Security White Paper

Multi-Sigma®（AI Analysis Platform）

Version 1.3

September 1, 2025

AIZOTH Inc.

Introduction

Purpose of this White Paper

Multi-Sigma® is our cloud-based service that applies machine-learning models including deep-learning networks to analyze your data. It supports:

- Predicting outputs for previously unseen inputs
- Identifying the factors that influence those outputs
- Optimizing input variables to achieve desired results

This document explains the security policies and process framework that govern the cloud services underpinning Multi-Sigma®. It also serves as our public disclosure in accordance with ISO/IEC 27017, the ISMS cloud-security certification.

Intended Audience

- Organizations and individuals considering the adoption of Multi-Sigma®
- Current users of Multi-Sigma®

Cloud Service Information Security Policy

We have established our Cloud Service Information Security Policy and are committed to delivering functional and secure services that satisfy our users.
Our Cloud Service Information Security Policy is available at the following URL:
https://aizoth.com/en/cloud-service-information-security-policy/

Information Security Policy

We have established our Information Security Policy and, as a provider of machine learning and data science solutions, regard the protection of information assets entrusted to us by our customers as a top management priority.
Our Information Security Policy is available at the following URL:
https://aizoth.com/en/security-policy/

Information Security Governance

We have appointed a Chief Information Security Officer (CISO) who holds overall authority and accountability for information security. In addition, we have established an Information Security Committee that oversees the operation and continual improvement of our

Information Security Management System (ISMS).

Organizational Controls

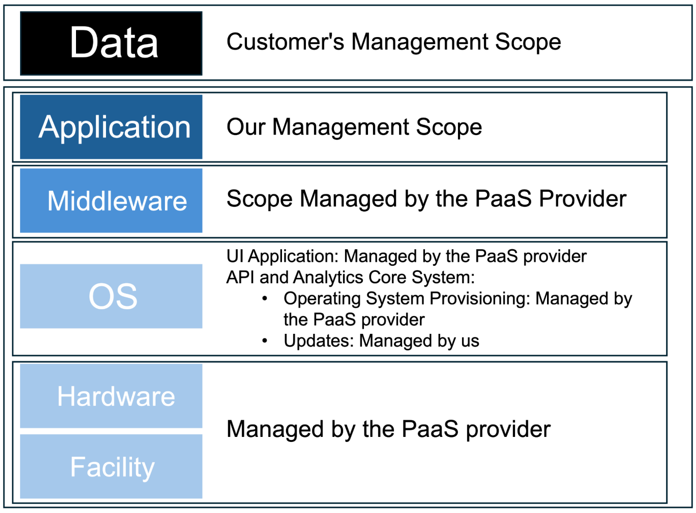
Scope of Responsibility (Shared Responsibility Model)

Virtual layer and facilities: Components in the virtual layer and at physical facilities are managed by the cloud-service provider that we use as our infrastructure.

Management of the cloud-service provider: In line with our Supplier Security Policy, we control the cloud-service provider through security reviews at the time of procurement and by monitoring its performance.

Applications: We are responsible for the applications we build on top of that infrastructure.

Data within the applications: Customers are responsible for protecting the data stored and processed in those applications.



Data	Customer's Management Scope
Application	Our Management Scope
Middleware	Scope Managed by the PaaS Provider
OS	UI Application: Managed by the PaaS provider API and Analytics Core System: • Operating System Provisioning: Managed by the PaaS provider • Updates: Managed by us
Hardware Facility	Managed by the PaaS provider

Responsibilities of Our Company

・Implementing security measures for Multi-Sigma®

・Protecting customer information stored in Multi-Sigma®

Responsibilities of the Customer

・Managing user accounts (creation, deletion, permission settings, administrator assignment, access-right configuration, etc.)

・Safeguarding users' secret authentication credentials such as passwords

・Backing up any data the customer handles

Geographic Location

Our company is headquartered in Japan, and customer data is stored in data centers located in Japan and the United States. If, due to the requirements of our underlying cloud platform (Google Cloud), it becomes necessary to store customer data in regions other than Japan or the United States, we will inform customers in advance before doing so.
For more information about our corporate address, please visit our website: https://aizoth.com/en/

Asset Management

Information Labeling

Multi-Sigma® offers directory-based file-management features that help customers classify their data. Within the service, this classification is handled through Project and Task management functions. For step-by-step instructions, please consult the Startup Guide.

Asset Segregation

Customer information assets stored on Multi-Sigma® are kept strictly separate from the assets we maintain to operate the service.

Data Handling After Service Termination

Customer data created or stored by users in Multi-Sigma® is deleted within 90 days of service termination. Including backup retention, the data may be preserved for up to 120 days after cancellation. Service-wide log data that does not contain customer information is exempt from this retention schedule.

Access Control

User Access Management

Multi-Sigma® provides intuitive, secure interfaces and functions that enable customers to manage user access with ease. Administrators can create accounts from the management console in just a few simple steps. For full instructions, please refer to the Startup Guide.

