Information Technology (IT) Policy

Information Technology (IT) Policy

Amarin Corporations Public Company Limited

Objective

To ensure that the information systems of Amarin Corporations Public Company Limited (the "Company") are secure and reliable, and to prevent any actions that may cause the information systems to malfunction, operate inconsistently with designated instructions, or otherwise disrupt their normal operations. This policy also aims to prevent any unauthorized access to information, as well as the improper modification, destruction, or disclosure of data belonging to other users within the information systems. In addition, the information systems must not be used to disseminate false information that may cause damage to the Company. The use of the Company's information systems must comply with applicable laws, including the Computer Crime Act B.E. 2550 (as amended).

Definitions

"The Company" means Amarin Corporations Public Company Limited.

"Managing Director" means the Managing Directors of the respective business units within the Company.

"Information Technology Department" means the Information Technology departments of the respective business units within the Company.

"Information Technology Manager" means the manager responsible for the Information Technology Department of the respective business units within the Company.

"Assets" mean the Company's hardware, software, and information data under the supervision of the Information Technology Department.

"Network System" means the Company's computer network infrastructure under the supervision of the Information Technology Department.

"User" means employees, staff, or any other persons authorized by the Company to perform work under contracts, agreements, or purchase orders.

"System Administrator" means an employee assigned by the Information Technology Manager to be responsible for maintaining and managing the network system, including access to network programs and the administration of network databases.

Responsibilities of the Information Technology Department

- Managing and safeguarding the Company's information technology assets, including hardware, software, and information systems.
- Ensuring that the Data Center Room is designated as a secure area with controlled access, allowing entry only to authorized personnel.
- Performing regular data backup in accordance with the Company's procedures for data backup and data restoration.
- Establishing and maintaining an Information System Disaster Recovery Plan (DRP) to ensure the Company can respond to incidents or disasters and restore systems within the defined recovery objectives.
- Managing user accounts and passwords to ensure that users can access the network and information systems according to their assigned access rights, including the management of privileged or special user accounts as specified in Appendix A.
- Managing and resolving information technology incidents and issues in accordance with the Company's IT incident management procedures.
- Reviewing and testing new or modified information systems before deployment to ensure that such changes do not adversely affect existing information systems, in accordance with the procedures for requesting program modifications in the computer system.
- Implementing measures to prevent and detect malicious software, such as viruses, worms, trojans, spyware, and other threats.
- Controlling and monitoring remote access to the Company's network systems to ensure secure connectivity.
- Supervising and controlling services provided by external service providers (outsourcing) related to the Company's information systems to ensure compliance with the Information Technology Policy.
- Maintaining and retaining computer traffic data (log files) in compliance with the Computer Crime Act B.E. 2550 (as amended).

Information Security Policy

1. Access Control Policy

The Information Technology Department shall establish formal procedures for the registration of new personnel within the Company to ensure that users are granted access rights to information systems based on necessity and in accordance with their roles and responsibilities. Such procedures shall include the provision, modification, and revocation of access rights to the Company's information systems, including but not limited to computer applications (Applications), electronic mail (E-mail), Internet access, and wireless network systems (Wireless LAN). In addition, procedures shall be established for the timely removal or adjustment of access rights in cases such as employee resignation, termination of employment, or changes in job position or responsibilities within the organization, in order to maintain the security and integrity of the Company's information systems.

2. Accountability, Identification, and Authentication

2.1 Users are responsible for protecting and maintaining the confidentiality of their user accounts, usernames, and passwords. Each user must have their own unique username and password and must not share them with others. Users are strictly prohibited from disclosing or allowing others to access their passwords.

2.2 Users must create strong passwords to ensure adequate security. Passwords must consist of at least seven (7) characters, including a combination of alphabetic characters, numerical characters, and special characters.

2.3 Users must not reuse previously used passwords and shall maintain a password history of at least four (4) previous passwords.

2.4 Users must change their passwords every ninety (90) days, or whenever prompted by the system to do so.

2.5 Users must complete the authentication process before accessing any of the Company's information assets or information systems. In the event of any authentication issues, such as account lockouts or password errors, users must immediately notify the System Administrator.

2.6 Users should avoid allowing computers or systems to store or remember usernames and passwords (e.g., "Remember Password"), as such practices may allow unauthorized persons to access the user's credentials.

2.7 Users shall be responsible for any actions performed under their user accounts, regardless of whether such actions were performed by the users themselves or by other persons who gained access to their accounts.

3. Asset Management

3.1 Users are strictly prohibited from entering the Data Center Room, which is designated as a restricted area, unless prior authorization has been granted by the Information Technology Manager.

3.2 Users must not connect any unauthorized devices, equipment, or tools to the Company's network for personal business purposes.

3.3 Users shall be responsible for any damage caused to the Company's assets if they install, modify, duplicate, or attach any hardware, software, or equipment to the Company's systems without prior authorization from the Information Technology Department, or without prior coordination and consultation with the System Administrator.

