# PG 05.01 EN
# INFORMATION SECURITY POLICY

INFORMATION SECURITY MANAGEMENT

LEXSOFT SYSTEMS

# DOCUMENT INFORMATION

## GENERAL INFORMATION

| | |
|---|---|
| **Document name** | GP 05.01 Planning |
| **ISO/IEC 27001 Reference** | 5.2 Policy |
| **Produced by** | External consultant<br>Responsible for the information security system |
| **Reviewed by** | Information Security Manager |
| **Authorized by** | Chief Executive Officer |
| **Creation date** | 05/10/2022 |

## VERSION CONTROL

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 05/10/2022 | | Initial documentation |

## 1. OBJECT

Compile the information security policies of **LEXSOFT SYSTEMS,** which will provide guidance for the management and support of information security, in accordance with the commercial requirements of the entity, with the applicable laws and regulations, in addition to establishing the scope of the information security management system [ISMS].

## 2. SCOPE

This procedure will apply to all **LEXSOFT SYSTEMS personnel** involved in the development, implementation, and maintenance of the information security management system.

## 3. REFERENCES

Sections of the ISO/IEC 27001:2013 standard

- 5.2 Policy
- A.5.1.1 Policies for information security
- A.5.1.2 Review of information security policies

## 4. DEVELOPING

### 4.1 . INFORMATION SECURITY MANAGEMENT GUIDELINES

This policy manages the information security of **LEXSOFT SYSTEMS** from the highest management level of the organization, establishing a framework to control the implementation of the information security management system, the approval of the security policy, the distribution of it to employees, suppliers, customers, and ultimately to all stakeholders, whether internal or external to the organization.

The information security policy is defined and approved by Senior Management of **LEXSOFT SYSTEMS** and has taken into account the characteristics of the business, the contractual requirements signed with the clients of consulting services to law firms, organization legal advice departments, legal compliance as well as the provision of computer services (implementation, maintenance and support) for the organization and implementation of software specialized in document and knowledge management for companies worldwide, as well as for compliance with the most relevant legislation that affects the **LEXSOFT SYSTEMS information security management system** .

### 4.2. CORPORATE INFORMATION SECURITY POLICY

At **LEXSOFT SYSTEMS,** information is a fundamental asset for the provision of its services and efficient decision-making, for which there is an express commitment to protect it as part of a strategy aimed at

business continuity, risk management and consolidation. of a safety culture. Based on this, on the three fundamental pillars of information security:

- → **Confidentiality:** it is the guarantee of access to the information of the users who are authorized for this purpose.
- → **Integrity:** is the preservation of complete and accurate information.
- → **Availability:** it is the guarantee that the user has access to the information they need at the precise moment they require it.

The pillars guarantee information security in the areas of physical, logical and institutional security.

Understanding the confidentiality, integrity, and availability of information as a reference framework, and aligning these with business requirements, **LEXSOFT SYSTEMS** establishes the following security objectives:

- ♦ Ensuring that information assets receive an adequate level of protection.
- ♦ Classify the information to indicate its sensitivity and criticality.
- ♦ Define the levels of protection and special treatment measures according to their classification.

To achieve these objectives, **LEXSOFT SYSTEMS** will meet the following requirements information security:

- Security in the management of Human Resources, before, during and at the end of employment.
- The proper management of assets that implies the classification of information and the handling of media
- Establishing robust logical access control to your systems and applications, managing user permissions and privileges.
- The protection of the facilities and the physical environment, through the design of safe work areas and the safety of the equipment.
- The guarantee of security in operations by protecting against malicious software, making backup copies, establishing records and monitoring them. control of the software in use. the management of technical vulnerabilities and the choice of techniques - suitable for the audit of the Systems.
- The security of communications, protecting networks and the exchange of information.
- The assurance of security in the acquisition and maintenance of information systems, limiting and managing change.
- Performing secure software development, separating development and production environments, and performing appropriate functional acceptance tests

- The control of relations with suppliers, contractually demanding compliance with the pertinent security measures and acceptable levels in the provision of their services.
- The effectiveness in the management of Security Incidents, establishing the appropriate channels for their notification, response and timely learning.
- Carrying out a business continuity plan that protects the availability of services during a crisis or disaster.
- Identification and compliance with applicable regulations, with a special interest in intellectual property and the protection of personal data.
- The review of these information security requirements to guarantee their compliance and effectiveness.

