Ref. Doc.	POL-10	Version	1.0
Owner	Cybersecurity	Effective Date	October 2024

Information Security Policy

MASORANGE Group

(This document has been translated from the current valid Spanish version for informational purposes only. If in doubt, please refer to the Spanish version)

Prepared by:	Reviewed by:	Approved by:
Cybersecurity	Audit and Risk Committee	Board of Directors

Distribution List
- Public document

Version Control

Version	Date of approval	Change from the last version
1.0	18/10/2024	*Initial release*

Reference to other documents

Ref. Doc.	Document
PSG-01	Global Security Policy
PR-53-01	Business Continuity Policy
POL-05	Internal Control Policy
POL-06	Risk Management and Control Policy
POL-07	Privacy Policy

Index

1. Executive Summary

The Board of Directors of MASORANGE, S.L., is competent to determine the policies and strategy of the Company and all the legal entities that make up its Business Group (hereinafter, the "Group"). In this sense, it decides to implement an Information Security Policy in accordance with the main applicable legislation and based on best practices, integrated into the daily activity and in which all areas of the company must participate.

2. Purpose

The information, services and processes and systems managed by the Group are fundamental assets that constitute a strategic and necessary element for the development of its activities and, as such, their protection and safeguarding are necessary.

This policy is based both on the recommendations of the international standard ISO/IEC 27001 and the good practices established by the UNE-ISO/IEC 27002 standard, as well as on the commitment to comply with the basic principles and minimum requirements of the Royal Decree that regulates the National Security Scheme (ENS). It is aligned with current legislation on the protection of personal data, security of networks and information systems, information society, electronic commerce, cybersecurity and telecommunications. All this in order to maintain the security and integrity of the information, establishing at each point the appropriate controls and measures to preserve its confidentiality, integrity, availability, authenticity and traceability.

All areas, departments and teams that are part of the Group must be prepared for the:

- **Prevention**: the security measures and controls identified through a threat and risk assessment must be implemented, these controls must be clearly defined and documented. To ensure compliance with the policy, departments should authorize systems prior to going into production, regularly assess security, and request periodic third-party review for independent evaluation.
- **Detection**: continuous monitoring of systems is essential to detect possible anomalies in the levels of service provision and act accordingly. Mechanisms for detection, analysis and reporting to those responsible will be established on a regular basis and when there is a significant deviation from the parameters pre-established as normal.
- **Response**: all areas, departments and teams of the Group must establish mechanisms to respond effectively to security incidents, establishing points of contact and protocols for the exchange of incident-related information.
- **Recovery**: to ensure the availability of critical services, information systems continuity plans should be developed as part of the overall business continuity plan and recovery activities.

The requirements arising from:

- the Group's strategic plan
- the context of the organization
- the general principles set out in this same document

- the legal, normative and regulatory framework under which the Group operates
- the current and anticipated environment of information security risks and threats,

have been taken into consideration for the development of this information security policy.

This Information Security Policy is aligned with the Global Security Policy that defines the principles, objectives and main security responsibilities in the Group.

3. Principles

In the development of its activities, the Group assumes and undertakes to comply with the following basic principles:

- Security as an integral process
- Risk-based security management
- Prevention, detection, response and conservation
- Existence of lines of defense
- Continuous surveillance
- Periodic re-evaluation
- Separation of duties and responsibilities

4. Mission and objectives of the organization

The purpose of the organization is to (re)connect people by putting technology at the service of the best customer experience and, to this end, the Information Security Policy establishes the following objectives:

- Ensure the protection of assets based on their criticality for the business, including technical, human, material and organizational elements of the Group in relation to the information.
- Establish the guidelines that must be complied with for the protection and secure management of information in an integrated and coordinated manner with the requirements of the business, the laws that may apply and the internal regulations of the company, based on internationally recognized standards.
- Implement mechanisms for authorization and control of access to information based on the principles of least privilege and need to know.
- Implement effective and efficient information protection measures through a risk-management and cost/benefit analysis approach.
- Define roles and responsibilities in information security.
- Foster a culture of information security at all levels of the organization.
- Respond quickly and effectively to potential security incidents, building resilience and improving business continuity capability.
- Ensure the confidentiality, integrity, availability, traceability and authenticity of information throughout its life cycle.

- Adopt a long-term strategy to ensure that security is part of a continuous improvement process.

5. Information Security Management System

The Group has defined an Information Security Management System (ISMS) based on continuous improvement, in order to ensure a systematic and coherent approach to information security, monitor the application of this policy, and comply with applicable legislation.

This Policy establishes the principles, basic requirements and the security framework that serve as the basis and govern a series of thematic policies, regulations and technical procedures that make up the Information Security Regulatory Framework (MNSI).

