General Information Security Policy

Document ID	SGSI.PL.01
Version	6.0
Version Date	July 6, 2026
Created by	Information Security and Privacy Committee
Classification Level	Public
Approved by	Board of Directors

Table of Contents

1 Organizational Commitment

Visabeira I&D, hereinafter referred to as the Organization, recognizes information as one of its most valuable assets, essential to the development of its research and innovation activities, the trust of interested parties, and business sustainability. Therefore, the protection of information and the systems that support it is a strategic commitment of the Organization, embedded throughout its structure and culture.

Through this General Information Security Policy, the Organization affirms its commitment to preserving the confidentiality, integrity, availability and privacy of information, promoting a security culture based on shared responsibility, legal and regulatory compliance, and continuous improvement.

2. Purpose

This Policy establishes the principles, commitments and strategic guidelines that support Information Security management within the Organization. It constitutes the fundamental reference framework for the Information Security Management System (ISMS) and for all related documents, processes and decisions.

3. Scope

This Policy applies throughout the Organization and to all entities under its responsibility, regardless of the location, format or medium in which information exists.

In particular, it covers:

- All employees, service providers, partners, suppliers and other external parties with access to the Organization's information or systems;
- All information assets, including physical, digital and in-transit data, systems, networks, applications, digital platforms and associated devices;
- All business processes, including research, technological development, innovation, data processing and the use of Artificial Intelligence;
- All operating environments, namely physical facilities, cloud environments, on-premises environments and remote workstations;
- The supply chain and the adoption of emerging technologies, under the terms defined in this Policy and in the supporting documents.

This Policy is operationalized in the following areas, detailed in specific policies, standards and procedures within the Information Security Documentation Framework:

- Information classification.
- Access control and identity management.
- Device and workstation management.
- Backups and data recovery.
- Information security incident management.
- Third-party and supply chain risk management.

4. Information Security Principles

Information Security management within the Organization is guided by the following principles:

5. Management Commitment

The Organization's Management, aware of the strategic relevance of Information Security, is committed to leading, supporting and ensuring the implementation, maintenance and continuous improvement of the ISMS.

In this regard, the Organization commits to:

- Comply with all applicable legal, regulatory, normative and contractual requirements, including, among others, the General Data Protection Regulation (GDPR), the Cybersecurity Legal Framework and other applicable national legislation on the security of networks and information systems, as well as ISO/IEC 27001 and other recognized frameworks relevant to its activity;
- Provide the human, technological, financial and organizational resources necessary for the effective operation of the ISMS;
- Promote regular training, awareness and capability-building activities suited to different functional profiles;
- Ensure dynamic risk management focused on the effectiveness of controls and the ability to respond to emerging threats and opportunities;
- Integrate Information Security into innovation initiatives, digital transformation programs and the adoption of emerging technologies, including Artificial Intelligence-based solutions;
- Ensure compliance with personal data protection principles and safeguard the rights of data subjects;
- Align Information Security with the Organization's sustainability, digital ethics, and Environmental, Social and Governance (ESG) policies.

6. Information Security Objectives

Consistent with the commitments undertaken, the Organization defines the following strategic objectives:

- Systematically assess, treat and monitor Information Security risks, maintaining residual risk within acceptable levels;
- Promote a strong and organization-wide security culture through continuous training, awareness and digital literacy programs;
- Manage user access and profiles securely and auditable, applying the principle of least privilege;
- Ensure the confidentiality, integrity, availability, traceability, auditability and privacy of information throughout its lifecycle;
- Embed security and privacy by design in all technological development and digital transformation projects;
- Consistently improve ISMS maturity through continuous improvement and adaptation to the technological, regulatory and threat landscape.

7. Risk Management

The Organization adopts a systematic and proportionate approach to Information Security risk management, based on recognized methodologies, namely ISO/IEC 27005 and the guidelines of the National Cybersecurity Center (CNCS). The process covers the identification, analysis, evaluation, treatment and monitoring of risks that may affect the confidentiality, integrity, availability or privacy of information.

The definition of risk appetite, acceptance criteria and treatment decisions - mitigate, avoid, transfer or accept - are approved by Top Management and reviewed periodically, with residual risks formally accepted under the terms defined in the ISMS risk management methodology.

