General Information Security Policy

Document ID	SGSI.PL.01
Version	5.0
Version Date	June 26, 2025
Created by	Information Security and Privacy Committee
Classification level	Internal Use
Approved by	Board of Directors

Index

1 Context

The **Information Security Policy (ISP)** is a strategic instrument within the document structure of Visabeira I&D, hereinafter referred to as the Organization. This policy guides decision-making in the field of Information Security, establishes clear priorities, and supports the promotion of an organizational culture focused on prevention and resilience.

Top Management, fully aware of the critical importance of Information Security for business sustainability and competitiveness, is committed to leading, promoting, and ensuring the implementation and continuous improvement of the **Information Security Management System (ISMS)**. In this context, it undertakes to involve and motivate all employees to:

- **Recognize** that information, systems, networks, supporting processes, and associated assets are vital for the Organization's activity. The confidentiality, integrity, and availability of information are fundamental requirements to ensure operational effectiveness, profitability, compliance, and the Organization's market reputation.
- **Proactively manage** risks related to information security, including those associated with the use of new technologies (e.g., Artificial Intelligence), remote work, and the supply chain, ensuring compliance with applicable legal, regulatory, and contractual requirements.
- **Apply** best practices, standards, and information security controls, supporting a continuous improvement process, guided by metrics, and capable of reinforcing a culture of security and shared responsibility.
- **Ensure** the continuity of critical business processes, supported by preventive measures, continuity plans, and a well-structured ISMS that is adaptable to the evolution of the internal and external context.

All documents within the organizational structure, whether specific policies, norms, regulations, processes, procedures, or evidence models, align with the principles and objectives of this Policy, coherently reflecting the commitments made regarding Information Security.

1.1 Scope

The **ISP** applies to the entire Organization and all entities under its responsibility, covering people, processes, technologies, and data that support organizational activities, regardless of the location, format, or medium in which the information resides. This policy is applicable to:

- **All employees**, service providers, partners, suppliers, and any other external parties who have access to the Organization's information or systems.
- **All of the Organization's information assets**, including physical, digital, and in-transit data, as well as systems, networks, applications, digital platforms, smart devices, and associated equipment.
- **All business processes**, including those involving technological development, innovation, data processing, and Artificial Intelligence (AI).
- **All organizational environments**, including physical facilities, cloud platforms, on-premises environments, and remote workstations.

The scope also includes:

- **The adoption and use of emerging technologies**, such as Artificial Intelligence and digital platforms supporting the business (e.g., Ticket systems - AMIGA Ticket).
- **Supply chain management**, imposing information security requirements on third parties based on the associated risk level.
- **Information governance and classification**, with a focus on protecting confidentiality, integrity, and availability of data, and complying with legal, regulatory, and contractual requirements (such as GDPR, AI Act, and fiscal or R&D requirements).
- **Business continuity**, through risk management, contingency and recovery plans, and the preservation of operational resilience.

All norms, procedures, instructions, and operational models must be aligned with this policy and interpreted considering its principles and commitments.

1.2 Purpose

The **ISP (Information Security Policy)** defines the principles, objectives, and strategic guidelines for Information Security within the Organization, establishing the foundation for effective and integrated information management across the entire Organization.

Its purpose is to:

a) **Establish the Information Security strategy**, aligning it with the organizational model, business objectives, and the principles of compliance and innovation.

b) **Promote a security culture**, encouraging responsible and conscious behaviors from all employees, partners, and service providers.

c) **Raise awareness within the organizational community** about the importance of information security literacy, fostering skills for identifying, preventing, and responding to risks and incidents.

d) **Integrate Information Security as a fundamental value**, essential for the Organization's continuity, competitiveness, and resilience.

e) **Assess and treat information security risks** by implementing appropriate controls that are proportionate to the acceptable risk level defined by Top Management.

f) **Strengthen the Organization's credibility, trust, and reputation** among its employees, regulatory bodies, partners, and other stakeholders.

g) **Protect information against unauthorized access, loss, alteration, or destruction** resulting from intentional actions, negligence, technical failures, or force majeure events.

