Information Technology Governance Policy

Information Technology Governance Policy

Amarin Corporations Public Company Limited ("the Company") recognizes the importance of information technology as a key tool supporting the enhancement of organizational capability, both in management and business operations. Therefore, in order for the information technology operations of the Company and its subsidiaries (collectively, the "Company Group") to be conducted efficiently, securely, and reliably, with the information and information technology assets of the Company Group properly maintained and protected — preserving Confidentiality, Integrity, and Availability — and to ensure that the Company Group's information technology operations comply with relevant laws, regulations, guidelines, or international standards, the Company has established this Information Technology Governance Policy to serve as a guideline for divisions and personnel at all levels of the Company Group.

1. Objectives

This Information Technology Governance Policy is established for the following objectives:

- To establish a governance, operational, and management framework for information technology at the organizational level, so that all internal personnel and external parties concerned have a clear operational framework.
- To build knowledge and understanding among the Company Group's personnel so that they can correctly comply with the laws, policies, guidelines, or requirements relating to information technology of regulatory authorities and of the Company Group.
- To prevent problems or damage to assets, impacts on business operations, or damage to the reputation and credibility of the Company Group that may arise from improper use of information technology, emergency situations, or various threats.

2. Scope

This Policy applies to the directors, executives, and employees at all levels of the Company and its subsidiaries, including external service providers (Outsource) engaged by the Company or its subsidiaries to carry out information technology operations, as well as external persons or external organizations authorized to access, provide services to, or use the network systems, application systems, or any assets within the information technology systems of the Company Group.

3. Relevant Definitions

- **Company** means Amarin Corporations Public Company Limited.
- **Subsidiary** means an entity in which Amarin Corporations Public Company Limited holds, directly or indirectly, more than 50 percent of the total number of shares with voting rights or has control over the business.

- **Company Group** means Amarin Corporations Public Company Limited and its subsidiaries.
- **Information** means data, facts, news, and knowledge that has been recorded, processed, or handled by any means, and which can be used for the benefit of administration, planning, decision-making, and other purposes.
- **Information Technology System Assets** means property or items that are part of, or used in connection with, the Company Group's information technology systems, whether tangible assets such as hardware, computer equipment, and servers, or intangible assets such as usage rights, software, IP addresses, and domain names.
- **Internal Information** means the Company Group's trade secrets, confidential information, or material information, including any other information relating to business operations, financial information, or the reputation of the Company Group, that has not yet been disclosed to the public.
- **Artificial Intelligence (AI)** means technology developed to enable computer processing systems, robots, machinery or other electronic devices to possess characteristics or behavior resembling those of humans, in accordance with objectives determined by humans — for example, learning, perceiving and responding to the environment, reasoning, imitating behavior and problem-solving. The Company procures and provides AI for use by the executives and employees of the Company Group.

4. Duties and Responsibilities

In order for the administration under this Information Technology Governance Policy to be carried out efficiently, the Company has assigned the following duties and responsibilities to the relevant divisions and individuals:

(1) Board of Directors: Approves and oversees the Policy to ensure alignment with the Company's strategic objectives and good corporate governance principles, and reviews the Policy as appropriate in response to changes in the business environment and relevant laws.

(2) Senior Management:

- Allocates personnel, budget, and technology sufficient and appropriate for operations relating to information technology governance, in order to achieve the objectives of this Policy.
- Monitors and oversees the relevant divisions in implementing the Policy, and establishes guidelines, criteria, and operating procedures relating to information technology governance.
- Promotes education and understanding among the Company Group’s personnel so that they can properly and correctly comply with the Information Technology Governance Policy.

(3) Information Technology Department:

- Controls, monitors, provides guidance to, and evaluates the Company Group’s personnel in complying with this Policy, as well as with laws and other policies or guidelines relating to information technology governance.

- Monitors technology and threat trends, and changes in relevant laws and standards, in order to develop or recommend approaches for developing the Company Group's information technology systems to be efficient and secure.
- Supports the organization of training or knowledge-review activities relating to information technology governance guidelines for the Company Group's personnel.

(4) The Company Group's Employees:

- Comply with the Information Technology Governance Policy, as well as laws and other policies relating to information technology governance.
- Notify their supervisor or the IT Department upon discovering any act that violates the law, this Policy, or other policies and/or guidelines of the Company Group relating to information technology governance.
- Attend training or knowledge-review activities relating to information technology governance guidelines organized by the IT Department or the Human Resources Department of the Company or its subsidiaries.

