POL Information security policy

Company name	Ermetix Srl
Effective date	30/03/2026

Version history

Version	Date	Description	Author	Approved by
1	30/03/2026	-- N/D --	Riccardo Poffo	Diego Fasano

Purpose

The purpose of this policy is to declare and communicate Top Management's commitment to protecting the organization's information assets. This document defines the framework for establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS), with the aim of protecting the confidentiality, integrity, and availability of information and supporting the company's strategic objectives.

Table of contents

Field of Application

This document defines the information security policy of Ermetix Srl. It establishes the framework and fundamental principles for the Information Security Management System (ISMS) to protect the company's information assets from all threats, whether internal or external, deliberate or accidental. This policy applies to all employees, contractors, and other parties who have access to Ermetix Srl's information systems and assets, and it governs the protection of all information processed and stored by the company.

Regulatory References

- ISO 27001
- ISO 27017
- General Data Protection Regulation (GDPR)

Terms and Definitions

- **Confidentiality** : The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity** : The property of safeguarding the accuracy and completeness of information and assets.
- **Availability** : The property of being accessible and usable upon demand by an authorized entity.
- **Information Security Management System (ISMS)** : A systematic framework of policies, procedures, and controls that an organization uses to manage and protect its confidential and sensitive information.
- **Risk** : The effect of uncertainty on objectives.

Roles and Responsibilities

- **Chief Executive Officer** : Ensures the establishment and maintenance of the information security policy framework and is accountable for the overall security posture of the organization.
- **Management System Manager** : Ensures that information security policies are effectively communicated, maintained, and integrated into the management system, and oversees the implementation of security controls.
- **Chief Information Officer** : Implements and enforces information security policies and technical controls across the IT infrastructure, manages security incident responses, and ensures the security of teleworking and mobile device usage.

- **Chief Technology Officer** : Ensures that the company's technology infrastructure and the Ermetix SaaS platform are designed, developed, and operated securely, integrating security controls throughout the product lifecycle.
- **Chief Product Officer** : Ensures that security requirements are integrated into the product design and development process and that the security value of the products is clearly defined.

Information Security Objectives

Ermetix Srl is committed to protecting the confidentiality, integrity, and availability of all information assets to maintain customer trust, ensure regulatory compliance, and support its strategic business goals. Top Management shall establish and review measurable information security objectives annually, or when significant changes occur, to drive the continual improvement of the Information Security Management System (ISMS).

The primary objectives of information security at Ermetix Srl are:

- **Confidentiality** : To prevent the unauthorized disclosure of sensitive information, including customer data, intellectual property, and employee information, by implementing robust access controls and data protection measures.
- **Integrity** : To ensure the accuracy, completeness, and reliability of information and information processing systems, protecting them from unauthorized modification.
- **Availability** : To guarantee that information and associated services are accessible to authorized users when needed, ensuring the resilience of critical business operations and the Ermetix platform.
- **Compliance** : To achieve and maintain compliance with all applicable legal, statutory, regulatory, and contractual requirements, including data protection regulations such as the GDPR.
- **Risk Management** : To systematically identify, assess, and treat information security risks to reduce them to an acceptable level, in line with the process defined in the "PRO Risk management procedure".

These objectives shall be communicated throughout the organization and are planned and monitored for their achievement as detailed in the "PRO Objectives and planning for their achievement" procedure.

Fundamental Information Security Principles

Policy Governance and Review

This policy and all related subject-specific information security policies constitute the formal framework for the ISMS. The Chief Executive Officer shall ensure this framework is established and maintained. All policies shall be formally approved by Top Management before publication.

The Management System Manager shall ensure that all policies are effectively communicated to relevant personnel and external stakeholders and that acknowledgment

is recorded where appropriate.

Information security policies shall be reviewed at least annually, or upon the occurrence of significant changes to the organizational context, business, legal, or technical environment. This review is a formal part of the "PRO Management Review Process" to ensure their continuing suitability, adequacy, and effectiveness.

Shared Responsibility and Acceptable Use

Information security is the shared responsibility of every member of Ermetix Srl. All personnel and external collaborators shall adhere to the established information security policies and procedures. Specific security duties are formally assigned to roles throughout the organization as defined in the "POL Information security roles and responsibilities policy" and the "PRO Roles and responsibilities procedure".

All users of company assets shall comply with the rules for the acceptable use of information and associated resources. These rules are established to protect against a wide range of threats and are further detailed in the "Code of conduct" and the "POL Operational security policy". The Chief Information Officer shall ensure that acceptable use rules are identified, documented, and implemented.

Cloud Security

Ermetix Srl, as both a provider and consumer of cloud services, is committed to implementing security best practices for cloud environments.

- **As a Cloud Service Provider** : The Chief Technology Officer and Chief Product Officer shall ensure that the Ermetix SaaS platform is designed and operated to protect customer information. This includes implementing a multi-tenant architecture that ensures the logical isolation of customer data, enforcing strong authentication and access controls for administrative personnel, securely managing the lifecycle of customer accounts, and establishing clear guidelines for information sharing to support forensic investigations.
- **As a Cloud Service Customer** : When utilizing third-party cloud services, the Chief Information Officer shall ensure that a risk-based approach is adopted. This includes evaluating the provider's security posture, understanding the geographic locations where data is stored, and assessing the security of processes running in multi-tenant environments.

Detailed requirements for securing cloud environments are documented in the "POL Cloud security policy".

Protection of Workspaces and Assets

- **Clear Desk and Clear Screen** : All personnel shall protect sensitive information in physical and digital forms. Papers and removable storage media containing sensitive information must be secured when unattended. All workstations and mobile devices shall be configured to automatically lock after a defined period of inactivity. The Chief Information Officer is responsible for enforcing clear screen rules through technical

controls. Further operational details are provided in the "PRO Physical and environmental security procedure".

- **Security of Off-site Assets** : All company assets used outside of company premises, including laptops and company-assigned vehicles, shall be protected against loss, damage, theft, and unauthorized access. Personnel are accountable for the assets assigned to them, as formally documented through instruments like the "MOD Asset assignment form". The management, protection, and disposal of all assets are governed by the "PRO Asset configuration, management and disposal procedure".

Remote Work and Mobile Devices

Remote access to Ermetix Srl's network and information systems is permitted only through secure and approved methods. All personnel working remotely shall comply with the security requirements defined in the "POL Operational security policy". This includes the obligation to secure their home network environment, use company-mandated VPN connections, and refrain from disabling or altering security controls on company-managed devices. The Chief Information Officer shall define and implement the necessary technical controls to ensure the security of teleworking activities and mobile devices.

Information Security Event Reporting

All personnel and contractors are required to promptly report any observed or suspected information security events, weaknesses, or threats. The Chief Information Officer shall ensure that clear channels and processes are available for reporting. All reported incidents shall be assessed and responded to in accordance with the "PRO Information security incident management procedure".

Archiving and Updates

This policy is managed as part of the ISMS documentation. It is reviewed at least annually, or upon significant changes to the business, legal, or technical environment, to ensure its continued suitability and effectiveness. Updates are approved by Top Management and communicated to all relevant parties.

Reference Documents

- PRO Risk management procedure
- PRO Objectives and planning for their achievement
- PRO Management Review Process
- POL Information security roles and responsibilities policy
- PRO Roles and responsibilities procedure
- Code of conduct
- POL Operational security policy

- POL Cloud security policy
- PRO Physical and environmental security procedure
- MOD Asset assignment form
- PRO Asset configuration, management and disposal procedure
- PRO Information security incident management procedure