Document Type: POLICY

Information Security Policy

Document classification: PUBLIC USE

CONTENTS

1. - OBJECTIVE, SCOPE, AND STANDARDS

Objective:

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

- Guarantee the security of the operations carried out through the Information Systems.
- Minimise the risks of damage.
- Ensure compliance with the Organisation's objectives.

The aim of Information Systems and Technology is to ensure that the principles of the Information Security Policy form part of the culture of PortAventura, for which it has implemented an Information Security Management System based on a globally recognised standard.

All Information Systems and Technology personnel, including partners, suppliers, and management, must know and comply with this Policy.

This Policy will be developed through regulations, procedures, operating instructions, guides, manuals and any other organisational instruments considered useful to achieve its objectives.

Scope:

These rules apply to the entire scope of action of Information Systems and Technology (hereinafter, IST), and its contents are based on the more general guidelines defined in the current legal system, in the Information Security Policy, and in the IST Security Standards.

The scope of the Information Security Policy coincides with the scope of the Information Security Management System (ISMS).

Standards:

The reference standards taken into account for the drafting of this rules are:

- ISO/IEC 27001:2013 in its domain N.5.2 "Policy"
- Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, regarding the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
- Law 3/2018 on Data Protection and Guarantee of Digital Rights (LOPD-GDD).

This procedure applies to all documents and records related to the ISMS, created by PortAventura.

2. – DEFINITIONS

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

- **Information**: data that have meaning, in any format or medium. This refers to any communication or representation of knowledge.
- **Information System**: a set of related and organised resources for the processing of information, according to specific procedures, both computerised and manual.

3. – SPECIFICATIONS

3.1 Objectives of the Information Security Policy

The main objective of the creation of this Information Security Policy, by the Information Security Management System (ISMS) Security Manager and the Information Systems and Technology Department, is to guarantee clients and service users access to information with the quality and level of service required for the agreed performance, as well as avoiding serious loss or alteration of information, and unauthorised access.

A framework is established to achieve the Information Security objectives for the Organisation. These objectives will be achieved through a series of organisational measures and specific and clearly defined rules.

This Security Policy will be maintained, updated, and adjusted for the purposes of the Organisation.

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

- **Confidentiality**: property by which the information managed by Information Technology and Systems can only be accessed by whoever is authorised to do so, subject to identification, at the authorised time and by the authorised means.
- **Integrity**: property that guarantees the validity, accuracy, and completeness of the information managed by Information Systems and Technology, its content being that provided by those affected without any type of manipulation and allowing it to be modified only by whoever is authorised to do so.
- **Availability**: property that can be accessed and used at agreed intervals. The information managed by Information Systems and Technology is accessible and usable by authorised and identified customers and users at all times, guaranteeing its own persistence in the event of any foreseen eventuality.

Additionally, given that any Information Security Management System must comply with current legislation, the following principle will apply:

- **Legality**: in reference to compliance with the laws, rules, regulations or provisions that govern Information Systems and Technology, especially regarding the protection of personal data.

3.2 Risk Management Control Policy

Information Security Management within the context of Information Systems is risk-based, in accordance with the international standard ISO/IEC 27001: 2013.

It is articulated through a general assessment and management of the risk, which can potentially affect the security of the information pertaining to the services provided, consisting of:

- **Identification of threats** that will take advantage of vulnerabilities in the Information Systems that support, or on which the information security depends.
- **Risk analysis** based on the consequences if the threat materialises and the probability of its occurrence.
- **Assessment of the risk** against a previously established and approved level of risk (broadly acceptable, tolerable, and unacceptable).
- **Dealing with an unacceptable risk** through appropriate controls or safeguards.

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

3.3 Roles, responsibility, and authority

The Information Security organisation revolves around an Information Security Management System (ISMS) and a series of committees and roles involved in its scope.

3.4 Framework for setting Information Security objectives

Information Security objectives are established by taking into account the following inputs:

- Reports from the Information Security Management System Security Manager, approved by the Information Systems and Technology Department.
- Opportunities for improvement found during the operation of the ISMS.

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

- What is going to be done
- The necessary resources
- Who will be responsible
- The deadline for achievement
- How the results will be evaluated
- If applicable, the indicator associated with the objective

The Department, together with the Information Security Management System Security Manager, will be responsible for defining the information security objectives for Information Systems and Technology, which must be specific and consistent with its Information Security Policy, mission, vision, and values.

3.5 Objective of the ISMS

The Information Systems and Technology ISMS must guarantee:

- That policies, regulations, procedures and operational guides are developed to support the Information Security Policy.
- That the information to be protected is identified.
- That risk management is established and maintained in line with the requirements of the ISMS Policy and the Information Systems and Technology strategy.
- That a methodology is established for risk assessment and management.
- That criteria are established with which to measure the level of compliance with the ISMS.
- That the ISMS compliance level is reviewed.
- That nonconformities are rectified through the implementation of corrective actions.
- That personnel receive information security training and awareness.
- That all personnel are informed about the obligation to comply with the Information Security Policy.
- That the necessary resources are assigned to manage the ISMS.
- That all legal, regulatory, and contractual requirements are identified and met.
- That the information security implications are identified and analysed with respect to business requirements.
- That the degree of maturity of the Information Security Management System itself is measured.

3.6 Organisation and responsibility

- The Information Systems and Technology Department is responsible for approving this policy.
- The Information Security Management Committee is responsible for reviewing this Policy.
- The ISMS Security Manager is responsible for maintaining this policy.

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

3.7 Policy Application

The Information Technology and Systems Department has developed this document, which contains the General Policy for Information Security and which has been approved by the General Management and made available to all personnel.

3.8 Training and awareness

The Information Security Management System Security Manager must guarantee that all personnel involved in the ISMS are aware of this Policy, its objectives and processes, through its dissemination, training actions, and awareness-raising actions.

They must also guarantee the distribution of the documents that apply to each level, according to the separate roles defined in IST.

3.9 Audit

The Information Systems and Technology Department must guarantee and verify, through internal and external audits, the degree of compliance and the correct compliance and operation of the guidelines of this Policy, taking responsibility for compliance with the corrective measures that may have been determined for the purposes of continuous improvement.

3.10 Validity and updates

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

The objective of the periodic reviews is to adapt the Policy following changes in the context of the Organisation, paying attention to external and internal issues, and analysing the Information Security incidents that have occurred and the non-conformities found in the ISMS. All this is harmonised with the results of the various risk assessment processes.

When reviewing the Policy, all the regulations and other documents that develop it will also be reviewed, following a process of periodic updating based on the relevant changes that may occur: growth of the IST area and organisational changes, changes in the infrastructure, or development of new services, among others.

Consequently, a list of objectives and actions to be undertaken and executed during the following year will be drawn up to guarantee Information Security and the proper use of the resources that support and manage it in Information Technology and Systems.

4. PENALTIES

Failure to comply with the Information Security Policy and the rest of the regulations and procedures that develop it, will result in the application of penalties, according to the magnitude and characteristics of the unfulfilled aspect, and in accordance with current labour legislation.