odontoprev	**Business Continuity Management Policy**	**Issue Date** 05/30/2023
Prepared by: Business Continuity Coordinator	**Approved by:** Risk Management Committee (04 to 04/05/2023) Crisis Committee (04 to 04/06/2023) Board of Directos (05/30/2023)	**11th version**

The Odontoprev S.A. and its controlled companies ("Company") **Business Continuity Management Policy** ("Policy") sets out basic guidelines:

1. PURPOSE

To present the guidelines of the Company's Business Continuity Program ("BCP").

2. SCOPE

This instrument applies to the Company's officers and all collaborators, as of its publication on the Corporate Intranet and on the website.

3. BASIC DEFINITIONS

The **BCM** is a component of the Company's risk management, which aims to ensure that the Company is always prepared to respond to incidents that may affect the maintenance of its operations, especially the operations carried out by the vital departments:

Vital departments are those that, when stopping operations, even for a short period of time, will have a severe impact on the Company's business, with serious operating, financial and/or image losses.

The **BCM** is formed by a set of previously documented documents that aim to clearly and transparently order the actions to be taken by the actors described in chapter 4 of this Policy, to respond, recover, resume and restore vital departments to a predefined level of operation after an unexpected interruption.

Incident is any situation that may represent or lead to interruption of business, losses, emergencies or crises, occurring due to unforeseen or accidental circumstances.

The main documents that form the **BCM** are:

Internal Business Continuity Management Policy: Details the Company's **BCM**, including procedures, reports and documents that must be carried out and generated annually for the purposes of verifying compliance with this program.
Operational Contingency Procedures (OCPs): These are the operational procedures that must be adopted by the IEMT (Incident and Emergency Management Teams) of all departments of the Company.
Disaster Recovery Procedures (DRP): These are the procedures that the Information Technology department must adopt to preserve the telecommunications infrastructure and computer systems.

Emergency Response Procedures (ERP): Describes how the Building Administration and Human Resources departments must act to, in an emergency, preserve the physical integrity of officers, employees, service providers and visitors, in addition to keeping the Company's facilities functional.

Incident Response Plan (IRP): document that describes the procedures to be adopted for dealing with information security and data privacy incidents, in accordance with the applicable regulations and other

corporate policies related to the subject.

The OCPs, DRP, ERP and IRP detail the technical, technological and people resources that will be used to mitigate the materialization of incidents that affect the continuity of the business.

Guidelines to be followed:

- As soon as an employee witnesses or becomes aware of an incident, he must alert his manager. The manager shall take the necessary measures to resolve the incident. If necessary, the OCPs, DRP, ERP and/or IRP Coordinators must be contacted.
- It is the duty of the OCPs, DRP, ERP and IRP Coordinators to issue, whenever applicable, the incident alert.
- The Crisis Committee shall evaluate every incident alert and, if applicable, declare a crisis.
- In a crisis situation, only authorized personnel may maintain contact with the press, investors, customers, etc.
- During a crisis, exceptions to existing policies must be approved by at least two officers.
- At the end of a crisis, the effectiveness of the **BCM** must be analyzed and the lessons learned identified, as well as the quantification of the impacts suffered by the Company.
- The officers or employees responsible for vital departments are responsible for identifying suppliers and service providers critical to their business, ensuring that the respective contracts contain clauses that guarantee the continuity of the Company's business.
- The Company's officers must avoid traveling together by air and land (eg same aircraft or vehicle) on business trips or visits.

4. ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES

Crisis Committee: Formed by the Executive Directors, the Crisis Committee is responsible for managing any incident with a crisis declaration. The Crisis Committee is responsible for authorizing the issuance of the crisis declaration; define the crisis response strategy, including internal and external communications; evaluate emergency investment proposals; monitor combat actions; and declare the crisis over. The Crisis Committee may be assisted by operational committees.

Business Continuity Coordinator (BCN): Is responsible for receiving and recording incident alerts; ensure that the Crisis Committee has been activated to analyze the incident alerts issued; coordinate and/or validate annual NCP tests; coordinate the process of permanent updating of **BCM** documents; and make officers, employees and third parties aware of the matter.

OCPs, DRP, ERP and IRP coordinators: They are responsible for analyzing incidents and, depending on their

criticality, issuing incident alerts; activate and manage your OCPs, DRP, ERP and/or IRP; coordinate and supervise the activities of their IEMT and/or other employees in their areas during a contingency; for participating in or coordinating annual **BCM** testing; for participating and encouraging its employees to participate in the training offered by CCN; and for keeping your OCPs, DRP, ERP and/or IRP up to date and correct. Whenever necessary, operational committees will be able to support the Coordinators in the analysis of incidents.

Incident and Emergency Management Teams (IEMT): The IEMT are made up of pre-selected employees who must work on the front lines of dealing with incidents and declared crises.

5. FINAL CONSIDERATIONS

This Policy is the basis for all the documents that make up the **BCM**, which must be complied with by those responsible for managing the Company's business continuity.

Both this Policy and the other **BCM** documents use the Brazilian Standards ABNT NBR ISO 22301 (Business Continuity Management System – Requirements) and 22313 (Business Continuity Management System – Guidelines) as a reference.
All **BCM** documents must be reviewed periodically, given the need for technology and operational defense systems to combat risks that affect business continuity to remain effective.

----------***----------***----------