Information Security Policy

Reviewed by the Board of Directors

on January 28, 2025

1 Purpose of the Policy

The purpose of this document, referred to as the Information Security Policy, is to define the principles and basic rules to ensure the security of information within Truck & Wheel, hereinafter TW Group, and to minimize non-financial risks. This, in turn, aims to enhance the security of the services the company offers to its clients as well as its own internal processes.

2 Scope

The scope of this Policy covers all information within TW Group, regardless of how it is processed, who accesses it, the medium in which it is contained, or its location, whether in printed or electronically stored form.

As a general policy, it is mandatory for all TW Group management teams to be aware of and comply with it, both in their internal relations and in interactions with other organizations.

3 General Principles of Information Security

This policy adheres to the recommendations outlined in the International Standard ISO/IEC 27001, as well as compliance with current legislation on personal data protection and any regulations related to information security that may affect TW Group.

It is established to ensure the adoption, implementation, and continuous operation of protocols and procedures based on the three fundamental components of information security:

- **Confidentiality.** Ensure that access to systems and data is granted only to authorized individuals.
- **Integrity.** Ensure the accuracy of information and systems against loss or destruction, whether accidental or intentional.
- **Availability.** Ensure that information and systems can be used in the required manner and within the necessary timeframes.

Additionally, TW Group establishes the following basic principles as fundamental guidelines for information security that must be considered in activities related to information processing:

- **Strategic Scope.** Information security must have the commitment and support of all management levels within TW Group, so that it can be coordinated and integrated into all strategic initiatives, forming a coherent and effective working framework.

- **Comprehensive Security.** Information security shall be understood as a comprehensive process composed of technical, human, material, and organizational elements, and must be considered an integral part of everyday operations.
- **Risk Management.** Risk analysis and management will be an essential part of the information security process, enabling the maintenance of a controlled environment and minimizing risks to acceptable levels. Risk reduction will be achieved through the implementation of security measures, establishing a balance between the information and its processing, the impact and probability of the risks it faces, and the effectiveness and cost of the security measures.
- **Proportionality.** The establishment of protection, detection, and recovery measures must be proportional to the potential risks and the criticality and value of the information and services affected.
- **Continuous Improvement:** Security measures will be periodically reassessed and updated to ensure their effectiveness in line with the continuous evolution of risks and protection systems. Information security will be managed, reviewed, and audited by qualified personnel.
- **Security by Default.** Systems must be designed and configured in a way that ensures an adequate level of security by default.

TW Group considers this policy to be mandatory for all personnel within the organization, and therefore, it must be understood and embraced by all levels of the organization.

The policy must be available on TW Group's corporate website at www.tw-group.com and in a shared repository of TW Group, ensuring it is accessible to all individuals within the group.

4 Management Commitments

The management of TW Group, aware of the importance of information security, declares the following commitments:

- Promote within the organization the functions and responsibilities related to information security.
- Provide the necessary resources to achieve the information security objectives.
- Promote the dissemination and awareness of the Information Security Policy among TW Group employees.

- Enforce compliance with the Policy, applicable legislation, and regulatory requirements in the field of information security.
- Consider information security risks in the decision-making process.

5 Roles and Responsibilities

TW Group is committed to safeguarding all assets under its responsibility through the necessary measures, always ensuring compliance with the various applicable regulations and laws.

The information security function falls under the Cybersecurity, Systems, and Infrastructure department, with the CISO being responsible for defining, implementing, and monitoring cybersecurity and information security measures.

Every user of the information systems is responsible for the proper use of these systems and for complying with the controls and recommendations established in the corresponding protocols, which are developed in alignment with this Policy.

On the other hand, employees have the obligation to act diligently with regard to information, ensuring that such information does not fall into the hands of unauthorized employees or third parties.

6 Information Security Objectives

TW Group will define a set of measurable objectives that contribute to minimizing and controlling the organization's risks.

These objectives must be measured at least semi-annually and reviewed annually to ensure they are aligned with the organization's strategy.

