ISO 27001

rev. 1 en (13-04-2025)

ISO 27001 – Information Security Management System (ISMS)

At **Scent Emotions**, data security, confidentiality, and business continuity are integral to how we operate and build trust with clients, suppliers, and institutional partners. The implementation and certification of our **Information Security Management System (ISMS)** under the **ISO 27001:2022** standard reflects our commitment to excellence, risk control, and regulatory compliance in the digital era.

Certification History

Scent Emotions obtained its first **ISO 27001 certification** in **December 2024**. The certification covers all critical systems and processes associated with the management of information and digital infrastructure, aligning us with global best practices in cybersecurity and governance.

What is ISO 27001?

ISO 27001 is the leading international standard for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). It helps organizations:

- Identify and manage **information security risks**
- Ensure the **confidentiality, integrity, and availability** of data
- Establish clear **security responsibilities and policies**
- Protect both **physical and digital assets**, including sensitive customer and employee information

Scope of Our ISMS

The **Scent Emotions** ISMS covers:

- Internal digital infrastructure, including cloud services and on-premises systems

- Supply chain communication, ERP systems, and customer data protection
- R&D knowledge, including technical documentation, formulations, and digital intellectual property
- Security of data in production and process control environments
- Compliance with data protection regulations, such as the **General Data Protection Regulation (GDPR)**

Key Controls and Practices

To meet the ISO 27001 standard, **Scent Emotions** has implemented:

- Risk assessment and treatment protocols for all information assets
- Encryption and access control systems for confidential and business-critical data
- Physical security measures for data centers and production environments
- Employee training on cybersecurity awareness and secure data handling
- Incident management procedures to respond effectively to cyber threats or breaches
- Regular audits, monitoring, and continuous improvement mechanisms

What This Means for Our Stakeholders

- For **clients**: assurance that their information and interactions are handled securely
- For **public institutions**: confidence in our regulatory compliance and IT governance
- For **partners and suppliers**: clear standards for secure information exchange
- For **internal users**: a culture of cybersecurity that enhances business continuity

(Here logo Financiado por la Union Europea Next GenerationEU)
(Herel logo Plan de Recuperaciñon, Transformación y Resilencia)
(Here logo Ministerio de Economía, Comercio y Empresa)
(Here logo Cámara de Comercio de España)