TERMINALES CANARIOS

1st Version

INFORMATION SECURITY POLICY

TERMINALES CANARIOS

Contents

TERMINALES CANARIOS

Version control.

Version	Date	Description	Author
1.0	17/11/2025	Initial version of the document	Information Security Officer

TERMINALES CANARIOS

1. Purpose

The purpose of this policy is to provide the guidelines that must be followed to protect Terminales Canarios S.L. information against a wide range of threats, in order to:

- Guarantee the security of operations carried out through Information Systems.
- Minimize the risk of damage.
- Ensure compliance with the objectives of Terminales Canarios S.L.

Terminales Canarios S.L. is committed to ensuring that the principles of the Information Security Policy form part of its culture, for which purpose it has implemented an Information Security Management System based on an internationally recognized standard.

The Management of Terminales Canarios S.L. endorses this Information Security Policy and undertakes to provide the resources necessary for its proper implementation and compliance.

2. Scope

This policy applies to all information processed and services provided by Terminales Canarios S.L. It is mandatory for all personnel who access the information systems of Terminales Canarios S.L.

The information security policy is binding on all external personnel of Terminales Canarios S.L. through service agreements or arrangements with third parties.

3. Regulatory Framework

This security policy is developed within the regulatory framework established by the following laws and standards:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- Directive (EU) 2022/2555 of the European Parliament of 14 December 2022 on measures for a high common level of cybersecurity across the Union.
- Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights.
- ISO 27001:2022 - Information Security, Cybersecurity and Privacy Protection -

Information Security Management Systems - Requirements.

4. Mission and services provided

Terminales Canarios, S.L. is a company incorporated in 1993 and engaged in the provision of logistics services for the receipt, storage, and supply of fuels and lubricants in the Canary Islands.

Terminales Canarios plays a key role in the logistics chain linked to mobility solutions in the Archipelago, operating with a firm commitment to sustainability and with the uncompromising ambition of becoming a “Net Zero Emissions” company.

Mission in the field of Information Security

Terminales Canarios mission in the field of Information Security is to guarantee the confidentiality, integrity, availability, and protection of the information it manages. To this end, the company is committed to ensuring operational continuity, regulatory compliance, and the trust of customers, suppliers, employees, and other stakeholders through the implementation of controls, processes, and good practices aligned with national and international standards.

5. Compliance with Basic Principles and application of Minimum Requirements

Terminales Canarios undertakes to align its Information Security System with the requirements established by the NIS2 Directive, the Cybersecurity Coordination and Governance Law that transposes it into Spanish law, and the good practices defined by ISO 27001. To this end, the organization will adopt the technical, organizational, and management measures necessary to ensure an adequate level of protection, resilience, and continuity, integrating these regulatory frameworks and standards as references for the continuous improvement of its security.

The basic principles constitute the fundamental guidelines that must be considered in any activity related to the use of information assets. The following are established:

- **Security as an integral process:** Information security shall be addressed as a cross-cutting process integrated into all company operations.
- **Risk-based security management:** Decision-making in security matters shall be based on a risk management approach.
- **Prevention, detection, response, and preservation:** Measures shall be established to prevent incidents, detect anomalous activities, respond effectively, and preserve the necessary evidence.

- **Existence of lines of defense:** Security shall incorporate different levels of control and verification acting as complementary lines of defense.
- **Continuous monitoring:** Continuous monitoring of systems and services shall be carried out in order to identify threats and guarantee their protection.
- **Periodic reassessment:** Risks, controls, and security processes shall be reviewed periodically to ensure their adequacy and effectiveness.
- **Differentiation of responsibilities:** Specific roles, duties, and responsibilities shall be defined to ensure orderly and effective management of information security.

Therefore, it will be developed by applying the following minimum requirements:

- **Organization and implementation of the security process:** Terminales Canarios shall establish the structure and procedures necessary to implement an effective security process.
- **Risk analysis and management**: Periodic risk analyses shall be carried out and proportionate measures shall be applied for their treatment.
- **Personnel management**: The company shall ensure that personnel are aware of their responsibilities and receive the necessary training in information security.
- **Professionalism**: Professional and ethical conduct shall be promoted in the use and handling of information assets.
- **Authorization and control of access**: Access controls based on need-to-use shall be applied, and granted authorizations shall be periodically reviewed.
- **Protection of facilities**: Facilities shall be protected by physical and operational measures that prevent unauthorized access and safeguard critical assets.
- **Acquisition of security products and procurement of security services:** The acquisition of technologies and services shall include security criteria that guarantee their suitability and reliability from the outset.
- **Least privilege:** Access to systems and information shall be granted only with the privileges strictly necessary for the performance of each function.
- **System integrity and updating**: Systems shall be kept updated and protected to preserve their integrity and reduce vulnerabilities.
- **Protection of stored and transmitted information**: Information shall be protected by controls that guarantee its confidentiality, integrity, and availability both at rest and during transmission.
- **Prevention regarding other interconnected information systems**: Preventive measures shall be adopted to mitigate the risks arising from interconnection with third parties and other information systems.
- **Activity logs and detection of malicious code**: Systems shall generate activity logs and have mechanisms to detect malicious code or anomalous behavior.
- **Security incidents**: A structured process shall be implemented for the notification, management, and resolution of security incidents in a rapid and effective manner.

