

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

INDEX

1. PURPOSE	2
2. SCOPE	2
3. BASIC DEFINITIONS	2
4. GUIDELINES, ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES	3
4.1 Guidelines	3
4.2 Organizational Structure and Responsibilities	3
5. GENERAL PROCEDURES.....	5
5.1 In case of an Incident	5
5.2 Incident Alert	6
5.3 Incident Rating and Categorization	7
5.4 Deploying the Crisis Committee	7
5.5 Crisis Declaration	8
5.6 Action in a Contingency Situation	8
5.7 Incident Follow-Up	9
5.8 Return to Normal Activities and Post-Crisis Report	9
6. SUPPLIERS AND SERVICE PROVIDERS	10
7. TRIPS OR VISITS	10
8. EXCEPTIONS TO THE POLICY IN CONTINGENCY SITUATIONS	10

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

1. PURPOSE

This policy sets out the Business Continuity Management Program (**BCM**) of Odontoprev S.A. and its controlled companies.

2. SCOPE

This instrument applies to Odontoprev S.A. and its controlled companies, as of its publication on the Corporate Intranet and on the website.

3. BASIC DEFINITIONS

Incident: Is an unplanned event, or chain of events, that causes or may cause damage (loss) or negative impacts on a company's activities, personnel, property and/or image. The incident is caused by a threat.

Threat: Is a physical, natural, human, or technological situation that may cause an incident to a company.

Company: means Odontoprev S.A., a publicly-traded company, based at Avenida Marcos Penteado de Ulhôa Rodrigues, 939, 14th Floor, suite 1401, Edifício Jatobá, Castelo Branco Office Park, in the city of Barueri/SP, enrolled in the CNPJ/MF under no. 58.119.199/0001-51, with its articles of incorporation filed with the São Paulo Board of Trade under NIRE 35.300.156.668, and its controlled companies.

Vital Departments: Are those departments whose downtime, if even for a short while, will have a serious impact on the Company's business, with serious operational, financial and/or image losses.

Essential Departments: A temporary stop to an essential department will not have a significant impact on the Company's business.

IEME: Stands for *Incident and Emergency Management Equipment*. The IEMEs are responsible for the operational incident response actions and their members are listed in the documents named *OCPs*, *DRP*, and *PRE*.

OCP: Are the *Operational Contingency Procedures*, a document that describes in detail the procedures to be adopted by the IEMEs from each vital and essential department. It is important to point that the OCPs describe how the IEMEs are to respond within the first 7 days of an incident. If the incident should last longer than the foregoing period, the Crisis Committee (see section 4.2 hereof) will decide on the next steps to be taken as of the 8th day of contingency.

DRP: Are *Disaster Recovery Procedures*, a document that describes in detail the procedures to be adopted by the Information Technology department to preserve the telecommunication and computer system infrastructures.

ERP: Are the *Emergency Response Procedures*, a document that describes in detail the procedures to be adopted by the departments of Building Management and Human Resources to, in an emergency, protect the physical integrity of management, collaborators, service providers and visitors, and also keep operative the Company's facilities.

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

4. GUIDELINES, ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES

4.1 Guidelines

The business continuity management is a component of the Company's risk management in place to ensure the maintenance of its operations, particularly the operations carried out by the vital departments.

This **BCM** has the following guidelines:

- Instruct management, collaborators, and service providers in the management of the vital operations if an incident is declared to be a crisis;
- Instruct management and collaborators of the essential department how to respond if their offices (main installation) become inoperative, on account of an incident.

4.2 Organizational Structure and Responsibilities

Executive Officers:

Are the **Crisis Committee** members.

Responsibilities: Primarily responsible for maintaining the operation of the vital departments and for the safety and physical integrity of all the people who work at or walk around the Company's facilities. Each executive officer has the duty to inform the **Crisis Committee** of each relevant incident, and also to act as described in the **Crisis Commit** topic below.

Managers:

Are the coordinators of the *IEMEs* from their departments.