1.3 Revision and Communication

The **ISP** is reviewed whenever significant changes occur that may impact its content, specifically:

- Changes in the scope of Information Security.
- Alterations in the organizational structure.
- Updates to applicable legal, regulatory, or contractual requirements.
- Alternatively, it is reviewed at least annually.

The objective of the review is to ensure that the ISP **remains adequate, effective, and aligned** with the Organization's strategic objectives and the current risk context.

Following each review, the ISP must be **formally communicated to all employees and made available to interested parties**, whenever requested or as stipulated in contracts, audits, or legal obligations.

2 Information Security

2.1 Definition of Information Security

Information and its repositories are **critical assets** for Visabeira I&D, essential for the Organization's operation, innovation, and sustainability. Regardless of its format, medium, collection method, transmission, or storage, information must be adequately protected against threats that could compromise its **confidentiality, integrity, availability, or privacy**.

Information Security involves applying a set of principles, practices, and controls, supported by a continuous risk management process, with the aim of:

- **Protecting information assets** from a comprehensive range of internal and external threats.
- **Ensuring the continuity** of the Organization's operations.
- **Maximizing the return** on investments in technologies and processes.
- **Ensuring compliance** with the international standard ISO/IEC 27001 and other applicable legal, regulatory, and contractual requirements.

Based on this standard, Information Security is formally defined as the preservation of the following fundamental pillars:

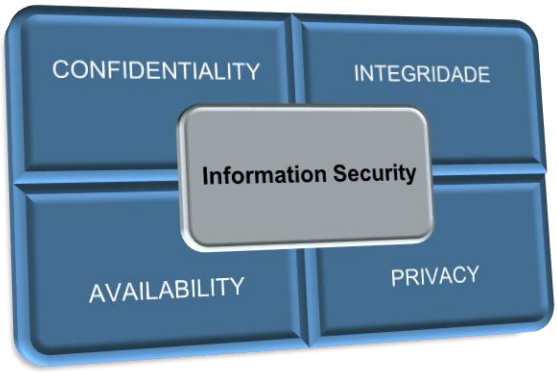

Figure 1 - Pillars of Information Security

Confidentiality: Guarantee that information is only accessible to authorized individuals.

Integrity: Safeguarding accuracy, consistency, and completeness of information.

Availability: Guaranteeing access to information and related assets whenever needed by authorized users.

Privacy: Protection of personal data and safeguarding the individual right to informational self-determination.

2.2 Organizational Commitment

The effectiveness of **Information Security** depends on the involvement and commitment of the entire organizational community. To achieve this, the following principles must be ensured:

- **Awareness:** All members of the Organization must be aware of the importance of information security and their role in maintaining it.
- **Shared Responsibility:** Security is everyone's responsibility, regardless of their role or hierarchical level.
- **Proactive Action:** Prevention, detection, and rapid response to incidents must be part of daily conduct.
- **Ethics:** Respect for the legitimate interests of others must guide the use of information.
- **Compatibility with Democratic Values:** The protection of information must respect fundamental rights, freedoms, and guarantees.
- **Risk Management:** Systematic risk analyses must guide the definition and application of controls.
- **Security by Design and by Default:** Security must be integrated from the conception, development, and implementation of infrastructures, systems, and processes.
- **Integrated Security Management:** There must be a coordinated and cross-cutting approach to information security management.
- **Privacy Management:** The protection of personal data must be ensured throughout its entire lifecycle, based on principles of minimization and accountability.
- **Continuous Improvement:** Policies, controls, and processes must be periodically reviewed and adjusted according to the needs of the Organization and the risk environment.

2.3 Top Management Commitment

Top Management is committed to leading, supporting, and actively promoting **Information Security** as a strategic element for the Organization's sustainability,

competitiveness, and innovation. To ensure the fulfillment of the objectives defined in the ISMS, Top Management commits to:

- **Comply with all applicable legal, regulatory, normative, and contractual requirements**, including those related to personal data protection, technological risk management, ethical use of Artificial Intelligence, cybersecurity, and compliance with the ISO/IEC 27001 standard.
- **Ensure alignment between information governance, system operations, and the organizational model**, promoting an integrated approach that involves all areas of the Organization.
- **Establish, implement, maintain, and continuously improve the ISMS**, based on dynamic risk management, ensuring the effectiveness of controls and the ability to adapt to new challenges, threats, and opportunities (technological, organizational, or legal).
- **Promote a culture of security and shared responsibility**, involving employees, partners, suppliers, and all interested parties.
- **Incorporate information security into innovation, digitalization, and emerging technology adoption processes**, ensuring that new systems (such as digital platforms, smart sensors, or AI-based solutions) integrate security requirements from the design phase.
- **Integrate information security with cross-cutting policies and objectives**, such as sustainability, digital ethics, ESG, and the protection of data subjects' fundamental rights.

