Electricity Generating Public Company Limited

Artificial Intelligence Policy

Version History

Version No.	Description and reason for change	Revised by	Revised date
1.0	Initial release		

Document Sign-off

Role	Name – Last name	Signature	Designation	Date
Authored by	Artit Laoonual		VP-Cybersecurity and Privacy	Jun 26
Reviewed by	Wutirat Chungsangsitiporn		SVP-Infrastructure and Information Security	Jun 26
Approved by	Prasert Sinsukprasert		Chairman	

1. Introduction

Electricity Generating Public Company Limited (EGCO) and its subsidiary in Thailand, or EGCO Group, has organized an information technology system of the EGCO Group to support its transition into the era of Artificial Intelligence (AI) and to utilize technology as a tool to enhance efficiency and effectiveness in operations, support decision-making, and drive business innovation. This shall be implemented under a responsible AI governance framework that is transparent, secure, auditable, and compliant with applicable laws and regulatory requirements. In this regard, management has recognized the importance of developing an AI policy to provide a framework for the responsible use of such technologies, in accordance with principles of ethics, transparency, and security.

2. Objectives

This Policy aims to:

- Establish EGCO Group's commitment to the responsible development, deployment, and use of AI systems across all business activities.
- Provide an AI management framework consistent with EGCO Group's strategic direction and sustainability commitments.
- Ensure AI systems are implemented and used in a manner that is ethical, transparent, accountable, and aligned with applicable legal and regulatory requirements.
- Foster a culture of responsible AI usage among EGCO Group's internal users and external parties.
- Support the continual improvement of the AI Management System.

3. Scope of Application

This policy applies to all users, including the Board of Directors, the President, executives, and employees of the EGCO Group as well as encourages external parties. It applies to all AI systems that develops, procures, deploys, or uses, including systems operated or on behalf of the EGCO Group, whether developed internally or by third parties.

4. Definitions

1) "EGCO Group" means to Electricity Generating Public Company Limited (EGCO) and its subsidiaries in Thailand.
2) "Executives" means to a person with direct managerial responsibility for a particular employee.
3) "Employee" means to a person employed for wages or salary, staff and executive level, including intern, contractors, and special worker undergo agreement with EGCO Group.
4) "User" means to all employees, contractors, vendors and any third-party relationship of EGCO Group who have the authorized to access EGCO Group's assets and information system.
5) "External Party "means to a person or another company who provide services to EGCO Group have the authorized to access EGCO Group's assets and information system for example;
    - Business Partner
    - Outsource
    - Supplier
    - Service Provider
    - Consultant
6) "Information Technology" or "Information" means to an asset that, like other important business assets such as business information, source code, image, voice, signal, and sign, is stored in direct format, computer format, or any other format that makes the recorded information visible.
7) "Artificial Intelligence (AI) System" means to a machine-based system that, for a given set of objectives, is designed to process data in order to generate predictions, recommendations, or decisions, or to produce content that may influence real or virtual environments. Such systems may operate with varying levels of autonomy. Examples include Generative AI, Predictive Analytics, and Computer Vision.
8) "Artificial Intelligence Management System (AIMS)" means to the set of interrelated elements established by the organisation to develop, implement, maintain, and continually improve system for responsible development, provision, and use of AI systems in line with EGCO Group's policies and targets.
9) "AI Policy" means to the intentions and direction of EGCO Group formally expressed by top management with respect to the responsible development, deployment, and use of AI systems
10) "Responsible AI" means to the design, development, deployment, and operation of AI systems in a manner that is ethical, transparent, accountable, fair, and aligned with applicable legal, regulatory, and societal expectations.

11) “Data Privacy (AI context)” means to protection of personal data throughout the full AI system lifecycle, including data collection, model training, inference, and decommissioning in compliance with applicable data protection laws, including Thailand’s Personal Data Protection Act B.E. 2562 (PDPA).
12) “Cybersecurity (AI context)” means to the Security measures applied to AI systems to prevent unauthorised access such as;
    - Data Poisoning
    - Model Stealing
    - Model Inversion Attacks
    - Prompt Shielding
    - Other AI-specific threats, including penetration testing, encryption, secure coding.
13) “Bias (AI context)” means to systematic and unfair discrimination in AI outputs arising from biases in training data, model design, or deployment context, resulting in disproportionate or unjust treatment of individuals or groups.
14) “Human-in-the-Loop (HITL)” means to a governance principle that ensures human oversight, review, or approval is maintained for AI-influenced decisions that are critical, high-stakes, or irreversible, with clearly defined authority to intervene, override, or escalate.
15) “AI-Generated Content” means to any content — including text, images, video, audio, decisions, or recommendations — produced by an AI system, which must be distinctly labelled as AI-generated to ensure transparency to users and affected parties.
16) “AIMS External Verification” means to the third-party assessment and verification of Artificial Intelligence Management System against an established standard such as ISO/IEC 42001 providing independent assurance to stakeholders.

