TCM CORPORATION PUBLIC COMPANY LIMITED
AI SECURITY POLICY

1. Purpose

This AI security policy establishes guidelines and principles for using AI technologies and applications (collectively called "AI systems") within TCM Corporation Plc. ("Company"). It aims to ensure that AI systems are utilised in a manner that prioritises ethical considerations, safeguards privacy and security, and aligns with the organisation's values and objectives.

2. Scope

2.1 Enforcement

This policy applies to all employees and third parties who interact with our AI systems.

2.2 Tools and Application

This policy governs the use of third-party or publicly available AI tools, encompassing platforms and analogous applications designed to simulate human intelligence for generating responses, thinking, calculating, analysing, producing work outputs, or executing specific tasks, as listed in Appendix A. It also includes any AI applications or systems designed to perform similar functions that may occur in the future.

3. Features of the AI system used in the workplace

In choosing an AI system to use in the Company's operations, it is essential to consider not only the efficiency and objectives of the organization but also the ethical principles of AI and relevant laws. The Company has established the following guidelines for considering AI systems that align with ethical principles, considering the context, risks, and potential impacts of AI applications:

(1) Fairness, Diversity, Inclusivity, and Equity of AI outcomes:
The AI systems should process data fairly, accurately, and without bias.

(2) Transparency in AI Operations:
The AI system should allow for the explanation of events, actions, processes, and activities retrospectively, enabling users to verify the activities are conducted correctly and predict future actions.

(3) Reliability of AI Operations:
The AI system should be reliable in terms of its accuracy, completeness, timeliness, relevance, and usability, ensuring high quality and trustworthiness for users.

(4) Security and Privacy of AI Systems:
The AI system should be secure, minimizing vulnerabilities and preventing threats that could result in negative outcomes. It must also comply with relevant data protection laws.

4. Guidelines for AI system users in the workplace

4.1 Dos:

- ✓ Study general knowledge about the benefits and necessary skills for using AI systems to ensure proper collaboration with AI in the workplace.
- ✓ Choose efficient AI systems that align with the company's operational objectives.
- ✓ Regularly follow news related to AI technology to be aware of new knowledge and be prepared to handle various threats.
- ✓ Prioritise ethical considerations and fairness in AI deployment.
- ✓ Acknowledge that AI tools can offer utility but should not replace human judgment and creativity.
- ✓ Recognise the potential for inaccuracies, including "hallucinations," false information, or incomplete information in AI outputs, and always verify responses meticulously.
- ✓ Ensure that any response from an AI tool intended for reliance is accurate, unbiased, compliant with intellectual property and privacy laws and aligns with company policies.
- ✓ When using AI for design, verify that the designs are original and do not infringe on existing copyrights. Additionally, ensure the design concepts align with current market trends and customer preferences.
- ✓ Treat all information provided to an AI tool as potentially public, regardless of tool settings or assurances from creators.
- ✓ Realize your own accountability in using AI systems
- ✓ Inform your supervisor when using an AI tool to complete tasks.
- ✓ Obtain explicit written permission from your supervisor and the IT Department before integrating any AI tool with internal company software.

4.2 If there are any questions/anything unusual

- ✓ Report any questions or unusual activity about AI security policies immediately to the IT security team, especially if it involves unauthorised access, data breaches, or policy violations.

4.3 Don'ts:

- × Rely solely on AI algorithms without human oversight and intervention in critical decision-making processes.
- × Using AI tools in employment decisions involving applicants or employees, including recruitment, hiring, performance monitoring, and termination.
- × Inputting confidential, proprietary, or sensitive company data into any AI tool, such as passwords, health information, personnel material, or any information that may lead to PDPA violation.
- × Upload personal information about any individual, including names, addresses, or any other information that similarly affects the data subject, into AI systems.
- × Misrepresent AI-generated work as your original creation.
- × Use AI tools not included in the IT department's approved list, as malicious chatbots could compromise information security.
- × Accept AI-generated designs without reviewing them for feasibility in terms of manufacturing capabilities and material constraints.

5. Violations

Violations of this AI security policy may result in disciplinary action, including but not limited to reprimands, training requirements, suspension of AI systems usage privileges, or termination of employment, depending on the severity and recurrence of the violation.

6. Disclaimer

This AI security policy is intended to provide general guidance and principles for AI's ethical and responsible use within TCM Corporation Plc. It does not constitute legal advice and TCM Corporation Plc. reserves the right to modify or amend this policy as necessary to address evolving regulatory requirements, technological advancements, or organisational needs.

Pursuant to a resolution of the Board of Directors' meeting on 14th August 2024.

TCM Corporation Public Company Limited

(Mr. Pimol Srivikorn)
Chairman

Appendix for Approved AI

Design Function

1. NedGraphics
2. Textronics Design Systems
3. Design2Fab
4. Adobe Textile Designer
5. Poincare
6. Digital Weaving Norway (DWN)

Sales and Marketing Function

1. HubSpot
2. Salesforce Einstein
3. Marketo
4. Conversica

Manufacturing & Operation

1. GE Predix
2. Spark Cognition
3. Uptake
4. Sight Machine

General AI Applications

1. OpenAI's ChatGPT
2. Google Assistant Gemini
3. Amazon Alexa
4. Canva
5. Gamma
6. Grammarly