2.4 Information Security Objectives

To continually improve its performance and the effectiveness of the ISMS, the Organization has defined **Strategic Information Security Objectives**. These objectives align with its values, internal policies, innovation goals, and organizational responsibility.

These objectives aim to protect information assets, ensure business continuity, guarantee legal and regulatory compliance, and foster an organizational culture of security and trust.

The Organization's Information Security Objectives are:

- **Assess, treat, and monitor information security risks** based on consistent risk management methodologies. This ensures effective controls are implemented and residual risks remain within the acceptance level defined by the Organization.
- **Promote a strong and pervasive security culture** through regular training, awareness, and capacity-building actions. These actions will be tailored to different functional profiles, including topics such as digital literacy, data protection, responsible AI use, and incident prevention.
- **Securely and auditable manage user access and profiles**, ensuring that assigned permissions are compatible with responsibilities, competencies, and the principle of least privilege.

- **Define and apply appropriate technical and organizational controls** to ensure the confidentiality, integrity, availability, traceability, auditability, and privacy of information throughout its entire lifecycle.
- **Integrate information security from the design phase** ("security and privacy by design") into all technological development projects, digital transformation initiatives, and new solution adoptions.
- **Adopt a continuous improvement approach** based on indicators, audits, reviews, and lessons learned. This ensures the ISMS evolves to higher maturity levels and responds with agility to changes in the technological, regulatory, and threat landscape.

3 Implementing the Information Security Policy

3.1 Context

- Information, along with all its supporting processes, systems, networks, and digital assets, are **strategic and essential resources** for the Organization's business. The **confidentiality, integrity, availability, and privacy** of this information are fundamental pillars for ensuring the Organization's competitiveness, revenue, profitability, and market reputation.
- In today's environment, securing information systems presents **growing challenges** due to the diversity and sophistication of threats. These include electronic fraud, advanced cyberattacks, corporate espionage, data breaches, sabotage, Denial-of-Service (DoS) attacks, and insider threats. All these threats are constantly escalating in scale and complexity.
- Our increasing reliance on **digital systems and services**, coupled with the widespread use of public and private networks and intensive information sharing, significantly complicates **access management and data protection**. This makes the Organization **more vulnerable to security incidents**.

- The identification of information security requirements is carried out by means of **structured risk analyses**. These analyses evaluate exposure to threats and vulnerabilities, thereby allowing for the prioritization of the most significant risks and the determination of effective mitigation measures, in alignment with best practices and international standards.
- The **ISP** is the core guiding document for creating, implementing, and reviewing all security-related documents, processes, and operational/tactical decisions. An integrated framework of **Policies, Standards, Procedures, Work Instructions, and Rules** underpins this policy, guaranteeing the Information Security Management System's consistency and effectiveness.
- Beyond that, the **ISP** integrates the need to align with personal data protection and privacy guidelines, ethical principles, and digital responsibility. It further supports the Organization's sustainability and environmental, social, and corporate governance initiatives, fostering an integrated and sustainable approach to information security.

3.2 Non-compliance

Any action that violates the **ISP**, as well as other policies, standards, procedures, rules, or work instructions related to the **ISMS**, and that compromises implemented security controls, will be subject to civil, criminal, and administrative sanctions. These sanctions will be applied in accordance with current legislation and applicable regulations and may be imposed individually or cumulatively.

Penalties will be applied proportionally to the severity of the infraction, following the Organization's internal disciplinary procedures, which ensure transparency and fairness in handling cases. Depending on the nature and impact of the contravention, disciplinary actions may include warnings, temporary suspension of access, suspension, or even the termination of the contractual or employment relationship with the Organization.

