INFORMATION SECURITY AND PRIVACY POLICY, AND ARTIFICIAL INTELLIGENCE MANAGEMENT

PUBLIC INFORMATION

Control Box

Title:	Information Security and Privacy Policy, and Artificial Intelligence Management
Document Type:	Policy
File Name:	PO-Information Security and Privacy Policy, and Artificial Intelligence Management
Classification:	Public
State:	Approved
Author:	IMS Manager

Review and approval		
Reviewed by:	IMS Manager	
Approved by:	Senior Management	

Distribution list	
Corporate	NPAW staff and relevant stakeholders

INDEX

1 OBJECT

This policy is intended to provide the directives or guidelines that must be followed to protect the Organization's information from a wide range of threats, in order to:

- Guarantee the security of the operations carried out, through the Information Systems.
- Guarantee the privacy in the processing of personal data in the operations carried out, through the Information Systems.
- Align the use of AI with the organization's values and ethical principles.
- Mitigate potential risks associated with AI, such as algorithmic bias, discrimination, and loss of privacy.
- Promote the responsible and beneficial use of AI for society.
- Minimize the risks of damage.
- Ensure compliance with the objectives of the Organization.

NPAW is willing to ensure that the principles of the Information Security and Privacy Policy, and Artificial Intelligence Management form part of the Organization's culture, for which it has implemented an Information Security and Privacy Management System based on an internationally recognized standard.

All NPAW personnel, relevant stakeholders, and management must be aware of and comply with this policy.

This Policy will be developed through regulations, procedures, operating instructions, guides, manuals, and all those organizational instruments considered useful to achieve its objectives.

Our mission is to bring the most accurate and innovative business intelligence tools to the industry. We are strongly committed to excellence, constantly innovating and improving our suite of apps to match all our customers' needs.

2 SCOPE

The scope of the Information Security and Privacy Policy, and Artificial Intelligence Management coincides with the scope of the Integrated Management System (IMS).

This document develops the requirements demanded by the ISO/IEC 27001 Standard in its section 5.2 "Policy", and those corresponding to the ISO/IEC 27701 Standard on Information Privacy Management System, the ISO/IEC 42001 Standard, and the ENS Royal Decree.

3 LEGAL FRAMEWORK

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 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.
- Organic Law 3/2018, of December 5, on the Protection of Personal Data and the Guarantee of Digital Rights.
- Royal Legislative Decree 1/1996, of April 12, Intellectual Property Law.
- Royal Decree-Law 2/2018, of April 13, amending the consolidated text of the Intellectual Property Law.
- Royal Decree 311/2022, of May 3, regulating the National Security Scheme.
- Royal Decree 203/2021, of March 30, approving the Regulations for the action and operation of the public sector by electronic means.
- Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council, of 13 June 2024, laying down harmonised rules on artificial intelligence.
- Regulation of the activity.

4 DEFINITIONS AND ACRONYMS

For the purposes of a correct interpretation of this Policy, the following definitions are included:

- **Information:** Data that has meaning, in any format or support. It refers to all communication or representation of knowledge.
- **Information System:** It refers to a set of related and organized resources for the treatment of information, according to certain procedures, both computer and manual.

5 SPECIFICATIONS

5.1 OBJECTIVES OF THE INFORMATION AND PRIVACY SECURITY POLICY, AND ARTIFICIAL INTELLIGENCE MANAGEMENT

The main objective of the creation of this Information Security and Privacy Policy, and Artificial Intelligence Management, by the Security and Privacy Manager of the Integrated Management System (IMS) and NPAW's Management, is to guarantee customers and service users access to information with the quality and level of service required for the agreed performance, as well as to avoid serious loss or alteration of information and unauthorized access to it.

A framework is established for the achievement of the information security and privacy objectives for the Organization. These objectives will be achieved through a series of organizational measures and concrete and clearly defined rules.

This Security and Privacy Policy will be maintained, updated, and adequate for the purposes of the organization.

The principles that must be respected, based on the basic dimensions of security and privacy, are the following:

- **Confidentiality**: Property through which the information managed by NPAW can only be accessed by whoever is authorized to do so, prior identification, at the time and by the means enabled.

- **Integrity:** Property that guarantees the validity, accuracy, and completeness of the information managed by NPAW, its content being provided by those affected without any type of manipulation and allowing it to be modified only by whoever is authorized to do so.

