Doc. Ref.	PSG-01	Version	1.0
Owner	Security	Effective Date	19/07/2024

Global Security Policy

MASORANGE

(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:
Global Security and Business Continuity Area	José Antonio Vázquez CSO Addresses of: Investor Relations & ESG Cybersecurity Security People	Meinrad Spenger CEO

Mailing List

- MASORANGE employees and collaborators
- MASORANGE Suppliers
- MASORANGE Customers
- Other Security Stakeholders

Version Control

Version	Date of approval	Change from the last version
1.0	19/07/2024	Initial version of the document

Executive Summary

The Global Security Policy sets out the principles, objectives and governance of security at MASORANGE. This policy promotes good security governance, risk management, personal safety, asset protection, protection of stakeholders' personal data, and compliance with applicable laws and regulations, as well as fostering a culture of security in line with the company's values and ethical approach to, ultimately, support the achievement of business objectives.

This Policy constitutes the security reference framework for each of the companies that make up MASORANGE, and applies to all of them.

The Chief Executive Officer (CEO) is the ultimate responsible for security in the organization, and together with the Executive Committee, ensures that security risks are managed and addressed at all levels. The CEO assigns the Chief Security Officer (CSO) security responsibilities related to the governance of Global Security and sets relevant security objectives, with a focus on continuous improvement.

As part of its commitment to the Global Security Policy, MASORANGE's management establishes and acquires the following principles and commitments:

- All stakeholders in the organization (customers, employees, collaborators, suppliers, etc.) are involved in security.
- Every asset (an element that has a value for the organization and is related to the fulfillment of its objectives), is a potential target that should be protected. The necessary measures will be adopted for its protection, in accordance with its intrinsic value and the interest it may represent for a third party.
- To identify and assess asset risks, a risk management method is used, which aims to:
    - Identify critical assets, assess the severity of any impacts related to their loss, and assess security needs.
    - Identify relevant threat scenarios and assess their risk based on the probability of occurrence and the severity of the potential impact.
    - Propose measures to mitigate risk and analyze the effectiveness of these measures through a continuous improvement approach.
- In order to maintain control over risks and achieve its commitments as a responsible company, MASORANGE will comply with its legal and regulatory obligations, as well as with the safety standards adopted by the organization.
- In order to meet MASORANGE's security requirements, specific security policies are defined: for information, physical goods, the health and safety of people and the environment.
- Each director is responsible for the implementation of security in his or her business. Each employee and collaborator is responsible for the security of the assets, information and resources they use within the framework of their functions.

Madrid, 19 July 2024

Meinrad Spenger
CEO

Index

1. Purpose

The Global Security Policy defines the principles, objectives and main security responsibilities at MASORANGE.

This policy promotes good security governance, risk management, the safety of people, the protection of assets and compliance with applicable laws and regulations, as well as the promotion of a culture of safety in line with the company's values and ethical approach to ultimately Support the achievement of business objectives.

Security management is based on a risk management process that seeks to identify and manage the most relevant threats to both the company and to people's rights and freedoms, implement preventive actions that prevent or hinder their materialization, and limit the impact of incidents and crises. This comprehensive security process contributes in particular to the fight against fraud and to the protection of the rights and freedoms of data subjects in relation to the processing of their personal data.

In order to encourage and promote compliance with the business strategy and corporate values, as well as legal and regulatory compliance, this policy establishes MASORANGE's Global Security Management System, with a threefold objective to be established:

- effective security organization at all levels;
- a reference system that defines the minimum security requirements in all corporate areas;
- an exhaustive monitoring process of MASORANGE's security, based on risks, which allows decision-making.

These principles are endorsed by the Executive Committee to define the resources necessary for each of them to achieve a satisfactory level of compliance and security and to comply with the requirements defined in the security policy for each of the dimensions identified above.

2. Scope

Taking into account the context of the organization, in which internal and external issues of the organization are determined, as well as the relevant stakeholders and their requirements for security, this Policy is applicable within the scope of the activity of MASORANGE and its consolidated subsidiaries, covering all their locations and locations.

It is also mandatory for all employees, collaborators and third parties who provide services to MASORANGE.

