INFORMATION SECURITY AND PRIVACY POLICY

NPAW

PUBLIC INFORMATION

Control Box

Title:	Information Security and Privacy Policy
Document Type:	Normative
File Name:	PO-Security and Privacy Policy
Classification:	Public
State:	Approved
Author:	Security and Privacy Manager

Review and approval		
Reviewed by:	Security and Privacy 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.
- 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 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.

2 SCOPE

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

This document develops the requirements demanded by the ISO/IEC 27001:2022 Standard in its section: 5.2 "Policy", and those corresponding to the ISO/IEC 27701:2019, Information Privacy Management System.

3 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.

4 SPECIFICATIONS

4.1 OBJECTIVES OF THE INFORMATION AND PRIVACY SECURITY POLICY

The main objective of the creation of this Information Security and Privacy Policy, 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.
- **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.

4.2 RISK MANAGEMENT

Information Security and Privacy management at NPAW is risk-based, in accordance with the international standard ISO/IEC 27001:2022 and ISO/IEC 27701:2019.

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, 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 risk** unacceptable, 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.

4.3 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.

4.4 FRAMEWORK FOR THE SETTING OF INFORMATION SECURITY AND PRIVACY GOALS

The setting of information security and privacy 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 (PTs), 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 objectives for NPAW. These must be specific and consistent with its Information Security and Privacy Policy, mission, vision, and values.

4.5 IMS OBJECTIVES

The NPAW IMS must guarantee:

- That policies, regulations, procedures, and operational guides be developed to support the information security and privacy policy.

- 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 and data protection.
- That all personnel be informed about the obligation to comply with the information security and privacy policy.
- 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.

4.6 ORGANIZATION AND RESPONSIBILITIES

- The General Directorate of NPAW is responsible for approving this policy.
- The Information Security and Privacy Management Committee 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 Data Controllers 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.

4.7 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.

4.8 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 Data Controllers.

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

4.9 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.

4.10 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 it to the changes in the context of the organization, with attention to external and internal issues, analyzing the incidents that have occurred in information security and the Non-Conformities found in the IMS. All this harmonized with the results of the different risk assessment processes.

When reviewing the Policy, all the Standards and other documents that develop it will also be reviewed, following a periodic update process subject to relevant changes that may occur:

company growth and organizational changes, changes in infrastructure, 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.

5 SANCTIONS

Failure to comply with the Information Security and Privacy Policy and other regulations and procedures that develop it, will result in the application of sanctions, according to the magnitude and characteristics of the non-compliance aspect, in accordance with current labor legislation.

6 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, November 15, 2023

33940740P
SERGI VERGES
(R: B64908460)

Firmado digitalmente
por 33940740P SERGI
VERGES (R: B64908460)
Fecha: 2023.11.15
11:48:21 +01'00'

Sergi Vergés

Senior Management

SERGI
LAENCINA
VERDAGUER -
DNI 33956835A

Digitally signed by
SERGI LAENCINA
VERDAGUER - DNI
33956835A
Date: 2023.11.15
12:37:00 +01'00'

Sergi Laencina

The person in charge of IMS