CHAPTER 10 BUSINESS CONTINUITY POLICY

10.1 OWNER OF THE POLICY
The Corporate Security Division.

10.2 SCOPE
This Business Continuity Policy is mandatory for all companies in the MAPFRE Group, regardless of whether they may require adjustments to its content to meet additional specific requirements from their respective local authorities or supervisors.

10.3 OBJECTIVES

This Policy establishes the global framework for the development, documentation, implementation, testing, review, and continuous improvement of Business Continuity Plans at MAPFRE and its Management Systems, including the different elements linked to the continuity of ICT activity and following a risk-based approach, so that they:

- Allow for, through the execution of Business Impact Analysis (BIA), the preliminary estimation of the potential repercussions, damages, and losses that a disruptive incident might cause to the company's business processes. The BIA will allow the potential impact of these incidents to be assessed using quantitative and qualitative criteria, taking into account the functions identified as critical[1] and the resources that support them.

- Enable an adequate and timely response to the materialization of a catastrophic security risk, resulting in a scenario where one of the basic components of the Group's activities becomes unavailable: personnel, buildings and offices, technology, information, and suppliers.

- Reduce the impact of possible catastrophes on business activities, ensuring that essential data and functions are preserved or, if this is not possible, that such data or functions are recovered, in a timely and progressive manner, until the return to normality.

- Allow for, after the occurrence of a disruptive incident, the recovery of functions identified as critical and the restoration of other normal business activities, meeting the time and recovery point objectives identified in the BIA. These objectives may vary depending on the nature of the incident and the criticality of the affected operations.

- Ensure that the activities can be properly operated for a sufficient period of time, in accordance with business needs and until normal operation has been restored.

- Contribute to the continuous improvement of the company's operational resilience capabilities, by conducting annual tests to verify the correct functioning of the strategies implemented and to help identify areas for improvement.

10.4 GENERAL PRINCIPLES
The Business Continuity Policy is based on the set of principles and commitments described below:

1. The protection and safety of individuals is the primary premise and the top priority, both in normal situations and during a crisis resulting from a disaster.

2. The appointment of representatives of the different areas with the appropriate experience and knowledge, to actively participate in the development, documentation, implementation, testing, review, updating, and continuous improvement of Business Continuity Plans and their Management Systems.

3. The development and implementation of Business Continuity Plans by Group companies, taking into account internal areas and departments, providers, and services and employing appropriate and

[1] Including those identified as Critical or Important Functions by the Digital Operational Resilience Act (DORA).

proportionate systems, resources, and procedures. Business Continuity Plans will include specific, appropriate, and documented provisions, plans, procedures, and mechanisms to guarantee the continuity of ICT activity, articulated through the recovery strategies associated with the unavailability of technology.

4. Taking advantage of the synergies generated and the lessons learned in the development and implementation of Business Continuity Plans and any other plans in the field of security in the Group's companies, considering the common means and resources available to MAPFRE

5. The adoption of reasonable measures for the operational continuity of processes and activities, including digital operational resilience, depending on their criticality as established by the Organization.

6. The inclusion of security, privacy, and reliability criteria that reasonably guarantee the continuity of critical services provided by third parties, in the event of their outsourcing.

7. The development of appropriate crisis communication procedures within Business Continuity Plans, which guarantee the transmission of relevant and timely information. These procedures must provide for:

    - Internal communication to all personnel, distinguishing messages directed at individuals involved in response and recovery efforts from messages intended for the rest of the personnel.

    - External communication, to enable proper execution and ensure the timely provision of information to all relevant stakeholders.

8. The communication of responsibilities and procedures relevant to all personnel involved in Business Continuity, through awareness and training efforts, as well as the dissemination of this Policy to the Organization’s personnel. The content to be disseminated will include procedures for escalating incidents that may occur, taking into account both their nature and the unavailability scenarios they might cause.

9. A framework that serves to establish Business Continuity objectives within a Management System that, while complying with legislative, regulatory, and applicable standards requirements, includes the periodic review, testing, and updating of Business Continuity Plans. These reviews and updates will take into account the lessons learned from past crises and incidents, and should be conducted (i) in response to significant changes in technological infrastructure, (ii) as a result of findings from testing, or (iii) due to the emergence of new threats. All of this as part of a process that allows for the regular evaluation of the effectiveness of implemented continuity measures and ensures the continuous improvement of the Organization's operational resilience capabilities.

10. The ongoing willingness to collaborate with authorities in the event of a disaster or need, as part of the service-oriented spirit that permeates all actions of MAPFRE and the responsibility towards the society in which it operates.

10.5 RESPONSIBILITIES

MAPFRE Group’s Security, Crisis, and Resilience Committee is the body responsible for promoting and directing the development, implementation, evolution, and continuous improvement of Business Continuity Plans in the companies of the Group, as well as for deciding and coordinating the activities of implementation, maintenance, and improvement of the Business Continuity Management System. The above actions will enable protection and reduction of the probability of the occurrence and impact of disaster or catastrophe events, as well as preparation, response, and recovery from any disruptions that may occur, including those affecting the ICT environment.

Depending on the potential impact estimated by the Committee after evaluating the incident, it will decide whether or not to activate the Continuity Plans without delay and any other supplementary action plans it may determine, including crisis communication plans. All of this in order to provide a centralized, timely, and effective response to incidents and limit their possible adverse effects.

In addition, this Committee assumes the leadership and control of Crisis Management that involves multiple companies of the Group or, due to their nature, have a broader scope than what is outlined in the Business Continuity Plans of the different entities. That is, they have multi-entity repercussions, affect more than one

region, require extraordinary financial investments that exceed the scope of the entities/units, or have the potential to significantly impact the competitive position and/or reputation of the MAPFRE Group.

In addition, it will determine the moment when the crisis situation is considered resolved and normalcy is restored. This return to normalcy may take place progressively, depending on the impact and effectiveness of the measures adopted.

The Group Security, Crisis, and Resilience Committee will also be responsible for ensuring compliance, dissemination, and periodic review of this Policy.

Furthermore, the Board of Directors of MAPFRE S.A. will be responsible for approving, supervising, and periodically reviewing the application of this policy.

The remaining roles and responsibilities associated with Business Continuity management are formulated with the necessary detail in the Crisis Management and Business Continuity Governance Framework of MAPFRE.

10.6 UPDATE

This Business Continuity Policy will be reviewed annually, taking into account the results of any tests carried out, recommendations arising from audit controls, or reviews that may occur by supervisory bodies.