5. Responsibilities

5.1. **Board of Directors:** Responsible for putting in place a comprehensive AI Policy and ensuring that an effective AI Management System is implemented. Formally endorses this policy.

5.2. **Corporate Governance and Sustainability Committee:** Responsible for reviewing, endorsing, and overseeing EGCO Group's policies, regulations, and practices related to the responsible use of AI across corporate governance, ethics, legal compliance, sustainability, and cybersecurity.

5.3. **Risk Oversight Committee:** Responsible for overseeing AI-related risks within the enterprise risk management framework, reviewing AI risk assessment results and mitigation plans, and ensuring significant AI risks are escalated appropriately.

5.4. **IT and Cyber Security Oversight Committee:** Responsible for overseeing implementation of the AI Management System, monitoring compliance with this Policy, reviewing AI impact assessments and cybersecurity controls.

5.5. **AI Working Group:** Responsible for developing this Policy, conducting AI risk and impact assessments, maintaining the AI system inventory, implementing training programmes, developing and maintaining AI controls and incident response procedures, and reporting to the IT and Cyber Security Oversight Committee.

5.6. **Employee:** Responsible for complying with this Policy and related procedures, completing required AI ethics and security training, and reporting concerns regarding AI system behaviour or non-compliance through established channels.

6. Requirements

The AI Policy is as follows:

1. Set AI objectives aligned with EGCO Group's business strategy, core values, culture, and risk appetite, in support of responsible and sustainable AI development and use.
2. Comply with applicable legal requirements and international practices and alignment following ISO/IEC 42001.
3. Develop and operate AI systems responsibly across their full lifecycle, covering design, development, verification, deployment, monitoring, and decommissioning, with defined boundaries for what each AI system can and cannot do, Human-in-the-Loop to decisions, and mechanisms to detect and correct model drift or degradation over time.
4. Identify and manage risks arising from the development, deployment, and use of AI systems, including risks related to data privacy, cybersecurity, bias, transparency, accountability, and ecological impact, in accordance with enterprise risk management framework.
5. Assess and manage the impact of AI systems on relevant interested parties, including employees, customers, communities, and society, to ensure that AI activities do not cause harm and affected parties have access to an appeals process to contest AI-driven decisions.
6. Define and maintain processes for handling deviations from and exceptions to this Policy; define AI system resources including data, tools, infrastructure, and human competencies; and conduct AI system impact assessments prior to deployment and at planned intervals thereafter.
7. Continually improve the suitability, adequacy, and effectiveness of the AI Management System through planned reviews, management evaluation, audit findings, and monitoring of AI system performance and regulatory developments.
8. Develop and comply with the EGCO Group Policy and Guidelines, which are reviewed and updated at planned intervals.
9. Communicate and train all relevant users on the responsible use, ethical considerations, data privacy implications, and security of AI systems, and ensure this Policy is publicly available and communicated to all stakeholders.

7. Regular review

We are committed to reviewing and revising this Policy at least once a year, or upon any significant change, to ensure that AI governance, scope of application, and accountability remain accurate, appropriate, and aligned with current business changes and requirements.

This Policy shall be effective as of 26th June 2026

Announced on 26th June 2026

(Mr. Prasert Sinsukprasert)

Chairman

Electricity Generating Public Company Limited

Electricity Generating Public Company Limited

IT System Security Guidelines for Users

1. Use of Artificial Intelligence (AI)

To provide guidelines for the responsible and lawful use of Public Artificial Intelligence (Public AI) and Corporate Artificial Intelligence (Corporate AI), taking into account potential impacts on other individuals, society, the Company, and legal compliance.