4. Corporate Information Management

4.1 Users must exercise due care and awareness when using any information, whether such information belongs to the Company or to external parties.

4.2 All information stored within the Company's information assets shall be considered the property of the Company. Such information must not be disclosed, modified, duplicated, or destroyed without prior authorization from the Managing Director.

5. IT Infrastructure Management

5.1 Users are prohibited from running Peer-to-Peer (P2P) applications or other programs with similar risk levels, such as BitTorrent, unless prior authorization has been granted by the Managing Director.

5.2 Users are prohibited from running entertainment-related programs, such as watching movies, listening to music, playing games, or similar activities during the Company's working hours.

5.3 Users are strictly prohibited from intercepting or capturing data, including messages, images, audio, or any other information transmitted within the Company's information systems or network by any means.

5.4 Users must not perform any actions intended to circumvent or violate software license protection mechanisms.

5.5 Users must not perform any actions that may grant themselves higher privileges or priority in accessing system resources than those assigned to other users.

5.6 Users must not attempt to obtain, access, or use another person's personal credentials, including passwords or authentication information, for the purpose of accessing data or system resources.

5.7 Users must not install any device or perform any action that enables unauthorized access to the Company's information systems without prior approval from the Information Technology Manager.

5.8 Users are prohibited from publishing, storing, or distributing obscene or immoral content, as well as edited or manipulated images of other individuals in a manner that may cause damage to reputation, defamation, hatred, or embarrassment.

5.9 Users must not engage in any activities that infringe upon the intellectual property rights of others.

5.10 Users must not use the Company's assets for personal commercial purposes.

5.11 Users must not perform any actions that may disrupt, damage, degrade, or cause interruptions to the Company's information systems or network operations.

6. Preventing Malware

6.1 All user computers must have anti-virus software installed in accordance with the Company's approved security standards.

6.2 Any data, files, software, or other digital materials received from other users or external sources must be scanned for viruses and malicious programs before being used or stored in the Company's systems.

6.3 Users must remain vigilant regarding viruses and other malicious software at all times. If any suspicious activity or abnormal system behavior is detected, users must immediately report the incident to the System Administrator.

6.4 If a user discovers that their computer is infected with a virus or malware, the user must immediately disconnect the computer from the Company's network and notify the System Administrator without delay.

6.5 Users are strictly prohibited from creating, distributing, or transmitting computer viruses, malware, or any malicious software that may cause damage to the Company's information systems.

7. Electronic Mail Usage

7.1 To register for an electronic mail (e-mail) account, users must complete and submit the e-mail service request form of the relevant department to the System Administrator.

7.2 Users should not use another person's e-mail address to read, receive, or send messages unless prior consent has been obtained from the account owner. The e-mail account owner shall be responsible for all activities conducted through their e-mail account.

7.3 Users should log out of the e-mail system after completing each session to prevent unauthorized access.

7.4 When sending confidential information via e-mail, users should avoid indicating the sensitive nature of the information in the e-mail subject line.

8. Internet Usage

8.1 Users must not use the Company's Internet system for personal commercial purposes or access inappropriate websites, including but not limited to websites containing immoral content, content that may threaten national security, religion, or the monarchy, content harmful to society, content that infringes upon the rights of others, or any information that may cause damage to the Company.

8.2 Users must not disclose confidential or sensitive information related to the Company's operations through the Internet before such information has been officially announced. Users must exercise caution when downloading programs from the Internet. Any software download or update must comply with applicable copyright laws and licensing requirements.

8.3 When using online discussion forums or social media, users must refrain from posting comments or messages that are offensive, defamatory, provocative, or that may damage the reputation of the Company or harm relationships with personnel from other organizations.

8.4 After completing Internet usage, users must close the web browser to prevent unauthorized access by other individuals.

9. Information Disclosure and Termination of Information System Services

9.1 The Information Technology Manager may access or disclose users' communication data when required by law, in response to lawful requests, or when necessary to protect the rights or property of the Company or other users.

9.2 The Information Technology Manager may suspend or revoke user access rights if a user account has not been used for a period exceeding ninety (90) consecutive days.

9.3 The Information Technology Manager may terminate system services without prior notice if it is found that a user has violated the Company's IT policies or caused disruption to the network services.

10. Software Licensing and Intellectual Property

10.1 The Company recognizes the importance of intellectual property rights. Users may request to use software licensed by the Company only when necessary for their work responsibilities. Users are strictly prohibited from installing or using any unlicensed software. Any violation involving copyright infringement shall be considered the personal responsibility of the user.

10.2 Software provided by the Company is intended solely for work purposes. Users are prohibited from installing, uninstalling, modifying, altering, or copying such software for use outside the Company without proper authorization.

11. Law and Compliance

All applicable laws and regulations in Thailand, together with the Company's Information Technology Policy, must be strictly observed by all users. Users must not engage in any activities that violate such laws or regulations. Any violation shall be considered a personal offense, and the user shall be solely responsible for the consequences arising from such actions.

Announced on 1 January 2026.