INFORMATION SECURITY POLICY
(GLOBALIA HANDLING)

Context

The management of Globalia Handling, aware of its responsibility to its customers and employees, considers that our mission is to achieve the entity's objectives and ensure the rights and guarantees of the customer, employees, and the importance of their business through information technology services, which are subject, among others, to compliance with requirements aimed at ensuring the security of the Organization's Information.

It aims to obtain external recognition of Globalia Handling, not only from the point of view of the quality of the service provided but also in the continuous improvement of its capabilities to ensure the confidentiality, integrity, availability, and authenticity of the data, assets, and information systems with which the Organization works.

Our vision is to be an agile company that can adapt to changes and maintain innovation as its hallmark, thus continuing to help our customers and collaborators.

Considering the importance of information security, especially related to employees, customers, and business processes, Globalia Handling has defined this Security Policy, implementing an information management system based on the ISO 27001 standard, committing to adopt the necessary measures to guarantee the adequate protection of its assets, systems, and information technology services.

Scope

The protection of the Organization's own information, customer information, and supplier information managed within the company's activities.

The scope of the policy includes the Information Systems that support the provision of Globalia Handling services, all of which are encompassed in the assurance of Globalia Handling's business.

Development

Information Security is a priority for Globalia Handling. Therefore, it is committed to compliance with business requirements and applicable laws, regulations, and standards, following market best practices:

- Ensure the confidentiality, integrity, and availability of the Organization's, customers', and employees' assets and information systems.
- Align Information Security Objectives with Business Objectives.
- To achieve the Information Security objectives, establish a preventive risk management strategy that may affect them, identify them, implement controls to act on them, establish regular procedures for their reevaluation, and maintain risk at an acceptable level.
- The Organization and its employees will comply with applicable legal, regulatory, and statutory requirements regarding Information Security and the protection of personal data and guarantees of digital rights, as well as contractual requirements with third parties in this regard.
- The Information Security Policy is developed through the Security Normative Body, which includes specific Information Security Policies and Procedures.
- The Information Security function must be governed within an Information Security Framework.
- Ensure that the services that support business operations are developed in accordance with Globalia Handling's specific Information Security Policies and Procedures.

- Establish the appropriate organizational and budgetary structure for the proper definition, implementation, monitoring, and supervision of all aspects included in this Policy and the Security Normative Body of Globalia Handling.
- Clearly define the responsibilities and obligations of the personnel and be accountable for their performance regarding information security.
- Ensure that personnel with responsibilities in Information Security have the appropriate qualifications and training to perform their function.
- The information owned and/or entrusted to Globalia Handling should only be accessible to duly authorized individuals, whether they belong to the Organization or not, and the Information will be used for appropriate and relevant purposes.
- All employees of the Organization will receive the necessary training and awareness on information security and personal data protection to perform their duties.

The legal and regulatory framework in which we carry out our activities is:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of individuals regarding the processing of personal data and the free movement of such data.
- Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.
- Law 2/2019, of March 1, amending the consolidated text of the Intellectual Property Law, approved by Royal Legislative Decree 1/1996, of April 12.
- Law 34/2002 of July 11, on services of the information society and electronic commerce.
- Regulation (EU) No. 910/2014 of the European Parliament and of the Council, of July 23, 2014, regarding electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- Law 6/2020, of November 11, regulating certain aspects of trusted electronic services.
- Law 10/2021, of July 9, on remote work.
- Implementing Regulation (EU) 2015/1998 of the European Commission of November 5, 2015, establishing detailed measures for the application of common basic security standards for aviation security.
- Annex 17 to the International Civil Aviation Organization (ICAO) Convention on the Protection of International Civil Aviation against Acts of Unlawful Interference in its current version.

This policy is developed and complemented with the rest of the policies, procedures, and documents in force to develop the management system, which is structured in a specific location in our documentation repository.

The document management aims to have a folder structure and store the generated documentation in such a way that it is correctly organized and accessible in a controlled manner through the corresponding authorizations.

Access to information is carried out according to the established profiles, following the access management process.

The management assumes these principles, having the necessary and appropriate means for their implementation, communicating them for compliance by all employees and collaborators of the company through this Security Policy.

Functions and Responsibilities

The roles or functions directly associated with the ISMS are:

- Information Security and ISMS Manager
- Data Protection Officer (DPO)
- Information Systems Manager
- Information Security Committee

Their responsibilities, competencies, and requirements are developed in the Roles and Responsibilities for information security policy or procedure. This definition is further complemented in job profiles and system documents. The procedure for their appointment and renewal is the ratification by the Security Committee.

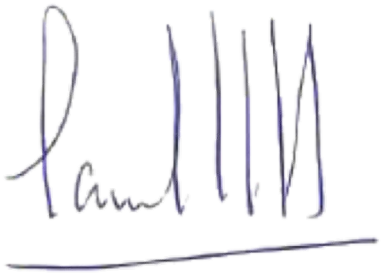
The mechanism for coordination and conflict resolution is the Information Security Committee, which can be convened on an extraordinary basis, if necessary, for example, to resolve conflicts among System managers. In any case, the final decision will always rest with the Management if necessary.

To achieve these objectives, the commitment and responsibility of the entire human team of Globalia Handling and its third parties and vendors are required, with the common goal of achieving the highest levels of quality and ethical behavior, and conducting our activities with respect for the law, internal principles and standards set forth in the Security Normative Body, Personal Data Protection, and E-commerce Policies and protocols.

Non-compliance

This mandatory Security Policy requires the collaboration of all Globalia Handling personnel to avoid damage to the corporate image, as well as potential economic sanctions that may arise.

Approval



Approved by Carmen Lopez Pintor
General Manager of Globalia Handling
December 2023