The Management of **LEXSOFT SYSTEMS,** through this security policy, undertakes to manage the security of the information, to meet the security objectives, set, carrying out risk treatment plans that have been the result of the corresponding analysis to which the users will be subjected. organization's information systems.

To this end, the Management of **LEXSOFT SYSTEMS** has appointed a Security Committee, whose main function will be to determine the security requirements associated with the services and measure the security objectives with predetermined metrics that offer objective and comparable results, and that allow their effectiveness to be determined to identify possible improvements.

### 4.3. HUMAN RESOURCES SECURITY

The objectives of controlling the security of personnel are:

- Reduce the risks of human error, start-up irregularities, improper use of facilities and resources, and unauthorized handling of information.
- Explain the security responsibilities in the personnel recruitment stage and include them in the agreements to be signed and verify their compliance during the performance of the employee's tasks.
- Ensuring that users are aware of information security threats and concerns and are trained to support the organization's information security policy, in the course of their normal duties.
- Establish confidentiality commitments with all personnel and users outside the information processing facilities.
- Establish the necessary tools and mechanisms to promote the communication of existing security weaknesses, as well as incidents, to minimize their effects and prevent recurrence.

This policy applies to all **LEXSOFT SYSTEMS** personnel and external personnel who perform tasks within the company.

HR will include information security functions in employee job descriptions, inform all contracting staff of their obligations regarding compliance with the information security policy, manage confidentiality commitments to staff, and coordinate user training tasks regarding this policy.

The security management officer [CISO] is responsible for monitoring, documenting, and analyzing reported security incidents, as well as communicating them to the Information Security Committee and data owners.

The Information Security Committee will be responsible for implementing the necessary means and channels so that the person in charge of Security Management [CISO] handles reports of incidents and system anomalies. The Committee will also be aware of, supervise the investigation, monitor the evolution of information, and promote the resolution of information security incidents.

The person in charge of Security Management [CISO] will participate in the preparation of the confidentiality agreement that will be signed by employees and third parties who perform functions in **LEXSOFT SYSTEMS,** in advising on the sanctions that will be applied for breach of this Policy and in the treatment of information security incidents.

All **LEXSOFT SYSTEMS personnel** are responsible for reporting information security weaknesses and incidents that are detected in a timely manner.

### 4.4. PHYSICAL AND ENVIRONMENTAL SECURITY

The objectives of this policy are:

- → Prevent unauthorized access, damage and interference to the headquarters, facilities, and information of **LEXSOFT SYSTEMS**
- → Protect the critical information processing equipment of **LEXSOFT SYSTEMS** by placing it in protected areas and protected by a defined security perimeter, with the appropriate security measures and access controls. Likewise, contemplate the protection of this in its transfer and remain outside the protected areas, for maintenance or other reasons.
- → Control the environmental factors that could harm the proper functioning of the computer equipment that houses the information of **LEXSOFT SYSTEMS.**
- → Implement measures to protect the information handled by the staff in the offices, within the normal framework of their usual tasks.
- → Provide protection proportional to the risks identified.

This policy applies to all physical resources related to **LEXSOFT SYSTEMS information systems:** facilities, equipment, wiring, files, storage media, etc.

The person in charge of Security Management (MSR) [CISO], together with the holders of the information, as appropriate, will define the physical and environmental security measures for the protection of critical assets, based on a risk analysis, and will monitor your application. It will also verify compliance with physical and environmental security provisions.

The heads of the different departments will define the levels of physical access for **LEXSOFT SYSTEMS personnel** to the restricted areas under their responsibility. Information owners will formally authorize off-site work with information about their business to **LEXSOFT SYSTEMS employees** when they deem it appropriate.

