Public

POL Information security policy

Version history

Version	Date	Author	Approved by
1	19/08/2024	Marzia Elia	Nicola Murino
2	11/03/2026	Marzia Elia	Nicola Murino

Table of contents

Version Description

Compared to the previous version, the main changes are:

- Redefined the purpose to articulate Top Management's strategic commitment to establishing, maintaining, and continually improving the Information Security Management System, replacing the previous operational orientation focused on system ownership and personnel protection
- Introduced formal sections for field of application, regulatory references, terms and definitions, and roles and responsibilities to bring the document into full alignment with ISO 27001 policy structure
- Added an Information Security Objectives section expressing strategic security goals derived from the organization's risk assessment and business context
- Consolidated the core security principles previously spread across standalone sections on mobile devices, acceptable use, and email and communication activities into a unified Fundamental Information Security Principles section
- Added a dedicated Protection of Off-site Assets section that reflects the organization's fully remote operating model and its commitment to securing information assets outside traditional premises
- Delegated operational details previously embedded in the policy (incident reporting channels, fraud reporting mechanisms, exception handling, violation enforcement, prohibited email activities) to the relevant topic-specific policies and procedures referenced in this document
- Replaced the appended policy reference table with a formal Reference Documents section listing all documents explicitly cited in the text

Purpose

Software Engineering S.R.L. recognises the protection of information as a strategic priority that underpins the trust its customers place in the SFTPGo managed file transfer platform and in every service the organization delivers. This policy articulates Top Management's commitment to preserving the confidentiality, integrity, and availability of all information assets and establishes the overarching framework for the Information Security Management System (ISMS).

Through this policy the organization undertakes to:

- Maintain an ISMS that is appropriate to its operating context, aligned with its strategic direction, and responsive to the evolving threat landscape
- Satisfy all applicable legal, regulatory, and contractual requirements related to information security
- Adopt a risk-based approach to identifying, evaluating, treating, and monitoring information security risks, as detailed in the *POL Information security risk management policy* and the *PRO Risk management procedure*

- Foster a culture in which every associate and collaborator shares responsibility for protecting information, supported by clearly defined roles documented in the *POL Information security roles and responsibilities policy*
- Pursue the continual improvement of the ISMS through periodic management reviews, internal audits, and the systematic treatment of findings

This policy is the highest-level reference for all topic-specific security policies and procedures within the ISMS. It is communicated internally through the organization's shared document repository and distributed by email, and it is made available externally on the company website, ensuring that all interested parties can access the organization's security commitments.

Field of Application

This policy applies to all activities, processes, and information assets of Software Engineering S.R.L., encompassing the development, delivery, and support of the SFTPGo platform in both its SaaS and on-premise configurations. It covers the cloud infrastructure hosted by external service providers, source code repositories, development and test environments, and every system that processes, stores, or transmits organizational and customer data. The policy extends to all associates, collaborators, contractors, consultants, and third parties who access the organization's information or systems, regardless of geographic location. Since the organization operates entirely in remote work mode from its registered office at Via Niccolò Tommaseo 4, Cesano Boscone (MI), the scope includes all remote working locations and the devices used for business activities. Physical security controls for dedicated office premises are excluded, as the organization does not maintain such facilities.

Regulatory References

- ISO/IEC 27001:2022
- Regulation (EU) 2016/679

Terms and Definitions

- **Information security** : preservation of confidentiality, integrity, and availability of information.
- **Confidentiality** : property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity** : property of accuracy and completeness of information.
- **Availability** : property of being accessible and usable on demand by an authorized entity.
- **Risk** : effect of uncertainty on objectives.
- **Information Security Management System (ISMS)** : part of the overall management system, based on a business risk approach, that establishes, implements, operates,

monitors, reviews, maintains, and improves information security.

- **Interested party** : person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity.
- **Continual improvement** : recurring activity to enhance performance.