- **Availability:** Property of being accessible and usable at agreed intervals. The information managed by NPAW is accessible and usable by authorized and identified clients and users at all times, its own persistence being guaranteed in the face of any foreseen eventuality.

- **Authenticity:** Property that guarantees that an entity (user, process, or system) is who it claims to be, ensuring the origin and receipt of data in order to prevent identity spoofing.

- **Traceability:** Property that allows an action or transaction to be unequivocally associated with the identity of a user, process, or system, keeping a complete audit log of accesses to and modifications of the information.

- **Privacy:** Property that guarantees the respect and protection of the personal data of individuals (data subjects) managed by NPAW, ensuring that they are treated in an appropriate, lawful and transparent manner.

Additionally, given that any Information Security and Privacy Management System must comply with current legislation, the following principle will be adhered to:

- **Legality:** Referring to compliance with the laws, rules, regulations, or provisions to which NPAW is subject, especially in matters of personal data protection.

NPAW, in order to offer its customers greater reliability in its services, and wanting to go beyond the requirements of data protection regulations, has implemented a privacy management system, integrating it into the Information Security and Privacy Management System. This

commitment is reflected in the involvement of NPAW employees, who are trained and participate in the system, and in the requirement of compliance to our service providers.

5.2 RISK MANAGEMENT

Information Security and Privacy management at NPAW is risk-based, in accordance with the international standards ISO/IEC 27001:2022, ISO/IEC 27701:2019 and ISO/IEC 42001:2023, and with the National Security Scheme (Royal Decree 311/2022).

It is articulated through a general process of assessment and risk treatment, which can potentially affect the information security and privacy of the services provided, as well as the use of artificial intelligence systems, consisting of:

- **Identify threats,** that will exploit vulnerabilities in the information systems that support, or on which information security and privacy depend.
- **Analyze the risk**, based on the consequence of materializing the threat and the probability of occurrence.
- **Assess the risk**, according to a previously established and approved level of broadly acceptable, tolerable, and unacceptable risk.
- **Treat unacceptable risk**, through appropriate controls or safeguards.

This process is cyclical and must be carried out periodically, at least once a year. An owner will be assigned for each identified risk, and multiple responsibilities may fall on the same person or committee.

5.3 ROLES, RESPONSIBILITIES, AND AUTHORITIES

The information security and privacy organization is organized around an Integrated Management System (IMS) and a series of committees and roles involved in its scope.

The defined security roles or functions are:

Function	Duties and responsibilities
Information Manager	Determine the security and privacy requirements of the information

	processed and make decisions regarding the information processed
Service Manager	Determine the security requirements of the services provided, including service levels
Security Manager	Determine the actions required to satisfy the information security and privacy requirements Supervise the suitability and effectiveness of the implemented security measures and report on the state of security
System Manager	Develop, operate, and maintain the Information System Implementation, management, and maintenance of security measures
Senior Management	Provide the necessary resources for the system Leading the system

This definition of duties and responsibilities is completed in the job profiles and in the internal regulations of the IMS.

5.4 THE COMMITTEE FOR THE MANAGEMENT OF SECURITY, INFORMATION PRIVACY AND ARTIFICIAL INTELLIGENCE

The Committee for the Management of Security, Information Privacy and Artificial Intelligence is the body with the greatest responsibility within the Integrated Management System, including the scope of the National Security Scheme (ENS), and is made up of the Information Manager, the Service Manager, the Security Manager, and the System Manager. Decisions will be made by voting among the members and with the only requirement being a simple majority. In the event of a conflict between the different managers, it will be resolved by the Committee itself, escalating to Senior Management those cases in which there is not sufficient authority to decide.

Security management within the scope of the ENS is entrusted to the Security Manager, who will inform the Committee of the need to issue policies and procedures complementary to corporate security policies to ensure compliance with Spanish regulations.

These members are appointed by the General Directorate of NPAW, the only body that can appoint, renew and dismiss them.

5.5 FRAMEWORK FOR THE SETTING OF INFORMATION SECURITY AND PRIVACY GOALS

The setting of information security and privacy, and artificial intelligence management objectives is carried out taking into account the following inputs:

- Reports from the Integrated Management System Security and Privacy Officer, approved by NPAW Management.
- Opportunities for improvement found during the operation of the IMS.
- Contributions of the Data Protection Officer (DPO), who supervises and advises on compliance with data protection and privacy regulations, as well as on the identification and mitigation of risks associated with the processing of personal data.
- Contributions from the Processing Owners (POs), who in the different areas supervise the performance of personal data processing in accordance with the established rules.

