SYNTHETRIAL

INFORMATION SECURITY POLICY

Synthetrial's Management, within the scope of its authority to establish the organization's policies and strategies, has approved this Information Security Policy (hereinafter, the “Policy”).

The objective of this Policy, aimed at all stakeholders, is to define and establish the principles, criteria, and objectives for improvement that govern actions in the area of information security in line with the guidelines set out in the ISO27001 standard.

1. Purpose

Synthetrial considers the security of the information associated with its services to be one of the key factors in carrying out its activities, with the aim of guaranteeing confidentiality, integrity, and availability, protecting personal data, information privacy, and information systems against improper access and unauthorized modifications.

Part of Synthetrial's strategic policy is the implementation and development of an Information Security Management System based on the identification, protection, detection, response, and recovery of information systems, with the company's management providing the necessary resources to achieve this.

Synthetrial, aware of the need to integrate all the tools and resources necessary to provide its services efficiently, with quality, and in a secure information management environment, will focus on all measures and actions that reduce, minimize, transfer, or avoid risks and allow it to take advantage of opportunities for its Management System.

To this end, Synthetrial's management is committed to continuously improving the Information Security Management System in place, through regular annual reviews and by setting improvement objectives and actions.

2. Guiding Principles

Through this Policy and the development and implementation of the Information Security Management System, Synthetrial's management assumes and promotes the following general principles that should guide all its activities:

- Direct our efforts towards the prevention of errors, as well as their correction, control, and management.
- Encourage everyone to participate in achieving the objectives set by Synthetrial, which will benefit our employees, customers, and other stakeholders.
- Consider continuous training and awareness as one of the main pillars on which information security is based, providing the necessary training in this area to stakeholders through the establishment of training plans.

- Ensure that the company complies with all requirements demanded by customers, various administrations, and public bodies, as well as all applicable legal and regulatory requirements, with special emphasis on those established by information security legislation.
- Establish the necessary procedures for the control, monitoring, and prevention of incidents.
- Equip ourselves with tools and procedures that allow us to adapt quickly to changing conditions in the environment.
- Ensure the confidentiality, integrity, availability, and proper protection of data and information systems against unauthorized access, cyberattacks, and unauthorized modifications.
- Ensure business continuity in terms of information security by protecting critical processes against significant failures or disasters and developing continuity plans in accordance with internationally recognized methodologies.
- Perform adequate assessment, management, and treatment of information security risk to achieve a high level of maturity and minimize risk, prioritizing the measures and controls to be implemented in accordance with the identified risks and business objectives.
- Act appropriately and jointly to prevent, detect, and respond to cyber incidents that could affect information security.
- Establish the consequences of security policy violations, which will be reflected in contracts signed with stakeholders, suppliers, and subcontractors.
- Improve the efficiency of security controls in place to adapt to evolving risks and new technological environments.
- Review and evaluate information security periodically, taking the necessary measures to correct any deviations that may be detected.

Consequently, Synthetrial maintains the following application guidelines to be taken into account within the framework of the Information Security Management System (ISMS):

- The protection of personal data and individual privacy.
- The safeguarding of the organization's records.
- The protection of intellectual property rights.
- The documentation of the information security policy.
- The assignment of security responsibilities.
- Training and education for information security.
- The recording of security incidents.
- The management of changes that may occur in relation to security.

To ensure the principles of information security, Synthetrial establishes the following:

- **Confidentiality:** The information processed by Synthetrial will be known exclusively by authorized persons, upon identification, at the time and by the means provided.
- **Integrity:** The information processed by Synthetrial will be complete, accurate, and valid, its content being that provided by the data subjects without any manipulation.
- **Availability**: The information processed by Synthetrial will be accessible and usable by authorized and identified users at all times, with its own persistence guaranteed in the event of any foreseeable contingency.
- **Resilience:** To guarantee the above, Synthetrial has the necessary technical and organizational measures in place to enable constant adaptation to change and continuous improvement of the duly implemented Information Security Management System.
- **Legal compliance:** Consequently, Synthetrial undertakes to ensure compliance with all applicable legislation. Specifically, this includes current regulations on data protection, privacy, and information security.

This Information Security Policy was approved on 20/08/2026 by the Management of Synthetrial.