- **Business continuity**: Operational continuity measures shall be established to maintain or restore essential services in the event of incidents or contingencies.
- **Continuous improvement of the security process:** The security process shall be subject to ongoing review and improvement to ensure its adequacy in the face of technological, regulatory, and operational changes.

6. Governance Model

The organizational structure for information security management is composed of the following roles:

- **Information Security Committee**: Responsible for aligning the organization's activities in matters of information security and is composed of:
  - Chair: General Manager.
  - Secretary: Information Security Officer
  - Members:
    - System Manager
    - Director of Human Resources and Legal Affairs
    - Director of Operations
- **Information Security Officer**: responsible for defining, supervising, and coordinating the implementation of information security measures, as well as ensuring proper risk management and compliance with the applicable cybersecurity regulations.
- **Data Protection Officer**: must oversee compliance with the regulation and cooperate with the Spanish Data Protection Agency.
- **Service Owner:** responsible for determining the security requirements of the services provided.
- **Systems Manager:** shall be responsible for developing the specific way to implement security in the system and for supervising its daily operation, and may delegate to administrators or operators under their responsibility.
- **Information Owner:** responsible for determining the requirements of the information processed.

As an integral part of this model, a formal process for ongoing monitoring and assessment has been defined through the Review by the Security Committee, in which the state of security is analyzed on the basis of indicators, risk assessment, and compliance with objectives.

6.1 Functions of the Information Security Committee

TERMINALES CANARIOS

For the management of Information Security, the Information Security Committee, hereinafter the Security Committee, is established within the scope of this Security Policy. It will coordinate the security activities and controls established at Terminales Canarios S.L. and ensure compliance with the applicable internal and external regulations on information security. It is responsible for promoting the implementation of this Security Policy.

The Security Committee **shall meet ordinarily at least twice a year**, and extraordinarily when there are duly justified reasons of urgency, or at the request of its Chair or the Information Security Officer.

The Committee may obtain from internal or external technical personnel any information relevant to its decision-making and may invite such personnel to meetings with voice but no vote.

The Information Security Officer will act as secretary, with voice and vote, and as such shall:

- Call meetings of the Information Security Committee.
- Keep minutes of the meetings of the Information Security Committee.
- Prepare the topics to be dealt with at Committee meetings, providing timely information for decision-making.
- Be responsible for the direct or delegated execution of the Committee's decisions.

Other persons with responsibilities shall be called as required by the Information Security Committee.

Its functions are:

- Address the concerns of the Board of Directors and the different departments.
- Regularly report the state of information security to the Board of Directors.
- Promote the continuous improvement of the information security management system.
- Prepare the organization's development strategy in relation to information security.
- Coordinate the efforts of the different areas in matters of information security to ensure that such efforts are consistent, aligned with the strategy decided in this area, and avoid duplication.
- Prepare (and regularly review) the Information Security Policy for approval by Management.
- Approve the Information Security Regulations.
- Prepare and approve training requirements.
- Monitor and approve the main residual risks assumed by the organization and recommend possible actions.

- Monitor the performance of security incident management processes and recommend possible actions in relation to them. In particular, ensure coordination among the different security areas in the management of such incidents.
- Promote the performance of periodic audits to verify compliance with the organization's obligations in matters of security.
- Approve information security improvement plans for the organization. In particular, ensure the coordination of the different plans that may be carried out in different areas.
- Prioritize actions in the field of security when resources are limited.
- Ensure that information security is taken into account in all ICT projects from their initial specification to their entry into operation. In particular, ensure the creation and use of horizontal services that reduce duplication and support homogeneous operation of all ICT systems.
- Resolve conflicts of responsibility that may arise between the different responsible parties and/or between different areas of the organization, escalating cases in which it does not have sufficient authority to decide.

