PUBLIC DOCUMENT

Information Security Policy

SILVIP, Sociedade Gestora de Organismos de Investimento Coletivo, S.A. (SILVIP)

Public version of the SILVIP Information Security Policy, setting out the main commitments and principles adopted by the Company regarding the protection of information and the security of its technology systems and services. The full version of the Policy is an internal document.

1. Commitment

Protecting information is essential to SILVIP's business and to the trust of its unitholders, clients, partners, suppliers and other entities with which it deals.

To this end, SILVIP has adopted an Information Security Policy, which sets out the principles and guidelines applicable to the protection of the information under its responsibility and of the technology systems and services that support its business.

Through this Policy, SILVIP undertakes to adopt security measures appropriate to the nature of the information and the associated risks, taking into account the applicable legal, regulatory and contractual requirements, including those relating to digital operational resilience in the financial sector.

2. Scope

The Policy is binding on all SILVIP departments and staff. It also applies to partners and suppliers that use, administer or maintain the Management Company's information and communication technology systems and services, or that access the organisation's information and data, whether in digital or physical form.

The Information Security Policy guides the conduct of SILVIP staff and, where applicable, of partners, suppliers and service providers that use its systems or have access to information under its responsibility.

SILVIP seeks to ensure that all entities involved in processing its information adopt appropriate security practices and comply with the applicable requirements.

3. Security objectives

SILVIP protects information in line with four core objectives:

- Availability: ensuring that information and services essential to the business remain accessible when needed;
- Confidentiality: preventing access to, or disclosure of, information by unauthorised persons;
- Integrity: protecting information against improper alteration and ensuring that it remains accurate and complete; and
- Authenticity: making it possible to confirm the origin of information and the identity of those accessing the systems.

These objectives guide the security measures adopted by SILVIP and are taken into account in the management of its systems, processes and third-party relationships.

4. Principles

SILVIP's approach to information security is based on the following principles:

- compliance with applicable legal, regulatory and contractual requirements;
- protection of information according to its importance and sensitivity;
- consideration of security risks when defining processes, projects and third-party relationships;
- prevention, detection and appropriate handling of incidents;
- preparedness to ensure the continuity and recovery of services;
- regular monitoring of the effectiveness of security measures;
- continual improvement of the practices adopted;
- staff training and awareness; and
- individual responsibility for the use and protection of the information to which each person has access.

SILVIP adapts its security measures to changes in risks, technology and the requirements applicable to its business.

Information classification

SILVIP classifies information according to its sensitivity and the impact that could result from its disclosure, alteration, loss or misuse.

This classification makes it possible to apply protection measures proportionate to the risk, particularly regarding the access, storage, sharing, retention and disposal of information.

Information is classified into one of three levels:

- Public: may be disclosed without restriction, such as information made available on the SILVIP website;
- Internal Use: intended for staff and for expressly authorised third parties; and
- Confidential: contains sensitive information and is subject to enhanced protection and access control measures.

SILVIP reviews the classification of information whenever its nature, use or level of sensitivity changes.

5. Security measures

SILVIP adopts organisational and technological measures to prevent, detect and respond to situations that may affect information security or the operation of its systems.

These measures include, in particular:

- control of access to information and systems;
- protection of devices, systems and digital identities;
- monitoring of relevant security events;
- identification and remediation of vulnerabilities;
- backups and recovery testing;
- controlled management of changes to systems;
- assessment of the risks associated with new systems and services;
- adoption of continuity and recovery measures; and
- periodic review of the effectiveness of the controls implemented.

The measures adopted are tailored to the nature of the information, the systems used and the risks identified.

6. ICT suppliers and service providers

SILVIP assesses the risks associated with engaging technology suppliers and service providers that may have access to its information or support systems relevant to its business.

The applicable security requirements are taken into account in the selection, contracting and monitoring of these providers, having regard to the nature of the services provided and their level of risk.

SILVIP monitors the services provided and seeks to ensure that suppliers adopt appropriate measures for information protection, incident reporting, continuity and compliance with applicable obligations.

7. Incident management

SILVIP has mechanisms in place to identify, analyse and handle situations that may compromise information security or the operation of its systems and services.

Whenever an incident occurs, measures are taken to:

- contain its effects;
- protect the affected information and systems;
- restore the operation of services;
- determine its causes;
- prevent similar situations from recurring; and
- make the notifications required by law.

Where applicable, SILVIP reports incidents to the competent authorities and to the affected persons or entities, as provided for by law.

8. Training and security culture

Information security depends not only on the technology used, but also on the conduct of staff.

SILVIP promotes training and awareness activities appropriate to the roles performed by its staff, with the aim of strengthening:

- the responsible use of information and systems;
- the recognition of risks and unusual situations;
- the prevention of incidents;
- knowledge of the applicable rules and responsibilities; and
- the adoption of secure behaviour in the course of their work.

Training and awareness are updated in line with changes in risks, the systems used and the applicable requirements.

9. Governance and review

The SILVIP Board of Directors approves the Information Security Policy and ensures that the resources needed to implement it are available.

The Policy is overseen by the internal functions responsible for information systems, risk management, operational risk and compliance.

SILVIP reviews the Policy periodically and updates it whenever there are relevant changes in risks, in the organisation, in the systems used or in the applicable legal and regulatory requirements.

10. Reporting vulnerabilities and incidents

Anyone who identifies a possible vulnerability, event or anomalous behaviour relating to SILVIP's systems or services may report it to the following address: incidente@silvip.pt

Reports should include, where possible:

- a clear description of the situation observed;
- the date and time of the occurrence;
- the system or service apparently affected; and
- information that helps to understand or reproduce the situation.

Reports must not include third-party personal data, access credentials, confidential information or material obtained through unauthorised access.

SILVIP analyses the reports received and handles the information provided with appropriate confidentiality.

Public version no. 2.0 | Approved on 29 October 2026.