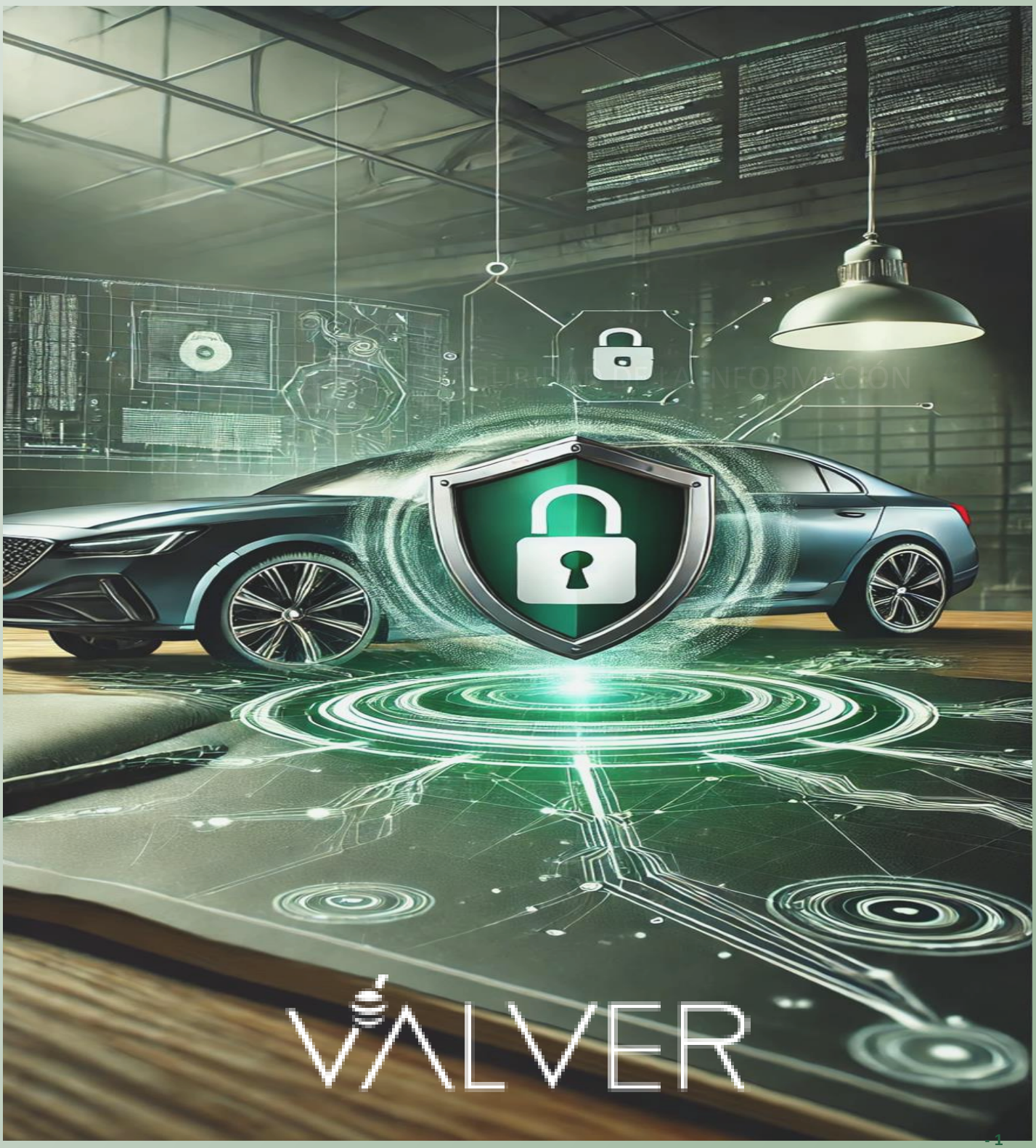
GENERAL INFORMATION SECURITY POLICY



GENERAL INFORMATION SECURITY POLICY

INFORMATION SECURITY

Protection of Sensitive Information

In the automotive industry, a large amount of sensitive information is handled, such as intellectual property, design drawings, manufacturing data, technological innovations and more. TISAX helps ensure that this information is properly protected against leaks, hacks or unauthorized access.

