Information Security Policy

DigiProces, as an EMS (Electronics Manufacturing Services) company, develops, manufactures and delivers product solutions for an ever-expanding range of applications at our facilities in Castellar del Vallès. We help meet specific needs with simple, personalized responses, optimized for maximum reliability. DigiProces has decided to implement an Information Security Management System based on the **ISO 27001:2022** standard with the aim of preserving the **confidentiality, integrity and availability** of information and protecting it from a wide range of threats. This system is intended to ensure the continuity of business lines, minimize damage, maximize the profitability of investments and business opportunities and promote continuous improvement. DigiProces's Management is aware that information is a valuable asset for the organization and therefore requires adequate protection.

The Management establishes the following as base, starting point and support objectives for the objectives and principles of information security:

- Protection of intellectual property and data of customers and suppliers, guaranteeing security in the management of designs, firmware and other critical assets.
- Safeguarding of the organization's records, ensuring their integrity and availability.
- Protection of personal data and privacy.
- Classification of information and application of encryption measures for the protection of sensitive data.
- Control and security in access management, both for employees and third parties (suppliers, subcontractors, etc.).
- Establishment of periodic internal and external audits to verify compliance with information security.
- Information security training and education to make employees aware of best practices and emerging threats.
- Registration and management of security incidents, with response mechanisms to cyberattacks, security breaches or information leaks.
- Business continuity management, through contingency plans and periodic simulations.
- Implementing a secure data deletion and retention process, ensuring that information is stored only as long as necessary and securely deleted.
- Security assessment of suppliers and subcontractors, ensuring they comply with DigiProces information security standards.
- Continuous monitoring and detection of advanced cyber threats, including APT attacks, ransomware, and targeted phishing.
- Management of organizational changes with an impact on information security.

And it acquires the following commitments:

- Comply with legal and contractual requirements applicable to information security.
- Prevent and detect viruses and other malware, establishing agreements with specialized organizations.
- Apply a continuous improvement approach to information security.
- Develop safety and awareness training plans for employees and collaborators.
- Conduct regular simulations of security incidents to assess the organization's readiness.
- Ensure that any violation of this policy carries clear consequences, reflected in contracts with employees, suppliers and subcontractors.
- Act at all times under strict principles of professional ethics.
- Commit to sustainability and climate change mitigation, reducing the company's environmental impact and promoting good sustainability practices.

This policy provides the framework for the continuous improvement of the information security management system and for establishing and reviewing its objectives. It is communicated to the entire Organization through the Intranet and business website, and is reviewed annually or when there are substantial changes in the Information Security Management System.
The Policy is available to the general public.

The Policy is generally available to the public.

Castellar del Vallès, March 31, 2025.