# INFORMATION SYSTEMS SECURITY POLICY

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

To ensure the effective delivery of services by ATEXIS, in terms of service levels, security, availability, and scope, the company's management is committed to strict adherence to all relevant legal requirements, creating value for its clients, and implementing a series of best practices through recognized reference models such as ISO Standards.

In addition, ATEXIS will take appropriate measures to safeguard against accidental or deliberate damage that may affect the **availability**, **integrity**, and **confidentiality** of the information processed or the services provided.

In line with this commitment, ATEXIS has developed its Information Security Policy, which establishes **security objectives** aligned with business needs, recognizes the value of the systems to be protected, and addresses the **risks** associated with these systems. That 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.
- **Information security risks**: By analyzing all services provided within the system's scope and establishing the necessary controls to mitigate identified risks.
- **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. ATEXIS executive management provide the necessary resources and support for its enforcement and assume responsibility for communicating its details, ensuring accessibility for all interested parties.

This document must be reviewed at least annually and/or whenever there is a change in context by ATEXIS Information Systems Security Officer (ISSO) and updated if any modifications are made.

**Denis Sauvage, CEO**

*Approved the 8th of October 2024*
*Updated the 17th of March 2025*