6.2 Functions of the Information Security Officer

- Maintain and verify the appropriate level of security of the information handled and the electronic services provided by the information systems.
- Promote training and awareness in matters of information security.
- Designate those responsible for carrying out the risk analysis and the statement of applicability; identify security measures; determine necessary configurations; and prepare system documentation.
- Provide advice for determining the system category in collaboration with the System Manager and/or the Information Security Committee.
- Participate in the preparation and implementation of security improvement plans and, where appropriate, continuity plans, validating them as required.
- Manage external or internal system reviews.
- Manage certification processes.
- Submit for approval by the Security Committee changes and other system requirements.
- Approve the Statement of Applicability on the basis of the required security measures.
- Approve the security procedures that form part of the Regulatory Map (and are not within the Committee's competence) and inform the Committee of the modifications made during the current period.
- Participate, within the framework of the Information Security Committee, in the preparation of the Information Security Policy for approval by Management.
- Act as Secretary of the Information Security Committee, performing the following functions:
    - Call meetings of the Information Security Committee.
    - Prepare the topics to be dealt with at Committee meetings, providing

timely information for decision-making.
- Prepare the minutes of the meetings.
- Be responsible for the direct or delegated execution of the Committee's decisions.

Coordination with Authorities and Incident Management

- Manage cybersecurity incidents from detection to resolution, including cooperation in their investigation.
- Report any anomaly, compromise, or vulnerability related to system security.
- Notify, without undue delay, the supervisory authorities, through the national reference CSIRTs, of incidents that have disruptive effects on service delivery and of detected vulnerabilities.
- Receive, interpret, and oversee the implementation of the instructions and guidelines issued by the supervisory authority, both for normal operations and for the remediation of deficiencies.
- Collect, prepare, and provide information or documentation to the supervisory authority and the national CSIRTs, whether upon request or on its own initiative.

Training, Oversight, and Relations with Third Parties

- Promote training and awareness in matters of information security.
- Oversee compliance, by external companies and suppliers, with the information security criteria established by the organization.

6.3 Functions of the Information and Service Owners (RS)

- Establish the security requirements applicable to Information (information security levels) and to Services (service security levels), and may request a proposal from the Information Security Officer while taking into account the opinion of the System Manager.
- Issue decisions regarding access rights to information and services.
- Accept the residual risk levels affecting information and services.
- Inform the Information Security Officer of any variation relating to the Information and Services for which they are responsible, especially the incorporation of new Services or Information under their charge. Such changes shall be communicated by the latter to the Information Security Committee at its next meeting.
- They bear ultimate responsibility for the use made of certain services and information and, therefore, for their protection.

6.4 System Manager (RSIS)

- Suspend or halt access to information or service provision if aware that they present serious security deficiencies.
- Develop, operate, and maintain the information system throughout its life cycle.
- Prepare the necessary operating procedures.
- Define the topology and management of the Information System, establishing the criteria for use and the services available within it.
- Ensure that specific security measures are properly integrated within the overall security framework.
- Provide the Information Security Officer and/or the Security Committee with advice for determining the System Category.
- Collaborate, if required, in the preparation and implementation of security improvement plans and, where appropriate, continuity plans.
- Carry out the functions of the system security administrator.

6.5 Functions of the Data Protection Officer

In compliance with Article 39 of the GDPR and Article 37 of the LOPDGDD, the functions of the Data Protection Officer (DPO) may be performed by an internal or external person designated by the organization in accordance with the applicable regulations.

Its functions are:

- Ensure compliance with the applicable regulations by collecting information, analyzing it, and reviewing compliance in relation to the data processing activities carried out within the organization, making any recommendations necessary to ensure compliance.
- Inform and advise the organization, and the users engaged in processing, of the obligations incumbent upon them under the applicable data protection regulations.
- Monitor compliance with the security regulations and the organization's internal policies on data protection, including the assignment of responsibilities, awareness and training of staff involved in processing operations, and the corresponding audits.
- Communicate the existence of a significant personal data breach to the governing and management bodies of Terminales Canarios S.L., proposing the necessary measures to prevent the continuation of such conduct.
- Provide the advice requested regarding the data protection impact assessment (hereinafter, "DPIA") and oversee its application, advising, among other matters, on:
    - Whether it is mandatory or appropriate to carry out a DPIA.
    - The definition of the methodology to be used for its development.
    - Whether the assessment should be carried out internally by the organization or outsourced.
    - The definition of the measures to be implemented.
    - The determination of the proper execution of the DPIA and the analysis of

whether the conclusions comply with the regulations.

- Cooperate with the Spanish Data Protection Agency when required, acting as its contact point for matters relating to data processing.
- The Data Protection Officer shall perform their duties independently, paying attention to the risks associated with processing operations. To do so, they must be able to:
    - Collect information to determine processing activities.
    - Analyze and verify the compliance of processing activities.
    - Inform, advise, and issue recommendations to the controller or processor.
    - Collect information to supervise the record of processing activities.
    - Advise on the principle of data protection by design and by default at all stages of the data life cycle.
    - Advise on whether or not DPIAs are carried out, the methodology, safeguards to be applied, etc.
    - Prioritize activities based on risks.
    - Advise the Data Controller on areas to be subjected to audits, training activities to be carried out, and processing operations to which more time and resources should be dedicated.
    - Address data subjects' questions regarding the processing of their personal data and the exercise of their rights under the General Data Protection Regulation.