All **LEXSOFT SYSTEMS personnel** are responsible for complying with the clean screen and desk policy, for the protection of information related to daily work in the offices.

## 4.5. ACCESS CONTROL TO INFORMATION SYSTEMS

The control of access to information systems aims to:

- Prevent unauthorized access to information systems, databases, and information services.
- Implement security in user access through authentication and authorization techniques.
- Control security in the connection between the **LEXSOFT SYSTEMS network** and other public or private networks.
- Review critical events and activities carried out by users on systems.
- Raise awareness of your responsibility for the use of passwords and equipment.
- Ensuring information security when using laptops and personal computers for remote work.

## 4.6. SYSTEM DEVELOPMENT AND MAINTENANCE

Security in the development and maintenance of systems aims to:

- Guarantee the inclusion of security controls and data validation in the development of computer systems.
- Define and document the standards and procedures that will be applied throughout the life cycle of the application and in the base infrastructure in which they are supported.
- Define methods to protect critical or sensitive information.

This policy applies to all computer systems, whether self-developed or third-party, as well as to all operating systems and/or software that make up any of the environments managed by **LEXSOFT SYSTEMS.**

The person responsible for Security Management (SRM) [CISO], together with the owner of the Information, will define the controls to be implemented in systems developed internally or by third parties, based on a prior risk assessment.

The person in charge of Security Management (RSM) [CISO] together with the Owner of the Information, will define the protection requirements by cryptographic methods based on the criticality of the information. Next, the CISO will define, together with the CTO, the encryption methods to be used.

## 4.7 INCIDENT MANAGEMENT

The main objectives of incident management are to:

- → Ensure IT services return to optimal performance.
- → Reduce the possible risks and impacts that the incident may cause.
- → Ensure the integrity of the systems in the event of a security incident
- → Communicate the impact of an incident as soon as it is detected to trigger the alarm; and implement an appropriate business communication plan.
- → Promote business efficiency.

## 4.8. BUSINESS CONTINUITY MANAGEMENT

The security in the administration of the continuity of the activities of **LEXSOFT SYSTEMS** has the following objectives:

- ♦ Minimize the effects of possible interruptions of the normal activities of **LEXSOFT SYSTEMS** (whether because of natural disasters, accidents, equipment failures, deliberate actions or other events) and protect critical processes through a combination of preventive controls and recovery actions.
- ♦ Analyze the consequences of the interruption of the service and take the appropriate measures to prevent similar events in the future.
- ♦ Maximize the effectiveness of **LEXSOFT SYSTEMS contingency operations by** establishing plans that include at least the following steps:

  1. **Notification/Activation:** Consisting of the detection and determination of damage and activation of the plan.
  2. **Resume:** Consisting of temporary restoration of operations and recovery of damage caused to the original system.

3. **Recovery:** Consisting of the restoration of the capabilities of the system process to normal operating conditions.

- Ensure coordination with **LEXSOFT SYSTEMS staff** and external contacts who will participate in contingency planning strategies. Assign roles for each defined activity.

The person in charge of Security Management (SRM) [CISO] will actively participate in the definition, documentation, tests and updating of contingency plans. The information owners and the person in charge of Security Management (SRM) [CISO] will perform the following functions:

- Identify the threats that may cause interruptions in the processes or activities of **LEXSOFT SYSTEMS**
- Evaluate the risks to determine the impact of said interruptions.
- Identify preventive controls.
- Develop a strategic plan to determine the global approach to address the continuity of **LEXSOFT SYSTEMS activities.**
- Prepare the necessary contingency plans to ensure the continuity of **LEXSOFT SYSTEMS activities.**

## 4.9. REVIEW OF THE INFORMATION SECURITY POLICIES

Each Department manager will guarantee the correct implementation and compliance with the established information security rules and procedures, within their area of responsibility.

The Responsible for Security Management (RSM) [CISO] will carry out regular reviews of all areas of **LEXSOFT SYSTEMS** to ensure compliance with information security policies, rules and procedures. Areas to review include:

- → Information systems.
- → System Providers.
- → Information Owners.
- → Users.

