MAPFRE GROUP'S CORPORATE SECURITY AND PRIVACY POLICY

CONTENTS

I. Definitions

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

Assets: all the capacities, goods, rights, means and intangible assets owned by a company, institution or individual, or whose possession or right of use it holds.

Cyber-risks: according to the definitions given by the CRO Forum and IAIS, these are risks associated with conducting 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 the data. This category also includes any applications for liabilities arising from the protection of the availability, integrity and confidentiality of the electronic information of individuals, companies or governments to which MAPFRE has access in the course of its business.

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.[1]

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, so as to make it possible to restrict and ascertain with the appropriate degree of detail for each of them, who accesses them, when and how, while facilitating and expediting the access of authorized persons.

Security, Crisis and Resilience Committee: the most senior management body of the Security Organization. This Committee will ensure that the objectives and business needs govern the activity of the Corporate Security Function and that it is deemed to be a component of corporate business processes, in line with the Security Master Plan. The Security, Crisis and Resilience Committee will also be responsible for management and control in the sphere of business continuity and crisis management.

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 will perform the functions of a crisis committee by managing incidents and breaches of personal data security, including coordination, monitoring and decision-making, and notifying the Control Authority and/or Affected Parties.

Corporate Security Function: set of activities, people, means and resources necessary to achieve the appropriate degree of protection for the assets of a

[1] As defined in the Digital Operational Resilience Regulation of the European Parliament and of the Council (DORA)

business organization against the established risks, safeguard the rights and freedoms of individuals with regard to the processing of their personal data, as well as to provide the organization with operational resilience capabilities, in line with the Security Master Plan.

MAPFRE, MAPFRE GROUP OR GROUP: the business group consisting of MAPFRE, S.A., as parent company, and its subsidiaries and affiliates in accordance with the Article 4 of the Spanish Securities Market Act.

Operational Resilience: the ability of an entity to build, secure and review its operational integrity and reliability by ensuring, directly or indirectly, through the use of services provided by third party providers, the full range of capabilities necessary to preserve the security of the networks and information systems used by the entity and which underpin the continued provision of its services and the quality of those services, even in the event of disruption.

Security Master Plan: strategic framework for the execution of the Corporate Security Function.

Privacy: private status that ensures the rights of natural persons with regard to the processing of their personal data, including observance of the right to honor and privacy.

Risk: the potential for future events to give rise to adverse consequences for the attainment of economic and business objectives, or for the Group's financial situation. The concept of risk should be understood in a broad sense, including events and combinations of events that affect one or several risks that, on account of their importance or scope, must be handled separately.

Security Risks: subset of risks whose management has been entrusted to the Security Organization, part of the total risks borne by the Group's assets.

Security:

1. Condition achieved when assets are protected against risks.

2. The quality of being secure, i.e., free from any damage, danger or risk.

3. Set of measures necessary to achieve the above condition. Depending on what assets are to be protected and the nature of the measures, we usually speak of different types of security, such as Information Security, Privacy, Workplace Security, Safety of People, Fire Safety, etc.

II. Introduction

The essential purpose of the Corporate Security Function is to enable the normal conduct of business by providing a safe environment in which MAPFRE can carry out its activities. To do so, it must protect its tangible and intangible assets and business processes on a permanent basis against security risks. Particularly, it must ensure the safety of people, information security, privacy, the operational resilience of services provided to third parties, preserve the company's good reputation, its sustainability and compliance with regulation in these areas.

In this regard, all MAPFRE employees, managers and collaborators are jointly responsible for the protection of such assets and processes. They will use the resources that MAPFRE places at their disposal in a professional and responsible manner, report any situation they become aware of that may pose a risk to the company and/or the people who make up the company and, in general, apply the measures established for this purpose with due care.

MAPFRE's striving for leadership and its global vocation underly, as in the rest of the GROUP's activities, its actions in the area of security, a field in which it also aspires to be a benchmark.