7. Designation Procedure

The various responsible parties shall be appointed by the Board of Directors of Terminales Canarios S.L. New appointments and renewals shall be recorded in the meeting minutes every two years, or according to the needs of the organization and in accordance with the principle of separation of duties.

8. Conflict Resolution

For the proper coordination of the security organization among the responsible parties, a hierarchy must be established in which the following levels can be distinguished:

- **Governing Bodies**: determine the objectives that Terminales Canarios S.L. aims to achieve and are responsible for ensuring that they are achieved.
- **Executive Management**: understand the needs of the departments and how they coordinate with each other to achieve the objectives proposed by Management.
- **Operations**: focus on carrying out and managing activities.

If the responsible parties in charge of the security organization of Terminales Canarios S.L. are unable to establish a common objective, mission, or conclusion, in order to avoid conflicts and preserve the good working environment of Terminales Canarios S.L., the

situation shall be resolved in the hierarchical order indicated.

The hierarchy to which the responsible parties must adhere is as follows:

Governance	Security Committee
Executive	Information Security Officer
Operations	Systems Manager / Service Owner / Information Owner

9. Personal Data

With regard to the personal data processing carried out by Terminales Canarios S.L., a Personal Data Protection Policy has been established in accordance with the General Data Protection Regulation (GDPR), the Organic Law on Data Protection (LOPDGDD), and other applicable regulations, defining the principles, responsibilities, and measures applicable to the processing of personal data. This policy guarantees the legitimacy, lawfulness, transparency, and security of data processing, protects the rights of data subjects, and includes procedures for incident management, international transfers, impact assessments, and regulatory compliance. Its implementation is mandatory for the entire organization and is subject to periodic reviews.

In addition, it has a Record of Processing Activities detailing the affected processing activities and the corresponding responsible parties, together with the risk analyses and impact assessments carried out on those processing activities. Terminales Canarios S.L. guarantees compliance with the security measures established in this policy for all processing activities that include personal data, as well as the application of the privacy principles required by the applicable regulations.

10. Development of the Information Security Policy

This Information Security Policy shall be complemented by other documents (standards, guides, and security procedures). Compliance with the objectives set out in this Security Policy is achieved through the development of documentation comprising the standards and security procedures. For their organization, a procedure for document management has been defined, establishing the guidelines for Terminales Canarios S.L., management, and access.

The annual review of this Policy corresponds to the Information Security Committee, which shall propose improvements where necessary for approval by the same body that initially approved it.

TERMINALES CANARIOS

11. Third parties

When Terminales Canarios S.L. uses third-party services or provides information to third parties, such third parties shall be made aware of this Security Policy and of the Security Regulations applicable to those services or information.

Such third party shall be subject to the obligations established in those regulations and may develop its own operating procedures to comply with them. Specific procedures for incident reporting and resolution shall be established. It shall be ensured that third-party personnel are adequately aware of security matters at least at the same level as established in this Policy.

When any aspect of the Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Information Security Officer shall be required specifying the risks incurred and how they are to be treated. Approval of this report by the Information and Service Owner shall be required before proceeding.

Providers of outsourced services that are related to the security of the elements of the information system of Terminales Canarios S.L., except where justified and documented otherwise, shall designate a Point of Contact (POC) to facilitate and promote proper coordination between the parties in security matters. The POC shall be the Information Security Officer of the contracted company, who shall channel and oversee both compliance with the security requirements of the service provided and communications related to information security, risk management, and incident management. Failing that, this role may be assumed by the head of service, project manager, or another equivalent person designated by the company.

12. Staff Obligations

The Security Policy must be read, understood, and applied in its entirety by all employees of Terminales Canarios S.L. Failure to comply with any obligation established in this Policy or in the internal regulations may be subject to investigation, documentation, and reporting to the competent internal body, as appropriate and in accordance with the applicable legislation. Based on the outcome of the investigations, disciplinary measures may be adopted.

70647939N SAMUEL LEONARDO PEREZ (C:B38318572)
Firmado digitalmente por 70647939N SAMUEL LEONARDO PEREZ (C:B38318572)
Fecha: 2026.03.18 09:25:16 Z

42871840R JUAN LUIS SANTANA (R: B38318572)
Firmado digitalmente por 42871840R JUAN LUIS SANTANA (R: B38318572)
Fecha: 2026.03.18 09:51:43 Z

43831748G SARA ORIHUELA (R: B38318572)
Firmado digitalmente por 43831748G SARA ORIHUELA (R: B38318572)
Fecha: 2026.03.20 20:47:46 Z