



Artificial Intelligence Usage Policy



Artificial Intelligence Usage Policy

Amarin Corporations Public Company Limited (the "Company") recognizes the importance of artificial intelligence technology (Artificial Intelligence : "AI") technology, which plays a role in business operations, including management systems, data processing, data preparation, and strategic management to enhance the efficiency of organizational operations, customer service, and competitiveness. Therefore, in order for the adoption of AI in the business operations of the Company and its subsidiaries (collectively, the "Company Group") to enhance the effectiveness of organizational operations and enable the Company Group's business to achieve its objectives, and to be carried out responsibly with due regard to the safety of technology use, in accordance with applicable requirements and laws, in order to reduce the risks and impacts that may arise from the development and use of AI in an inappropriate manner, the Company has established this Artificial Intelligence Usage Policy to serve as a guideline for personnel at all levels of the Company Group.

1. Objectives

This Artificial Intelligence Usage Policy is established for the following objectives:

- To control the use of AI safely and responsibly, without causing negative impact on stakeholders, with due regard to the safety and protection of important data, confidential information, personal data, and copyrighted data, whether belonging to the Company Group or to relevant stakeholders, so that the use of AI complies with relevant requirements and laws, such as the Computer-Related Crime Act B.E. 2550, the Cybersecurity Act B.E. 2562, the Personal Data Protection Act B.E. 2562, the Copyright Act B.E. 2537, and their amendments.
- To enhance efficiency in various processes within the organization and in the Company Group's business operations by supporting the Company Group's executives and employees to learn and apply AI to business processes and business risk management appropriately and responsibly.

2. Scope

- This Policy applies to directors, executives, and employees at all levels of the Company and its subsidiaries, external service providers (Outsource) engaged by the Company or its subsidiaries to carry out information technology functions, and encourages customers, business partners, trading partners, and stakeholders of the Company Group to support and comply with this Policy.

- This Policy applies to the Company Group's operations in all activities that involve the use of AI and/or that relate to AI of all types and forms, whether currently existing or to be developed in the future, including AI developed by other persons and adopted by the Company Group, as well as AI developed by the Company Group itself.

3. Relevant Definitions

- **Company** means Amarin Corporations Public Company Limited.
- **Subsidiary** means an entity in which Amarin Corporations Public Company Limited directly or indirectly holds more than 50 percent of the total voting shares, or over which it has control.
- **Company Group** means Amarin Corporations Public Company Limited and its subsidiaries.
- **Artificial Intelligence (Artificial Intelligence : AI)** means technology developed to enable computer processing systems, robots, machinery, or various electronic devices to possess characteristics or behavior resembling that of humans, for the purposes determined by humans, such as learning, perceiving and responding to the environment, reasoning, imitating behavior, and problem-solving, among others. The Company procures and provides AI for use by the Company Group's executives and employees.
- **User Account** means the identification credentials (User Account) or access rights to and use of AI granted by the Company to executives, employees, or authorized persons to access and use AI
- **Internal Information** means the Company Group's confidential business information, confidential information, or important information of the Company Group, including any other information related to business operations, financial information, or the reputation of the Company Group, that has not yet been disclosed to the public.

4. Duties and Responsibilities

In order for the management under this Artificial Intelligence Usage Policy to be effective, the Company hereby sets out the duties and responsibilities of the relevant departments and individuals as follows:

(1) Board of Directors: To approve and oversee the Policy to ensure alignment with the Company's strategic objectives and good corporate governance principles, and to review the Policy to keep it appropriate for changes in the business and legal environment.

(2) Senior Executives:

- To allocate personnel, budget, and technology sufficiently and appropriately for operations related to information technology security and the use of AI.

- To promote knowledge and understanding among the Company Group's personnel and relevant stakeholders, emphasizing the importance of using AI responsibly, appropriately, and safely.

(3) Departments and Subsidiaries:

- To develop systems for storing and managing information and data related to AI so that they are secure and in compliance with applicable laws and requirements.
- To provide information on the development of systems for storing and managing information and data related to AI in use, including information on the control and management of security in the use of AI to the Information Technology Department ("IT Department") of the Company or its subsidiaries.
- To coordinate with the executives and IT Department of the Company or its subsidiaries, as well as relevant external agencies, in managing risks and disputes.

(4) Information Technology Department:

- To control, monitor, and provide advice on the development of systems for storing and managing information and data related to AI so that they are secure and in compliance with applicable laws and requirements.
- To monitor technology trends and threats related to information security and AI in order to recommend appropriate development approaches.
- To examine and monitor threats related to AI and to seek methods or establish appropriate preventive measures.

(5) Employees:

- To comply with relevant laws, as well as the policies, guidelines, and various measures established by the Company.
- To notify their supervisor and relevant persons upon discovering a threat, data breach, or use of information technology systems and AI in an inappropriate manner.
- To participate in training as required by the Company, or review activities, or activities to enhance knowledge and understanding related to information security and AI in order to be able to perform their duties in accordance with relevant laws, as well as the policies, guidelines, and measures established by the Company.