In all cases, the provisions of the Penal Code and the Civil Code, as well as the Organization's internal norms, regulations, processes, and procedures, will apply.

3.3 Exceptions Handling

Information Security objectives are more easily achieved when requirements, processes, and procedures are uniform and applied across all the Organization's functional units, roles, and services.

However, it's recognized that certain standards, processes, or procedures might not be viable or suitable for specific units, ongoing projects, new equipment, or recently implemented applications. It's expected that, within the scope of the Organization's activities, exceptional situations or scenarios will arise that cannot be effectively managed strictly within the requirements established in the ISP or related documentation.

While deviating from standard processes and procedures is discouraged, exceptional situations may justify adopting alternatives, provided these are properly substantiated with a consistent justification, aligned with Information Security principles, and have the necessary resources to ensure the adequate implementation and maintenance of these alternative requirements.

4 Organization of Information Security

4.1 Documented Information

To meet the requirements of the ISO/IEC 27001 normative standard, the Organization has developed a set of specific policies, procedures, and their key controls.

The Information Security and Privacy Committee is responsible for the creation, maintenance, critical review, improvement, and distribution of all **ISMS** documents. This committee consults with other relevant areas whenever necessary.

4.1.1 Documentation Structure

To ensure effective Information Security management, a documentary structure exists and is maintained. This structure is responsible for guiding, planning, implementing, maintaining, and improving Information Security practices.

This structure encompasses several levels to decentralize Information Security management responsibilities across the Organization's various areas. The levels at

which the Information Security Management System (ISMS) established by the Organization is documented and maintained are:

- **Level 1: General Guidelines and Commitments** of the Organization within its internal context and its relationship with the external context.
- **Level 2: Base Documents** that constitute and explain the functioning of the ISMS, thus providing support for all other information security documents, considering the requirements of reference standards, applicable legal requirements, and applicable work methodologies.
- **Level 3.1: Policies** that disseminate guidelines, controls, duties, and specifications for the various areas of information security.
- **Level 3.2: Procedures** are a means of clarifying details and specific aspects of activities or tasks within a given policy. **Work Instructions** are documents with detailed "how-to" descriptions, serving as reference documents when a specific task, activity, or service needs to be performed.
- **Level 3.3: Records** are the result of filling out a form template. Records provide elements for evaluating the ISMS's performance, supporting or creating evidence of the conformity of actions performed.

The Information Security documentary structure is defined in the Organization's **Information Security Documentation Framework**.

4.2 Responsibilities

The Organization clearly establishes the **roles, responsibilities, and authorities** of all employees through the following foundational documents:

- **Job Descriptions Manual**
- **Processes**
- **Information Security Policies and Procedures**
- **Operational Documentation**, such as Work Instructions, Records, and other supporting documents

Specific responsibilities within the ISMS should be consulted in the relevant documents that comprise it. However, regardless of their role or hierarchical level, all users, including Top Management and members of the Information Security organizational structure, have a duty to adopt **responsible behaviors** aligned with Information Security principles and objectives.

In this regard, each employee of the Organization must:

- **Understand, respect, and apply** the rules and responsibilities defined in this Policy, as well as internal standards and procedures, especially regarding the use of Information and Communication Technologies (ICT) resources.
- **Comply with the code of conduct** and observe all legal requirements applicable to their role, with particular attention to data protection and confidentiality legislation.
- **Take responsibility for their actions**, including violations of the rules for using information systems and resources, and be subject to the penalties provided in internal regulations and applicable legislation.

- **Immediately communicate** any failure, incident, or non-conformity related to Information Security, as established in the Incident Management Procedure.
- **Refrain from hiding their identity** or assuming the identity of others when using the Organization's information systems or resources.
- **Protect their authentication means**, such as passwords, cards, tokens, or other security devices, ensuring their confidentiality and never sharing them with third parties.
- **Assume full responsibility** for the use of their user account, including improper actions performed under their credentials.
- **Disclose confidential and internal information** only under legally provided terms, always seeking legal or ethical advice when necessary before doing so.
- **Adopt good practices** in the use of equipment and in information processing, actively contributing to the robustness and effectiveness of the ISMS.

