INFORMATION SECURITY POLICY

Contents

1.INTRODUCTION ____ 4
2.SCOPE ____ 4
3.INFORMATION SECURITY OBJECTIVES ____ 4
4.INFORMATION SECURITY PRINCIPLES ____ 5
5.RESPONSIBILITIES ____ 6
6.AUDIT AND CONTROL ____ 7
7.REVIEW OF THE POLICY ____ 7

KEY INFORMATION ON THIS DOCUMENT	
Identification document	Information Security Policy
Version	1.0
Lead Information Security Manager	Information Security Manager
Author	CIO
Approval Authority	Steering Committee
Approval date	15 December 2021

1. Introduction

At its meeting of 15 December 2021, the Steering Committee approved this Information Security Policy, which establishes the principles and guidelines with which ATLS (hereinafter the "Company") will protect your information in accordance with applicable regulations, ethical standards and any other applicable internal regulations.

This Policy will be available on the intranet for all employees and will be available on the corporate website for all the Company's interest groups. The Policy will also be subject to appropriate communication, training and awareness-raising activities for its timely understanding and implementation.

2. Scope

This Policy will be applied to ATLS and will bind all its employees, regardless of their position and functions.

ATLS will ensure that the information is protected, regardless of how it is communicated, shared or stored. This protection applies to both the information existing within the Company and to the information shared with third parties.

Information security is understood as the conservation and protection of:

- Information owned by the Company, regardless of whether it is in its own systems or those of third parties.
- Information owned by third parties in the Company's systems.

In accordance with the Policy, ATLS may develop procedures and instructions to implement and comply with its obligations, as well as to adapt it to any local legislation applicable to the Group.

Similarly, the application of this Policy is complementary to other mandatory internal standards, such as the Compliance Policy on personal data protection and privacy, and other regulations on matters related to Company information.

3. Information security objectives

This Policy establishes the reference framework by which ATLS defines the basic principles and rules of protection of the data managed by the Company, and has the following objectives:

- Understand and process operational and strategic **risks** in information security matters so that they remain at acceptable levels for the Company.
- Guarantee the level of **confidentiality** required of each type of data and prevent information leaks.
- Maintain the **integrity** of the data, avoiding alterations when it is generated by the owners or managers of the same.
- Ensure the **availability** of the data on all media and whenever necessary, ensuring business continuity and compliance with the obligations required of the Company.

4. Information security principles

This Policy is in response to the recommendations of best practices in information security, as well as in compliance with the current legislation on the subject of personal data protection and the regulations that, in the scope of information security, may affect the Company.

In addition, ATLS establishes the following basic principles as fundamental guidelines for information security that must always be taken into account in any activity related to data processing:

- **Use of information systems.** The use of information systems will be limited exclusively to performing tasks related to the job. These means and systems are not intended for personal use and may not be used for any unlawful purpose.
- **Information security in developed systems.** Development and production environments will be maintained in independent systems. The development and maintenance of information systems must take into consideration the implementation of the safety specifications.
- **Segregation of duties.** The risks arising from the absence of segregation of functions and the unipersonal dependence of critical functions for the business must be avoided.
- **Information retention.** Retention periods for the information will be set by category, when it is appropriate for operational or regulatory compliance needs.
- **Required resources.** Financing will be available to manage operational controls related to information security and management processes for its implementation and maintenance.
- **Risks.** The Company accepts the risks and is willing to tolerate those that, based on the information available, are understandable, controlled and processed when necessary.
- **Continuity.** A continuity management process will be established to ensure the recovery of critical data for the Company in the event a disaster event, reducing the time of business disruption to an acceptable level.
- **Compliance.** The Company's information and communications systems must be permanently in accordance with the requirements of the current legislation, as well as with the applicable internal development regulations.
- **Legal compliance.** Situations that expose the organisation to a breach of law and legal regulations will not be tolerated.

5. Responsibilities

Responsibility for the protection of data, and the systems that process, store or transmit it extends to all the organisational and functional levels of ATLS, each to the extent appropriate, as detailed below:

- All Company employees must know and comply with the Policy, and must maintain the confidentiality of the data handled in their workplace environment and must report any potential security incidents or problems detected immediately.
- Employees' use of digital systems or services, including email and instant messaging services, will be limited to legal purposes and exclusively related to job tasks. Thus, these services and systems are not intended for personal use and may not be used for any unlawful purpose.
- Contracts with third parties that involve access to data belonging to the latter, including those for the provision of services or contracts for outsourcing, must ensure that suppliers, subcontracted personnel or any external company that use or accesses the data, know and comply with the Policy as applicable, and must maintain the professional secrecy and confidentiality of the information handled in relation to the Company.
- The Information Security Officer is responsible for implementing this Policy and monitoring its compliance, as well as for all requirements arising from applicable laws, standards and good practices in the area of information security. The Information Security Officer will:
    - Implement an information security strategy to ensure compliance with the basic principles of this Policy.
    - Establish and review the relevant controls to ensure compliance with this Policy and its implementation regulations.
    - Prevent, detect and respond to any incident regarding information security and act in accordance with the provisions of the Incident Response Plan.
    - Promote training and awareness activities in the area of information security processes.
    - Establish a continuous improvement approach.
    - Ensure compliance with the current legislation in the field of the competences assigned to it by this Policy.
    - Review, update and report any changes resulting from variations to this Policy.

6. Audit and control

ATLS expressly reserves the right to adopt, with proportionality, the necessary surveillance and control measures to check the correct use of the systems it makes available to its employees, including the content of the communications and devices, in accordance with the current legislation and guaranteeing the dignity of the employee. The communication and acceptance of this Policy shall constitute legal employee notification.

The Company will undergo periodic reviews and controls, as well as internal and external audits to assess compliance with this Policy.

7. Review of the Policy

The approval of this Policy implies that its implementation will be supported by the Steering Committee to achieve all the objectives set out in it, as well as to meet all its requirements.

This Information Security Policy will be reviewed and updated whenever necessary, in order to adapt it to any changes that may arise, albeit operational, legal, regulatory or contractual, thus ensuring that the Policy is adapted at all times to the reality of the Company.