Artificial Intelligence (AI) Usage Policy
I.C.C. International Public Company Limited

1. Introduction

AI—particularly generative AI—can create text, images, videos, audio, and code based on user instructions, thereby helping to save time and improve efficiency across various tasks, from drafting documents and writing computer code to producing promotional materials.
However, the use of AI carries risks that require Users to exercise caution. AI-generated content may appear credible yet be inaccurate or unsuitable for the Thai context or the Company's specific circumstances. Common risks include:

- False or inaccurate information shared unintentionally (misinformation), or false or misleading information deliberately created or shared to deceive (disinformation).
- AI-generated content that lacks factual support (confabulation).
- Biased or prejudiced content that could lead to discrimination (bias and discrimination).
- Disclosure of personal data or infringement of the copyright of others through AI-generated content.
- Risks to the security of the Company's data and systems.

The Company has therefore established this policy to enable employees to use AI effectively, safely, and responsibly.

2. Objectives

1. To provide all Users with guidelines for using AI correctly and appropriately in line with the Company's objectives.
2. To ensure that AI use complies with applicable laws and regulations and to prevent issues arising from misuse.
3. To ensure that all Users understand and remain mindful of their responsibilities when using AI.

3. Scope of Application

This policy applies to:

- Directors, executives, employees at all levels, affiliated companies, and external parties granted access to the Company's systems (collectively referred to as "Users").
- The use of all types of AI tools, whether provided by the Company or adopted by Users themselves.
- AI use on both Company-owned devices and personal devices connected to the Company's systems.

4. Definitions

Term	Meaning
the Company	I.C.C. International Public Company Limited
Chief Executive / CIO	Chief Information Technology Policy Officer or authorized representative
Supervisor	Unit managers or supervisors who oversee Users' work activities.
Users	Directors, executives, employees at all levels, affiliated companies, and external parties who use the Company's information system resources.
Artificial Intelligence (AI)	Technology that enables computers or systems to possess capabilities similar to those of humans, such as learning, reasoning, problem-solving and Machine Learning.
Generative AI	AI that can generate new content—such as text, images, videos, or code—based on instructions.
Agentic AI	AI that can autonomously execute multi-step processes to achieve a goal, including invoking tools and accessing systems on behalf of a human.
Personal data	Information that can identify an individual, either directly or indirectly, pursuant to the Personal Data Protection Act B.E. 2562 (2019).

Term	Meaning
Sensitive personal data	Data under Section 26 of the Personal Data Protection Act B.E. 2562 (2019), including information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disabilities, trade union membership, genetic data, biometric data, or any other data that may similarly affect the data subject, as prescribed by the Board of Directors.

5. Types of AI Covered by This Policy

Type of AI	Description and Examples
Generative AI	Generates new content based on user instructions, such as text, images, code, or audio. Examples include ChatGPT, Claude, Gemini, DeepSeek, GitHub Copilot, and Midjourney.
Agentic AI	Can autonomously execute multi-step workflows, such as invoking tools, retrieving data, or performing tasks on behalf of a person. Examples include automated AI assistants, workflow automation systems, and AI integrated with accounting or customer management systems.

6. Principles for Using AI

The Company encourages the use of AI to improve work performance, subject to the following four principles:

1. **Human oversight** — AI-generated outputs must always be reviewed by a human before use.
2. **Transparency and accountability** — Each use of AI must have a clearly explained basis and be traceable.
3. **D**ata security — Data security must be given top priority.
4. **Clear responsibility** — Users are responsible for the outcomes of their use of AI.

7. Authorized Usage

Users may use AI to assist with the following tasks, provided that such use is solely for the benefit of the Company:

- Analyzing data and preparing reports;
- Writing code and supporting software development;
- Drafting documents, official letters, memoranda, and other communications for internal and external use;
- Suggesting initial approaches to problem-solving;
- Summarizing content, translating text, and conducting general research; and
- Assisting with brainstorming, developing concepts, or creating promotional materials.

8. Restrictions on AI Usage

The use of AI must remain within appropriate boundaries and must not cause harm to anyone. Users are prohibited from:

1. Using AI to make decisions on behalf of humans in critical areas, such as legal, medical, or financial matters, or in matters that affect people's lives, property, and rights.
2. Using AI to create false information or content that misleads people or incites conflict.
3. Inputting the Company's confidential information into unauthorized AI tools.

   When entering Company-related information into AI tools, Users must use only tools provided by the Company, such as Google Workspace Enterprise, Gemini, or NotebookLM.
4. Using the personal data of others without authorization or violating applicable personal data protection laws, including the Personal Data Protection Act (PDPA).
5. Using AI incorrectly or inappropriately, or with the intent to commit wrongdoing.
6. Using AI to create content that infringes the copyright or other intellectual property rights of others.
7. Using AI to create content that is discriminatory or disparaging based on race, religion, gender, age, disability, or social status.
8. Using AI in a manner that interrupts or obstructs the Company's activities or transactions.
9. Using AI to perform any action that may violate applicable laws or regulations.

