ISMS

Information Security Management System

POLICY
Doc. **PO-ISMS.201.EN** Rev. 0 del **10/01/2026**
Classification: **C1 – PUBLIC**

INFORMATION SECURITY POLICY

GIOBERT DO BRASIL SISTEMAS AUTOMOTIVOS LTDA
Legal and operational headquarters: Avenue Vicenzo Granguelli João Aldo Nassif - N 85613916058 Jaguariúna San Paolo (Brazil)
CNPJ: 13.258.571/0001-72
T +55 (19) 3837-5525 / 3837-7224

1 DOCUMENT SHEET

List of revisions

Rev.	Emission	Changes	Approval	
0	RSI	First Edition in the ISMS	General Management Giobert do Brasil Sist Aut Ltda	10/01/2026

Regulatori references

LGPD Lei n. 13.709/2018
TISAX VDA ISA 6.03 - : 1.1.1
ISO/IEC 27001:2022 - A5.1

Related documents

2 CONTENTS

1 DOCUMENT SHEET 2
2 CONTENTS 3
3 PREMISE 3
4 PURPOSE 3
5 DEFINITION OF INFORMATION SECURITY 3
6 SCOPE 4
7 OBJECTIVES 4
8 STRATEGY 4
9 PRINCIPLES 4
10 MANAGEMENT COMMITMENT 5
11 RESPONSIBILITY 5
12 EXCEPTIONS 5
13 VIOLATIONS AND PENALTIES 6
14 REPORTING VIOLATIONS 6
15 VALIDITY, REVISION AND APPROVAL 6

3 PREMISE

Giobert do Brasil Sist Aut Ltda (hereinafter referred to as the organization) is a company specialized in the design and production of mechatronic components for the automotive sector, particularly locking systems and vehicle keys.
In a context marked by increasing digitalization and complex cyber threats, the organization places the utmost importance on the protection of corporate information, to safeguard its competitiveness and the trust of customers, partners, and stakeholders.

4 PURPOSE

This policy defines the organization's approach to information security, with the objective of preventing unauthorized access, loss, tampering, destruction, or unavailability of the information managed, thereby safeguarding the company's information assets and those of all its stakeholders.

5 DEFINITION OF INFORMATION SECURITY

Information security encompasses the set of measures, controls, and practices aimed at protecting information from unauthorized access, improper modifications, loss, destruction, or disruption, with the goal of ensuring:

- Confidentiality: Ensuring that information is accessible only to authorized individuals, preventing any form of unauthorized disclosure.
- Integrity: Guaranteeing that information is accurate, complete, and protected from unauthorized, intentional, or accidental alterations.
- Availability: Ensuring that information and the systems processing it are accessible and usable in a timely manner by authorized individuals when needed.

6 SCOPE

This Information Security Policy applies to:

- All information processed by Giobert do Brasil Sist Aut Ltda,regardless of its format or medium (digital, paper-based, verbal), its nature (technical, commercial, administrative, personal, etc.), and its classification level.
- All individuals who, in any capacity, access, process, transmit, or manage company information, including employees, collaborators, consultants, suppliers, business partners, and any other formally authorized external parties.
- All business processes, information systems, applications, technological infrastructures, devices, and physical locations — including offices, production departments, archives, cloud environments, or remote sites — where information is created, processed, transmitted, or stored.
- The scope also extends to all business activities and initiatives involving the use of information, to ensure an adequate level of protection and operational continuity, in alignment with applicable regulatory, contractual, and organizational requirements.

7 OBJECTIVES

The primary information security objectives for Giobert do Brasil Sist Aut Ltdainclude:

- Ensuring business continuity and the resilience of corporate systems.
- Protecting intellectual property and company know-how.
- Preventing and minimizing the impact of cybersecurity incidents.
- Ensuring compliance with regulatory, contractual, and industry-specific requirements (e.g., ISO 27001, TISAX, VDA/ISA).
- Promoting staff awareness on information security matters.
- Demonstrating the organization's commitment to information security to its stakeholders.

8 STRATEGY

To achieve its objectives, the organization adopts the following strategies:

- Implement and maintain an Information Security Management System (ISMS) in compliance with ISO/IEC 27001:2022 and, where applicable, the VDA/ISA 6.0.3 framework.
- Provide ongoing training and awareness programs for all personnel.
- Conduct periodic risk assessments related to information security.
- Implement technical and organizational controls based on information classification.
- Monitor security events and ensure a structured response to incidents.
- Perform regular audits to verify the effectiveness of the implemented measures.