5. Guidelines

(1) Do not use AI under the Company Group's user account to create content that violates applicable laws, rules, or regulations that are relevant, including content that is infringing or inappropriate; and do not use AI to create or disseminate content that is false, or intended to distort or

misrepresent information, or to mislead others, as well as content that infringes the copyright or any intellectual property of others.

(2) Do not use AI under the Company Group's user account to carry out any action that would cause the Company Group's activities or operations to be disrupted, delayed, or unable to function normally.

(3) Comply with the various requirements and standards established for the development and use of AI.

(4) Do not use AI to analyze or make decisions related to personal rights, such as discrimination or differentiation based on race, gender, religion, or individual capability.

(5) Do not use AI for significant decisions or matters that require human judgment, without human review, screening, and verification, in order to prevent errors, injustice, or undesirable effects on the rights and/or interests of the Company Group, such as decisions on actions that will have legal effect.

(6) Do not use AI under the Company Group's user account to seek personal benefit or benefit for others unrelated to the Company Group's work activities, such as using AI to make personal profit from information obtained through work, or using AI in activities that conflict with the interests of the Company Group.

(7) Do not use AI under the Company Group's user account to falsify or manipulate the results of information obtained from AI in order to produce untrue results or for the purpose of deception.

(8) Do not use AI in a manner that causes damage or negative impact to the Company Group, whether directly or indirectly; and do not use or disclose internal information, confidential information, important documents, or information that may affect the Company Group's operations, in the use of AI under any circumstances.

(9) Do not use AI under the Company Group's user account to violate the privacy of any person; and do not use personal data, such as national ID numbers, copies of national ID cards, financial information, or the personal data of customers, business partners, directors, or executives, including the personal data of other employees or any other person, in the use of AI.

(10) Do not use or input into AI any internal information, information of the Company Group, confidential information, personal data, or any copyrighted or intellectual property information, or usage history, for processing, training, or developing/improving the AI of external parties, in order to prevent the risk of data leakage as well as damage to the reputation and image of the Company Group, unless approved by the top executive and the Information Technology Department.

(11) Do not fail to clearly and appropriately identify the source of content generated by AI as appropriate, so that the Company can trace the source, and in order to prevent the risk of unintentional infringement of the intellectual property of others, as well as breach of confidentiality obligations.

6. Usage Control

The Company requires the control of the use of AI in order to maintain the organization's information security, as well as to address the various risks that may arise from the use of AI that has not been approved by the Company, with the following principles:

(1) Require the use of AI approved by the Company for work related to the Company Group's business, and permit access to and use of AI only through the Company's user account.

(2) Establish a process for requesting approval to use AI in cases where it is necessary to use other AI that has not yet been approved by the Company.

7. Risk Management

The Company requires the risk management of the use of AI in various areas, such as data risk, risk arising from cyber threats, and risk of violation of personal data protection laws or personal rights, among others, so as to be appropriate to the nature of use, with the following principles:

(1) Identify the risks arising from the use of AI and establish an acceptable risk target (Risk Appetite), and ensure regular assessment and monitoring of the risks of using AI so as to control risks appropriately for the use, within the framework of the acceptable risk management policy.

(2) Manage the risks of using AI covering the development and use processes of AI appropriately, whereby the AI selected for use by the Company Group should be secure, accurate, and reliable, capable of controlling risks and explaining the source of the results from the AI used.

(3) Be responsible for the actions and outcomes of decisions made by AI adopted, within an appropriate governance framework, in accordance with the principles of using AI responsibly, transparently, and fairly.

8. Security

(1) Do not use information that may affect system security, such as passwords, details of system configuration, including important information of the Company Group that is not protected against data leakage, in conjunction with AI.

(2) The Company has appropriate information technology security measures in place to protect against unauthorized access to or use of AI that could lead to cyberattacks or cause damage to the security of the Company Group's information systems, or give rise to other threats, and to establish a plan to respond to and manage security incidents arising from the use of AI.

9. Responsibility for the Use of Artificial Intelligence

(1) All executives and employees of the Company Group must comply with this Artificial Intelligence Usage Policy, as well as any rules and guidelines the Company may subsequently establish, and any laws, regulations, rules, and orders of relevant government or regulatory agencies, or laws relating to

activities involving the adoption of AI for use, such as laws relating to personal data protection, intellectual property laws, laws protecting against violations of personal rights, among others, whether currently in force or to be enacted in the future.

(2) In the event that the Company Group suffers direct or indirect damage from an act or omission, negligence, intent, carelessness, deficiency, or violation of this Policy and applicable laws, the person responsible shall be deemed at fault and shall be subject to disciplinary action according to the severity of the offense. In addition, the Company Group retains the right to seek other legal remedies, such as compensation for damages incurred, and if such act constitutes an offense for which a penalty is prescribed by law, the person responsible shall also be subject to the penalty prescribed by law.

10. Communication and Training

The Company will ensure communication and promote training to build awareness and review the various guidelines related to the use of AI in a responsible manner, for executives and employees.

11. Policy Review

The Company requires this Artificial Intelligence Usage Policy to be reviewed annually or whenever there are significant changes in technology and law, and shall submit any amendments or changes to this Policy to the Board of Directors for approval.

This Artificial Intelligence Usage Policy shall take effect from 14 August 2026 onward.