Information owners will support periodic review of compliance with applicable information security policies, standards, procedures, and other requirements.

Likewise, the information security policies will be reviewed at least annually or when deemed appropriate due to incidents or changes in the system. The results of the reviews will always be supervised by the person in charge of Security Management (RSM) [CISO].

The results of the reviews will be included in the annual report of the review of the system by the Directorate.

### 4.10 NON-COMPLIANCE WITH THE POLICIES

Failure to comply with policies, standards and procedures of **LEXSOFT SYSTEMS** in terms of information security is considered a serious or very serious crime, giving rise to the application of sanctions in accordance with current legislation, without prejudice to any other liability derived from themselves. It is considered missing:

- **"Serious"** that breach of policies, rules, and procedures of **LEXSOFT SYSTEMS** in terms of information security that affects the obligations and responsibilities of the staff.
- **"Very serious"** that breach of policies, rules and procedures of **LEXSOFT SYSTEMS** in terms of information security that affects the obligations and responsibilities of the staff and, in addition to that, involves a grievance for the organization or the people who are part of it, whether due to professional secrecy, economic losses or damages morals or reputation of **LEXSOFT SYSTEMS** or of the people who are part of **LEXSOFT SYSTEMS.**

These breaches are also included in document **PG-08.01 Acceptable Use.**

## 5. FORMATS AND RECORDS

FPG-05.01/01 Policy Deployment

## 6. RESPONSIBILITIES

The responsibilities defined by the methodology and activities described in the procedure are as follows:

| Roles | Responsibilities |
|---|---|
| **Management** | ♦ Define and approve the security policy<br>♦ Appoint the Security Committee |
| **H.R Manager** | ♦ Inform all contracted personnel of their obligations regarding compliance with the information security policy<br>♦ Manage confidentiality commitments with staff<br>♦ Coordinate user training tasks regarding this policy. |

| | |
|---|---|
| **Responsible for Security Management (RSM) [CISO]** | ♦ Monitor, document and analyze reported security incidents<br>♦ Communicate security incidents to the Information Security Committee and information owners.<br>♦ Participate in the preparation of the confidentiality agreement to be signed by employees and third parties who perform functions in **LEXSOFT SYSTEMS.**<br>♦ Define the physical and environmental security measures for the protection of critical assets, based on a risk analysis, and will supervise their application<br>♦ Verify compliance with physical and environmental security provisions.<br>♦ Define the controls to be implemented in systems developed internally or by third parties, based on a prior risk assessment.<br>♦ Define, based on the criticality of the information, the protection requirements by cryptographic methods<br>♦ Define, together with the CTO, the encryption methods to be used<br>♦ Actively participate in the definition, documentation, testing and updating of contingency plans<br>♦ Carry out periodic reviews of all areas of **LEXSOFT SYSTEMS** to guarantee compliance with information security policies, rules, and procedures.<br>♦ Monitor the results of policy reviews |
| **Head of Area / Department / Project [Affected]** | ♦ Define the levels of physical access for **LEXSOFT SYSTEMS** personnel to the restricted areas under their responsibility<br>♦ Guarantee the correct implementation and compliance with the established information security rules and procedures |
| **Security Committee** | ♦ Implement the necessary means and channels so that the person in charge of Security Management (SRM) [CISO] handles reports of incidents and system anomalies |

| | |
|---|---|
| | ♦ Supervise the investigation, supervise the evolution of the information, and will promote the resolution of information security incidents. |
| **Information Owners** | ♦ Authorize off-site work with information about your business to **LEXSOFT SYSTEMS** employees when they deem it appropriate.<br>♦ Define the controls to be implemented in systems developed internally or by third parties, based on a prior risk assessment.<br>♦ Define, based on the criticality of the information, the protection requirements by cryptographic methods<br>♦ Periodically review compliance with applicable information security policies, standards, procedures, and other requirements. |
| **All the staff** | ♦ Report information security weaknesses and incidents that are detected in a timely manner.<br>♦ Comply with the clean screen and desktop policy, for the protection of information related to daily work in offices. |