In this regard, where damage occurs to the Company Group's information or information technology systems as a result of deficiency, negligence, or violation of the Information Technology Governance Policy, including laws and policies or guidelines relating to information technology governance, such act shall constitute an offense subject to disciplinary action under the regulations of the Company or its subsidiaries, or under the terms of the employment contract, and may also be subject to penalties as prescribed by relevant laws, rules, regulations, or orders.

5. Policy

5.1 Allocation and Management of Information Technology Resources

In order for the allocation and management of information technology resources to align with the organization's strategy, the Company requires Senior Management, the IT Department, and relevant divisions of the Company or its subsidiaries to:

(1) Establish criteria and factors for prioritizing information technology plans in line with the organization's strategy or business objectives.

(2) Define the duties and responsibilities of divisions and IT Department personnel for allocating and managing information technology resources.

(3) Prepare and approve an information technology budget consistent with the organization's budget and strategy.

(4) Provide sufficient human resources for information technology work, continuously develop the skills of such personnel, and consider engaging external IT personnel when necessary.

5.2 Information Technology Risk Management

(1) Requires that information technology risk be managed in accordance with the organization's Risk Management Policy.

(2) Requires that the security of information technology systems be maintained so that the Company Group's information systems remain continuously available, as part of the Company Group's business continuity management.

(3) Requires the management of incidents that may affect the security of information systems, with clearly defined management procedures and responsible persons, so that such incidents are resolved or handled correctly, efficiently, and within an appropriate timeframe.

(4) Requires the management of assets within the information technology system, with clearly designated responsible persons and duties, so that important IT system assets are appropriately protected.

5.3 Information Security, Cybersecurity, and Data Protection

The Company requires policies and guidelines on maintaining security within information technology systems to control, oversee, and set standards for the use of, or operations relating to, information and the information technology systems ("IT Systems") of the Company Group, and to serve as guidelines for the Company Group's employees and relevant parties to follow, covering the following matters:

(1) Access Control and Information Technology System Security

(1.1) Access to the Company Group's IT Systems is controlled and restricted by the Information Technology Department ("IT Department") in accordance with operational necessity, appropriately tiered, and limited to legitimate access rights only. Important application systems and data shall be maintained, stored, and protected in accordance with the Company Group's policies and applicable laws, and auditable records of access requests shall be kept.

(1.2) Access to the Company Group's IT Systems requires user registration following identity verification, using the individual's own username and password only. Employees are prohibited from sharing usernames and passwords with other employees, and are prohibited from granting, delegating, or allowing any other employee or person to use their username and password under any circumstances. In addition, passwords must be set securely to enable identity verification for system use, to enable identification of the person responsible for records entered into the system, to enforce tiered access to data according to appropriate access rights, and to enable identification of users on the Company Group's network traffic.

(1.3) Access to data according to its level of sensitivity, and the storage of information in application systems, requires data to be classified by level of importance and categorized according to function, mission, division, or department, with defined methods for managing and protecting each data category, including access to and protection of sensitive personal data (as defined under the personal data protection law), and defined procedures for handling important data prior to the disposal, replacement, or reuse of equipment.

(1.4) Access to server rooms is controlled to maintain the security of application systems, network systems, and data of the Company Group, by restricting access to rooms where network equipment or equipment used with the Company Group's IT systems is installed and stored. Where a person without a related duty needs to access such a room, a record of the name, time, and reason for entry must be kept for later audit purposes, and a person responsible for the server room must oversee and control visitor access to that area.

(1.5) Server room security requires the installation of fire suppression systems suitable for computer and electronic equipment in such rooms, to minimize damage to equipment when activation is necessary, along with backup air-conditioning systems and adequate emergency backup power systems appropriate to the importance level of each system, and a maintenance schedule for equipment to ensure continuous availability of application and network systems.

(1.6) Control of network access, both from internal and external networks, requires that any person seeking access first obtain approved access rights from the IT Department, undergo an authentication process using a username to establish identity and a password to enter the domain before use, and requires that the connection path between the Company Group's computer network and the internet be routed through the control, monitoring, and security systems designated by the Company Group, with the network designed with zoning to enable effective, secure, and auditable protection against threats in the event of abnormal incidents.

(1.7) Control of wireless network access, to prevent unauthorized access to the Company Group's IT systems, requires an authentication process using a username to establish identity and a password to enter the domain before use; or, in the case of visitors conducting business with the Company Group (Guests), requires approval through the Company Group's guest wireless network registration system (Guest Wi-Fi), or registration of the connecting device's MAC Address (Media Access Control Address) with the IT Department for approval prior to use.

