POL Information security policy

Company name	Lexroom
Effective date	15/10/2025

Version history

Version	Date	Description	Author	Approved by
1	30/09/2025	-- N / D --	Andrea Lonza	Paolo Fois

Scope

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.

Index

1. Field of Application

This policy establishes the framework for information security at Lexroom. Its purpose is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental. This document applies to all personnel, processes, systems, and data within the organization's Information Security Management System (ISMS), ensuring the confidentiality, integrity, and availability of corporate and client information.

2. Regulatory References

- ISO/IEC 27001:2022

3. Terms and Definitions

- **Information Security**: The preservation of confidentiality, integrity, and availability of information.
- **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 on demand by an authorized entity.
- **Information Security Management System (ISMS)**: A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's information security to achieve business objectives.

4. Roles and Responsibilities

- **Top Management**: Responsible for supporting the continuous improvement of the ISMS, ensuring its alignment with strategic objectives, and providing the necessary resources. Approves information security policies and ensures they are communicated throughout the organization.
- **Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI)**: Responsible for the implementation, management, and continuous improvement of the ISMS in accordance with the ISO/IEC 27001 standard. This role owns the policy, oversees its maintenance, and supports management in security-related decisions.
- **Chief Technology Officer (CTO)**: Responsible for overseeing the technical infrastructure and ensuring that mechanisms for information security, such as event reporting channels, are effectively implemented and communicated.

5. Information Security Objectives

Lexroom is committed to establishing and maintaining an Information Security Management System (ISMS) to protect its information assets from all threats, whether internal or external, deliberate or accidental. The primary objectives of this policy are to ensure the confidentiality, integrity, and availability of all corporate and client information.

The strategic objectives for information security at Lexroom are:

- To ensure that information assets receive a level of protection appropriate to their importance and sensitivity.
- To comply with all applicable legal, regulatory, and contractual requirements.
- To protect the confidentiality of client and corporate data against unauthorized disclosure.
- To maintain the integrity of information by protecting it from unauthorized modification.
- To ensure the availability of information and associated services to authorized users when required.
- To establish a culture of security where all personnel understand and are accountable for their responsibilities.

These high-level objectives are supported by specific, measurable goals that are regularly monitored and reviewed. The definition and planning for these goals are detailed in the "PRO Objectives and planning for their achievement" procedure and are derived from the results of the "PRO Information security risk assessment" procedure.

6. Fundamental Information Security Principles

All activities within Lexroom shall be governed by the following fundamental security principles:

- **Risk-Based Approach:** Information security measures shall be proportional to the risks identified through a formal assessment process. This process is defined in the "PRO Information security risk assessment" and "PRO Risk management procedure".
- **Shared Responsibility:** Every employee and contractor is responsible for information security. Specific duties are formally assigned and documented in the "POL Information security roles and responsibilities policy" and integrated into the "Code of conduct".
- **Acceptable Use of Assets:** All information and associated assets shall be used in an acceptable, ethical, and lawful manner. Rules for the use of corporate resources, including systems, data, and networks, are defined to prevent misuse and protect assets throughout their lifecycle.
- **Clear Desk and Clear Screen:** All personnel shall ensure that sensitive information, in both physical (papers, removable media) and digital form, is protected when workstations are unattended. This includes locking screens, securing printed documents, and storing media appropriately to prevent unauthorized access.
- **Security of Off-Site and Remote Work:** All assets used outside company premises, including for remote work, must be protected in accordance with company standards. This includes the mandatory use of company-provided security software (e.g., VPN, antivirus), secure configuration of home networks, and adherence to all security protocols as if working on-site.
- **Information Lifecycle Management:** Information shall be managed based on its value and sensitivity. Lexroom has established a framework for the classification, handling, retention, and secure disposal of information, as detailed in the "POL Information classification and labelling policy" and "POL Information retention and deletion policy".
- **Principle of Least Privilege:** Access to information and systems shall be granted based on business requirements and limited to the minimum necessary for individuals to

perform their roles. This principle is enforced through the processes described in the "PRO Logical access management and control procedure".

7. Information Security Event Reporting

All personnel are required to promptly report any observed or suspected information security events, incidents, or vulnerabilities. This obligation is crucial for enabling a timely and effective response to potential threats.

The mechanism for reporting ensures that events are received, assessed, and managed consistently. The Chief Technology Officer (CTO) is responsible for ensuring that appropriate channels for reporting are available and communicated to all personnel. The detailed process for handling, investigating, and resolving such events is documented in the "PRO Information security incident management procedure".

8. Policy Governance and Review

- **Policy Approval and Ownership:** This Information Security Policy is formally approved by Top Management. The Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI) is the owner of this policy and is responsible for its implementation and maintenance.
- **Communication and Awareness:** This policy shall be published and communicated to all personnel and relevant interested parties. All personnel must acknowledge their understanding of and agreement to comply with this policy. Communication and training activities are managed in accordance with the "PRO Human resources management procedure".
- **Review and Update:** This policy shall be reviewed at least annually, or when significant changes occur in the business, technology, or risk environment, to ensure its continuing suitability, adequacy, and effectiveness. The review process is an integral part of the management review activities detailed in the "PRO Top management review management" procedure. Any modifications to this policy shall be managed through the "PRO Change management procedure".
- **Compliance and Enforcement:** Compliance with this policy and the entire ISMS is mandatory for all personnel. Violations of this policy may lead to disciplinary action, as specified in the "Code of conduct".

9. Archiving and Updates

This document shall be reviewed at least annually or upon significant changes to the organization, technology, or risk landscape. The RSGSI is responsible for managing the review and update process. All versions of this document are archived electronically in a secure and accessible repository to ensure a complete audit trail.

10. Reference Documents

- PRO Objectives and planning for their achievement
- PRO Information security risk assessment
- PRO Risk management procedure

- POL Information security roles and responsibilities policy
- Code of conduct
- POL Information classification and labelling policy
- POL Information retention and deletion policy
- PRO Logical access management and control procedure
- PRO Information security incident management procedure
- PRO Human resources management procedure
- PRO Top management review management
- PRO Change management procedure