Information Security Policy

Approved by the Board of Directors on March 26, 2024

1 Policy objective

The purpose of this document called Information Security Policy is to define the basic principles and rules to ensure the security of Truck & Wheel's information, hereinafter TW Group, and to minimize non-financial risks, resulting in an improvement in the security of the services the company offers to its customers and in the organization's own internal processes.

2 Scope

The scope of this Policy covers all information of TW Group companies regardless of how it is processed, who accesses it, the medium containing it or the place where it is located, whether it is printed or stored electronically. As a general policy, it is mandatory knowledge and compliance by all TW Group management, both internally and in their relations with other organisations.

3 General principles of information security

This policy responds to the recommendations set out in the International Standard ISO/IEC 27001, as well as compliance with current legislation on personal data protection and the regulations that may affect TW Group in the field of information security.
This policy is established to achieve the adoption, implementation and continuous operation of protocols and procedures based on the three basic components of information security:

- Confidentiality. Ensuring access to systems and data only by those authorised to do so.
- Integrity. Ensuring the accuracy of information and systems against accidental or intentional loss or destruction.
- Availability. Ensuring that information and systems can be used as and when required.

In addition, TW Group establishes the following basic principles as fundamental information security guidelines to be taken into account in information processing activities:

- Strategic scope. Information security must have the commitment and support of all levels of TW Group management so that it can be coordinated and integrated into all strategic initiatives to form a coherent and effective framework.
- Comprehensive security. Information security shall be understood as an integral process consisting of technical, human, material and organisational elements and should be considered as part of normal operations.
- Risk management. Risk analysis and management will be an essential part of the information security process and will enable the maintenance of a controlled environment, minimising risks to acceptable levels. Risk levels shall be reduced through the deployment of security measures and a balance shall be struck between the information and its processing, the impact and probability of the risks to which it is exposed and the effectiveness and cost of the security measures.

- Proportionality. The establishment of protection, detection and recovery measures should be proportionate to the potential risks and the criticality and value of the information and services affected.
- Continuous improvement: Security measures shall be periodically reassessed and updated to adapt their effectiveness to constantly evolving risks and protection systems. Information security shall be monitored, reviewed and audited by qualified personnel.
- Security by default. Systems should be designed and configured to ensure a sufficient degree of security by default.

TW Group considers that this policy is mandatory for all the staff of the organisation, so it must be understood and accepted by all levels of the organisation. The Policy must be available on TW's corporate website www.tw-group.com and in a common TW Group repository, so that it is accessible to everyone in the group.

4 Management commitments

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

- Promote information security roles and responsibilities in the organisation.
- Provide adequate resources to achieve information security objectives.
- Promote the dissemination and awareness of the Information Security Policy among TW Group employees.
- Enforce compliance with the Policy, current legislation and the requirements of regulators in the field of information security.
- Consider information security risks in decision-making.

5 Roles and responsibilities

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

The information security function falls to the Cybersecurity, Systems and Infrastructures department in the figure of the CISO, who is responsible for defining, implementing and monitoring cybersecurity and information security measures.

All users of the information systems are responsible for their proper use and for complying with the controls and recommendations established in the corresponding protocols drawn up in line with this Policy.

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

6 Information security objectives.

TW Group shall define a set of measurable objectives that contribute to minimising and controlling the organisation's risks.These objectives shall be measured at least semi-annually and reviewed annually in order to be aligned with the organisation's strategy.

7 Regulatory compliance

TW Group is committed to providing the necessary resources to comply with all applicable legislation, rules or regulations arising from the protection and security of information and to establish the responsibility for such compliance for all members of the organisation.

The requirements of the laws applicable to the processing and security of information shall be identified and appropriate and reasonable mechanisms and measures for compliance shall be established. The regulations issued by supranational bodies of which Spain is a member and EU and/or non-EU regulations will also be taken into account, depending on the areas in which the TW Group provides its services. Any rules or codes of conduct issued by the TW Group will also be taken into account.

8 Implementation of the security policy

In order to apply the principles set out in this policy, action plans or continuous improvement actions must be defined, drawn up, implemented and maintained. The elaboration of these plans and actions shall be based on formal risk analysis processes, risk assessment and management criteria or objective business needs, which allow for the implementation of the most suitable solutions.

At the operational level, the organisation shall develop its own security procedures, standards and guidelines to guarantee the integrity, confidentiality and availability of information.

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

9 Classification and processing of information

The organisation's information shall be classified by virtue of its importance and shall be treated in accordance with that classification. To this end, an information classification model must be defined to determine the technical and organisational measures necessary to maintain its availability, confidentiality and integrity.

TW Group shall classify information according to the medium on which it is being used:

- Software. Information that is being used by means of office automation, electronic mail or information systems.
- Physical support. Information that is on paper, magnetic media such as usb, dvd, etc.

Depending on the sensitivity of the information, TW Group should categorise the information into five levels.

- Public use
- Limited distribution
- Confidential information
- Restricted information
- Secret information

See definition in the classification levels standard.

10 Training and awareness

The organization shall establish training plans for all personnel on information security. These plans shall be in accordance with the target area and target audience as deemed necessary. Likewise, periodic information security awareness campaigns shall be conducted for all personnel through the most effective means.

Likewise, employees shall be informed of updates to the security policies and procedures of those affected and of existing threats, so that they can ensure compliance with this policy.

11 Business continuity management

TW Group shall have a Business Continuity Plan as part of its strategy to ensure continuity in the provision of its services and the adequate management of business impacts in the event of possible crisis scenarios.

The Business Continuity Plan should be periodically updated and approved together with the Disaster Recovery Plan aligned with business continuity, including the continuity of the operation of information and communication technologies.

In addition, employees should be trained in Business Continuity. The plan should be reviewed periodically to ensure that it is aligned with the existing plan.

12 Security audits and vulnerability management

A periodic identification of technical vulnerabilities of the information systems and applications used in the organization shall be carried out, according to their exposure to such vulnerabilities and adopting the appropriate measures to mitigate the associated risk.

Once vulnerabilities have been identified, the organization shall implement the necessary corrective measures as soon as possible. The identification, management and remediation of vulnerabilities should be done according to a risk-based approach, taking into account the criticality and exposure of the assets.

13 Non-compliance and disciplinary sanctions

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

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

14 Continuous Improvement

TW Group considers it essential to monitor continuous improvement, therefore, it will define actions to improve the performance of the organization in terms of availability, integrity and confidentiality of information.

15 Validity

The Information Security Policy shall be effective as of the day of its publication. This policy will be reviewed and approved annually by the Board of Directors. However, if relevant changes take place in the company or significant changes are identified in the environment of threats and risks, whether legal, operational, regulatory or contractual, it will be reviewed whenever deemed necessary.