SAMPOL

Version 2.0

SAMPOL GROUP **INFORMATION SECURITY POLICY**

Approved by Carmen Sampol Massanet on
10 February 2025

01. APPROVAL AND EFFECTIVE DATE

Text approved on 10 February 2025 by Carmen Sampol Massanet, CEO of SAMPOL.

This Information Security Policy takes effect from that date and will remain in force until replaced by a new policy. This document supersedes Version 1.0 and constitutes the Information Security Policy 2.0.

02. REVIEW

The policy will be reviewed annually by the ICT Security Committee unless significant changes warrant an earlier revision.

03. INTRODUCTION

SAMPOL relies on Information and Communication Technology (ICT) systems to achieve its objectives. These systems must be managed diligently, with appropriate measures in place to protect them against accidental or intentional damage that could compromise the availability, integrity, confidentiality, traceability or authenticity of the information handled or the services provided.

The goal of information security is to ensure the quality of information and the continuous delivery of services by taking preventive action, monitoring daily operations and responding swiftly to incidents.

ICT systems must be protected against rapidly evolving threats that could affect the confidentiality, integrity, availability, intended use and value of information and services. To counter these threats, a strategy is required that adapts to changing environmental conditions to guarantee uninterrupted service delivery. This means departments must implement the minimum security measures mandated by the National Security Framework (ENS for its initials in Spanish), continuously monitor service performance levels, track and analyse reported vulnerabilities and prepare an effective response to incidents to ensure service continuity.

Each department must ensure that ICT security is an integral part of every stage of a system's life cycle,

from its conception to decommissioning, including development or procurement decisions and operational activities. Security requirements and funding needs must be identified and incorporated into planning, request for proposals and tender specifications for ICT projects.

Departments must be prepared to prevent, detect, respond to and recover from incidents, in accordance with Article 7 of the ENS.

Prevention

Departments must prevent, or at least minimise as much as possible, any security incidents that could compromise information or services. To this end, departments must implement the minimum security measures established by the ENS, along with any additional controls identified through a threat and risk assessment. These controls, as well as the security roles and responsibilities of all personnel, must be clearly defined and documented.

To ensure compliance with this policy, departments must:

- Authorise systems before they go into operation.
- Request periodic reviews by third parties to obtain an independent assessment.
- Regularly assess security, including routine evaluations of configuration changes.

Detection

Since incidents can rapidly degrade service quality, ranging from minor slowdowns to complete outages, services must be continuously monitored to detect anomalies in service performance levels and take appropriate action in accordance with Article 9 of the ENS.

Monitoring is particularly critical when establishing lines of defence as outlined in Article 8 of the ENS. Mechanisms for detection, analysis and reporting must be implemented to ensure that responsible parties are regularly informed whenever there is a significant deviation from predefined normal parameters.

Response

Departments must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or external organisations.
- Set up protocols for exchanging information related to incidents. This includes two-way communication with Emergency Response Teams (CERT).

Recovery

To ensure the availability of critical services, departments must develop ICT system continuity plans as part of their overall business continuity and recovery strategy.

04. SCOPE

This policy applies to all ICT systems within SAMPOL and to all members of the organisation working with them, without exception.

05. MISSION AND OBJECTIVES OF THE ORGANISATION

SAMPOL's mission is clear: to meet the energy and technology needs of its clients by creating and designing tailored solutions through its business units, ensuring that energy and technology contribute to a better life and more efficient energy consumption.

Its vision is to be a leader in energy generation and distribution, as well as in telecommunications infrastructure and installations, actively contributing to social well-being, sustainable development and value creation for its stakeholders.

06. REGULATORY FRAMEWORK

SAMPOL has a dedicated department and team responsible for regularly reviewing legislative changes, whether due to amendments to existing laws or the introduction of new regulations that may be applicable. For further information, please contact **Yolanda Rodríguez García.**

Within the regulatory framework applicable to SAMPOL, the following security-related regulations apply:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016.
- ORGANIC LAW 3/2018, of 5 December, ON PERSONAL DATA PROTECTION AND THE GUARANTEE OF DIGITAL RIGHTS.
- ROYAL DECREE 311/2022, of 3 May, regulating THE NATIONAL SECURITY FRAMEWORK (ENS).

07. SECURITY ORGANISATION

Committees: Duties and responsibilities

The **ICT Security Committee** will be composed of **Carmen Sampol Massanet,** CEO of the company.

This committee will be responsible for approving rules and procedures governing the use of ICT, as well as defining training requirements for ICT personnel.

The **Secretary of the ICT Security Committee** will be **Juan del Junco,** who will be responsible for drafting the Information Security Policy document, ensuring compliance with regulations, staying up to date with technological changes and conducting risk analyses.

