MS-Sec ISMS Standard — Security Whitepaper (Public Edition)

Version: v2.0 (Public Edition) | Updated: Sep 2025
Company: MILLENNIUM SCIENCE GROUP CORP.

Disclaimer: This document provides an external overview of our security governance and control domains aligned with ISO/IEC 27001:2022. It is not a certification claim and does not disclose full internal standards or configurations.

1. About the MS-Sec ISMS Standard

The MS-Sec ISMS Standard defines our security governance model and requirements across the organization. It is aligned with ISO/IEC 27001:2022 and designed for a cloud-first, fully remote operating model. The standard is maintained by our internal security governance team and evolves through the Plan-Do-Check-Act cycle.

2. Alignment with ISO/IEC 27001:2022

Guided by ISO/IEC 27001:2022, this whitepaper outlines our security governance and key control domains.
We perform annual reviews to ensure our controls stay aligned with international best practices and continuously evolve with the threat landscape.

3. Scope

Our ISMS scope covers company information assets, cloud accounts and resources, source code and CI/CD pipelines, documents and communications, third-party suppliers (including AI/SaaS tools), and customer data processing activities.

4. Governance & Leadership

Executive commitment is set at the founder/CISO level with annual security objectives (e.g., zero material data breaches, 24-hour initial response to security incidents). Policies and procedures are version-controlled and reviewed annually.

5. Risk Management

We follow a structured cycle — identify, assess, treat, and monitor. Risks are quantified by likelihood and impact; both inherent and residual risk are tracked with defined treatment plans and due dates.

6. Control Framework (Overview)

Key control domains include:

• Identity & Access: SSO + MFA (FIDO2 first), least privilege, quarterly access reviews, break-glass safeguards.

• Cloud Baseline & Configuration: Infrastructure-as-Code baselines (e.g., CIS), private networking/endpoints, segmentation, and egress controls.

• Secure Development: Branch protections, SAST/DAST/dependency scanning, secrets management, SBOM, environment separation and data masking.

• Monitoring & Resilience: Centralized logging and alerting, daily backups with quarterly restore tests, multi-AZ architecture.

• Supplier & Privacy: Due diligence, contractual security clauses, DPA/SCC where applicable, and data subject request handling.

7. Cloud Shared Responsibility

We distinguish responsibilities between cloud providers and our organization: providers handle data center and hardware security, while we own identity/accounts, data and application configurations, secure development, monitoring, and response.

8. Compliance & Assurance

We do not claim ISO 27001 certification. The MS-Sec ISMS Standard is reviewed annually by our internal security governance team. Management review consolidates audit outcomes, key metrics, and risk status to ensure continual improvement.

9. Responsible Disclosure & Contact

Security researchers are encouraged to report potential vulnerabilities via responsible disclosure. Contact: contact@millenniumscience.io