	INFORMATION SECURITY POLICY	ELA-SI-PSP05
	Clasificación de seguridad: PUBLICO	Rev:2 190224

ELAUSA ELECTRONICS S.L. establishes this policy as a framework for company-wide action in the field of information security.

This policy is based on the following principles:

- **Protect** information resources and the technology used for their processing, against deliberate or accidental internal or external threats, to ensure compliance with the confidentiality, integrity, and availability of information.
- **Implement security measures** in information systems from their development and implementation, as well as during their maintenance, to reduce the risks of human error, accidents, and natural disasters.
- **Ensure the continuous improvement** of the Information Security Management System by implementing the international standard VDA-ISA (TISAX).
- **To keep** this Information Security Policy up to date to ensure its validity and effectiveness.
- **Prevent unauthorized access** to information systems, databases, and information services.
- **Establish** a clear and efficient information security management methodology through guidelines and policies.
- **Guarantee** secure access to information and with total confidence to users through the design and operation of an IT and communication infrastructure in accordance with the current risks of technology.
- **Establish safety objectives** under a continuous improvement approach. These objectives are defined in the TIS-OBJ registry, and their follow-up is carried out through the meetings of the ELA-SI-PO-019 Security Committee and the Management Review.
- **Knowledge of information security** to avoid situations that may lead to a security incident.
- **Provide appropriate investments** according to identified risks and protection needs.
- Ensure **security in the exchange of information**, internally and for all stakeholders.
- **Comply with the** privacy **and** personal data protection requirements of our customers, employees, and suppliers.
- **Comply with** the requirements of **the legislation applicable** to our activity, the **commitments made** to customers **and interested parties**, and any internal rules or guidelines to which the company is subject.
- **Obtain measurable results** that enable the analysis and evolution of information security.

The Information Security Manager will be directly responsible for the maintenance of this policy, providing advice and guidance for **its implementation and corrections in the event of deviations in compliance with defined security policies**.

This policy will always be aligned with the company's general policies and with those that serve as a framework for other internal management systems, such as the quality and environmental policies and the internal code of ethics.

The Management

Vic, February 19, 2024