Responsibilities: Responsible for identifying and treating the incidents, with the support of their teams of collaborators and service providers. In some situations, to treat an incident, the manager will need to request assistance from a supporting department (e.g.: Service Desk, Building Management, Human Resources, Legal, etc.) or call out the Fire Department, SAMU, Civil Defense, etc. However, if the incident is relevant, the manager must also deploy the **Crisis Committee**, by directly contacting its executive officer or the **Business Continuity Coordinator (BCC)**.

Notes:

- The managers must follow this policy and the **OCPs, DRP** and/or **ERP** to respond to any relevant incidents.
- The managers have to ensure that their collaborators and service providers are fully aware of the rules laid down in this policy and deeply know about their **OCPs, DRP** and/or **ERP**.
- The managers must take their doubts to the **BCC** or **Substitute BCC**.

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

Collaborators:

Are all the people who hold a permanent position at the Company, regardless of their type of employment.

Responsibilities: The collaborators' basic responsibility in the **BCM** is to, whenever they detect an incident, promptly report the fact to their manager, and also follow the instructions received from him/her, their executive officer, Human Resources, or the **Crisis Committee**. Furthermore, collaborators must know and understand beforehand the **OCPs, DRP** and/or **ERP** for their departments.

Crisis Committee:

Composed of the Executive Board, the **Crisis Committee** is in charge of managing crises (i.e.: when an incident becomes or may become serious), outlining the response strategy, including internal and external communication. Additionally, the Crisis Committee assesses, as applicable, the proposals for emergency investments to handle a crisis. The Crisis Committee is also in charge of declaring a crisis and declaring the end of a crisis.

Notes:

- The executive officers may call on collaborators and/or invite outside personnel (e.g.: consultant, public relations, etc) to compose the **Crisis Committee**.
- During a crisis, the executive officers may decide whether the Crisis Committee will play either a strategic or a strategic and operational role. If decided that their role will not be just strategic, the **Crisis Committee** has to call on the **Business Continuity Management Committee - BCMC** to play an operational role in the crisis.
- The **Crisis Committee** is totally free to change the **BCMC's** composition at any time.

Business Continuity Management Committee (BCMC):

Composed of a preselected group of managers and collaborators described in the charter of said body, the **BCMC** plays an operational role in the **BCM**, supporting the **Crisis Committee**, if the latter so desires.

The **BCMC** is responsible for making sure that the incident response actions, as defined or confirmed by the **Crisis Committee**, will be properly implemented.

Business Continuity Coordinator (BCC):

A manager mentioned in the **BCMC's** charter, the **BCC** is in charge of receiving, analyzing, and recording the **incident alerts**; in the relevant incidents, deploy the **Crisis Committee** and **BCMC**, if necessary; coordinate and validate the annual **BCM** tests, except **DRP**; supervise and validate the annual **DRP** tests; coordinate the permanent **BCM** updating process and instruct management and collaborators in the matter.

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

 odontoprev	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

ERP Coordinator:

In charge of deploying and managing the **ERP** in an **emergency**, in order to protect the physical integrity of management, collaborators, service providers and visitors, and also keep operative the Company's facilities and keep his/her **ERP** updated and correct. The **ERP Coordinator** is identified in the **PRE**.

Note:

The **ERP** also includes the Fire Brigades.

DRP Coordinator:

In charge of deploying and managing the **DRP** in incidents that involve the telecommunication and/or information technology assets, supporting both the vital and essential departments. The **DRP Coordinator** is also responsible for coordinating the annual **DRP** tests and taking the necessary actions to correct any flaws found in such tests, in addition to keeping his/her **DRP** updated and correct. The **DRP Coordinator** is identified in the **DRP**.

OCP Coordinator:

In charge of deploying and managing the **OCP** for his/her business or operational department; coordinating and supervising the activities of his/her **IEME** and/or of the other collaborators from his/her department; and of keeping his/her **OCP** updated and correct. The **OCP Coordinator** is identified in the **OCP** for his/her department.

