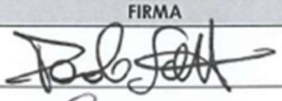
	RUOLO	NOME E COGNOME	FIRMA	DATA
Redattore	IT Manager ISMS Manager	Paolo Scotti		01/09/2025
Verificatore	COO & CIO	Jean-Paul David		01/09/2025
Approvatore	CEO	Thibaut Fraisse		01/09/2025

INDEX OF REVISIONS	
Rev.	**Reason for review**

ATTIVITÀ DI DIVULGAZIONE	MODALITÀ DI DIFFUSIONE
☑ INFORMAZIONE ☐ FORMAZIONE (in carico al responsabile di reparto/funzione o da QA/HSE) ☐ ADDESTRAMENTO (in carico al responsabile di reparto/funzione o da QA/HSE)	☑ Notifica Sinergest ☐ Notifica portale Zucchetti ☐ Archiviazione presso Quality Info Point ☐ M18_c Registro formazione/addestramento ☐ OPL n° _____ ☐ Scheda incontro Sinergest ☐ Altro:
La comunicazione alle funzioni coinvolte avviene tramite notifica e-mail del sistema Sinergest secondo quanto inserito nella sezione "Gruppi di distribuzione".	

Sommario

1. Scope

The widespread adoption of ICT technologies at all levels of society leads to an increase in security risks in terms of data loss, intrusions, loss of confidentiality, and privacy breaches. This is particularly true for IT systems and therefore requires a careful analysis of their weaknesses and the potential for their insecure use. The implementation of an adequate information protection system is based on a systematic analysis of potential threats and the identification of the precautions to be adopted. This policy describes, at a high level, the principles and objectives adopted by the company in order to ensure a management system that minimizes, as far as possible, the risks associated with different threats and serves as a tool for continuous improvement.

On this basis, Chromavis Spa has decided to establish an Information Security Management System (ISMS) defined according to the rules and criteria set out by best practices and international reference standards, in compliance with the UNI CEI ISO/IEC 27001:2022 standard.

Policy application context

This policy applies to all software and hardware infrastructures, devices, systems, and company data. It covers all company products and services and must be complied with by all employees and suppliers.

1.1 Objective of the policy

The Information System (including technological resources, hardware, software, information in any format, data, documents, networks, and the human resources dedicated to their administration, management, and use) represents a tool of primary importance for achieving the strategic and operational objectives of Chromavis Spa, given the criticality of the business processes that depend on it.

This document aims to define policies for information systems and the information security policy in order to develop an efficient and secure Information Security Management System (ISMS) through compliance with the following principles:

- **Confidentiality:** ensuring that information is accessible only to duly authorized individuals and/or processes
- **Integrity:** safeguarding the consistency of information from unauthorized modification or deletion
- **Availability:** ensuring that authorized users have access to information and associated architectural components when required
- **Control:** ensuring that data management is always carried out through secure and tested processes and tools
- **Authenticity:** ensuring the reliable origin of information
- **Privacy:** ensuring the protection and control of personal data

Compliance with the security levels established by Chromavis Spa through the implementation of the ISMS allows the company to:

- best preserve the company's image as a reliable and competent provider
- effectively protect its own information assets and those of its customers
- increase awareness and competence among its personnel on data security issues
- fully comply with applicable laws, regulations, and international data security standards.

2. Information Security Policy

The information security policy of Chromavis Spa represents the organization's commitment towards customers and third parties to ensure the security of information, as well as the physical, logical, and organizational tools used for processing information in all activities.

The information security policy of Chromavis Spa is based on the following principles:

- Ensure that the organization has full knowledge of the information it manages and an assessment of its criticality, in order to facilitate the implementation of appropriate protection levels.
- Ensure secure access to information, in order to prevent unauthorized processing or processing carried out without the necessary rights.
- Ensure that the organization and third parties collaborate in the processing of information by adopting procedures aimed at maintaining appropriate levels of security.
- Ensure that the organization and third parties involved in information processing have full awareness of security-related issues.
- Ensure that anomalies and incidents affecting the information system and the company's security levels are promptly identified and properly managed through effective systems of prevention, communication, and response, in order to minimize their impact on the business.
- Ensure that access to company premises and individual areas is granted exclusively to authorized personnel, to guarantee the security of areas and assets.
- Ensure compliance with legal requirements and adherence to security commitments established in contracts with third parties.
- Ensure the detection of anomalous events, incidents, and vulnerabilities affecting information systems, in order to maintain the security and availability of services and information.
- Ensure business continuity and disaster recovery through the application of defined security procedures.

The information security policy formalized within the ISMS is continuously updated to ensure ongoing improvement and is shared with the organization, third parties, and customers through the company intranet and specific communication channels.

3. Political responsibility

Chromavis Spa has defined the organizational model for managing information security, as described in its Information Security Management System (ISMS). For each role, within the context of the Information Security Management System, responsibilities and authorities are clearly specified.

Within the Information Security Management System (ISMS), each corporate role must be clearly defined in terms of responsibilities and authorities, as required by ISO 27001, clause 5.

The organizational entities involved are:Steering Committee

- Chief Information Officer – CIO
- Head of Human Resources – VP HR
- IT Manager & CISO
- IT Compliance Manager
- Infrastructure Manager
- Application Manager

4. Policy Review

This Corporate Information Security Policy will be reviewed periodically in response to external events, such as changes in external regulations or guidance from Authorities, as well as organizational and operational changes that may impact Information Systems and information security.

In any case, this Policy will be reconfirmed and signed on an annual basis. Its approval will take place during the ISMS Management Review activity.

In particular, updating the Policy and operational procedures is essential when the Management Review identifies:

• significant business developments
• new threats compared to those considered during the risk analysis process
• significant security incidents
• new requirements and pressures from reference markets
• changes in the regulatory or legislative framework concerning the secure processing of information