(1.8) Control of access to application systems, operating systems, databases, applications, and utility programs, to prevent unauthorized access, requires that any person seeking access first obtain approval from the IT Department, undergo an authentication process using a username to establish identity and a password before use. Access to critical application systems shall be granted only within the scope of the user's job duties, subject to written approval from the relevant supervisor or authorized approver, or through a request made via the Company Group's access request system, to be recorded as auditable evidence. Access rights shall be revoked upon a change of duties or resignation, and granted access rights shall be reviewed regularly. In addition, the Company Group’s computers connected to the internet shall have antivirus software installed, and internet connections shall be routed through control, monitoring, and security systems.

(1.9) Requires the security of the Company Group's electronic mail (email) system to be maintained, including defining the duties and responsibilities of users in using the Company Group's email system. Employees must use only the Company Group's email system for communications relating to the Company Group's business, and the IT Department shall establish prohibitions, precautions, and usage rights, having regard to the security of the Company Group's IT systems.

(1.10) To prevent unauthorized access to the Company Group's IT systems, as well as to prevent the disclosure or theft of data, the Company Group's employees are responsible for setting and changing passwords for access to the Company Group's IT systems in accordance with the IT Department's control policy, must not leave their computer screens unattended without protection against unauthorized use by others, and must keep IT system assets of the Company Group in a safe place to prevent malicious persons from using such assets in a manner that could cause damage to the Company Group.

(1.11) To prevent risks from vulnerabilities that could be attacked application systems, the IT Department is required to continuously manage the installation of operating system patches. For the ERP system, which is a critical system of the Company, software and operating system patches deemed necessary shall be managed and installed within an appropriate timeframe, with testing conducted in a safe environment prior to production deployment. Where a critical system cannot be patched, the IT Department shall record it in the IT system's security exception list, for tracking and risk management in accordance with the defined management process.

(1.12) To monitor that patching of the ERP system is carried out continuously and effectively, the IT Department is required to conduct or coordinate a review of software and operating system vulnerability assessment results at least once a year, and submit the assessment report to management for acknowledgment and signature, for appropriate management consideration.

(2) Data Backup and Preparedness for Emergency Situations and Cyber Threats

(2.1) Requires a backup system for important data within the Company Group's IT systems, to ensure continuous, stable, and secure service availability, and requires that the backup system be inspected and maintained in a state of constant readiness for use, prioritizing backup of data within the Company Group's IT systems from most to least necessary, and assigning duties and responsibilities to officers responsible for inspecting and maintaining the data backup system.

(2.2) Requires regular backup of data in critical application systems within the Company Group's IT systems, considering the backup frequency, methods, and technology used to be appropriate to the importance of the data in the Company Group's application systems, as well as considering storing important application systems and data at another safe location ready for use. An IT Contingency Plan shall be prepared and a backup processing system arranged, so that the Company Group's core transactions can continue without interruption.

(2.3) Requires the IT Department, or in agreement with the division owning the data, to determine the backup cycle and data retention period, ensuring that the Company Group's data and databases are backed up regularly, completely, and continuously, and ready to be restored within the specified time when an emergency occurs.

(2.4) Defines the duties and responsibilities of IT Department officers in backing up data, verifying backed-up data, and restoring data, including the duty to evaluate and review the contingency plan for emergency situations, as well as defining responsibilities and procedures for handling emergency situations

that occur, whereby access to and retrieval of the Company Group's backup data shall be performed only by persons authorized by the Company Group and by the system administrators.

(2.5) Requires regular testing, at least once a year, of the media and systems used to store backups of the Company Group's important data and databases, with the test results reported to IT Department senior management, to ensure that application systems and data can be restored for use at all times or in the event of an emergency.

(2.6) Employees are responsible for keeping the Company Group's data in the designated safe locations, so that the backup system can restore the Company Group's data, and to prevent malicious persons from using such data in a manner that could cause damage to the Company Group. Employees are prohibited from backing up personal data or data unrelated to the Company Group's operations onto the Company Group's data systems.

(2.7) Requires the preparation of an appropriate Data Breach and Personal Data Breach management plan, covering incident notification, reporting, impact assessment, damage control, and compliance with relevant laws or requirements, and requires communication and awareness-building regarding such procedures among employees and relevant parties, so that incidents can be reported and responded to correctly and promptly.

(2.8) Employees and relevant parties are responsible for monitoring, reporting, and cooperating in the Company Group's Data Breach and Personal Data Breach management procedures. Upon discovering or suspecting that such an incident may have occurred, they must notify the Data Protection Officer (DPO) and the IT Department without delay, so that the impact can be assessed, damage controlled, and relevant legal and regulatory requirements complied with in a timely manner.

