Information Security Policy

MOTIVATION

The lack of control by companies over how data and information are generated, where they are stored, and to whom they are transmitted entails the risk of security and regulatory compliance incidents that may have a negative impact on the business itself. Information security is, in fact, a primary asset of the company, and implementing effective measures can constitute a strategy that, over time, turns into a competitive advantage.

For this reason, Artificialy SA, specialized in artificial intelligence solutions, has always been at the forefront of information protection and security. A fundamental measure in this regard has been the implementation of an Information Security Management System, a set of organizational, technical, and procedural processes based on best practices and reference standards, also in compliance with the directives and the international standard ISO/IEC 27001:2022.

OBJECTIVES

The objective of Artificialy SA's Information Security Management System is to ensure a level of protection and security appropriate for the circulation of information within the organization, in order to best carry out the design, development, and delivery of company services.

Without procedures for identifying, evaluating, and analyzing risks, the security threats to which company services and procedures are exposed on a daily basis may compromise their proper functioning, with possible economic consequences.

The set of organizational, technical, and procedural measures established by Artificialy SA's Information Security Management System satisfies the following basic security requirements:

- Confidentiality: access to information is permitted only to those who have the appropriate privileges.
- Integrity: the management of information (including its modification) is subject to precise constraints established by the company's governance.
- Availability: authorized users may freely access information whenever they need to use it within operational processes, and retrieval is performed quickly and intuitively.

Artificialy SA aims to position itself in the field of information security as:

- A reliable and competent provider in preserving the company's image.

- A hub where the company's information assets are stored, safeguarded, and protected.
- A facilitator of business continuity for operational processes.
- A tool fully compliant with applicable and mandatory regulations, resulting in the growth of the company's information security expertise.

POLICY CONTENT

Any information necessary for carrying out internal activities, from product/service data to their configuration, must be protected throughout its lifecycle, from creation to use and finally disposal. The Information Security Management System is part of this process, enabling secure, accurate, reliable information management and timely information retrieval.

In accordance with the current ISO/IEC 27001:2022 standard, among the preventive measures required by the Information Security Management System is the mandatory assessment of security risks and their potential impact on the company, which must be carried out periodically by the Information Security Manager. The Information Security Manager must verify whether the above-mentioned security requirements are being met, analyze the critical factors that have led to security incidents, and place them within the broader context of strategic, business, and technological changes already implemented or to be implemented.

The purpose of this analysis is to assess the risk associated with each asset to be protected against the identified threats. The procedure adopted by the Information Security Manager to perform this assessment is shared with Management, which must approve the document de scribing the methodology to be applied. Furthermore, Management also contributes to defining the parameters used to determine the level of risk. Once the Information Security Manager has completed the assessment, the results are jointly reviewed with Management, which deter mines whether the level of risk is acceptable according to the previously established metrics. Finally, where deemed necessary, risk mitigation measures and actions to improve system security are defined based on priorities, the company budget, and the need to comply with applicable regulations. All decisions are made while taking into account the value of the information to be protected and the occurrence of events that may significantly affect system security.

RESPONSIBILITIES

Responsibilities are distributed as follows:

PERSONNEL, who are responsible for complying with the agreed information security policy and must report any anomalies they identify to the responsible manager.

THE INFORMATION SECURITY COMMITTEE, which meets at least every six months. It is composed of Management and the Information Security Manager, although employees with the necessary technical expertise may also be involved in evaluating specific matters. Management is responsible for establishing priorities and promoting information security initiatives while ensuring alignment with company strategies and the budget allocated to the project.

THE INFORMATION SECURITY MANAGER, who is responsible for drafting and de signing the Information Security Management System. Specifically, the Information Security Manager performs risk analysis and risk management by identifying the most ap propriate criteria and methodologies and is responsible for maintaining the necessary documentation, including document classification procedures. The role also includes proposing appropriate security measures and reviewing security incidents, together with the related corrective actions. Furthermore, the Information Security Manager is commit ted to promoting a culture of information security and proposing training programs for personnel.

EXTERNAL PARTIES who interact with Artificialy SA must comply with the specified security principles and, where this is not explicitly stated in the contract, sign a confidentiality agreement for the assigned engagement.

APPLICABILITY

This Information Security Policy applies to all internal and external bodies of the company and is binding on all Artificialy SA personnel. It also applies to any external party who becomes aware of information managed by the company. This requires prior regulation of agreements to ensure that communication with external parties takes place in compliance with applicable rules and regulations.

REVIEW

Artificialy SA shall ensure the periodic verification of the effectiveness and efficiency of the In formation Security Management System. Where necessary, and in accordance with the con text and business objectives, it shall adopt the measures required to improve the security policies and ensure their proper implementation, so as to guarantee the continuous and secure execution of all company processes.