Credential Management

Initial account registration: Please follow the instructions we provide. During registration, you will be prompted on screen to create a password.
Password configuration: Set passwords in accordance with your own security policy.
Administrator privileges: Manage administrator rights strictly in line with your security policy.

Privileged Access

Administrator consoles and other privileged utility programs are accessible only to users with administrator rights. Strict control of these rights limits and secures the use of such utilities. For detailed instructions, please refer to the Startup Guide.

Cryptography

Data Encryption

All customer data stored in our databases is automatically encrypted with the AES-256 algorithm before being written to disk. No additional configuration is required, nor do customers need to modify the way they access the service. When an authorized user retrieves data, it is decrypted automatically and transparently. Communication between Multi-Sigma® and the customer is encrypted with SSL/TLS to mitigate the risk of eavesdropping and other threats.

Restrictions on Encryption Features

Multi-Sigma® is not provided in regions subject to export controls on encryption technology.

Operational Security

Changes

We notify customers in advance of any Multi-Sigma® updates that may affect them, using the email address registered with the service. Details of change-management activities are also available in the administrator console.

Backups

System and customer data are backed up daily. Backup files are retained for 30 days, full database backups and all stored files remain available for up to 30 days and are automatically deleted on the 31st day. We do not provide backup-data restoration or other recovery services at the customer’s request.

Logs

We collect the logs required to maintain and operate Multi-Sigma®. If you need access to these logs, please contact us via the inquiry form inside Multi-Sigma®. Multi-Sigma synchronizes its system clock with the time-synchronization service provided by our cloud platform (Google Cloud); all log timestamps are recorded and delivered in Coordinated Universal Time (UTC).

Operating Procedures

A Startup Guide is available that covers all operating procedures for Multi-Sigma®, including those for critical administrative tasks.

Clock Synchronization

Multi-Sigma® uses Google Cloud’s internal NTP service to keep its clocks synchronized with UTC. All virtual machines and containers in the cloud environment are synced to the same NTP source by default, and every log entry is timestamped in UTC. Because combining multiple NTP sources can introduce time discontinuities, we recommend synchronizing to a single authoritative clock.

Technical Vulnerability Management

If a vulnerability is discovered in the software used to build our applications, we notify customers on the Multi-Sigma® home page and immediately investigate the potential impact. Vulnerability information is gathered from:

- Advisories issued by the JPCERT Coordination Center, the Information-technology Promotion Agency (IPA), and Japan Vulnerability Notes (JVN)
- Findings reported by our own personnel
- Information supplied by customers, our cloud-service provider, or other external sources

Any detected vulnerability is promptly assessed and remediated, and the status of corrective actions is posted on the Multi-Sigma® home page as updates become available.

Administrator Procedures

In addition to manuals such as the Startup Guide, we offer Q&A support through the service’s inquiry form.

Cloud-Service Monitoring

Availability of the Multi-Sigma® web-application layer is managed by our PaaS provider. For the Multi-Sigma® APIs and analytics core, the provider is responsible for the underlying hardware, while the operating system is designed to revert to a clean state within one day.
We continuously monitor to confirm that Multi-Sigma® is operating normally, is not being misused (e.g., as a platform for attacks), and that no data leakage has occurred. The service does not currently expose these monitoring results to customers; if you require them, please contact us via the inquiry page within Multi-Sigma®.

Capacity and Performance Management

We monitor both server and network resources.

Load Balancing / Redundancy

Multi-Sigma® uses managed services provided by our cloud platform to distribute workloads across multiple virtual servers, implementing load balancing. The application architecture is saved as machine images, allowing replicas to be created instantly whenever needed.

Blue-Green Deployment

When a new version is released, our cloud service follows a blue-green deployment strategy. Both the current environment (green) and the new environment (blue) run in parallel, and traffic is switched over in an instant, enabling seamless migration to the new version.

Secure Disposal or Reuse of Equipment

We centralize responsibility for equipment disposal and reuse under our information-systems administrators, eliminating ad-hoc handling by individual employees and ensuring secure, reliable processes. For storage devices and other hardware within the cloud provider’s environment, disposal is performed in accordance with the provider’s official destruction procedures.

Communication Security

Network

Multi-Sigma® uses a Virtual Private Cloud (VPC) to construct its virtual network. Network isolation between different customers is implemented through logical separation of access resources by user ID. The customer environment and the management environment are each placed in separate network segments.

System Acquisition, Development, and Maintenance

Information Security Features

This White Paper describes the information security features that customers will primarily consider, as follows:

Functions (ISO/IEC 27017 Control Measures)	Descriptions in White Paper
5.16 Management of Identifiers	User Access Management
5.17 Authentication Information	Credential Management
5.18 Access Rights	User Access Management
8.2 Privileged Access Rights	Credential Management
8.3 Restriction of Access to Information	User Access Management
8.13 Information Backup	Backup
8.15 Logging	Logs
8.24 Use of Cryptography	Encryption
CLD.12.4.5 Monitoring of Cloud Services	Cloud Service Monitoring

Development Process

The development of our cloud services is guided by a policy that ensures not only functionality and usability, but also rigorous attention to information security. During development, we conduct tests in the development environment to detect potential bugs, performance issues, and insecure coding patterns. Moreover, we engage third-party vulnerability assessments both before and regularly after each release.