Key principles of use are as follows:

1. AI should be used constructively to create beneficial work and outcomes, and must not violate the law.
2. Safety in use must not cause harm or damage to individuals, property, or the Company.
3. The accuracy of AI-generated information must be verified before use.
4. Use must respect the privacy rights of others; information must not be used inappropriately.
5. Users are responsible for the correct and appropriate further use of information obtained.

1.1 Guidelines for Acceptable Use of Artificial Intelligence Technology

1.1.1 Acceptable Uses

Users must apply artificial intelligence technology to support operations within the following specified contexts:

1. Data analysis, trend forecasting, and report generation
2. Writing and reviewing code or programs
3. Drafting letters or various documents
4. Providing advice or assisting as a preliminary problem-solving aid
5. Supporting research and academic work, such as assisting with literature/article reviews
6. Creating content for communications and public relations
7. Other tasks assigned by a supervisor

1.1.2 Prohibited Uses

1. AI must not be used for high-stakes or irreversible decisions (e.g., approvals, disciplinary considerations) without effective human-in-the-loop (HITL) oversight, ensuring human authority to intervene, override, or escalate before implementation.
2. Unverified data, or data that may distort or corrupt model performance (data poisoning), must not be input into AI systems.
3. AI systems must not be misused or deliberately used as a tool to compromise cybersecurity or carry out cyberattacks, without explicit authorization — including but not limited to using AI to search for vulnerabilities in other systems, generating malware

code, creating deepfakes for deceptive purposes, or writing highly convincing phishing messages.

4. Company data or personal data must not be entered into Public AI, to respect data privacy, safeguard personal data throughout its lifecycle, and comply with applicable data protection laws, thereby preventing leakage of sensitive information.
5. AI must not be used to create content that is illegal, violates moral standards, or may cause harm to individuals, the organization, or society.
6. AI must not be used to generate harmful content, such as content related to violence, terrorism, sexual abuse, racism, hate speech, or other unlawful acts.
7. AI must not be used to create content that infringes on the copyright or intellectual property of others.
8. Personal data should not be disclosed unnecessarily — such as facial scans, photographs, videos, or voice recordings. If contacted by, or in cases of impersonation of, an individual or a trusted organization, the authenticity of the source must first be clearly verified, in order to respect data privacy and prevent misuse of personal data — for example, to create realistic AI-generated fake information for deceptive purposes, or information that could mislead, distort facts, or potentially lead to unlawful acts.

1.1.3 Confidentiality and Personal Data Protection

1. Internal EGCO Group information and confidential data — such as passwords, contract documents, and project information — must not be used in conjunction with Public AI.
2. Company data must be used with Corporate AI, as Corporate AI provides data privacy protection, encryption, and secure coding practices, and will not use such data to train foundation models within Public AI.

1.1.4 Maintaining Information Technology System Security

1. Source code or scripts generated by AI must always be reviewed before actual use, applying secure coding practices to identify vulnerabilities and errors, thereby supporting the cybersecurity of the organization's information systems.
2. If any abnormal or suspicious AI behavior is detected, or a potential security vulnerability is identified, the supervisor or the IT Infrastructure and Security Department must be notified immediately.

1.1.5 Output Verification and Bias Mitigation

1. Users must always review content and outputs generated or analyzed by AI before use or publication, in order to identify and mitigate potential bias and ensure fair, non-discriminatory outcomes.

2. Caution must be exercised when using AI related to the evaluation or decision-making concerning individuals, to avoid bias and prevent impact on rights and equality.

1.1.6 Duties and Responsibilities

1. Users are responsible for the final decisions resulting from the use of data, advice, or outputs from AI systems, supporting clear accountability for AI-influenced outcomes.
2. Users must always review AI outputs before use or publication, as such outputs may contain bias or inaccuracies, taking into consideration accuracy, legal impact, fairness, and information security.
3. Users must report to their supervisor immediately if an AI system is found to be malfunctioning, producing biased outputs, or potentially causing negative impacts, supporting a clear process of accountability for investigating and addressing AI-related errors or harm.
4. When using content generated with AI assistance, the source must be appropriately disclosed to ensure transparency, so that stakeholders are clearly informed when interacting with AI-generated rather than human-generated content.
5. Users must be aware of the limitations of AI, which cannot yet think and respond in the same way as humans, and may still contain inaccuracies.
6. AI may be used as a tool to assist with work, but users should not rely entirely on it; outputs must always be reviewed and corrected.