4.3 Performance Evaluation

4.3.1 Key Performance Indicators (KPI)

Key Performance Indicators (KPIs) are **fundamental tools for evaluating Information Security performance** and the effectiveness of controls implemented within the ISMS.

The definition of KPIs follows the **SMART methodology** (Specific, Measurable, Achievable, Relevant, and Time-bound) and adheres to the following guiding principles:

- **Strategic alignment** with the Information Security Policy (ISP) and the defined objectives for Information Security.
- **Measurability and reliability**, allowing for the collection of consistent, objective, and verifiable data over time.
- **Comparability and reproducibility**, ensuring that results can be consistently analyzed across different periods or contexts.
- **Relevance and practical utility**, ensuring that the selected indicators effectively contribute to the continuous monitoring and improvement of the ISMS.

KPIs are **monitored and measured with a defined periodicity** and are reviewed annually as part of the Management Review. This review aims to validate their current relevance and their ability to support decision-making regarding the ISMS's performance and effectiveness.

4.3.2 Internal Audit

Internal audits of the ISMS (Information Security Management System) are **planned and executed annually** by the **Information Security and Privacy Committee** (ISPC) with the aim of systematically evaluating the **effectiveness, efficiency, and compliance** of implemented policies, procedures, and controls, as well as promoting the **continuous improvement of the ISMS**.

As part of the annual audit plan, at least one internal audit is conducted, which includes the following areas:

- **Data Protection**, based on the General Data Protection Regulation (GDPR) and applicable internal standards.
- **Information Security**, based on the requirements of the ISO/IEC 27001 standard, supplemented by recognized industry best practices.

Audits are conducted by qualified personnel who are independent of the activities being audited. Their **results are documented in audit reports**, which include any non-conformities, opportunities for improvement, and recommended corrective or preventive actions.

These reports are presented to **Top Management, Business Management, and the Organization's Information Security Team**, ensuring the involvement of stakeholders and proper accountability in following up on the audit findings.

4.3.3 Management Review

The Information Security Management System (ISMS) implemented by the Organization is reviewed at least once a year by the Information Security and Privacy Committee to ensure its continued suitability, adequacy, and effectiveness. This review is based on the requirements of ISO/IEC 27001, as well as applicable complementary guidelines.

The conclusions of the Management Review are **documented in formal minutes**, including decisions and actions to be taken to **continuously improve the ISMS**, address needs for change, optimize resources, and ensure sustained achievement of information security objectives.

5 Information Security for Suppliers

To safeguard the Organization's information assets and ensure the continuity and resilience of operations, **a structured and controlled process has been established for the selection, contracting, monitoring, and review of suppliers and service providers**, as defined in the ISMS documentation.

This process aligns with **supply chain risk management** principles, focusing on protecting the confidentiality, integrity, availability, and traceability of information shared with or accessible by external entities.

5.1 General

The security requirements applicable to suppliers include:

- **Clear Responsibilities:** All external entities providing services to the Organization must understand and accept their responsibilities and roles to mitigate the risk of theft, fraud, unauthorized access, or misuse of information and data processing infrastructures.
- **Mandatory Contractual Clauses:** All contracts with suppliers must include specific clauses on **confidentiality, data protection, information security**, and **legal compliance**. This ensures that third parties commit to safeguarding

all information they access, whether it's technical, organizational, or financial in nature.

- **Non-Disclosure Agreements (NDAs):** Where applicable, external entities accessing or using the Organization's infrastructures, systems, or data must sign supplementary NDAs. These agreements define their duties regarding information protection, especially when such aspects are not sufficiently detailed in the main contracts.
- **Risk Assessment:** The selection and ongoing relationship with suppliers include an **information security risk assessment**, proportional to the impact and criticality of the services provided, as defined by the ISMS methodology.

5.2 Performance Monitoring and Evaluation

Services provided by suppliers are subject to **systematic monitoring** based on predefined criteria aligned with information security objectives. Continuous evaluation ensures that suppliers maintain adequate levels of compliance and performance, as well as the evolution of their security controls.

5.3 Changes to Services

Changes to service provision, including maintaining and improving existing information security policies, procedures, and controls, must be managed with consideration for system criticality and based on a re-evaluation of risks. The Organization will control how changes to services provided by suppliers are developed and implemented.