7 Regulatory Compliance

TW Group is committed to providing the necessary resources to comply with all applicable legislation, regulations, or standards related to information protection and security, and to establishing the responsibility for such compliance across all members of the organization.

The requirements of applicable laws related to the processing and security of information will be identified, and appropriate and reasonable mechanisms and measures will be established to ensure compliance. The standards from supranational organizations of which Spain is a member, as well as community and/or non-community regulations, will also be considered in relation to the areas where TW Group provides services. Additionally, the standards or codes of conduct originating from TW Group will also be taken into account.

8 Implementation of the Security Policy

To apply the principles outlined in this policy, action plans or continuous improvement actions must be defined, developed, implemented, and maintained. The development of these plans and actions should be based on formal risk analysis processes, evaluation criteria, risk management, or objective business needs, which will allow the implementation of the most suitable solutions.

At an operational level, the organization will develop its own security procedures, standards, and guidelines to ensure the integrity, confidentiality, and availability of information.

Similarly, the necessary information security management standards will be defined, in line with recognized international standards, to ensure effective and efficient monitoring of security actions, as well as the processes for continuous review and improvement of security.

9 Classification and Handling of Information

The organization's information must be classified based on its importance and handled according to that classification. To achieve this, an information classification model should be defined to determine the necessary technical and organizational measures to maintain its availability, confidentiality, and integrity.

TW Group must classify information based on the medium in which it is being used:

- Logical Medium: Information being used through office tools, email, or information systems.
- Physical Medium: Information stored on paper, magnetic media such as USB drives, DVDs, etc.

Based on the sensitivity of the information, TW Group must categorize the information into five levels.

- Public Use
- Limited Distribution
- Confidential Information
- Restricted Information

- Secret Information

Please refer to the definition in the classification levels standard.

10 Training and Awareness

The organization must establish training plans for all personnel on information security. These plans should be tailored to the target audience and specific area as deemed necessary. Additionally, periodic awareness campaigns on information security will be carried out for all staff through the most effective medium.

Furthermore, employees must be informed of updates to security policies and procedures that affect them, as well as existing threats, so they can ensure compliance with this policy.

11 Business Continuity Management

TW Group must have a Business Continuity Plan as part of its strategy to ensure the continuity of its services and the proper management of business impacts in potential crisis scenarios.

The Business Continuity Plan must be updated and approved periodically, along with the Disaster Recovery Plan, aligned with business continuity, covering the continuity of information and communication technologies.

Additionally, employees must be trained and educated in Business Continuity, which should be reviewed periodically to ensure it is aligned with the existing Plan.

12 Security Auditing and Vulnerability Management

A periodic identification of technical vulnerabilities in the information systems and applications used within the organization must be carried out, based on their exposure to such vulnerabilities, and appropriate measures should be adopted to mitigate the associated risks.

Once vulnerabilities are identified, the organization must apply the necessary corrective measures as soon as possible. The identification, management, and correction of vulnerabilities should follow a risk-based approach, considering the criticality and exposure of the assets.

13 Non-compliance and Disciplinary Sanctions

Non-compliance or deviations from the principles or guidelines outlined in this policy must be justified for business reasons and agreed upon with the Cybersecurity, Systems, and Infrastructure department.

Otherwise, total or partial non-compliance with the provisions in this document will result in disciplinary actions in accordance with TW Group's internal process. It is the responsibility of all employees of TW Group to report to the Information Security officer any event or situation that may constitute a breach of any of the guidelines defined in this policy.

14 Continuous Improvement

TW Group considers continuous improvement essential, and therefore, will define actions to enhance the organization's performance regarding the availability, integrity, and confidentiality of information.

15 Validity

The Information Security Policy will come into effect on the same day it is published.

This policy will be reviewed and approved annually by the Board of Directors. However, if significant changes occur in the organization or if major changes are identified in the threat and risk environment, whether legal, operational, regulatory, or contractual, it will be reviewed whenever deemed necessary.