OD-00403-003-EN
Information Security Policy

Prepared by:	Reviewed:	Authorisation:
Quality and Regulatory Affairs Coordinator	**Information Security Committee**	**Chief Executive Officer**

	Date	Revision No. / Amendment No.	Description
REVIEW HISTORY	30/10/2024	001	Document creation
	11/06/2025	002	The Third Parties section is updated to incorporate the security requirements applicable to information service providers.
	27/11/2025	003	- Document updated following structural review, in accordance with UNE-EN ISO/IEC 27001 - The section aim and scope is updated to include the objectives of the ISMS and this policy. - The section on IS Roles and Responsibilities has been updated in accordance with the ISMS. - The section Management Commitment is included.

vitro [illegible]

Ferran Prat
CEO

Contents

1. AIM AND SCOPE

This Policy reflects VITRO, S.A.'s commitment to protecting information and the systems that manage it. Our objective is to ensure that information and the systems that process it are adequately protected against internal and external threats, minimising business risks and guaranteeing business continuity. This commitment is realised through the implementation and maintenance of an Information Security Management System (ISMS) certified in accordance with the international standard UNE-EN ISO/IEC 27001.

This Policy applies to all VITRO, S.A**.** personnel, as well as to third parties who access, process or manage corporate or customer information. It is mandatory for all processes, systems and services included in the scope of the ISMS.

The **general objectives** of the ISMS and this Policy are:

- To protect information by ensuring its confidentiality, integrity, availability, authenticity and traceability.
- To comply with applicable legal, regulatory and contractual requirements, especially in relation to personal data protection.
- To reduce the risks associated with threats and vulnerabilities that may affect information assets.
- To ensure operational resilience and business continuity through incident prevention, detection and response.
- To promote a culture of security based on awareness and individual responsibility among all employees.

2. REGULATORY FRAMEWORK

This Information Security Policy complements the Company Policy and Data Protection Policy of VITRO, S.A. and is based on the following standards and reference frameworks:

- **ISO/IEC 27001:2022**, Information Security Management Systems.
- **ISO/IEC 27002:2022**, Information Security Controls.
- **Regulation (EU) 2016/679 (GDPR)** on the protection of natural persons with regard to the processing of personal data.
- **Organic Law 3/2018 (LOPDGDD)** on the Protection of Personal Data and Guarantee of Digital Rights.
- **Law 34/2002 (LSSI)** on Information Society Services and Electronic Commerce.

3. DESCRIPTION

3.1. Context of the Organisation

VITRO, S.A. is a biotechnology company that operates in the field of diagnostics and related services. We are an organisation focused on the research, development, production and marketing of research and diagnostic products for laboratories specialising in pathological anatomy, microbiology, immunology and molecular biology.

Information systems are an essential element in the provision of our services and the operational functioning of the organisation. Management establishes this Policy as a guiding framework for the protection of information and the fulfilment of the ISMS objectives.

Systems must:

- Be managed diligently to protect them from accidental or deliberate damage.
- Be protected against rapidly evolving threats that could affect information or service delivery.
- Have an adaptive security strategy that preserves the continuity and quality of services.

3.2. Prevention

VITRO, S.A. must avoid, or at least prevent, as far as possible, information or services from being compromised by security incidents. To this end, minimum security measures must be implemented, as well as any additional controls identified through a threat and risk assessment. These controls, and the security roles and responsibilities of all personnel, must be clearly defined and documented.

To ensure compliance with the policy, the following must be done:

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

3.3. Detection

Given that services can quickly deteriorate due to incidents ranging from simple slowdowns to complete shutdowns, services must be continuously monitored during operation to detect anomalies in service delivery levels and act accordingly.

Monitoring is particularly relevant when lines of defence are established. VITRO, S.A. will establish detection, analysis and reporting mechanisms that reach those responsible on a regular basis and when there is a significant deviation from the parameters that have been pre-established as normal.

3.4. Response

VITRO, S.A. will establish mechanisms to respond effectively to security incidents, defining the following:

- A point of contact for reporting security incidents.
- Protocols for the exchange of information related to the incident, including two-way communications with Emergency Response Teams.

3.5. Recovery

To ensure the availability of critical services, VITRO, S.A. will have ICT system continuity plans as part of its overall business continuity and recovery activities plan.

3.6. IS Roles and Responsibilities

VITRO, S.A. defines a clear structure of roles to ensure the governance of the ISMS. The strategic functions are set out in this Policy and the operational details in the internal ISMS procedures.

3.6.1. Information Security Committee:

The IS Committee is the body responsible for the strategic oversight of the ISMS. Its main functions are:

- Establishing guidelines and priorities around information security.
- Approving the criteria for risk assessment and treatment.

- Analysing relevant incidents and proposing improvement actions.
- Monitoring regulatory compliance and the effectiveness of the ISMS.
- Coordinating the areas involved in security.

The IS Committee reports to the Management Committee and is made up of:

- Chief Information Security Officer (CISO)
- Data Protection Officer (DPO)
- Chief Information Officer (CIO)
- System Administrator
- Quality and Regulatory Affairs Coordinator

The members of the VITRO ‘s IS Committee are documented in the IS Committee’s appointment minutes.

3.6.2. Chief Information Security Officer (CISO)

The CISO is responsible for leading the implementation, management and continuous improvement of the ISMS. Their responsibilities include:

- Proposing security strategies and submitting reports to the Management Committee.
- Overseeing the risk management of information security.
- Ensuring that the controls defined by the ISMS are correctly applied.
- Coordinating the response to security incidents.
- Promoting security training and awareness.
- Coordinate internal audits and ISMS reviews.