6. Scope

The Information Security Policy:

- It applies to all the Group's entities and activities, covering all its locations and locations.
- It is mandatory for all employees, both in their internal relations and with third parties, for collaborators and service providers of the Group, as well as for any other person who has access to the information assets, either physically or logically.
- It includes all the Group's information systems and supports, as well as the telecommunications network.

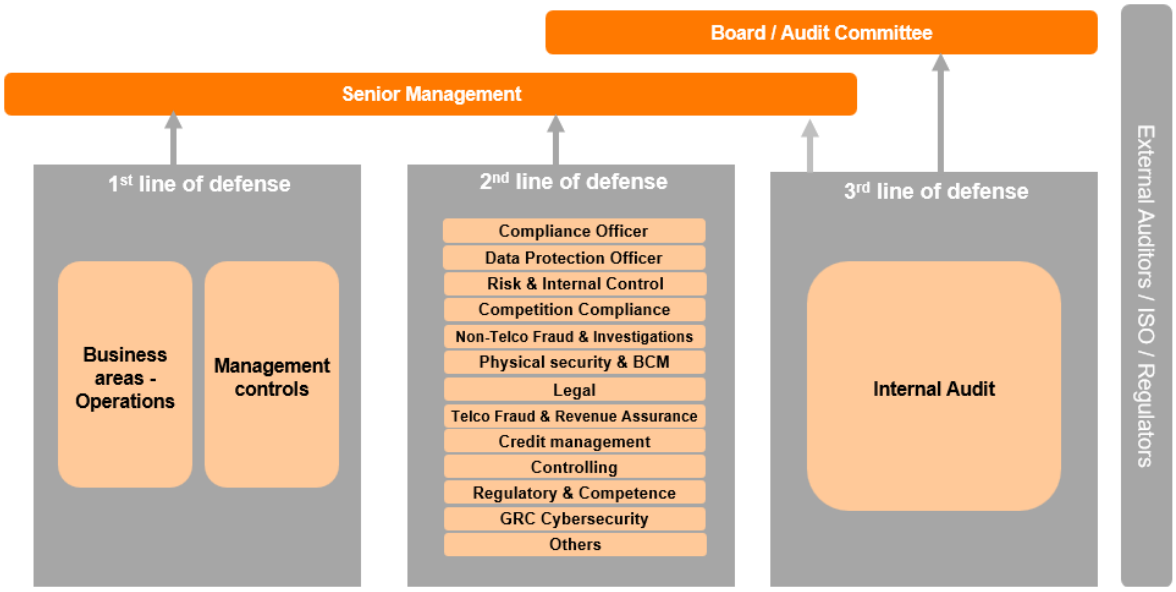
7. Management Commitment

The Group's Management, aware of the importance of information security to successfully carry out its business objectives, is committed to:

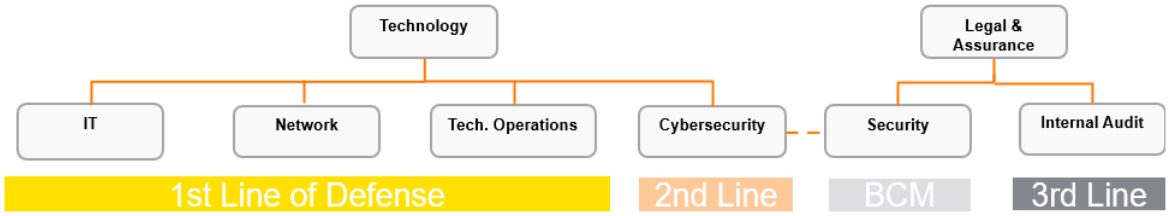
- Comply with and enforce the principles of the Information Security Policy in corporate areas.
- Provide adequate resources to ensure the establishment of the Policy, thus achieving the information security objectives defined therein and satisfying the security requirements set out in the MNSI.
- Promote the proper definition and assignment of roles and responsibilities in the field of information security in the Group.
- Promote dissemination and knowledge, as well as demand compliance with the information security policy among the Group's stakeholders.
- To promote continuous improvement in the field of information security in the Group, extending it to corporate processes.

8. Organization and responsibilities

As stipulated in the Group's Internal Control Policy, MASORANGE follows the 3 lines of defense assurance model (IIA: Institute of Internal Auditors):



Specifically for information security, the following scheme of lines of defense is followed:



In the management of Information Security at MASORANGE, the following roles are defined:

Board of Directors / Audit and Risk Committee

The determination of the Information Security Policy is the responsibility of the Group's Board of Directors as a non-delegable power.

Management

Management must assume and control the cyber-risks necessary to implement its strategy and carry out its activities. Management is responsible for identifying, managing and controlling cyber risks to itself and all its stakeholders, whether internal or external. Management must ensure the correct application within its scope of the Information Security Policy established by MASORANGE and a corporate culture focused on security.