(2.9) Requires the preparation of an information technology business continuity and disaster recovery plan to serve as an operational guideline, including the preparation of a backup processing system and the resources necessary to connect to the primary and backup networks, so that the Company Group's core transactions can continue without interruption.

(2.10) To respond to IT system emergencies that affect the Company Group's business operations, a working group and personnel shall be established to manage such emergencies, with clearly defined roles, responsibilities, necessary procedures, and communication methods, in order to carry out the prepared plan.

(2.11) Requires the preparation of a Cyber Incident Response Plan, developed to cover information as well as the critical infrastructure components of application and network systems required by the Company Group's core business activities, with regular annual drills and reviews to ensure the plan can be effectively applied in an actual situation, with relevant management and employees required to be aware of and understand the prescribed procedures.

(2.12) To effectively respond to cyber threat incidents, a working group and personnel shall be established to respond to cyberattacks, with clearly defined roles, responsibilities, necessary procedures, and

communication methods, so that involved employees understand their roles and can perform their duties correctly and quickly when a cyber threat occurs.

(3) Audit, Risk Assessment, and Internal Data Control

(3.1) The Company requires an assessment of the Company Group's information technology risk, conducted by the Company Group's internal auditors or an independent External Auditor, at least once a year, so that the Company and its divisions are informed of the level of information technology risk and security within the Company Group.

(3.2) The Company requires every division to organize its work systems and workplaces to safeguard the Company Group's internal information, preventing such information from being disclosed to unauthorized persons or those without a need-to-know. The use or transmission of internal information shall be carried out only by persons with responsibility for it or who are authorized by an approving authority, and such processes shall be subject to review by the IT Audit.

(3.3) Employees whose work involves the Company Group's internal information are prohibited from disclosing such information, directly or indirectly, to any person, unless assigned as part of their duties and authorized by an approving authority.

(4) Building Awareness and Security Regulations within Information Technology Systems

(4.1) Regularly provide training on information security, cybersecurity, and data protection guidelines under the Company Group's Information Technology Governance Policy, and provide knowledge of relevant laws and regulations concerning their use.

(4.2) Publish the Information Technology Governance Policy on the Company Group's intranet, so that all Company Group employees can access it conveniently.

(4.3) Provide preventive measures by educating on usage guidelines and precautions for using the Company Group's IT systems, and establish penalties for employees found to have committed violations or improperly used IT systems, such as suspension of access or usage rights.

(4.4) Employees are responsible for strictly complying with this Policy. Any person who violates any provision of this Policy, or infringes the copyright of the Company Group's computer programs for their own benefit or that of others, or uses the Company Group's IT systems outside the scope of their duties or not for the benefit of the Company Group, shall be considered a breach of employee discipline.

(4.5) In the event that any computer or computer equipment is damaged or lost, the employee user, custodian, or assigned person shall immediately notify management or the designated representative, so that corrective action or damage mitigation can be carried out.

(5) Practices Relating to Computer Programs Procured, Created, or Developed by the Company Group or Employees

(5.1) The creation or development of computer programs for use by the Company Group must receive written approval from management or an authorized person designated by the Company Group.

(5.2) Copyright in computer programs created or developed by an employee in their capacity as an employee of the Company Group shall belong to the Company Group.

(5.3) Batch Processing must be carried out under appropriate controls, with a defined batch processing schedule and verification of data accuracy after processing, and must include data backup measures and monitoring systems to prevent damage that may arise from processing errors.

(5.4) The use of computer programs involving Artificial Intelligence ("AI") in work shall comply with the Company's AI use policy and guidelines, with due regard to data security. It is prohibited to use or disclose internal information, confidential information, important documents, or information that may affect the Company Group's operations, including personal data, in the use of AI. Furthermore, the accuracy of information obtained from AI must be verified before use, and the approval procedures for adopting secure AI for use within the Company Group must be followed.

(6) Management of External Information Technology Service Providers

(6.1) To ensure that the operations of the ERP system service provider, or any other system that the Company assesses to be equally critical to business operations, can comply with the security requirements under the Company's policy, the IT Department shall, prior to selecting a service or entering into a contract, have the right to access, review, and assess the service agreement, to ensure that the services received comply with the Company's security requirements.

(6.2) Requires the regular management, monitoring, review, and evaluation of the performance of the ERP system service provider, or any other system that the Company assesses to be equally critical to business operations, in order to prevent risks that may arise from the operations of external service providers.

6. Policy Review

The Company requires this Information Technology Governance Policy to be reviewed annually, or whenever there is a significant change, and to be submitted to the Board of Directors for consideration and approval if any revision or amendment to the Policy is made.

This Information Technology Governance Policy shall be effective from August 14, 2026 onward.