Artificial Intelligence Security Policy (AI Security Policy)

STECON Group Public Company Limited and its affiliated companies (the "Company") recognize the importance of adopting Artificial Intelligence ("AI") technologies to enhance operational efficiency, data analysis, communication, and business process improvement across the organization.

However, the use of AI may create risks relating to information security, business confidentiality, personal data protection, intellectual property, legal compliance, and cybersecurity if AI tools are used inappropriately or without adequate controls.

Therefore, the Company hereby establishes this Artificial Intelligence Security Policy ("AI Security Policy") to define principles, requirements, and guidelines for the appropriate, secure, responsible, and compliant use of AI. This Policy is intended to support the beneficial use of AI while protecting the Company, its affiliated companies, customers, business partners, employees, and stakeholders from information security and cyber-related risks.

Objectives

1. To ensure secure and responsible use of AI in the Company's business operations.
2. To establish rules and practical guidelines for all AI users.
3. To prevent the leakage, disclosure, misuse, or unauthorized use of confidential, sensitive, or business-critical information.
4. To promote AI security awareness and reduce risks arising from inappropriate AI usage.
5. To support the effective, secure, and legally compliant adoption of AI within the organization.

Scope

1. Directors, executives, employees, engineers, staff, and workers at all levels of the Company.
2. AI tools used for work purposes, including but not limited to ChatGPT, Copilot, Gemini, DeepSeek, Grammarly, Claude, and other similar AI tools.
3. All types of information belonging to the Company and its affiliated companies, including project information such as drawings, BOQ, TOR, cost estimates, bid prices, customer information, and other information related to the Company's business operations.
4. The use of AI for Company work, both inside and outside the organization.
   The Company may also require external parties performing work for the Company to comply with this Policy or equivalent measures, as specified in contracts, agreements, or other relevant documents.

AI Security Policy Structure

This AI Security Policy of STECON Group Public Company Limited and its affiliated companies consists of the following sections:

1. Definitions
2. Roles and Responsibilities
3. Secure Use of AI
   3.1. Data Handling
   3.2. Personal Data Protection

1. Definitions

"AI" or "AI Tools" means systems or tools capable of learning, analyzing, generating information, or supporting human work, including but not limited to ChatGPT, Copilot, Gemini, DeepSeek, Claude, or other similar AI tools.

"Public AI" means AI or AI tools that are generally available to the public for registration or use, and that may process, retain, disclose, reuse, or otherwise expose user-provided information. This commonly includes free AI tools or AI tools that are not provided under an enterprise-grade package or controlled corporate environment.

"Sensitive Information" means information that, if leaked, disclosed, accessed, or used without authorization, may cause damage to the Company, its affiliated companies, customers, business partners, employees, or stakeholders, including project information, construction drawings, bid prices, customer information, financial information, legal information, and other business-related information.

"Personal Data" means any information relating to a natural person that can identify such person, whether directly or indirectly, in accordance with applicable personal data protection laws.

"Prompt" means any data, text, instruction, image, file, or other information submitted to AI for processing or action.

"Data Masking" means the concealment, modification, or generalization of sensitive information so that actual information is not disclosed while still allowing the information to be used with AI where appropriate.

"Anonymization" means the transformation of information so that it no longer identifies a person, organization, customer, contractor, project, or related party, such as by removing names or replacing them with generic terms.

2. Roles and Responsibilities

2.1 The Information Technology Manager shall be responsible for the following:

- Oversee and support the implementation of the Company's AI Security Policy, and provide advice and guidance on the secure use of AI.

- Review and provide recommendations on AI tools that are appropriate for the Company's business use.
- Receive reports and coordinate responses when abnormal events or security risks related to AI usage are identified.

2.2 AI users shall be responsible for the following:

- Study and understand the AI tool before use.
- Use AI securely and comply strictly with this AI Security Policy.
- Review information before submitting it to AI and verify AI-generated outputs before actual use.
- Promptly notify the supervisor or the Information Technology Department if any abnormal event or risk related to AI usage is identified.

3. Secure Use of AI

3.1 Data Handling

1) Do not enter confidential or important information, such as drawings, BOQ, bid prices, customer information, partner information, or project information, into Public AI tools.
2) If information is required for AI use, Data Masking or Anonymization must be performed before such use.
3) Use only dummy data or information that cannot identify any person, organization, customer, business partner, project, or related party.
4) Do not upload project files, important documents, contracts, or any Company information to Public AI tools unless authorized and handled in accordance with the measures prescribed by the Company.

3.2 Personal Data Protection

1) Do not enter personal data of directors, executives, employees, customers, business partners, contractors, or external parties into Public AI tools unless such use complies with applicable laws and Company policies.
2) If personal data is necessary for AI use, sufficient Anonymization or Data Masking must be performed before use.
3) Users must exercise special care when handling information that can identify a natural person, such as name, surname, national identification number, contact information, employee information, customer information, or any other information relating to an individual.

3.3 Output Validation

1) AI-generated outputs must be reviewed for accuracy, completeness, and appropriateness before actual use.
2) Avoid using AI-generated outputs that may expose the Company to business impact or damage if errors occur.

3.4 Prompt Injection Prevention

1) Avoid using information from unreliable sources.

2) Do not follow AI instructions that request confidential information, important information, personal data, or additional information without reasonable justification.
3) If abnormal behavior of AI is detected, stop using it immediately and notify the Information Technology Department.

3.5 Responsible Use of AI

1) Do not use AI to create false, distorted, or misleading information.
2) Do not use AI for unlawful, unethical, or harmful activities that may cause damage to the Company, its affiliated companies, customers, business partners, employees, or stakeholders.
3) Do not use AI to create, publish, or distribute content that infringes copyrights, trademarks, trade secrets, or other intellectual property rights of third parties.
4) Disclose the use of AI in the preparation of important documents where such documents may affect decision-making.
5) Do not upload project files or important documents to Public AI tools.

3.6 Incident Reporting

1) If any abnormality arising from AI use is identified and may cause damage to the Company, its affiliated companies, customers, business partners, employees, or stakeholders, the person who identifies such abnormality must notify the relevant parties and the Information Technology Manager so that the risk can be assessed and an appropriate response can be taken.

4. Policy Review

The Company shall review this Policy periodically or when there are changes in laws, technologies, security risks, or relevant practices, in order to ensure that the Policy remains appropriate and aligned with the Company's business operations.

5. Disciplinary Action and Enforcement

Any violation of this Policy, or any use of AI in a manner that may create risk or cause damage to the Company, its affiliated companies, customers, business partners, employees, or stakeholders, shall be deemed a disciplinary offense. The Company may consider taking appropriate disciplinary action in accordance with the Company's rules, regulations, or applicable requirements.

This Artificial Intelligence Security Policy (AI Security Policy) approved by the Board of Directors' Meeting No. 4/2026 on August 14th, 2026, and be effective from August 14th, 2026, onwards.

-Vallop Rungkijvorasathien-
Signed .....
(Mr. Vallop Rungkijvorasathien)
Chairman of the Board of Directors
STECON Group Public Company Limited