Global Security Function

Leads and coordinates MASORANGE's security actions. From a global and transversal approach, it ensures the coherence of the different initiatives and the control of security

risks in the company, related to the domains of Information Security, Physical Security, Personal Safety and Environmental Safety.

Cybersecurity Function

At MASORANGE, the Cybersecurity function is the second line of defense in everything related to information security. This function involves the management of cyber-risks in different areas of the organization, in a coordinated manner and under the supervision of MASORANGE's governing bodies.

Its main functions are the following:

- Design, keep up to date and monitor a cybersecurity master plan for the entire Group.
- Define and ensure the governance of cybersecurity in the Group, establishing the relationship models and responsibilities between lines of defence, business areas and cybersecurity services. Define the MNSI, including associated regulations, procedures, standards, and guidelines.
- Identify and assess the Group's existing cybersecurity risks, as well as existing controls and mitigating measures, to determine residual risk, define the Risk Treatment Plan and coordinate the said plan.
- Implement the reference standards in the field of Information Security and the Information Security Management System (ISO, ENS, PCI-DSS, etc.).
- Support Business Owners in the development of their functions.

Business Areas (Business Owner)

They are responsible for the proper functioning of corporate processes, as well as the owners of the information that is used. Therefore, they are responsible for ensuring that the appropriate measures are applied to guarantee information security throughout the life cycle of the process.

Governing bodies

- **Audit and Risk Committee**: in its advisory and informative role, it provides assistance to the Board of Directors with respect to its supervision of compliance with the Information Security management policies and procedures at MASORANGE.
- **Committee on Global Security:** It is the highest level body for corporate security governance. It is made up of all the interlocutors designated by each of the areas of MASORANGE with an impact on the security of the organization, and with the main representation of the management of each of the security domains (Information Security, Physical Security, People Safety and Environmental Security).
- **Cybersecurity Committee**: it is the body responsible for making decisions with an impact on information security, as well as for monitoring the Group's compliance with legislation in this area. Its function is to coordinate the policies and actions of the different areas involved in the management of Information Security, as well as informative meetings and monitoring of the evolution of the main cyber-risks, their

controls, action plans and indicators, providing the means and capabilities to achieve these objectives.

MASORANGE has established and documented, within the MNSI, the roles and responsibilities in the field of information security, defining in greater detail the different designated security roles, their functions and the appointment and renewal process.

9. Applicable legislation

Compliance with applicable legislation on Information Security is considered essential within the Group. The list of legal and regulatory requirements applied will be identified and kept up to date, analyzing the scope of application and launching the necessary actions to ensure due compliance.

This list can be found in the applicable legislation document included in the MNSI.

10. Personal data

The Group considers full compliance with the requirements established in the applicable legislation on data protection to be a priority, and in particular, in the provisions of EU Regulation 2016/679, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) and Organic Law 3/2018. of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), in line with the values and corporate culture of the organization.

The aforementioned regulation defines as one of the principles of the processing of personal data the adoption of appropriate technical and organizational measures, in order to guarantee the protection of the rights and freedoms of natural persons with regard to the processing of personal data. Therefore, one of the objectives of information security is to guarantee the protection of personal data. The Group has a Regulatory Framework based on data protection that develops the fulfilment of this objective, as well as a set of tasks, processes, rules and responsibilities, i.e. a management system, to be carried out.

11. Conflict resolution

The Cybersecurity Committee, whose members and responsibilities are detailed in the MNSI documentation, as the highest cybersecurity body, will be responsible for resolving any conflicts of interest and responsibilities that may arise in the interpretation of what is described in the policy and in the rest of the ISMS and MNSI documents.

12. Responsibilities

It is the responsibility of all Group personnel to comply with this Information Security Policy. They must also ensure that they have access to, know and apply the current versions of this standard.

Any situation in which compliance with this policy is not possible will be considered an exception and will be handled as such by the Cybersecurity area.

Those responsible for the preparation of the documents are responsible for communicating the availability of said documentation in the organization and reviewing its content at least annually.

13. Review and Monitoring

This Policy is approved by the Board of Directors and shall enter into force on the day of its approval.

The application of this Policy will be subject to the modifications that, according to the legislation in force at any time or the interpretation of the Company itself and deems appropriate to include.

The Board of Directors will periodically evaluate the effectiveness of this Policy and will adopt the appropriate measures to solve its deficiencies, making the appropriate modifications.

14. Glossary of Terms

The terms and acronyms used in the document are described below, in alphabetical order:

- **ENS**. National Security Scheme.
- **LOPDGDD**. Organic Law on the Protection of Personal Data and Guarantee of Digital Rights.
- **MNSI**. Information Security Regulatory Framework.
- **RD**. Royal Decree
- **RGPD**. General Data Protection Regulation.
- **SGSI/ISMS**. Information Security Management Systems.
- **UE/EU.** European Union.