POL Management system policy

Company name	Lexroom
Effective date	13/10/2025

Version history

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

Scope

Lexroom promotes production/service delivery policies that take into account the needs of economic development and value creation, inherent to its business activities, while also addressing the requirements of environmental protection, social responsibility, and information and data security. The company is also committed to complying with applicable legislation and promoting a culture of respect for legal principles.

Index

1. Field of Application

This policy establishes the foundational directive for the Information Security Management System (ISMS) at Lexroom. It applies to all of the company's information assets, business processes, and personnel. The policy's purpose is to protect the confidentiality, integrity, and availability of all information, with a particular focus on client data and proprietary AI models, in the context of Lexroom's operations as an AI-based platform for lawyers.

2. Regulatory References

- ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

3. Terms and Definitions

- **Availability**: The property of being accessible and usable on demand by an authorized entity.
- **Confidentiality**: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Continual improvement**: A recurring activity to enhance performance and the effectiveness of the management system.
- **Documented information**: Information required to be controlled and maintained by the organization, along with the medium on which it is contained.
- **Information Security**: The preservation of confidentiality, integrity, and availability of information.
- **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.
- **Integrity**: The property of accuracy and completeness of information and assets.
- **Interested party (stakeholder)**: A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
- **Objective**: A result to be achieved.
- **Policy**: Intentions and direction of an organization, as formally expressed by its top management.
- **Risk**: The effect of uncertainty on objectives.
- **Top Management**: The person or group of people who directs and controls an organization at the highest level.

4. Roles and Responsibilities

- **RSGSI - Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni**: Responsible for the implementation, management, and continual improvement of the ISMS. This role coordinates risk analysis, defines security measures, ensures policy compliance, and supports Top Management in information security matters.

- **Top Management**: Responsible for supporting and continuously improving the Information Security Management System (ISMS), ensuring its alignment with strategic objectives, providing necessary resources, and ensuring the information security policy is defined and communicated.

5. Management System Commitment and Objectives

Top Management at Lexroom establishes and endorses this policy as the foundational directive for the Information Security Management System (ISMS). This policy is designed to be appropriate for the company's purpose as an AI-based platform for lawyers, supporting its strategic direction and reflecting the principles outlined in the "Context analysis". The primary goal is to protect the confidentiality, integrity, and availability of all information assets, particularly client data and proprietary AI models, against all internal, external, deliberate, or accidental threats.

Top Management is committed to the following principles:

- **Setting of Objectives**: To establish a framework for setting information security objectives that are consistent with the company's strategic goals. These objectives shall be derived from the assessment of risks and opportunities and will be managed in accordance with the "PRO Objectives and planning for their achievement" procedure.
- **Fulfillment of Requirements**: To satisfy all applicable legal, regulatory, contractual, and other requirements related to information security. The process for identifying and managing these obligations is defined in the "PRO Compliance obligations" procedure.
- **Continual Improvement**: To ensure the continual improvement of the ISMS to enhance information security performance. This commitment is fulfilled through ongoing monitoring, performance evaluation, and periodic reviews as detailed in the "PRO Top management review management" procedure.

6. Policy Maintenance and Communication

- **Documentation**: This policy shall be maintained as documented information and managed throughout its lifecycle in accordance with the "PRO Documented information management procedure".
- **Internal Communication**: Top Management, with support from the RSGSI - Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni, shall ensure this policy is communicated to, understood by, and applied by all personnel within the organization. Communication activities are governed by the "PRO Communication management" procedure.
- **External Availability**: This policy shall be made available to relevant interested parties, such as clients, partners, and regulatory bodies, as deemed appropriate and in line with the "PRO Communication management" procedure.

7. Archiving and Updates

This document is managed as controlled documented information. It is subject to periodic review by Top Management and updated as necessary to reflect changes in the organization, legal requirements, or the information security landscape, ensuring its continued suitability and effectiveness.

8. Reference Documents

- Context analysis
- PRO Objectives and planning for their achievement
- PRO Compliance obligations
- PRO Top management review management
- PRO Documented information management procedure
- PRO Communication management