Roles and Responsibilities

- **CEO** : Approves the information security policy, allocates the resources necessary to sustain the ISMS, and ensures that information security objectives remain aligned with the organization's strategic direction.
- **Information Security Management System Manager** : Coordinates the design, implementation, and continual improvement of the ISMS, oversees risk assessment and treatment activities, and serves as the primary point of contact for all information security matters.
- **Management System Manager** : Maintains and updates ISMS documentation, supports periodic reviews of this policy, and ensures its controlled distribution to all relevant parties.
- **IT and Software Development Manager** : Integrates information security requirements into IT operations and the software development lifecycle, and monitors technical infrastructure for vulnerabilities and threats.
- **Administrative Manager** : Safeguards the confidentiality and integrity of administrative, financial, and personnel-related information processed within the scope of this policy.
- **Commercial and Marketing Manager** : Upholds confidentiality commitments in client relationships and ensures that commercial and marketing activities comply with the organization's information security requirements.

Information Security Objectives

Software Engineering S.R.L. pursues information security objectives that are measurable, consistent with this policy, and derived from the organization's context analysis, risk assessment, and stakeholder expectations. The objectives address the following areas:

- Preserving the confidentiality of customer data processed through the SFTPGo platform and all supporting systems, ensuring that access is granted strictly on the basis of operational need
- Safeguarding the integrity of source code, configurations, and operational data so that unauthorized or undetected modifications cannot compromise the reliability of the services delivered
- Maintaining the availability of the SaaS infrastructure and related services at levels that meet contractual commitments and business continuity requirements
- Ensuring compliance with applicable legal and regulatory obligations, including those related to the protection of personal data

- Strengthening the organization's capacity to detect, respond to, and recover from information security incidents
- Fostering security awareness among all associates and collaborators so that informed behaviour becomes an integral part of daily activities

Each objective is accompanied by defined indicators, timelines, and an assigned owner, as governed by the *PRO Objectives and planning for their achievement* . The **CEO** , supported by the **Information Security Management System Manager** and the **Management System Manager** , reviews progress during the management review, evaluates overall ISMS performance, and authorizes adjustments to the improvement programme where needed.

Fundamental Information Security Principles

The information security posture of Software Engineering S.R.L. rests on a set of interdependent principles that guide every policy, procedure, and operational decision within the ISMS.

Risk-based decision-making. The organization adopts a systematic approach to information security risk management, identifying threats and vulnerabilities, evaluating their likelihood and potential impact, and selecting proportionate controls. Risk assessments are conducted at planned intervals and whenever significant changes occur, following the methodology defined in the *PRO Risk management procedure* . Treatment decisions consider acceptance, mitigation, transfer, or avoidance, and are formally documented in the risk register maintained under the *POL Information security risk management policy* .

Shared responsibility. Protecting information is a collective obligation that extends to every associate, collaborator, and third party who interacts with the organization's systems or data. Each person is accountable for understanding and applying the security requirements relevant to their role, as formalized in the *POL Information security roles and responsibilities policy* . Top Management fosters this culture by ensuring that security expectations are clearly communicated and that adequate awareness initiatives are sustained.

Information classification and handling. All information is classified according to its sensitivity and business value, following the tiered framework established in the *POL Information classification and labelling policy* . Classification determines the protection requirements for processing, transmitting, and storing data and guides the acceptable handling practices that personnel are expected to observe. Complementary rules on the acceptable use of IT resources, systems, applications, and connectivity are set out in the *POL Operational security policy* , while the *POL Information retention and deletion policy* governs the lifecycle of information from creation through secure disposal.

Least privilege and need-to-know. Access to information and information systems is granted only to the extent necessary for each person's assigned responsibilities. The organization enforces role-based access control, unique user identifiers, multi-factor authentication on sensitive resources, and periodic review of access rights, as defined in the *PRO Logical access control management procedure* . Authorization records are

maintained in the *Register of users authorized to use the information* to ensure full traceability.

