

We have established an Information Security Policy.

Arithmer Inc. (hereinafter referred to as "the Company"), as an AI solution company, recognizes the proper management of all information assets handled in the course of the Company's business activities, including information entrusted by customers, as an important management issue, and considers it the Company's responsibility to protect such information assets from various security risks and maintain customer trust. We believe that it is our responsibility to protect these information assets from various security risks and maintain the trust of our customers. In order to achieve this, the Company will establish a basic policy and individual policies for information security, set appropriate security objectives in consideration of legal and regulatory requirements and contractual security obligations, and promote activities related to information security.

1. Basic Policy

- 1) We shall establish a secretariat to establish and operate an ISMS (Information Security Management System), take optimal security measures, and promote security activities.
- 2) Directors and employees shall act in accordance with the Company's security rules and strive to prevent the occurrence of accidents related to information assets, and in the event of an accident, promptly take appropriate measures, including measures to prevent recurrence.
- 3) We will conduct information security education and awareness activities.
- 4) We will periodically review our information security policy in response to changes in our business, organizational changes, and technological changes, and continuously improve our information security system.
- 5) We will fulfill our responsibilities as top management to implement and support the Information Security Policy.

2. Individual Policy Groups

- 1) Mobile Device Policy [JIS Q 27001:2014 Appendix A, Control Measure A.6.2.1].
 - (a) We will limit the use of mobile devices for business purposes to those authorized by the company.
 - (b) We will apply security settings to mobile devices.
 - (c) Consider encrypting files.
 - (d) Protect against malware.
 - (e) We restrict the use of mobile devices outside the company.
 - (f) We will use mobile devices with the utmost care.

- 2) Access control policy [JIS Q 27001:2014 Annex A, Control Measure A.9.1.1]
 - (a) Access rights to the system are granted according to business needs.
 - (b) Access rights are periodically reviewed.
 - (c) Passwords are managed.
 - (d) Unnecessary external connections are not made.
- 3) Encryption management policy [JIS Q 27001:2014 Annex A Control measure A.10.1.1].
 - (a) The use of encryption shall be limited and restricted.
 - (b) Encryption key administrators shall be limited.
 - (c) Encryption keys, including technical vulnerabilities, shall be managed.
- 4) Clear Desk/Clear Screen Policy [JIS Q 27001:2014 Annex A Control Measure A.11.2.9]
 - (a) All employees shall keep their desks clean and tidy at all times and shall not leave unnecessary information assets on their desks after work.
 - (b) Important information assets that require careful handling shall be handled only when necessary, with paper media kept under lock and key and electronic media kept within appropriate access privileges.
 - (c) Terminals will be logged off when away from the office for extended periods of time and locked or wired and password-protected when not in use.
 - (d) A password-protected screen saver will be set.
 - (e) Information assets will not be left unattended for extended periods of time at mail drop points or unattended facsimile machines. In addition, we will promptly retrieve highly confidential documents from the printer.
- 5) Backup policy [JIS Q 27001:2014 Annex A Control measure A.12.3.1]
 - (a) Backups shall be limited.
 - (b) Backups shall be distributed.
- 6) Outsourcing policy (access control) [JIS Q 27001:2014 Annex A control measure A.15.1.1]
 - (a) The number of contractors shall be limited.
 - (b) The security-related contract with the recipient is clarified.
 - (c) Security agreements with contractors are periodically reviewed.
 - (d) Access rights granted to contractors are limited and periodically reviewed.

September 2, 2019
Arithmer Inc.
Founder & CEO
Yoshihiro Ohta