And, therefore, it is applied to the assets that support the processes and services of the organization, an asset being understood as an element that has a value for the company and is related to the fulfillment of its objectives.

Every asset is a potential target that should be protected, therefore, the necessary measures will be adopted for its protection in accordance with its intrinsic value and the interest it could represent for a third party.

Assets include, but are not limited to:

- Business processes;
- Auxiliary services that support business processes;
- Information, whether in digital or physical format;
- The personal data of the interested parties;
- The software that allows information to be handled;
- The hardware that allows you to host the information, software, and services;
- The telecommunications network;
- The locations;
- People and;
- Reputation, company image, brand value, etc.

3. Organization

The Security Directorate 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.

To manage security risks in a complete and transversal way, a **Global Security Management System** is established, which includes four security dimensions dependent on the Global Security Policy:

Global Security Policy	
Information Security	MASORANGE *Cybersecurity* Management
Physical Security	MASORANGE *Security* Management
Health and Safety	MASORANGE *People* Management
Environmental Safety	MASORANGE*'s Investor* Relations & ESG Management

Board 1: Security Domains

Crisis **and business continuity management** is transversal to these four security dimensions and its responsibility corresponds to MASORANGE's Security Department.

The protection of personal data of interested parties is also transversal to these four security dimensions and its responsibility corresponds to the Data & Consumer Affairs Department, specifically to the MASORANGE Privacy Office. The Privacy Office is therefore responsible for the Data Protection Policy.

Each address responsible for a security domain (see **¡Error! No se encuentra el origen de la referencia.**) will be responsible for managing security and risk control initiatives, implementing their activity programmes and the preparation of indicators and reports within their domain:

- MASORANGE's Security Department is responsible for the Global Security Policy and the Physical Security Policy, as well as the Business Continuity Policy.

- MASORANGE's Cybersecurity Department is responsible for the Information Security Policy.
- MASORANGE's People Management is responsible for the People's Health and Safety Policy.
- MASORANGE's Regulation, Public Affairs and Sustainability Division is responsible for Environment and Energy Policy.

The Chief Security Officer (CSO) will be in charge of organising the security function in a transversal manner, coordinating security actions within the framework of MASORANGE's Global Security Management System. To extend governance and management to the entire company, he will act as coordinator of the Global Security Committee, whose main mission will be:

- Integrate management representation from the main groups with an impact on Security and constitute an effective communications channel
- Ratify the security strategy and objectives, aligned with the business strategy
- Review and approve compliance with key project objectives and approval of associated action plans
- Monitor safety indicators and the status of risks
- Provide the resources for the implementation of the necessary security controls

MASORANGE's Global Security Committee is made up of all the interlocutors appointed by each of the MASORANGE areas with an impact on the organization's security, and with the main representation of the management of each of the security domains. The Committee shall be held every two years and shall report to the Executive Committee.

4. General principles of the Global Security Management System

In order to comply with the provisions of the Policy, the Global Security Management System is based on the following principles:

4.1. Security as a sovereign function

MASORANGE security is a sovereign function that plays an active and direct role in protecting people, their reputations and their assets from numerous forms of risks and threats.

To this end, the Security Directorate establishes, promotes and coordinates, together with the rest of the organisation's directorates, the measures it deems necessary to manage risks, and in particular, when they affect essential assets.

To ensure the effectiveness of these protection measures throughout the MASORANGE Group, the Security Department will monitor the risks and the level of security controls in a transversal and continuous manner.

In the event of any manifest failure in security or in the event of the appearance of serious or urgent situations that compromise MASORANGE's people or assets, the Security

Management may take over the management of the situation, involving the necessary parties and the corresponding management bodies.

The Directorate of Security exercises its sovereign authority in the following areas:

- The definition of the security policy and the control of its application;
- Security risk management;
- Coordinating findings and supporting the Internal Audit Division for security-related audit activities, including regulatory issues and monitoring corrective action plans;
- MASORANGE's crisis management.

4.2. Security as a transversal function

The Safety Directorate defines and organises MASORANGE's security function with a view to improving the effectiveness and efficiency of controls and risk control.