The Secretary will report any changes or modifications to the Security Committee.

Roles: Duties and responsibilities

A detailed breakdown of this section is provided in document PR.E.8.P.24 – Roles and Responsibilities. The following roles are included:

- Information Manager: **Rafael Aldana.**
- Service Manager: **Juan del Junco.**
- Controller (Data Protection): **SAMPOL.**
- Security Manager: **Roberto Negro Gil.**
- Data Protection Officer: **Yolanda Rodríguez García.**
- System Manager: **Yolanda Rodríguez García.**
- System Security Administrator: **José Manuel Valle Gómez.**

Appointment procedures

The Information Security Manager will be appointed at the proposal of the ICT Security Committee. The appointment will be reviewed every two years or whenever the position becomes vacant.

The ICT Security Committee will appoint the System Manager, defining their duties and responsibilities within the framework of this policy.

Information security policy

The ICT Security Committee is responsible for conducting an annual review of this Information Security Policy and proposing updates or maintaining its current version. The policy will be approved by the Information Security Manager and communicated to all relevant parties to ensure awareness.

08. PERSONAL DATA

SAMPOL processes personal data. The Security Document, accessible only to authorised personnel, contains details on the affected files and their respective responsible parties. All of SAMPOL's information systems must comply with the security levels required by applicable regulations, based on the nature and purpose of the personal data recorded in the Security Document.

09. AWARENESS AND TRAINING

The goal is to ensure full awareness that information security affects all SAMPOL members and all activities, in line with the Integral Security Principle outlined in Article 5 of the ENS. Additionally, the necessary measures must be implemented to ensure that all individuals involved in the process, as well as their hierarchical supervisors, develop an understanding of the associated risks.

10. RISK MANAGEMENT APPROACH

Risk analysis will serve as the foundation for determining the security measures to be implemented, in addition to the minimum requirements established by the National Security Framework (ENS), in accordance with Article 6 of the ENS.

All systems subject to this policy must undergo a risk analysis, assessing the threats and risks to which they are exposed. This analysis will be conducted:

- Regularly, at least once a year.
- Whenever there is a change in the information being handled.
- Following a major security incident.
- When significant vulnerabilities are reported.

To standardise risk assessments, the ICT Security Committee will establish benchmark risk evaluations for different types of information managed and services provided. The ICT Security Committee will also facilitate the allocation of resources to meet security needs across different systems, promoting cross-cutting investments.

11. DEVELOPMENT OF THE INFORMATION SECURITY POLICY

This policy will be developed through security regulations that address specific aspects of information security. These security regulations will be made available to all members of the organisation who need to be aware of them, especially those who use, operate or administer SAMPOL's information and communication systems.

The security regulations will be accessible in the Cybersecurity folder within Public Resources of the corporate document management system, which is available to SAMPOL employees.

12. STAFF OBLIGATIONS

All members of SAMPOL are required to be aware of and comply with this Information Security Policy and the Security Regulations. It is the responsibility of the ICT Security Committee to ensure that the necessary means are in place for all affected personnel to receive this information.

All SAMPOL members must attend an ICT security awareness session at least once a year. A continuous awareness programme will be implemented to reach all SAMPOL members, particularly new employees.

Individuals responsible for the use, operation or administration of ICT systems will receive training on secure system management, as needed for their job roles. This training will be mandatory before assuming any responsibility, whether it is their first assignment, a job transfer or a change in responsibilities within the same role.

13. THIRD PARTIES

When SAMPOL provides services to other organisations or handles information belonging to third parties, those organisations will be informed of this Information Security Policy. Communication channels will be established for reporting and coordination between the respective ICT Security Committees, along with incident response procedures.

When SAMPOL uses third-party services or shares information with third parties, they will be made aware of this Information Security Policy and the Security Regulations relevant to the services or information in question. Such third parties will be subject to the obligations set out in these regulations, while retaining the ability to develop their own operational procedures to comply with them.

Specific reporting and incident resolution procedures will be established. It will be ensured that third-party personnel receive adequate security awareness training, at a level at least equal to that required by this Policy.

If a third party is unable to fully comply with any aspect of this Policy as outlined above, a Security Manager report will be required, specifying the risks involved and how they will be addressed. Approval of this report will be required from the Information and Service Managers before proceeding.

SIGNATURE OF THE PERSON APPROVING THE POLICY

Carmen Sampol Massanet
CEO of SAMPOL

SAMPOL

Camí del Reis, 308 B. 1ª Planta. Edificio Mapfre
07011 Palma de Mallorca. Islas Baleares. Spain
+34 971 76 44 76
www.sampol.com