INFORMATION SYSTEMS SECURITY POLICY

ATEXIS Security Policy reflects our fundamental principles and goals concerning information security, enabling us to improve how information is managed both internally and externally.

By developing, communicating, and continuously updating this policy, ATEXIS reinforces its dedication to protecting the **confidentiality** of the information we handle in the delivery of our services. We ensure the **integrity** of all processing activities and the **availability** of the associated information systems.

To accomplish this, we have established and implemented an **Information Security Management System** (ISMS) that ensures compliance with the highest standards for both our information systems and the data they handle—whether created, collected, stored, or processed. This includes:

- **Security in Human Resources Management** throughout the employee lifecycle.
- **Proper asset management** including information classification, appropriate handling of media, and implementing strong logical access controls for our systems and applications while effectively managing user permissions and privileges.
- **Protection of facilities and the physical environment** by designing secure workspaces and safeguarding equipment.
- **Operational security measures** that defend against malicious software, conduct regular backups, maintain monitoring logs, and oversee active software.
- **Management of technical vulnerabilities** along with the use of appropriate auditing techniques for our systems.
- **Secure communication protocols** to protect networks and ensure the integrity of information exchanges.
- **Ensuring security** during the acquisition and maintenance of information systems, while effective change management.
- **Safe software development practices** including separating development and production environments and conducting proper functional acceptance testing.
- **Control of supplier relationships**, with clear procedures for notification, response, and prompt learning.
- **Effective management of security incidents** through the establishment of clear channels for notification, response, and timely learning.
- **Implementation of a business continuity plan** to ensure service availability in the event of crises or disasters.
- **Compliance** with applicable regulations and legal requirements.
- **Regular review and continuous improvement** of our ISMS to ensure ongoing compliance and effectiveness.

All personnel within the organization are required to comply with this policy. We provide the necessary resources and support for its enforcement and assume responsibility for communicating its details, ensuring accessibility for all interested parties.

Approved by ATEXIS CEO the 8th of October of 2024