ALMAVIVA GROUP INFORMATION SECURITY POLICY

04.08.2024
Version 1.0

ALMAVIVA GROUP INFORMATION SECURITY POLICY

TABLE OF CONTENTS

1. INTRODUCTION

Almaviva Group accompanies the growth of the country's system, supporting enterprises in the new challenges they must face in order to remain competitive in the digital age and innovating its own business model, organization, corporate culture, and information and communications technology.

Within the Group, information serves as a strategic business asset and violation or compromise of these assets can have serious repercussions for both the Group and the communities in which it is located in terms of: financial losses, higher operating costs, decreased efficiency, delays, inactivity and non-productivity of resources, legal and contractual violations, and, more generally, loss of competitiveness and reputation.

As a technology company, we are committed to contributing to sustainable development by leveraging the potential of technology for the benefit of society and driving transformation responsibly towards a better future for all.

2. OUR COMMITMENT

As the information society continues to evolve, with the interconnection of public and private networks, sharing of information, and interdependence between systems and services, it is crucial for all stakeholders to have a strong sense of responsibility in defending information assets and the tools used to manage them. To this end, we uphold the highest standards in the handling of the personal data of all stakeholders with whom we work, respecting their fundamental rights and freedoms, as well as the dignity of all those involved, and guaranteeing the confidentiality, integrity, and availability of information, protecting it from possible attacks or unauthorized use.

The protection strategy that we pursue as a Group in order to ensure the safety of the data and information we process is based on the principles of:

- ✓ confidentiality, to ensure that only authorized individuals have access to information
- ✓ integrity, to safeguard the accuracy and completeness of the information and methods used to process it
- ✓ availability, to ensure that authorized users have access to the information and to associated assets when required.

3. OUR PRINCIPLES

3.1. Information Security Management System

We place particular emphasis on the protection of information assets as a fundamental value of our corporate culture, within which we foster a culture of information security as a shared value to guide daily operations.

From this perspective, we are committed to respecting current regulations and the directives of our clients, implementing all possible measures to ensure the proper handling of personal data relating to our employees, representatives, service users, and, more generally, stakeholders.

In this regard, we have implemented an Information Security Management System (ISMS) inspired by international industry standards and best practices, such as standards ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1, and ISO/IEC 27018 and guidelines ISO/IEC 27017, ISO/IEC 27701, and ISO/IEC 27005.

The ISMS aims to:

- ✓ ensure the confidentiality of information
- ✓ prevent the alteration or loss of information assets
- ✓ guarantee the availability of information and services, including through suitable business continuity plans
- ✓ guarantee the authenticity of a piece of information's origin (non-repudiation)
- ✓ implement procedures for detecting and managing events and incidents
- ✓ guarantee the same level of information security, also with regard to the cloud services for which the Almaviva Group operates as both client and provide, in compliance with international guidelines.

We are committed to respecting all obligations of compliance with national and international legislation regarding the protection of personal data, cybercrime, intellectual property rights on software, and any other regulation applicable to the context, also with regard to the cloud services used or provided.

We guarantee the availability of information and services also through suitable business continuity plans, pursuant to the principles of the ISO 22301 standard.

3.2. Identification of Risks and Adoption of Safety Measures

We identify, evaluate, and analyze the risks that threaten the security of the company's information assets, implementing appropriate technological and organizational countermeasures and identifying opportunities for improvement.

We provide our employees with organized support, resources, and technologies according to specific policies and operational procedures.

3.3. Continuous Training

We develop a corporate culture of information security as a shared value to inspire daily activity.

To empower our employees and collaborators, as the organization's first line of defense we provide mandatory training in cybersecurity, teaching them how to recognize and avoid the primary risks associated with the use of digital technologies and avoid becoming unwitting victims of fraud, both in the workplace and in their personal lives.

Our goal is to transform individual behaviors, through the development of certain human characteristics, such as risk perception and readiness.

3.4. Supply Chain

In the Supplier Code of Conduct, we expressly commit to ensuring that the principles recognized and implemented by the Group regarding information are acknowledged and adopted throughout the supply chain.

We respect the contractual clauses with clients and suppliers that establish security constraints and guarantee the exercise of access rights.

4. ADDITIONAL INFORMATION

In implementing this Policy, the Almaviva Group pledges to continuously improve the document in order to verify the adequacy and functionality of the ICT System and review the measures put in place so that these remain consistent and appropriate with the corporate work environment.

The Information Security Policy of Almaviva Group is supplemented by other corporate policies and other principles, specifically:

- Group Policy
- Code of Ethics
- Supplier Code of Conduct
- Human Rights Policy
- Organizational Model "231"
- Whistleblowing Procedure
- Principles of the ISO/IEC 27001 standard on Information Security Management Systems
- Principles of the ISO/IEC 20000-1 standard on Service Management Systems
- Principles of the ISO 22301 standard on Business Continuity Management Systems

Details on the Almaviva Group's commitment to information security are available on Almaviva website in the *Corporate Governance* section and in the published *Sustainability Reports*.