9 PRINCIPLES

The management of information security and personal data protection at Giobert do Brasil Sist Aut Ltdais based on the following set of fundamental guiding principles:

1. Information Classification
   All information is classified according to its sensitivity, value, and criticality to the organization, assigning an appropriate level of protection based on the type of information being processed.
2. Access Control
   Access to information is governed by the "need-to-know" principle, ensuring that only duly authorized individuals can access information relevant to their role, thereby minimizing the risk of unauthorized or improper access.
3. Encryption
   The use of encryption is mandatory for protecting high-risk classified information, both when stored on digital or physical media and during transmission over internal or public networks. This serves as a key safeguard against loss of confidentiality and unauthorized data interception.
4. Integrity and Availability of Information

Technical and organizational measures are adopted to ensure the authenticity, integrity, and reliability of data. These include regular backup systems, redundant infrastructures, procedures for periodic verification of data authenticity and accuracy, as well as preventive maintenance of information systems.

5. Information Retention and Disposal
   Information is retained for a defined period based on legal, contractual, or operational requirements and is securely disposed of at the end of its lifecycle. Retention and disposal procedures are documented to ensure the protection of confidentiality and compliance with applicable regulations.
6. Adequacy and Proportionality of Security Measures
   Security measures are designed and implemented in a manner that is adequate and proportionate to the level of risk associated with information processing.

10 MANAGEMENT COMMITMENT

The Management of Giobert do Brasil Sist Aut Ltda recognizes that information represents a strategic and essential asset for the company's continuity and success, and is formally committed to ensuring an adequate level of information security through:

- Reviewing information security objectives and policies to ensure their alignment with corporate strategies and applicable regulatory frameworks.
- Providing the necessary economic, technological, and organizational resources for the effective implementation of the measures outlined in this policy and in the adopted Information Security Management System (ISMS).
- Promoting and supporting a corporate culture based on security awareness, through regular training and continuous awareness initiatives for all personnel and external collaborators involved in information processing.
- Periodically verifying the effectiveness of implemented security measures through audits and reviews, to promptly identify any weaknesses and undertake appropriate corrective or continuous improvement actions.
- Assigning clear and well-defined roles and responsibilities in the field of information security, ensuring that everyone within the organization actively contributes to achieving the established objectives.
- Strict compliance with all applicable regulations, including ISO/IEC 27001:2022, TISAX, LGPD Lei n. 13.709/2018, and other relevant national and international regulations.
- The Management ensures that this commitment is communicated, understood, and adopted throughout the organization to guarantee the highest level of protection for the company's information assets and the personal data it handles.

11 RESPONSIBILITY

Within the organization, responsibilities for information security are distributed as follows:

- **Process Owners**: They are responsible for implementing, maintaining, and monitoring information security measures within their respective business processes. They must ensure that processes and services comply with corporate policies and collaborate with other functions or services to mitigate security risks.
- **Employees and Collaborators**: They are required to fully comply with the company's information security policies and procedures. They must adopt responsible behaviour in handling information and promptly report any security incidents, vulnerabilities, or non-compliant behaviour.
- **Suppliers and Third Parties**: They must strictly adhere to the security requirements defined in contractual agreements and information security policies. They are responsible for ensuring that their activities and systems do not compromise the information security of Giobert do Brasil Sist Aut Ltda, and must promptly report any incidents, breaches, or anomalies through the established contact points.

12 EXCEPTIONS

Exemptions and exceptions to this policy are generally not permitted. However, in extraordinary and strictly necessary cases, the Top Management of Giobert do Brasil Sist Aut Ltda may approve exceptions. Such exceptions must be documented and regularly reviewed to verify the continued validity of the principle of extreme necessity that justified them.

13 VIOLATIONS AND PENALTIES

Any violation of the provisions contained in this document, or its annexes may result in the application of disciplinary measures and/or legal action, considering the potential negative impacts caused by negligent or intentional behaviour. Any infraction committed by employees, collaborators, or third parties acting on behalf of the organization will be considered a serious breach of contractual obligations and may be sanctioned in accordance with applicable laws, current employment contracts, and internal policies. Where necessary, the organization reserves the right to report such violations to the competent authorities, in compliance with local and international laws, to assess any civil or criminal implications.

14 REPORTING VIOLATIONS

Any violations or suspected violations of this policy, as well as any vulnerabilities, incidents, or anomalies related to information security, must be reported to the Information Security Manager (ISM) by writing to the dedicated email address: ism@giobert.com. Such reports enable the company to respond promptly, minimizing potential negative impacts and contributing to the continuous improvement of the information security management system.

15 VALIDITY, REVISION AND APPROVAL

This policy is formally approved by Top Management and is subject to periodic review, at least annually, or whenever there are significant changes in the organization, regulations, or the operational and technological context. Any modification must be formally approved before it comes into effect, and all updated versions of the policy are promptly communicated to the relevant parties. The updated version entirely replaces the previous one, becoming immediately binding for all employees, collaborators, and suppliers of the organization.

Date: 10/01/2026
General Management
Giobert do Brasil Sist Aut Ltda

FINE