Information Security Policy

Firmato digitalmente da:
Gruber Martin
Firmato il 25/09/2025 09:54
Seriale Certificato: 4630568
Valido dal 16/06/2025 al 16/06/2028
InfoCamere Qualified Electronic Signature CA

Table of Contents

GOAL AND FIELD OF APPLICATION 2

LAWS AND REGULATORY REFERENCES 2

DESCRIPTION 2

SCOPE 3

POLICY DESCRIPTION 3

RESPONSIBILITIES AND UPDATES 4

NONCONFORMITY MANAGEMENT 4

Document revision

1	11.09.2025	Update paragraph NC management	Mauro Sgarbossa	CEO	Public
0	30.08.2024	First release	Management	CEO	Public
Rev.	**Date**	**Description**	**Modified**	**Approved**	**Classification**

Firmato digitalmente da:
Gruber Martin
Firmato il 25/09/2025 09:54
Seriale Certificato: 4630568
Valido dal 16/06/2025 al 16/06/2028
InfoCamere Qualified Electronic Signature CA

Goal and field of application

The purpose of this document is to describe the general information security principles defined by Gruber Logistics in order to develop an efficient and secure Information Security Management System.

Laws and Regulatory References

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements
- ISO 9001:2015 Quality Management System
- Regulation (EU) 2016/679 on Data Protection (GDPR)

Description

For Gruber Logistics the primary goal of information security is to protect data and information, as well as the technological, physical, logical, and organizational infrastructure, and its management. This involves implementing and maintaining a secure information management system by adhering to the following principles:

1. **Confidentiality:** Ensuring that information is accessible only to authorized individuals and processes.
2. **Integrity:** Safeguarding the accuracy and consistency of information by preventing unauthorized alterations.
3. **Availability:** Ensuring that authorized users can access information and related systems when needed.
4. **Control:** Ensuring that data management is performed using secure and validated processes and tools.
5. **Authenticity:** Guaranteeing that information is reliably sourced and verified.
6. **Privacy:** Ensuring the protection and control of personal data.

In managing its services, adherence to established security levels aims to ensure:

- The selection of a trustworthy partner for handling information assets.
- A strong corporate reputation.
- Full compliance with Service Level Agreements (SLAs) with customers.
- High customer satisfaction.
- Compliance with current regulations and international safety standards.

To achieve these objectives, Gruber Logistics has implemented a Secure Information Management System in line with the ISO/IEC 27001:2022 Standard and relevant legal requirements, providing a structured approach to managing information security within its operations.

Firmato digitalmente da:
Gruber Martin
Firmato il 25/09/2025 09:54
Seriale Certificato: 4630568
Valido dal 16/06/2025 al 16/06/2028
InfoCamere Qualified Electronic Signature CA

Scope

The information security policy of Gruber Logistics applies to all internal staff and third parties involved in managing information, as well as to all processes and resources related to the design, implementation, initiation, and continuous delivery of its IT services.

Policy Description

The information security policy of Gruber Logistics demonstrates the organization's commitment to protecting data, along with the physical, logical, and organizational tools used for information processing across all activities.

Gruber Logistics' information security policy is based on the following principles:

1. Ensuring a comprehensive understanding of the information handled and assessing its criticality to implement appropriate protection measures.
2. Providing secure access to information to prevent unauthorized processing or access without the necessary rights.
3. Ensuring that both the organization and any third parties involved follow procedures that maintain appropriate security levels.
4. Promptly identifying and effectively managing anomalies and incidents affecting the information system and security levels, through efficient prevention, communication, and response mechanisms to minimize business impact.
5. Restricting access to company facilities and specific locations to authorized personnel only, ensuring the security of these areas and assets.
6. Complying with legal requirements and honoring security commitments outlined in contracts with third parties.
7. Detecting anomalies, incidents, and vulnerabilities in information systems to maintain service and information security and availability.
8. Ensuring business continuity and disaster recovery through the implementation of established security procedures.

Gruber Logistics defines and documents its information security policies, objectives, and commitments, taking into account stakeholder expectations, potential risks and opportunities, and compliance with legal and customer requirements.

To implement these policies, management sets and defines measurable objectives.

The information security policy is regularly updated to ensure continuous improvement and is communicated throughout the organization, to third parties, and to clients through an internal documentation system and specific communication channels.

Firmato digitalmente da:
Gruber Martin
Firmato il 25/09/2025 09:54
Seriale Certificato: 4630568
Valido dal 16/06/2025 al 16/06/2028
InfoCamere Qualified Electronic Signature CA

Responsibilities and Updates

The management team at Gruber Logistics is accountable for ensuring the secure management of information, ensuring alignment with changes in the business and market environment. This includes evaluating and implementing necessary actions in response to:

- Major business changes;
- Emerging threats not previously identified in risk assessments;
- Significant security incidents;
- Changes in relevant regulations or legislation concerning information security.

Non-conformity Management

All nonconformities related to information security shall be reported immediately to the **Information Technology** and **QHSE** departments. Reports may be submitted via email to **security@gruber-logistics.com.** These functions are responsible for managing nonconformities in accordance with the established procedures of the Integrated Management System. Reports shall be accurate, timely, and complete, enabling the prompt initiation of corrective and, where applicable, preventive actions. This process ensures the effective mitigation of risks, compliance with applicable standards and regulations, and supports the continual improvement of the Information Security Management System (ISMS).

Firmato digitalmente da:
Gruber Martin
Firmato il 25/09/2025 09:54
Seriale Certificato: 4630568
Valido dal 16/06/2025 al 16/06/2028
InfoCamere Qualified Electronic Signature CA