6 PDCA Cycle of the Information Security Management System

The PDCA (Plan–Do–Check–Act) cycle is the methodology adopted by the Organization to structure, implement, and continuously improve the ISMS. This cycle ensures that processes are strategically planned, executed with appropriate resources, monitored using relevant indicators, and systematically reviewed, promoting evidence-based decision-making.

The PDCA approach thus enables the identification of improvement opportunities and ensures the **effectiveness, suitability, and alignment of the ISMS with organizational objectives as well as legal and regulatory requirements**.

This methodology is illustrated in the following figure

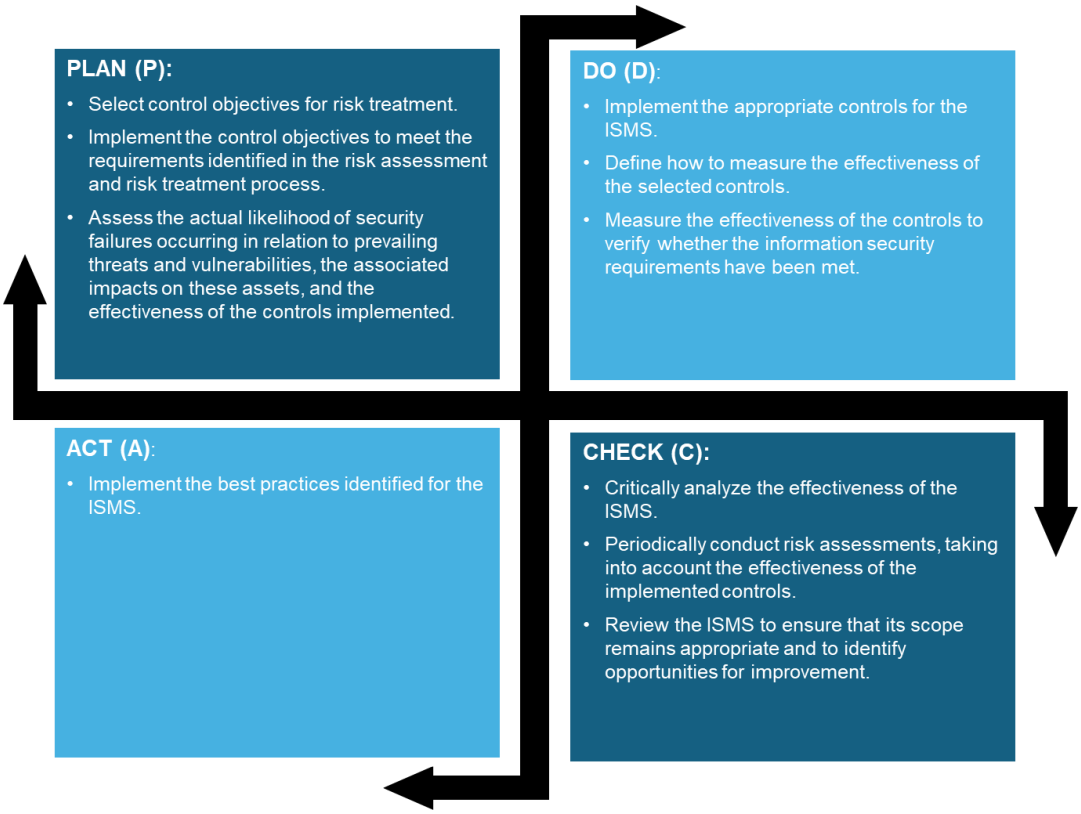

Figure 2 – PDCA Cycle of the Information Security Management System

6.1 Continual Improvement

The Organization is committed to the **continual improvement** of the ISMS, ensuring that it remains effective, up to date, and aligned with both internal and external contexts. To achieve this:

- **Periodic reviews** are conducted, either pre-scheduled or triggered by **significant changes**.
- **Nonconformities, audit results, corrective actions, lessons learned, and performance indicators (KPIs**) are taken into account as a basis for decision-making.
- Improvement actions may include **updating policies and procedures**, strengthening controls, providing additional staff training, or redesigning processes.

7 References

This document was created based on the market's best practices and standards, namely:

- ISO/IEC 27001 standard.