



SECURITY INFORMATION AND PERSONAL DATA PROTECTION STANDARDS

Version 3.0

Madrid, 4th January 2023

Authors: Chief Compliance Officer
Validated by: Compliance Committee
Approved by: Management Body

Project: Integrated Management System
Classification: Public





NWorld understands the importance of information security and personal data protection as a key factor in achieving organizational excellence, market competitiveness, business sustainability and regulatory compliance.

Consequently, the group has established in the organization the processes for planning and implementing controls, as well as supervision and improvement, in order to guarantee confidentiality, integrity, authenticity, traceability and availability of information and services.

This document is integrated into **NWorld's** Integrated Management System (IMS). All its content is **mandatory knowledge and compliance** by all personnel and employees of third parties who have access to the information handled, and especially to automated personal data and information systems.

The **NWorld** management team is responsible for implementing, updating, improving, accrediting and maintaining an Information Security Management and Personal Data Protection (IMS) System, in accordance with the standard "*UNE-EN ISO / IEC 27001: 2017. Information technology. Security techniques. Information Security Management Systems. Requirements*", and pay particular attention to the postulates of Data Protection Act 2018 on the Protection of natural persons with regard to data processing and the free movement of such data (hereinafter, GDPR)

To respond, in a timely manner, to the requirements of any interested party, they are the following:

- Establish an Information Security and Personal Data Protection Committee, with authority and competence to guarantee the confidentiality, authenticity, integrity, availability and traceability of information.
- Implement the organization of security, designating those responsible for security, services, information, protection of personal data and information systems. NWorld has a Data Protection Officer (DPO) responsible for overseeing data protection compliance.
- Analyze the risks and threats to the security of the information handled and implement the organizational, operational and technical measures necessary for its proper treatment.
- To Ensure business continuity in the event of events that could affect critical assets.
- Plan the resources, human and technological, to provide services to customers in accordance with the requirements of information security and compliance with current legislation.
- Raise awareness and train all staff and collaborators on the risks and threats of information, the regulations for its prevention and mitigation and the notification of incidents.
- Measure and analyze the objectives and indicators of information security and data protection management, which allow the monitoring of security risks and incidents and the management and improvement of the effectiveness of measures and controls.
- Implement the processes of review, audit and continuous improvement, which guarantee the maintenance of the established controls and security measures.



- Comply with and demonstrate the applicable legal, normative and regulatory requirements, with special emphasis on those that guarantee digital rights and the protection of personal data.

The actions of the group and all its employees when carrying out the Processing of personal data are aligned with the basic principles of the GDPR:

- a. Principle of lawfulness, transparency, and fairness.
- b. Principle of purpose limitation. It implies that the data must be treated for specified, explicit and legitimate purposes, and prohibits data collected for one purpose to be subsequently processed in an incompatible manner for those purposes.
- c. Principle of data minimization. Technical measures must be applied and organizational measures must be implemented to ensure that only data is processed strictly necessary ("adequate, relevant and limited") for each of the Purposes.
- d. Principle of accuracy. The data must be updated and must be deleted or rectified when they are inaccurate.
- e. Principle of limitation of the storage period. Once the ends are achieved of the treatment, the data must be erased, blocked or anonymized.
- f. Principle of integrity and confidentiality. Treatment must ensure the integrity, availability and confidentiality of personal data.
- g. Principle of Accountability. The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles

The General Management of **NWorld**, therefore, is committed to the allocation of human and material resources, reasonable and proportionate, for the achievement of the above objectives.

The responsibility for the proper functioning of the Information Security and Data Protection Management System therefore lies with the General Management, delegating to the Chief Security Officer and DPO the authority and powers necessary for its effective implementation, accreditation, maintenance and improvement, with the support of the management team and the staff and collaborators of **NWorld**.