Information Security Policy

Scope and Objective

The Information Security Policy applies to information assets and to the entire Organisation, namely the management structure and employees, and to all Stakeholders who are in any way related to Ascendi Information Systems, including suppliers, consultants and partners.

Its aim is to establish the guidelines and orientations for the Organisation's Information Security activity, in order to ensure a high level of protection for information and information assets and to promote the mobilisation and involvement of everyone, so as to guarantee compliance with the main pillars on which it is based: Confidentiality, Availability and Integrity.

Guidelines

- Ensure compliance with business, legal and regulatory requirements, as well as other relevant national and international Information Security standards;
- Ensure continuous improvement of the Information Security Management System as an integral part of information systems throughout the life cycle of applications and assets;
- Establish guidelines and tools for managing and controlling access to the organisation's information systems, ensuring appropriate levels of segregation of access to critical business information;
- Prevent unauthorised access to facilities, damage to the Organisation's physical assets and interference with its normal activity;
- Ensure proper management of incidents and vulnerabilities that could compromise Information Security, the protection of personal data or business continuity;
- Ensure periodic, systematic risk analysis in Information Security with a view to continuous improvement, enabling potential internal and external threats to be identified and the appropriate technical and organisational measures to be adopted;
- Promote awareness and provide ongoing training on Information Security so that all internal and external employees understand the importance of Information Security in the performance of their duties and responsibilities.

20th June 2023