Blue-Green Deployment

When releasing a new version of our cloud service, we employ a blue-green deployment strategy. We provision the current virtual environment (green) and the new environment (blue) in parallel, then switch traffic instantly to the new version to enable seamless cutover.

Supply Chain

We manage the suppliers and overall supply chain for our cloud service delivery according to the following policies:

- Conduct pre-engagement reviews to verify that each supplier’s information-security posture is equal to or stronger than our own.
- Secure confidentiality obligations through binding contractual agreements.
- When a supplier relies on its own sub-suppliers to deliver services, evaluate the supplier’s capability to enforce security controls across its supply-chain partners.

Management of Information Security Incidents

Incident Response Process

We have established a standardized information security incident response process in accordance with ISO/IEC 27001. All procedures related to incident reporting and escalation are documented and centrally managed by our Information Security Committee. Reported incidents are handled based on their impact and urgency.

Incident Notification

If an information security incident related to Multi-Sigma® is detected, we will promptly notify affected parties with the following details:

Item	Details
Scope of Reporting	Information security incidents that may have a significant impact on customers, such as data loss or prolonged system downtime.

Disclosure Level of Response	Any information security incident caused by our company that affects customers will be handled at the same level of priority and transparency.
Notification Target Time	We aim to notify affected parties within 72 hours of incident detection.
Notification Procedure	Notification will be sent to the registered email address and displayed on the administrator console (Phone or other methods may be used as needed).
Contact Point	Multi-Sigma Support (for contracted customers only).
Applicable Response Measures	For any information security incident caused by our company that affects customers, we will take **all necessary actions** to address the situation.

If you detect, or suspect, a potential information security incident, please contact us through the inquiry form available within Multi-Sigma®.

Incident Report

If an information security incident related to Multi-Sigma® occurs, we will notify users using the methods described in Incident Notification above and also disclose it on our website. To date, there have been no information security incidents related to Multi-Sigma®.

Compliance

Applicable Laws and Contractual Requirements

The governing law for service agreements shall be the laws of Japan. For further details, please refer to our Terms of Use.

Evidence Collection

Pursuant to laws and regulations or requests from competent governmental or public authorities, we may disclose or submit information, including data on Multi-Sigma®, to such authorities or their designated recipients. When we receive a lawful request from these bodies, we will review its legal validity and, where permitted, provide prior notice and limit the disclosure to the minimum necessary. After the expiration of any period during which disclosure is prohibited, we will notify the customer to the extent possible. For details on consent and conditions, please refer to our Terms of Use.

Intellectual Property Rights

All intellectual property rights—including copyrights—related to the tangible and intangible components that make up this service (including but not limited to programs, databases, images, manuals, and other associated documentation) belong to AIZOTH Inc. For more information, please refer to our Terms of Use.

If you have any complaints or inquiries regarding intellectual property rights, please contact our support desk.

Protection of Records

Logs related to data operations within the application must be protected by the customer. We retain logs related to access to the virtual network as well as internal work logs associated with service version upgrades for a specified period.

Evaluation of Information Security Performance

We conduct internal audits of information security on a regular basis, at least once per year. In addition to scheduled audits, we perform independent internal audits in response to significant changes in organizational structure, facilities, technologies, or processes.

Disclosure of Internal Audit Results

Upon request from existing or prospective customers and other stakeholders, we can provide a summary of our internal audit results. We notify readers of this in this white paper and disclose the information according to the procedure below. The summary includes the audit period, scope, methodology, and whether corrective action plans are in place.

[Procedure]

Request: Contact the address below with the subject line “Request for Disclosure of Internal Audit Results Summary.”

Contact: info@aizoth.com

Eligibility Check: We confirm the requester’s legitimate interest and, where necessary, execute a Non-Disclosure Agreement (NDA).

Preparation: We compile a summary based on the latest audit results (with redactions

where appropriate).
Delivery: Provided as a PDF or equivalent format.

Information Security Awareness, Education, and Training

We provide regular information security training to all employees to raise awareness and promote secure practices. We also require contractual partners involved in cloud computing to maintain an equivalent level of education and awareness.

Scope of Security Responsibilities

For details on the delineation of responsibilities related to Multi-Sigma®, please refer to the Scope of Responsibility section under Organizational Controls.

Public Disclosure of System Status and Incidents

We publish information regarding Multi-Sigma®'s operational status, planned maintenance, and incident history on our website: https://aizoth.com/status-page/

Contact Information for Multi-Sigma®

Customer Support Desk
Phone：+81-050-3557-9379
Email：info@aizoth.com