



**CORPORATE SECURITY AND PRIVACY POLICY**

## **CORPORATE SECURITY AND PRIVACY POLICY**

### **1 Introduction**

The Board of Directors of Mapfre, S.A. (the “**Company**”) is the competent body for defining the general strategy and establishing the basis for appropriate and efficient coordination between the Company and the other companies within the corporate group of which Mapfre, S.A. is the controlling company within the meaning of Article 42 of the Spanish Commercial Code (the “**Group**” or the “**Mapfre Group**”).

In exercising these responsibilities, the Board of Directors approves and updates the corporate policies that govern the Company’s activities; that establish the guidelines and fundamental principles that inspire and orient the mandatory rules that the Group’s other companies approve within the scope of their own decision-making capacity and responsibility; and that form the basis for mandatory compliance with those rules.

Likewise, in accordance with the *Regulations of the Board of Directors of Mapfre, S.A.*, this body is responsible for approving a Security policy, including cybersecurity, and a Privacy policy.

In this context, the Company’s Board of Directors has approved this *Corporate Security and Privacy Policy* (the “**Policy**”), with the aim of formalizing the Mapfre Group’s response to a global and constantly evolving environment, by equipping itself with an effective Corporate Security Function aligned with the Purpose, Vision, and Values set out in the *Institutional and Business Principles of the Mapfre Group* approved by the Company’s Board of Directors.

The purpose of the Corporate Security Function is to enable the normal conduct of business by providing a secure environment in which the companies that make up the Mapfre Group can carry out their activities. To this end, it must permanently protect the Group’s tangible and intangible assets and business processes against Security Risks, with particular attention to the safety of individuals, regulatory compliance, information security, privacy, the operational resilience of services provided to third parties, the preservation of the Group’s good reputation, and its sustainability.

Accordingly, all directors, officers, employees, executives, and collaborators of the Mapfre Group share responsibility for protecting these assets and processes and shall therefore: (i) use the resources made available by Group

companies in a professional and responsible manner; (ii) report any situation they identify that may pose a risk to the Group and or to the individuals who make it up; and (iii) in general terms, apply with due diligence the measures established for this purpose.

The Mapfre Group's aspiration to leadership and its global vocation guide its actions in the field of Security, an area in which it also seeks to be a benchmark, as it is in the rest of its activities.

## 2 Classification

This standard is a corporate-level policy in accordance with the classification set out in the *Policy on the Development and Organization of the Rules that Comprise the Mapfre Group's Corporate Governance System*.

## 3 Purpose

This *Policy* seeks to ensure the protection of the Group's assets, compliance with Security and Privacy regulations, the operational resilience of services provided to third parties, the preservation of the Mapfre Group's reputation and image, and its sustainability.

## 4 Scope of application

This *Policy* applies to all companies that make up the Mapfre Group. It is also applicable, as appropriate and in accordance with the relevant shareholder agreements, to the various partnerships and joint ventures in which companies of the Group participate.

## 5 Definitions

For the purposes of this Policy, the following definitions apply:

- a) **Assets:** all the capacities, goods, rights, means, and intangibles owned by a company, institution or individual, or over which they hold possession or exploitation rights.
- b) **Cyber-risks:** following the definitions of the CRO Forum and the International Association of Insurance Supervisors ("IAIS"), these are the risks associated with carrying out a business activity, including the management and control of data, in a digital or "cyber" environment. These risks stem from the use, processing, and transmission of electronic data via information systems, communication networks and the Internet, and they include physical damage caused by cyber-incidents, as well as fraud committed by the inappropriate or improper use of data. This category also includes any petitions for liabilities arising from the

protection of the availability, integrity, and confidentiality of the electronic information of individuals, companies or governments to which any Mapfre Group company has access in the course of its business.

- c) **ICT risk:** Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialized, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment.
- d) **Access Control:** set of design measures, software, equipment, and technical means intended to regulate the entry or passage to the facilities, spaces, systems, applications, devices, information, and other assets of the Mapfre Group, in a way that allows each of them to be restricted and tracked with an appropriate level of detail—who accesses them, when, and how—while also facilitating and streamlining access for authorized individuals.
- e) **Security, Crisis and Resilience Committee:** committee created by the Executive Committee of the Society, which is entrusted with the functions of: (i) ensuring that business objectives and needs govern the activities of the Corporate Security Function; and (ii) ensuring that the recommendations of the Corporate Security Function are taken into account in corporate business processes, in accordance with the *Mapfre Group's Security Strategic Framework* approved by the Company's Board of Directors. The Security, Crisis, and Resilience Committee is also vested with authority for direction and oversight in the areas of business continuity and crisis management.
- f) **Privacy and Data Protection Committee:** specific committee under the Security, Crisis and Resilience Committee for management and control of privacy and protection of personal data, supporting the DPO in the performance of their functions. This committee shall act as a crisis committee with respect to the management of personal data security incidents and breaches, including coordination, monitoring, decision-making, and notification to supervisory authorities and or affected parties.
- g) **Company Corporate Security Function:** the set of activities, personnel, means, and resources necessary to achieve an adequate level of protection for an organization's assets against identified risks, to ensure the rights and freedoms of natural persons with regard to the processing of their personal data, and to provide the organization with operational

resilience capabilities, in accordance with the *Mapfre Group's Security Strategic Framework*.