Since the scope established by the Global Security Policy is comprehensive throughout the organization, the Global Security Management System is implemented in a transversal manner, involving participants in all areas and at all levels of management.

Working closely with business, technology and support departments, the Global Security Management System promotes the implementation of cross-cutting controls, monitors their relevance (based on risk and economic criteria) and ensures their effectiveness.

4.3. Security as a business enabler

The Global Security Management System pursues the implementation of appropriate security measures in order to protect its assets and mitigate risks, enabling the company to operate reliably, maintain the trust of customers and business partners, comply with regulations and standards, and minimize disruptions and financial losses.

Security plays a key role in supporting and driving MASORANGE's business activities and is understood as a business enabler and competitive advantage.

4.4. Risk-based management

Security risk management within the Global Security Management System is based on three fundamental pillars:

- **Risk identification:** A risk is an event that can compromise the achievement of objectives. The identification of risks that threaten the integrity of employees and essential assets is carried out as a matter of priority. This risk assessment takes into account internal and external stakeholders as well as their expectations.
- **Risk assessment:** Risk assessment helps to classify risks according to their likelihood and impact and to track their evolution over time. It is presented in accordance with corporate risk management. Each Directorate concerned regularly communicates its security risk assessment to the Directorate of Security.

- **Risk management:** Security risks that threaten critical assets are the subject of priority action plans. Any residual risk that exceeds the risk appetite following the implementation of these plans must be formally accepted by management.

Risk-based security management allows resources to be allocated efficiently, prioritising those security measures that reduce the greatest risks with a cost-benefit approach.

Employing a risk-based management approach enables better decision-making at the management level.

4.5. Continuous improvement

The Global Security Management System will employ a continuous improvement approach in order to be able to iteratively adapt to emerging threats and new security challenges, pursuing persistence in protection.

Continuous improvement is based on making the right decisions to optimize the organization's security measures. It consists of four phases:

- **Anticipating** risks through surveillance, analysis and security planning.
- **Prevention** by reducing or eliminating the possible appearance of a risk.
- **Protection** by limiting the effects of the risk in the event that it occurs.
- **Evaluation** by learning lessons from audits and feedback received after incidents with a high impact on the organization.

Illustration 1: Continuous improvement cycle

4.6. Compliance with legal obligations

MASORANGE complies with local, national and international laws and regulations that impact the safety of the organization. Therefore, the list of applicable legal and regulatory requirements is identified and kept up to date, analyzing the scope of application and planning the corresponding actions for their due compliance.

This management extends to each of the departments involved in the management of Global Security, in a manner consistent with each of the security policies associated with the dimensions.

5. Security criteria, threats and associated risks

To estimate risk levels, the risk assessment methodologies implemented at MASORANGE use the different security criteria established in the corresponding security policies and regulations. The loss of one or more security criteria for your assets results in damage to MASORANGE. These damages can be of different types: human, financial, legal, environmental, image, operational, etc.

To establish the potential impact that the loss of these security criteria may have, the directorates establish a simple scale of levels, from least to highest impact.

Threats, which if they materialize could lead to a security breach of MASORANGE's assets, can be of an accidental or malicious nature, the result of damage related to natural or environmental phenomena, or intentional human actions (cybercrime, terrorism, sabotage, etc.) or involuntary (error, accident, etc.).

Threats are generally based on the exploitation of vulnerabilities in assets. MASORANGE uses recognized risk analysis and assessment methodologies that comply with internationally recognized standards.

Each of the security dimensions requires a series of security requirements in order to be aligned with the business objectives set by MASORANGE. These requirements are based on a risk assessment taking into account the safety criteria affected, the potential impact and the probability of occurrence, always in accordance with the risk scale established by the Internal Control, Risk & Compliance Department.

6. Policy Review

The Global Security Policy will be reviewed annually and updated at least every five years, or whenever necessary due to significant changes affecting MASORANGE's structure, business or applicable legislative context.

7. Compliance

Compliance with this Policy is mandatory for all employees, collaborators and service providers of the company within the specified scope.

Any violation of this policy may result in contractual claims and/or termination of contracts with contractors or third parties, as well as contractual claims and/or disciplinary measures for MASORANGE employees.

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