When setting objectives, it must be taken into account that they must be measurable and achievable, hence the planning for their achievement must include:

- What is going to be done
- The necessary resources

- Who will be responsible
- The deadline for its achievement
- How the results will be evaluated
- If applicable, the indicator associated with said objective

The Management, together with the Security and Privacy Manager of the Integrated Management System, will be responsible for defining the information security and privacy, and artificial intelligence management objectives for NPAW. These must be specific and consistent with its Information Security and Privacy Policy, and Artificial Intelligence Management, mission, vision, and values.

5.6 IMS OBJECTIVES

The NPAW IMS must guarantee:

- That policies, regulations, procedures, and operational guides be developed to support the information security and privacy policy, and artificial intelligence management.
- Identify the information that must be protected.
- That risk management be established and maintained in line with the requirements of the IMS policy and the NPAW strategy.
- That a methodology be established for the assessment and treatment of risk.
- That criteria be established with which to measure the level of compliance with the IMS.
- That the level of compliance of the IMS be reviewed.
- That non-conformities are corrected through the implementation of corrective actions.
- That personnel receive training and awareness on information security, data protection and the responsible use of artificial intelligence.
- That all personnel be informed about the obligation to comply with the Information Security and Privacy Policy, and Artificial Intelligence Management.
- The allocation of the necessary resources to manage the IMS.
- The identification and compliance with all legal, regulatory, and contractual requirements.
- That the security and privacy measures implemented are monitored and periodically reviewed to ensure their effectiveness and adaptation to changes in the regulatory, technological and business environment.

- That the information security and privacy implications with respect to business requirements be identified and analyzed.
- That the degree of maturity of the information security and privacy management system itself be measured.
- That continuous improvement be carried out on the IMS.

5.7 ORGANIZATION AND RESPONSIBILITIES

- The General Directorate of NPAW is responsible for approving this policy.
- The Committee for the Management of Security, Information Privacy and Artificial Intelligence is responsible for reviewing this policy.
- The IMS Security Manager is responsible for maintaining this policy.
- The Data Protection Officer supervises and advises on compliance with the measures implemented.
- The Processing Owners supervise the processing of personal data.

This policy must be reviewed regularly along with the rest of the Corporate Policies based on the agreed review scheme, and whenever relevant changes are made, in order to ensure that it is aligned with the company's strategy.

5.8 APPLICATION OF THE POLICY

NPAW has developed this document that contains the General Policy for Information Security and Privacy and that has been approved by the General Management and made known to all company personnel.

5.9 TRAINING AND AWARENESS

The Security and Privacy Officer of the Integrated Management System must ensure that all personnel involved in the IMS are aware of this policy, its objectives and processes, through its dissemination, training and awareness-raising actions. In the case of data protection training, it shall take into account the requirements of the Data Protection Officer and the Processing Owners.

It must also guarantee the distribution of the documents that apply to each level, according to the different roles defined in the company.

5.10 AUDIT

The General Directorate of NPAW must guarantee and verify, through internal and external audits, the degree of compliance with the guidelines of this Policy and that these are operated and implemented correctly, taking responsibility for compliance with the corrective measures that may have been determined in order to maintain continuous improvement.

5.11 VALIDITY AND UPDATE

This policy is effective from the moment of its publication and is reviewed at least once a year.

The objective of the periodic reviews is to adapt the policy to changes in the context of the organization, paying attention to external and internal issues, and analyzing information security and privacy incidents, as well as the findings found in the IMS. During these reviews, all the Standards and other documents that elaborate on the policy will also be updated, following a periodic update process subject to relevant changes such as company growth, organizational changes, infrastructure changes, and the development of new services, among others.

As a consequence, a list of objectives and actions to be undertaken and executed during the following year will be drawn up to guarantee Information Security and Privacy and the proper use of the resources that support and process it in NPAW.

6 SANCTIONS

Non-compliance with the Information Security and Privacy Policy, and Artificial Intelligence Management, as well as other related standards and procedures, will result in the application of sanctions in accordance with the magnitude and nature of the non-compliance, pursuant to the applicable labor legislation.

7 RATIFICATION

All the undersigned assume and fully accept the contents of this Policy and undertake to apply it in their respective areas in order to achieve the proper functioning of the Integrated Management System.

Barcelona, July 30, 2026

Sergi Vergés
Senior Management

Sergi Laencina
IMS Manager