3.6.3. Chief Information Officer (CIO)

The CIO is strategically responsible for aligning the technological infrastructure with the objectives of the ISMS. Their main responsibilities include:

- Managing technological resources to protect systems and ensuring the continuous availability of ICT services.
- Overseeing the implementation and maintenance of systems and leading the organisation's digital transformation.
- Ensuring the adequate continuity of ICT services.

3.6.4. System Administrator

The System Administrator is responsible for day-to-day technical operations and maintenance of technical security controls, including:

- User administration and access management.
- Patching, hardening and technical maintenance.
- System monitoring and detection of technical incidents.
- Application of technical controls defined in the ISMS.

3.6.5. Data Protection Officer (DPO)

The DPO oversees compliance with the GDPR and Spanish data protection regulations. Their responsibilities include:

- Advising the organisation and supervising regulatory compliance.

- DPIA (Data Protection Impact Assessment)
- Serving as a point of contact with the supervisory authority.
- Monitoring incidents affecting personal data.

3.6.6 General responsibilities of staff

All VITRO, S.A. staff must:

- Comply with this Policy and associated internal regulations.
- Protect the information they access or manage.
- Report security incidents or weaknesses.
- Participate in training and awareness-raising activities.

3.7. Management Commitment

The Management of VITRO, S.A. takes an active role in the governance of the ISMS, ensuring that the necessary human, technical and financial resources are available for its proper implementation. Its responsibilities include:

- Approving and reviewing the ISMS policy and objectives.
- Evaluating the results of audits, incidents and reviews.
- Promoting continuous improvement and internal communication on information security.
- Promoting a culture of compliance and the integration of the ISMS into the overall management of the organisation.

3.8. Risk Management

All systems subject to this Policy shall conduct a risk analysis, assessing the threats and risks to which they are exposed. This analysis shall be repeated:

- regularly, at least once a year
- when the information handled or the services provided change
- when a serious security incident occurs
- when serious vulnerabilities are reported

To harmonise the risk analysis, the Information Security Committee shall establish a benchmark assessment for the different types of information handled and the different services provided. The Information Security Committee shall streamline the availability of resources to meet the security needs of the different systems, promoting horizontal investments.

Further details on risk management are set out in the Information Security Risk Management procedure.

3.9. Staff obligations

All VITRO, S.A. personnel are responsible for protecting the information they access or manage, actively participating in the preservation of data security. We promote continuous training and a culture of security as essential pillars for the responsible and secure use of corporate systems and resources.

It is the obligation of all staff to be familiar with and comply with this Information Security Policy and the internal guidelines and directives in force regarding information security that develop it.

3.10. Third Parties

When VITRO, S.A. provides services to other organisations or uses third-party services that involve the handling of confidential information, information systems or personal data, it shall ensure that such parties this Information Security Policy and the applicable Security Regulation.

The aim is to ensure that all third parties of VITRO, S.A. that provide services or products involving the handling of confidential information, information systems or personal data related to the operations of VITRO, S.A. are aware of and comply with the security requirements and expectations established by the company.

Specific channels and procedures will be established for reporting and resolving security incidents, as well as for interacting with the Information Security Committees where appropriate. Third parties may develop their own operating procedures to comply with the established obligations. It will be ensured that third-party personnel are adequately aware of security matters, at least to the same level as that established in this Policy.

In the event that any part of this Policy cannot be complied with by the third party, the express approval of the Chief Information Security Officer (CISO) shall be required, who shall assess the associated risks and establish the relevant treatment measures.

3.10.1. Security requirements

3.10.1.1. Confidentiality and Integrity of Information

- Suppliers must ensure that the information handled is kept confidential and protected against unauthorised access, modification or disclosure.

3.10.1.2. Regulatory Compliance

- Suppliers must comply with applicable regulations, including the GDPR (General Data Protection Regulation) and the LOPDGDD (Organic Law on Personal Data Protection and Guarantee of Digital Rights).

3.10.1.3. Information Exchange

- The exchange of information between VITRO, S.A., and its suppliers is carried out within the contractual framework, limiting its use exclusively for the purposes of the contract, with clear prohibitions on unauthorised or illegal transmission, and with security controls for the protection of information.

3.10.1.4. Appropriate use of corporate resources

- The corporate resources of VITRO, S.A. must be used exclusively to fulfil the obligations of the contracted service, prohibiting their use for unauthorised or illegal activities, with controls and audits to ensure their correct use.

3.10.1.5. Controlled Access

- Suppliers must establish and maintain adequate access controls to ensure that only authorised personnel have access to VITRO, S.A.'s confidential information.

3.10.1.6. Certification of contracted services

- For particularly critical services, VITRO, S.A. may require certifications relating to information security management, such as ISO 27001 certification, the National Security Scheme or equivalent.

3.10.1.7. Notification of Security Incidents

- Suppliers must report any security incidents related to the services provided or the information handled, in accordance with the procedures established by VITRO, S.A.

3.10.1.8. Audit and Compliance

- VITRO, S.A. may conduct audits or request external assessments to ensure that suppliers comply with established security requirements.

3.10.1.9. Subcontracting

- Suppliers must ensure that any subcontracting in the provision of services to VITRO, S.A. is communicated and also complies with the same information security standards.

3.11. Security Policy Review

This policy is reviewed periodically, at least once a year, by the Information Security Committee and Senior Management to ensure its continued suitability considering technological, organisational and regulatory changes.

With this policy, VITRO, S.A. reaffirms its commitment to information protection, the trust of our customers and compliance with the highest international standards in information security.