- h) **Operational Resilience:** the ability of an entity to build, ensure, and review its operational integrity and reliability by ensuring, directly or indirectly through the use of services provided by third-party suppliers, the full range of capabilities required to preserve the security of the networks and information systems it uses and that support the continuous provision and quality of its services, even in the event of disruption.
- i) **Privacy:** the condition of being private, ensuring the rights of individuals with regard to the processing of their personal data, including respect for the right to honor and personal privacy.
- j) **Risk:** the possibility that future events may lead to adverse consequences for the achievement of economic and business objectives or the financial position of the Group. Risk is understood in a broad sense, encompassing events or combinations of events affecting one or more risks that, due to their significance or scale, require separate treatment.
- k) **Security Risks:** the subset of risks whose management has been entrusted to the Security Organization<sup>1</sup>, from among all risks affecting the Group's assets.
- l) **Security:** (i) the condition achieved when assets are protected against risks; (ii) the quality of being secure, that is, free from damage, danger, or risk; and (iii) the set of measures necessary to achieve that condition. Depending on the assets protected and the nature of the measures applied, reference is commonly made to different types of security, such as information security, privacy, occupational safety, personal safety, fire safety, among others.

## 6 Commitments

The Mapfre Group undertakes the following commitments in the area of security and privacy:

- a) The safety of individuals, the most valuable asset of the Mapfre Group, is a top priority, including protection in the workplace, facilities, and

---

<sup>1</sup> In accordance with the *Mapfre Group's Security Strategic Framework*, this refers to the organization responsible for developing the Corporate Security Function, integrating the human teams, resources, and means of all kinds required to carry out the mission defined in the *Strategic Security Framework of the Mapfre Group*, in line with the established principles and through the operating model set out therein.

business travel, and ensuring appropriate training and prevention in relation to risks.

- b) Strict compliance with Security and Privacy regulations, in line with the Group's ethical and social commitment.
- c) The integration of Security and Privacy as an additional component of business processes, contributing to their quality, sustainability, and operational resilience. To this end, security threats will be proactively monitored, deploying protection and detection capabilities that enable early response to potential incidents, minimizing their impact through appropriate mitigation actions and implementing lessons learned.
- d) The adoption of a comprehensive and global Security model to protect the Group's assets and processes against Security and Privacy risks of any nature, regardless of where they may materialize, with particular attention to ICT-related risks and Cyber Risks, in order to ensure operational resilience. In this context, Group suppliers will be required to meet Security requirements proportional to the risk of the services they provide, in order to ensure consistent protection of corporate assets and operational resilience.
- e) Providing added value to the Group and its business and support processes through the identification and leveraging of synergies with other areas and functions, fostering collaboration and efficiency in the performance of activities.
- f) The application of principles of resource optimization, timeliness, economies of scale, and continuous improvement, as an expression of the innovative spirit and pursuit of excellence that characterize the Mapfre Group.
- g) Fostering the trust of stakeholders by enabling them to carry out their activities and or interact with the Group without Security Risks affecting their ability to make free decisions and act independently.
- h) Ensuring appropriate protection of information owned by the Mapfre Group and by its customers, collaborators, employees, and other stakeholders to which the Group has access, guaranteeing its confidentiality, authenticity, privacy, availability, and integrity, as well as that of the systems that store, transmit, or process such information. To this end, the necessary measures and controls, including access controls, will be implemented based on a risk management approach, and shall also ensure compliance with the privacy principles and criteria established in applicable regulations. Particular protection shall be

afforded to facilities where such data are processed and stored, including data processing centers and data centers.

- i) Training and awareness-raising for Group personnel in matters of Security and Privacy, as well as the dissemination of the rules and procedures approved in this area. In this regard, employees must ensure, among other matters, the confidentiality of information and compliance with data protection regulations, as provided for in the Mapfre Group *Code of Ethics and Conduct* and its *Telematic Code*. Failure to comply with these obligations may give rise to the application of the corresponding sanctions under the applicable disciplinary regime.
- j) A permanent willingness to cooperate with public authorities, as part of the spirit of service that permeates all actions of the Mapfre Group and its responsibility toward the society in which it operates.

## **7 Responsibilities**

The responsibilities associated with the management of Security and Privacy are set out in detail in the *Mapfre Group Security Governance Model: Organization*, approved by the Company's Board of Directors.

## **8 Oversight, dissemination, and monitoring of this Policy**

The Corporate Security Division is the Sponsor of this Policy, as defined in the *Policy on the Development and Organization of the Rules that Comprise the Mapfre Group's Corporate Governance System*.

The Group Security, Crisis, and Resilience Committee is the body responsible for promoting the development and implementation of this *Policy*.

The Company's Board of Directors, with the support of the Risk, Sustainability, and Compliance Committee, and with the collaboration of the Group Security, Crisis, and Resilience Committee and the Sponsor of this *Policy*, shall periodically, and at least annually, assess the level of compliance with and effectiveness of this *Policy*.

Notwithstanding the foregoing, the governing and management bodies of the Group companies—at the corporate, regional, and local levels—are responsible for disseminating and ensuring compliance with this *Policy* within their respective companies. To this end, they must take the necessary measures to do so, and, where applicable, report any areas of non-compliance or partial compliance through the established channels.

As part of the Company's commitment to its stakeholders, this *Policy* shall be published on the corporate website.



## **9 Approval and entry into force of this *Policy***

This *Policy* was initially approved by the Company's Board of Directors on July 23, 2025, and last amended on December 22, 2025, repealing and replacing the previous version.