9. Data Prohibited from Being Entered into AI Systems

Do not input the following information into AI tools that have not been authorized by the Company:

Data Type	Examples
Customer information	Full names, phone numbers, email addresses, His&Her membership information
Financial information	Financial statements, product costs, negotiated prices, commercial contracts
Trade secrets	Undisclosed strategies, roadmaps, and business plans
Employee information	Salary, performance evaluation history, health information
Passwords and access keys	Passwords, system access keys/codes (API keys, tokens), and database connection details
Internal system information	Confidential source code, database structures, system configurations, network data

If AI must be used with internal or personal data, only tools designated by the Company may be used, and prior approval must be obtained from the relevant unit manager in each case.

10. Confidentiality and Protection of Personal Data

Many free AI tools may retain user inputs or use them to train AI models, posing a risk of data leakage. Users must comply with the following requirements:

- Do not enter internal or confidential information (such as passwords, contracts, sensitive documents, or internal project data) into AI tools.
- If internal or personal data must be used, use only tools designated and pre-approved by the Company.
- If you have any questions regarding safety or legal matters, consult your supervisor or the relevant personnel before proceeding.

11. System Security When Using AI

- Do not enter information that could compromise system security (such as passwords, API keys, or system configuration details) into AI tools.

- Always verify the accuracy of AI-generated code and check for any vulnerabilities before use.
- If a security breach involving AI use is discovered, the relevant supervisor must be notified promptly, and security incident response procedures must be followed immediately.
- The Company may continuously monitor AI usage to ensure security.

12. Reducing Bias, Addressing Discrimination, and Respecting Intellectual Property

- Content generated by AI must be reviewed before use or publication to reduce bias and unfair discrimination.
- Exercise caution when using AI for tasks that could affect individuals' rights or the principle of equality.
- AI-generated content must be checked to ensure that it does not duplicate, copy, or adapt the work of others without authorization.
- Only the AI tools specified by the Company may be used in the public dissemination of content.

13. Additional Requirements for Autonomous AI Systems (Agentic AI)

Since this type of AI operates autonomously and has access to various systems, compliance with the following additional requirements is necessary:

- Approval from the Director of Information Technology must be obtained before an Agentic AI system is deployed to the production environment.
- Access must be limited to what is necessary to perform the assigned tasks, and all actions must be logged for audit purposes.
- For high-impact tasks, such as modifying data in accounting or human resources systems (ERP, HR) or in the OBSD and QRMS systems, human approval must be obtained before AI is permitted to perform the action.
- Granting AI the authority to delete Company data or modify data access permissions requires approval from the Director of Information Technology before any such action is taken.
- A function must be in place to restore data to its original state, together with a mechanism to halt operations immediately if the system malfunctions.

14. Disclosure of AI-Assisted Content

To ensure transparency and prevent misunderstandings, please indicate, where appropriate, that "this content was created with the assistance of AI technology" when using or publishing AI-assisted content.

15. Responsibilities

15.1 Users

- Always verify the accuracy of AI-generated outputs before use, especially those involving legal or financial content or sensitive information.
- Strictly adhere to this policy.
- Notify your supervisor or the IT Security team immediately upon discovering any risks or irregularities related to the use of AI.

15.2 Supervisors / Unit Managers

- Oversee AI use within the team to ensure compliance with this policy.
- Review and approve the use of automated AI and the use of AI with internal or personal data.
- Continuously monitor and evaluate the effectiveness of AI use within the work unit.

15.3 Information Technology Division

- Create and maintain a list of AI tools approved for use by the Company (Approved AI Tools List).
- Review and update the policy at least once a year, or whenever significant new technology emerges.
- Provide employees with training on the fundamentals of AI use and how to use AI safely.

15.4 BUSINESS PROCESS OPERATION Division, Business Support Unit

- Oversee and ensure compliance with this policy.

16. Training and Education

The Company will conduct training for employees on the proper use of AI, including its risks, limitations, and potential impacts, at least once a year.

17. Violations and Penalties

Any violation of this policy is considered a breach of the Company's regulations. The Company will take disciplinary action commensurate with the severity of the incident, ranging from a written warning or suspension to termination of employment. Legal action may also be taken if the conduct causes damage to the Company or any third party.

18. Policy Review

This policy must be reviewed annually (every 12 months) to ensure that its content remains current and appropriate to prevailing circumstances. An ad hoc review may be conducted sooner if there are significant changes in laws, regulations, or technology.

Any amendment or revision to this policy must be reviewed and approved by the President and the Chairman of the Executive Committee and subsequently communicated to employees via Google Workspace or other internal Company communication channels.

.....

This policy on the governance of AI use was approved by the Board of Directors at its meeting No. 6/2026, held on September 11, 2026, and shall take effect on September 11, 2026.