This Policy is aligned with MAPFRE's Security Master Plan, which sets out the Strategic Framework and the model for implementing the Group's different security and environmental management actions.

III. Scope

This Corporate Security and Privacy Policy is mandatory throughout the MAPFRE Group.

IV. Objectives

This Policy formalizes the MAPFRE Group's response to a global and changing scenario, enabling it to equip itself with an effective corporate security function in accordance with Institutional and Business Principles in order to protect MAPFRE's assets. It also ensures regulatory compliance in security and privacy matters, the operational resilience of the services provided to third parties, the preservation of the company's good reputation and image and the company's sustainability.

V. Commitments

The MAPFRE Group assumes the following security and privacy commitments:

1. The safety of people, MAPFRE's most valuable asset, is the first objective and a permanent concern.

2. Compliance with security and privacy regulations, with scrupulous observance of current legislation, in accordance with the Group's principle of being ethically and socially responsible.

3. Integration of security and privacy within business processes as an essential component of such processes, thus contributing to their quality and sustainability.

4. Adoption of a comprehensive and global security model for the protection of the Group's assets and business processes against security and privacy risks of any nature, regardless of the place where they are likely to materialize. With special attention paid to ICT risks and CyberRisks, with the aim of ensuring operational resilience. Accordingly, security requirements proportional to the risk of the services they provide for the MAPFRE Group will be transferred to third party providers in order to ensure uniform protection of corporate assets and operational resilience.

5. Contribution of added value to MAPFRE and its business or support processes by finding and using synergies with other areas and functions of the Group in the performance of its activity.

6. The application of principles of resource optimization, timeliness, economy of scale and continuous improvement as a manifestation of MAPFRE's spirit of innovation and pursuit of excellence.

7. Strengthening the confidence of stakeholders, thus enabling them to carry out their work and/or relate to the Group free of any security risks that might perturb their intentions or their ability to decide and act freely.

8. Adequate protection of the information owned by MAPFRE and that belonging to its customers, collaborators, employees and other stakeholders and to which MAPFRE has access by virtue of its relationship with them, guaranteeing its confidentiality, authenticity, privacy, availability and integrity, as well as that of the systems that store, transmit or process it. For this purpose, the necessary measures and controls will be put in place, including access controls, in accordance with a risk management approach. This will also ensure processing in conformity with the privacy principles and criteria established in current legislation. In particular, the centers in which the aforementioned information and data is processed and stored (DPCs-Data Centers) will be provided special protection.

9. Training and awareness-raising of all personnel in security and privacy matters, as well as the dissemination of rules, procedures and

responsibilities. As a result, all employees are aware of the obligations to ensure, among other things, the confidentiality of information as well as compliance with data protection regulations. MAPFRE's Code of Ethics and Conduct, as well as its Telematic Code, provide for appropriate sanctions in accordance with the current disciplinary regime in the event of a breach of these principles.

10. Permanent readiness to collaborate with the authorities as part of the spirit of service that imbues all MAPFRE's actions and its responsibility towards the society in which it operates.

VI. Responsibilities

The Group's Security, Crisis and Resilience Committee is the body responsible for managing development and implementation of this Policy, and for ensuring that it is appropriately complied with, publicized and periodically reviewed.
The other responsibilities associated with Security and Privacy management are outlined with the necessary detail in MAPFRE's Security Governance Framework.

VII. Approval, entry into force and subsequent reviews

This Corporate Security and Privacy Policy was approved by the MAPFRE S.A. Board of Directors on June 26, 2024, upon which it entered into force. It replaces the previous version of the policy (MAPFRE Group Corporate Security and Privacy Policy) approved by the Board of Directors of MAPFRE, S.A. on December 13, 2018.

The policy will be reviewed at least once a year and may be amended at any time at the proposal of the Executive Committee of MAPFRE to adapt it to any significant change that affects any of its contents.

Approved on July 23, 2015 Latest

change approved on June 26, 2024