ensure it remains relevant and responsive to changes in business conditions, legal requirements and international standards
- Review annual reports on information security and AI performance, including the management of key risks and opportunities
- Provide strategic guidance to senior management to support sustainability and resilience in technology and risk management

4.2 Senior Management

- Allocate sufficient and appropriate resources, including personnel, budget and technology, to support information security and AI operations
- Regularly monitor the progress of implementation and threat management activities, including system audits and security assessments
- Support the development of ethical AI management processes and ensure AI development aligns with the Company's guidelines
- Promote knowledge, awareness and understanding among employees and suppliers of the importance of information security and ethical AI use
- Report performance and key challenges to the Board or relevant sub-committees on a periodic basis

4.3 Relevant Functions

- Develop and maintain secure systems for storing and managing information and AI-related data in compliance with applicable requirements
- Conduct monitoring and audits of cybersecurity threats and develop appropriate response plans
- Coordinate with senior management and external parties to manage risks and disputes
- Monitor technology trends and emerging threats related to information security and AI, and recommend timely improvements
- Provide training to relevant personnel to build understanding of systems and tools related to security management

4.4 Employees

- Comply with the Company's policies, practices and measures related to information security and AI
- Use Company data and technology appropriately, avoiding actions that could result in damage or rights violations
- Report any cybersecurity threats, data breaches, or inappropriate use of AI to a supervisor
- Participate in training or activities related to information security and AI to enhance awareness and understanding of their responsibilities

5. Policy and Practices

5.1) Employees must comply with the Company's policy and measures on information security, and must protect confidential information belonging to the Company, customers, suppliers and employees, to prevent data leaks or unauthorized use.

5.2) The use or disclosure of internal Company data for personal gain or for the benefit of third parties is prohibited unless prior authorization has been granted.

5.3) Access to Company data must be appropriately managed using up-to-date security systems that align with applicable standards and best practices.

5.4) Employees must use Company systems and technology devices solely for work purposes. Any use that may result in damage or risk to information security is prohibited.

5.5) Installation of software or programs on Company devices is prohibited unless explicitly authorized, to prevent exposure to malware or computer viruses.

5.6) All AI development and use must be conducted responsibly, with consideration for transparency and fairness, and the avoidance of negative stakeholder impacts.

5.7) Employees must avoid using AI in ways that create bias or discrimination, that may lead to bias or discrimination, and must assess the potential impact of AI on data privacy.

5.8) AI usage must be regularly reviewed and evaluated to ensure ethical use and compliance with applicable laws.

5.9) The Company maintains robust cybersecurity measures, including regular system testing and monitoring, data encryption and contingency planning.

5.10) Employees are required to immediately report any incidents relating to cybersecurity threats or system breaches.

5.11) All employees must comply with the Company's measures and guidelines, and participate in training activities to strengthen their knowledge and understanding of information security and AI.

5.12) Employees are expected to exercise caution and sound judgment when handling and using the Company's data and technology.

5.13) Personal data must be managed in compliance with applicable laws, with privacy protection measures in place in every process.

5.14) The Company is committed to aligning its practices with internationally recognized standards on information management and technology.

5.15) The Company will regularly review and update its policy and measures on information security and AI to remain responsive to the evolving technological and business landscape.

6. Training

The Company is committed to promoting knowledge, understanding and compliance with this Policy across the Board, management and employees at all levels. This is achieved through activities, such as training sessions, workshops and seminars, covering principles of data security, ethical AI use, cybersecurity threat prevention and the secure handling of personal data. Training content is tailored to align with job roles and organizational needs, to ensure practical application in day-to-day operations. The Company also prioritizes the ongoing monitoring and evaluation of knowledge transfer efforts to ensure that all personnel have a clear understanding and can effectively comply with the Company's policies and procedures.

7. Complaints and Whistleblowing

The Company provides designated channels for employees and stakeholders to raise complaints or report suspected breaches of this Policy. All reports will be handled in accordance with the Company's Whistleblowing Policy, which ensures the safety, confidentiality and rights of complainants, and protects them against retaliation or any adverse consequences throughout the investigation process. The Company places strong emphasis on transparency, integrity and fostering an organizational culture of accountability in data protection and the ethical development of technology.

8. Disciplinary Action

The Company affirms the importance of strict compliance with this Policy. All employees are required to fully cooperate with any reviews or investigations into potential policy breaches. Where non-compliance or violations are identified, disciplinary action will be taken in accordance with the Company's internal regulations. This approach supports the establishment of transparent and sustainable operational standards, promote the development of safe and ethical technologies, and maintains the trust of stakeholders.

9. Policy Review and Update

This Policy will be reviewed and updated at least annually, or changes in applicable laws, regulations or relevant practices occur. The review process ensures the Policy remains relevant, effective and responsive to the evolving business and technological landscape. The Company is also committed to continuously improving its information security and AI processes to meet stakeholder needs and support long-term sustainable growth and responsible business conduct.

This Policy is effective from May 2, 2025 onward.