MAPFRE GROUP CORPORATE SECURITY AND PRIVACY POLICY

TABLE OF CONTENTS

I. Definitions

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

Assets: A set of all capabilities, property, rights, resources and intangible assets owned by a company, institution or individual, or the possession or right of use held by such parties.

Cyber Risks: In accordance with the definitions of the CRO Forum and the International Association of Insurance Supervisors (IAIS), cyber risks 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 encompass physical damage caused by cyber attacks, as well as fraud committed by the inappropriate or improper use of the data. This category also includes potential liabilities arising from protection of the availability, integrity and confidentiality of the electronic information of individuals, companies or governments to which MAPFRE has access within the scope of its activities.

Access Control: The set of design measures, software, equipment and technical resources aimed at regulating the entry or access to facilities, sites, systems, applications, devices, information and other MAPFRE Group assets, so as to restrict access and identify by whom, when and how they are accessed with the appropriate level of detail, while facilitating and streamlining the access of authorized persons.

Security and Environment Committee: The most senior management body of the Security and Environment Organization. This committee ensures that business objectives and requirements govern the activity of the Corporate Security and Environment Area, and guarantees that this area is treated as a constituent element of corporate business processes, in line with the provisions of the Security and Environment Master Plan.

Privacy and Data Protection Committee: A specific committee subordinate to the Security and Environment Committee for management and control in the area of privacy and personal data protection, supporting the DPO in the performance of their functions. This committee will exercise the functions of a crisis committee in relation to the management of incidents and breaches of personal data security, including coordination, monitoring and decision making, in addition to notification to the Control Authority and/or Affected Parties.

Crisis and Business Continuity Committee: A specific committee subordinate to the Security and Environment Committee for management and control in the area of business continuity and crisis management. It is responsible for implementing the instructions of the Security and Environment Committee to ensure correct governance of the activities within its scope, in line with the Security and Environment Master Plan.

Corporate Security and Environment Area: A set of activities, people and resources required to achieve the appropriate level of protection for the assets of a business organization against identified risks, guarantee the rights and freedoms of individuals regarding the processing of their personal data, and achieve sustainable management from an environmental and energy perspective, in line with the Security and Environment Master Plan.

MAPFRE, MAPFRE Group or the Group: The business group comprised of MAPFRE S.A., as parent company, and its subsidiaries and dependent companies in accordance with the provisions of Article 4 of the Securities Market Law.

Environment: The environment in which an organization operates, including the air, water, land, natural resources, flora, fauna, human beings and the interactions between them, as established in the Security and Environment Master Plan.

Security and Environment Master Plan: The strategic framework for the development of the Corporate Security and Environment Area.

Privacy: Private status guaranteeing the rights of individuals with regard to the processing of their personal data, including respect for the right to dignity and privacy.

Risk: The possibility that future events may give rise to adverse consequences for economic and business objectives, or for the financial situation of the Group. For these purposes, the concept of risk is understood in its broadest sense, encompassing events or combinations of events that may affect one or more risks which, due to their importance or nature, may require separate management.

Security and Environment Risks: A subset of risks, within all risks affecting the Group's assets, whose management has been entrusted to the Security and Environment Organization.

Security:

1. Status achieved when assets are protected against risks.

2. The attribute of being secure, i.e. exempt from all damages, hazards or risks.

3. A set of measures required to achieve this status or attribute. There are different types of security depending on the assets protected and the nature of the measures adopted, i.e. information security, privacy, occupational safety, safety of people, fire safety, etc.

II. Introduction

The rationale behind the Corporate Security and Environment Area is to enable normal business operations by facilitating a secure environment in which MAPFRE can conduct its activities. To do this, the organization must provide permanent protection against security risks for its tangible and intangible assets and business processes, with a particular focus on the safety of people, regulatory compliance, information security, privacy, and preservation of the company's good reputation and sustainability.

All MAPFRE employees, managers and collaborators have a shared responsibility to protect these assets and processes, using the resources that MAPFRE provides in a professional and responsible manner, reporting any situation they detect which could entail a risk for the company and/or its people, and in general implementing with due diligence the measures established for these purposes.

MAPFRE's leadership aspirations and its global commitment influence, as in the other Group activities, actions related to security, an area in which MAPFRE also aims to be a benchmark.

This Policy is in line with MAPFRE's Security and Environment Master Plan, which sets out the strategic framework and model for the Group's security and environmental management initiatives.

III. Scope

Compliance with this Corporate Security and Privacy Policy is mandatory across the entire MAPFRE Group.

IV. Objectives

This Policy formalizes the MAPFRE Group's response to a changing global scenario. It constitutes an effective corporate security function, in line with the Institutional and Business Principles, enabling MAPFRE to protect its assets. Furthermore, it ensures compliance with regulations on matters of security, privacy, and the preservation of the company's good reputation, image and sustainability.

V. Commitments

The MAPFRE Group assumes the following commitments regarding security and privacy:

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

2. Compliance with security and privacy regulations, scrupulously respecting the legislation in force and the Group's principle to be ethically and socially responsible.

3. The integration of security and privacy into all business processes as a standard component, contributing to their quality and sustainability.

4. The adoption of a comprehensive global security model to protect the Group's assets and business processes from security and privacy risks of any nature, irrespective of the place where they may occur, with a particular focus on cyber risks.

5. The contribution of added value to MAPFRE and its business and support processes by searching for and harnessing synergies with other Group areas and functions carried out in its operations.

6. The application of the principles of resource optimization, opportunity, economies of scale and continuous improvement as a manifestation of MAPFRE's innovative mindset and quest for excellence.

7. Contribution to the trust of stakeholders, enabling them to carry out their work and/or interact with the Group without any security risks compromising their willingness and ability to choose and act freely.

8. Adequate protection of the information belonging to MAPFRE and its clients, collaborators, employees and other stakeholders, as well as the information to which MAPFRE has access by virtue of its relationship with these parties, guaranteeing the confidentiality, privacy, availability and integrity of this information and of the systems that store, transmit and process it. To this end, the necessary measures and controls, including access controls, will be implemented in line with a risk management approach, to ensure that information is processed in accordance with privacy principles and criteria established in the current legislation. In particular, centers in which the aforementioned information and data is processed and maintained (data centers) will receive special protection.

9. The training and awareness of all personnel regarding security and privacy, as well as the dissemination of the relevant standards, procedures and responsibilities.

10. Ongoing willingness to collaborate with authorities as part of the spirit of service that defines all MAPFRE undertakings and the social responsibility with which it conducts its business.

VI. Responsibilities

The Group's Security and Environment Committee is the body responsible for promoting the development and implementation of this Policy, and for ensuring its compliance, dissemination and periodic revision.

VII. Approval, entry into force and subsequent revisions

This Corporate Security and Privacy Policy was approved by the MAPFRE Board of Directors on December 13, 2018, at which time it took effect. It replaces the previous version (Corporate Security Policy) approved by the MAPFRE S.A. Board of Directors on July 23, 2015.

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

Approved on July 23, 2015

Last modification approved on December 13, 2018