

Information Security Management Basic Policy

September 2nd, 2019

Arithmer Inc. (hereinafter "we" or "the company") recognizes the importance of managing all information assets handled in the company's AI solution business activities, including information entrusted by our customers. We also believe that it is the company's responsibility to protect such information from various security risks and to maintain trust of our customers. In order to achieve this, we will promote activities related to information security by establishing basic and individual policies on information security, and by setting appropriate security objectives while considering legal and regulatory requirements and providing security related contract obligations.

1. Basic Policy

- (1) We will establish an office to build and operate the Information Security Management System (ISMS) and will take the most appropriate security measures in promoting security activities.
- (2) Directors and employees will act in accordance with the company's security rules and will strive to prevent the occurrence of incidents, and in the unlikely event of a security incident, appropriate measures, including measures to prevent reoccurrences will be taken.
- (3) We will conduct educational activities related to information security.
- (4) We will periodically review our information security policy in response to changes in business operations, organization, and technologies. Additionally, we will continuously improve our information security system.
- (5) In order to practice the information security policy, we will emphasize top management responsibilities to enhance security.

2. Individual Policies

- (1) Mobile Device Policy JIS Q 27001:2014 Appendix A Management Policy Item A.6.2.1
 - A. The use of mobile devices for business purposes will be limited to those permitted by the company.
 - B. Security settings will be applied to mobile devices.
 - C. Files used by the mobile devices will be encrypted.
 - D. The devices will be protected against malware.
 - E. The usage of the devices outside of the company will be restricted.
 - F. We will take great care when handling the mobile devices.
- (2) Access Control Policy JIS Q 27001:2014 Appendix A Management Policy Item A.9.1.1
 - A. Access to the system will be granted on a business need basis.
 - B. Access rights will be reviewed regularly.
 - C. Passwords will be management by our officers.
 - D. No unnecessary external connections will be made.
- (3) Cryptographic Controls Policy JIS Q 27001:2014 Appendix A Management Policy Item A.10.1.1

- A. The use of encryption will be limited or restricted.
 - B. The number of administrators responsible for managing the cryptographic keys will be limited.
 - C. All types of cryptographic keys, including those with technical vulnerabilities, will be managed promptly.
- (4) Clear Desk and Clear Screen Policy JIS Q 27001:2014 Appendix A Management Policy Item A.11.2.9
- A. All employees will always keep their desks organized and will not leave unnecessary information assets on their desks after work.
 - B. Important information assets that require careful handling will be used only when necessary. Paper documents will be kept under lock and key, and electronic medium will be kept within appropriate access control.
 - C. Personal computers will be logged off when they are not used for an extended period. They will be protected by locks and secured by passwords.
 - D. We will set up passwords for when screen savers are activated.
 - E. We will not leave information assets unattended for an extended period at delivery locations and fax machine trays. In addition, sensitive documents will be promptly retrieved from the printer.
- (5) Backup Policy JIS Q 27001:2014 Appendix A Management Policy Item A.12.3.1
- A. The amount of data used for backup will be limited.
 - B. Backup data will be decentralized.
- (6) Commissioning Policy (Access Management)
- JIS Q 27001:2014 Appendix A Management Policy Item A.15.1.1
- A. The number of commissioners will be limited.
 - B. We will clarify security agreements with our commissioners.
 - C. Security agreements with commissioners will be reviewed regularly.
 - D. The access rights granted to the commissioners will be limited and regularly reviewed.

Yoshihiro Ohta
President, Chief Executive Officer
Arithmer Inc.