INFORMATION SECURITY POLICY

The purpose of this policy is to describe the general information security principles defined by Visia Lab in order to develop an efficient and secure Information Security Management System pursuant to ISO 27001.

For Visia Lab, information security has as its primary objective the protection of data and information, of the technological, physical, logical and organizational structure, responsible for their management. This means obtaining and maintaining a secure information management system, through compliance with the following properties:

1. **CONFIDENTIALITY:** ensure that information is accessible only to those who are duly authorized to process;
2. **INTEGRITY:** safeguarding the consistency of the information from unauthorized changes;
3. **AVAILABILITY:** ensure that authorized users have access to the associated information and architectural elements when they request it;
4. **CONTROL:** ensure that data management is always carried out through secure and tested processes and tools

As part of the management of the services offered through its technological infrastructure, Visia Lab ensures:

- the guarantee of having appointed reliable partners to process its information assets;
- a high corporate image;
- full compliance with the Service Levels established with customers;
- customer satisfaction;
- compliance with current regulations and international safety standards.

For this reason, Visia Lab has developed a secure information management system following the requirements specified by the UNI CEI EN ISO/IEC 27001:2024+A1:2024 Standard and mandatory laws as a means of managing information security within its business.

Visia Lab's information security policy applies to all internal staff and third parties (e.g. service providers, maintenance, support...) who collaborate in the management of information and to all processes and resources involved in the design, implementation, start-up and ongoing provision of services.

Visia Lab defines, and validates at least once a year, the context in which it operates, the actors involved, the opportunities and possible risks impacted on its Information Security Management System.

Visia Lab's information security policy represents the organization's commitment to customers and third parties to ensure the security of information, physical, logical and organizational tools suitable for processing information in all activities.

The information security policy is based on the following principles:

a) ensure access control;
b) establish the classification (and processing) of information;
c) guarantee the physical and environmental safety of one's workplace;
d) adopt end-user themes, such as:
    1. acceptable use of assets;
    2. best practices regarding clean desk and screen;
    3. adequate transfer of information;
    4. regulated use of mobile devices and teleworking;
    5. limitations on the installation and use of software;
e) establish and perform backups at regular intervals;
f) establish procedures for the transfer of information in a secure manner;

g) provide protection against malware;
h) identifying, monitoring and managing the technical vulnerabilities found;
i) provide, if necessary, cryptographic controls;
j) ensure the security of communications;
k) comply with current regulations in the field of privacy and personal data protection;
l) regulate relations with suppliers from an ISO 27001 perspective.

This policy applies to all processes included in the ISMS (Information Security Management System).

Date: 03/06/2026

The Management

Marco Meoni