8. Security Controls

The Organization adopts a set of Information Security controls that are proportionate to the identified risk and appropriate to the technological, organizational and regulatory context in which it operates. These controls are organized into four macro areas, aligned with international best practices:

- **Organizational controls:** which define governance, policies, processes and responsibilities regarding Information Security;
- **People controls:** which ensure the competence, awareness and secure behavior of employees and other parties with access to information;
- **Physical controls:** which protect the facilities, equipment and environment that support information systems;
- **Technological controls:** which ensure the protection of networks, systems, applications and data throughout their lifecycle.

The applicability, detail and metrics associated with each control are defined in the policies, standards and procedures that form part of the Information Security Documentation Framework, and are periodically reviewed according to the evolution of risk and the Organization’s context.

9. Training and Awareness

The Organization recognizes the human factor as an essential element of Information Security. The Organization promotes continuous training, awareness and digital literacy programs, adapted to different functional profiles and levels of responsibility, including members of management bodies. These programs cover, among other topics, cyber hygiene practices, personal data protection, responsible use of technologies, fraud prevention and incident response.

10. Information Security Organization and Governance

The Organization's ISMS is supported by an Information Security Documentation Framework, organized into levels, which integrates policies, standards, procedures, work instructions and records. This structure ensures the consistency, traceability and operationalization of the principles and commitments defined in this Policy.

The Information Security and Privacy Committee (CSIP) is responsible for creating, maintaining, reviewing and improving ISMS documentation, liaising with the Organization's other areas whenever necessary.

ISMS performance is assessed through key performance indicators (KPIs), internal audits conducted at least annually and management review, the results of which support decision-making and the definition of improvement actions. The methodological details are described in the Information Security Documentation Framework and the respective procedures.

11. Responsibilities

The specific roles, responsibilities and authorities within the scope of Information Security are defined in the Role Manual, organizational processes and ISMS operational documents.

Regardless of their role or hierarchical level, every employee, service provider or partner of the Organization must, in particular:

- Know, respect and apply this Policy, as well as the applicable internal standards and procedures;
- Comply with the Organization's code of conduct and applicable legislation, with particular attention to data protection and confidentiality;
- Assume responsibility for their actions and for the use of their access credentials;
- Immediately report any failure, incident or nonconformity related to Information Security;
- Protect their authentication means by not sharing them with third parties or using another person's credentials;
- Disclose confidential or internal information only under legally permitted and duly authorized terms;
- Adopt good practices when using the Organization's equipment, systems and information resources.

12. Information Security in the Supply Chain

The relationship with suppliers and service providers is managed in a structured manner, based on risk criteria proportionate to the criticality of the services provided and the sensitivity of the information involved. In this regard, the Organization ensures, namely:

- Clarity of the responsibilities of external entities regarding the protection of the information and resources to which they have access;
- The inclusion, in contracts, of specific clauses on confidentiality, data protection, information security and legal compliance;
- The execution of complementary confidentiality agreements whenever justified;
- The prior assessment of Information Security risks associated with supplier selection and maintenance;
- The continuous monitoring of supplier performance and compliance, as well as controlled management of changes to the services provided.

13. Non-Compliance and Exception Management

Non-compliance with this Policy, or with the other documents that are part of the ISMS, may give rise to disciplinary, civil, criminal or administrative sanctions, proportionate to the severity of the infringement and in accordance with applicable legislation, namely the Criminal Code and the Civil Code, as well as the Organization's internal regulations.

Exceptional situations that justify deviation from the defined requirements may only be accepted when duly justified, approved by the competent entities and documented, while maintaining alignment with Information Security principles.

14. Review, Communication and Continuous Improvement

This Policy is reviewed at least annually or whenever significant changes occur that may impact its content, namely changes in the scope of Information Security, the organizational structure or applicable legal, regulatory or contractual requirements.

Continuous improvement of the ISMS is ensured through application of the PDCA cycle (Plan-Do-Check-Act), supported by audit results, performance indicators, incident analyses, lessons learned and management reviews.

After each review, the Policy is formally communicated to all employees and made available to interested parties whenever requested or under the terms provided for in contracts, audits or legal obligations.

15. References

- ISO/IEC 27001 standard - Information Security Management Systems;
- General Data Protection Regulation;
- Cybersecurity Legal Framework and other applicable national legislation on the security of networks and information systems;
- National Cybersecurity Reference Framework (QNRCS) of the CNCS.