Clear desk and clear screen. To prevent unauthorized access to information left unattended, the organization requires that devices be configured with automatic screen locking after a defined period of inactivity and that authentication be required to unlock them. Personnel manually lock their screens whenever they step away from their workstation, even briefly. Information classified as limited or confidential is not left visible on screen when not actively in use, and sensitive documents are stored securely at the end of the working day. The *POL Operational security policy* provides the full set of requirements applicable to workstation and device management.

Reporting of information security events. The organization fosters an environment in which all personnel are encouraged and expected to report observed or suspected information security events promptly and without fear of reprisal. Timely reporting enables rapid triage, containment, and recovery, significantly reducing the potential impact of incidents. Reporting channels, the severity classification system, and escalation paths are defined in the *PRO Information security incident management procedure* , and all incidents are recorded in the *MOD Log of information security incidents* .

Secure development. Because software development is the core of the organization's business, security is embedded at every stage of the development lifecycle, from design through coding, testing, and release. The *PRO Secure development procedure* governs the specific standards and controls that apply, including secure coding practices, code review requirements, and environment segregation.

Cryptographic protection. Robust cryptographic controls safeguard the confidentiality, integrity, and authenticity of information both in transit and at rest. The selection of algorithms, key management practices, and the complete cryptographic key lifecycle are governed by the *PRO Cryptography and cryptographic key management procedure* .

Third-party security. External parties that access, process, or store the organization's information are expected to meet equivalent security standards. Contractual agreements include appropriate security clauses, and supplier performance is monitored over time. The *POL Third-party management policy* and the *PRO Purchasing and third party management procedure* set out these commitments in detail.

These principles function as an integrated whole, reinforced by the organization's dedication to continual improvement. Internal audits, management reviews, corrective actions, and the ongoing monitoring of security objectives generate insights that feed back into the risk assessment cycle and into the refinement of every policy and procedure within the ISMS.

Protection of Off-site Assets

Software Engineering S.R.L. operates entirely in remote work mode, which means that information assets are routinely accessed and processed outside traditional office premises. The organization treats this operating model as a defining characteristic of its business and is committed to ensuring that off-site use does not diminish the level of protection afforded to its information. The *POL Asset management policy* establishes the

broader framework for asset identification and protection responsibilities, of which the commitments below form a critical part.

Custody. Personnel treat every device used for business activities as a high-value asset. Laptops and mobile devices are never left unattended in vehicles, public transport, common areas of hotels, or coworking spaces. When travelling, devices remain under the personal custody of the assignee or are secured in a locked location.

Secure configuration. All devices used to access company information carry full-disk encryption and automatic screen lock activated after a defined period of inactivity, with authentication required to resume use. Home networks are secured with current encryption protocols, default credentials are changed, and public Wi-Fi networks are not used for accessing company data. All remote communications involving classified information use approved encrypted channels. The *POL Operational security policy* specifies the full configuration requirements, including rules applicable to bring-your-own-device scenarios and the prior approval process for additional software installations.

Reporting of loss, theft, or damage. Personnel report any loss, theft, or damage of an information asset to the **Information Security Management System Manager** without delay. Such a report triggers the activation of remote-wipe capabilities and the revocation of the associated access credentials. The event is registered as an information security incident in accordance with the *PRO Information security incident management procedure* and recorded in the *MOD Log of information security incidents* .

Monitoring and compliance. The organization reserves the right to audit devices used for business activities to verify adherence to the security requirements established in this policy and in the related operational procedures. The **IT and Software Development Manager** monitors the technical infrastructure on an ongoing basis to confirm that off-site assets remain aligned with the ISMS.

The organization promotes awareness of off-site security risks through its internal communication channels and expects all personnel to exercise diligence in protecting information assets wherever they work.

Archiving and Updates

This policy is a controlled document within the ISMS. It is reviewed at least annually, and additionally whenever significant changes occur in the organization's structure, technology environment, regulatory landscape, or threat context. The **Information Security Management System Manager** coordinates the review and submits proposed updates to the **CEO** for approval. Approved versions are distributed internally through the organization's shared document repository and by email, and published on the company website for external interested parties.