Compliance with rules and regulations

TISAX allows companies to comply with safety regulations required by their Business partner, especially within the European automotive industry. It is a way to standardize and simplify the audit and evaluation process for companies.

Requirements of Customers and OEMs (Original Equipment Manufacturers)

Many large automotive companies, such as Audi, BMW, Daimler and Volkswagen, require their suppliers to be TISAX certified to ensure that they all comply with safety regulations. This way, manufacturers can be confident that sensitive data is handled properly.

Trust and Reputation

Earning a TISAX certification increases trust among business partners and can improve a company`s reputation by demonstrating that its security practices are aligned with the best industry standards.

Standardization in Security Assessment

TISAX standardizes how information security risks and vulnerabilities are assessed within the supply chain. This simplifies audit processes as all participating companies can access the same assessment and share results with multiple business partners.

Competitiveness

That Valver has TISAX certification is, in many cases, a requirement to remain competitive in the automotive industry. Without it, companies may be excluded from certain important projects or collaborations.

In short, **TISAX is crucial to ensuring information security in the automotive supply chain, meeting customer requirements and maintaining competitiveness in a highly regulated sector.**

ANNEX 3 V.01 – General Information Security Policy. Tisax Certification.

VALVER, aware of the importance of information security in the current context, has promoted the establishment of an Information Security Management System in accordance with the requirements of the TISAX VDA-ISA standard based on the family of ISO 27000 standars. This is done in order to identify, evaluate and minimize the risk to which your information is exposed and guarantee compliance with the established objectives. This security policy is aplicable to group companies in Spain and Portugal.

Through the preparation, communication and maintenance of this policy, VALVER's Management shows its commitment to protecting the confidentiality of the information in the provision of its services, guaranteeing its integrity in all the processes carried out, as well as the availability of the information systems involved in these treatments.

This policy is based on the following principles to ensure that information systems and the information that is created, collected, stored and processed comply with:

• Security in human resources management, before, during and at the end of employment.

• The proper management of assets that involves the classification of information and the manipulation of media.

• The establishment of appropriate measures for the treatment of risks derived from the identification and evaluation of assets.

• Establishing robust logical access control to systems and applications, managing user permissions and privileges.

• The protection of facilities and the physical enviroment, through the design of safe work areas and the safety of equipment.

• Ensuring operational security by protecting against malicious software, making backup copies, establishing logs and monitoring them. Control of the software in operation. The management of technical vulnerabilities and the choice of appropriate techniques for auditing the systems.

• Communications' security by protecting networks and the exchange of information.

• Ensuring security in the acquisition and maintenance of information systems, limiting and managing change.

• Establishment of a clear and efficient information security management methodology through guidelines and policies.

• The guarantee of secure access to information and with complete confidence to users through the design and operation of an IT and communication infrastructure in accordance with current technology risks.

• The guarantee of the correct condition of the fecilities and appropriate equipment, so that they are in accordance with the activity, objectives and goals of the company.

• Performing secure software development, separating development and production environments, and performing appropriate functional acceptance testing.

• The control of relationships with suppliers, contractually requiring compliance with the relevant security measures and aceptable levels in the provision of their services.

• Effectiveness in the management of security incidents, establishing the appropriate channels for their notification, response and timely learning.

• Implementing a business continuity plan that protects the availability of services during a crisis or disaster.

• Identification and compliance with aplicable regulations, placing special interest in intelectual property and the protection of personal data.

• The review of these information security requirements to guarantee compliance and their effectiveness.

The Security Manager will be directly responsible for mantaining this policy, providing advice and guidance for its implementation and corrections in the event of deviations in its compliance. This policy will always be aligned with the general policies of the company and with those that serve as a framework for other internal management systems, such as quality and IATF.

All staff of the organization have the duty to comply with this policy. Management will provide the necessary means and sufficient resources for its compliance, and will assume the responsibility of communicating it and keeping it accesible to all interested parties.

You name it. We print it

VALVER

VALVER SLU

Parque Empresarial Areas
Rúa 6, Número 39
36711 Tui
Pontevedra (Spain)

T: +34 986 288 012
E: contact@valvergroup.com

Oct, 2024