IEMEs:

The *Incident and Emergency Management Teams* are described in the **OCPs** for the vital and essential departments, as well as in the **PRE** and **DRP**.

5. GENERAL PROCEDURES

5.1 In case of an Incident

As soon as a collaborator witnesses or learns about an incident, he/she must warn his/her manager. The **manager will assess the seriousness of the incident and, if necessary, take the following emergency measures, either alone or in conjunction:**

- 1) Solve the incident alone or with the assistance of his/her collaborators.
- 2) For incidents concerning telecommunications and/or information technology: the manager will reach the Service Desk or **DRP Coordinator**, requesting that the problem be solved and setting an estimated time for the solution.

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

- 3) For incidents concerning water, sewage or gas leak; failure in the electric power, water, gas supply; ect.: the manager will reach the department of Building Management.
- 4) Strike: the manager will contact the department of Human Resources.
- 5) For life-threatening incidents: the manager (or the collaborator who detected the incident) will immediately call out the Fire Department, Police and/or SAMU, and afterwards reach the **ERP Coordinator** or the **Fire Brigade**, in addition to his/her executive officer.
- 6) For relevant incidents (categories 1 and 2 of section 5.3 hereof): the manager will contact his/her executive officer to issue the incident alert (section 5.2 hereof) and deploy the **Crisis Committee**.
Note: If the manager has any doubts as to the relevance of the incidence, he/she should discuss the matter with his/her executive officer.
- 7) For **irrelevant** incidents (categories 3 of section 5.3 hereof): the manager will contact his/her executive officer to analyze whether an incident alert (section 5.2 hereof) should be issued.
Note: If the manager has any doubts as to the relevance of the incidence, he/she should discuss the matter with his/her executive officer.

Note:

If the incident causes the **unavailability of the property** where the department, unit or branch undertakes its daily activities, a **category 1 or 2** incident alert (depending on whether the department is vital or essential) must be issued and the **Crisis Committee** deployed.

5.2 Incident Alert

As soon as the emergency phase of the incident is over, the **manager** must **communicate** the fact to the **BCC** through an **incident alert**. The **Incident Alert** may be sent by e-mail, SMS, WhatsApp, telephone or in person, and must provide the following information:

What?	What incident "alert type" .
What Category?	See section 5.3 below.
Who?	Parties involved in the incident (collaborator, customer, ordinary visitor, etc).
When?	Day and time of incident
Where?	What is the affected department, unit or branch
How?	How the event took place - if possible.
Status?	Disrupted activities, media onsite, first aid, etc.

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

 odontoprev	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

5.3 Incident Rating and Categorization

The manager must rate the incident as follows:

Rating	Category	Description
Occurrence	3	Incident that poses a low risk to the operation, where the necessary human, financial and logistical resources already exist and can ensure the proper management of the incident. Furthermore, this incident does not threaten the Company's image or people's physical integrity. Note: Category 3 incidents are managed and solved by the very collaborators of the affected departments, just with the assistance of the traditional supporting departments (i.e.: Service Desk, Building Management, etc.). For this reasons, issuing an incident alert is not mandatory.
Incident	2	Incident that poses a medium or high risk to the operation, with the possible or probable need for extraordinary resources and/or (minor or major) delay in the delivery of the services on account of real or potential disruption to the operation. Additionally, the incident poses no risk to the Company's reputation and/or people's lives. The closing of the essential department offices must also be placed in this category. The BCC must be warned.
Crisis	1	Incident that poses a medium or high risk to the operation, with the possible or probable need for extraordinary resources and/or (minor or major) delay in the delivery of the services on account of real or potential disruption to the operation. Additionally, the incident poses imminent risk to the Company's reputation and/or people's lives. The closing of the vital department offices must also be placed in this category. The BCC must be alerted.

Notes:

- If the manager or executive officer so requires, the **BCC** can be involved to help them assess the criticality of the ongoing incident.
- The **Crisis Committee** must be **warned** of any **category 1 and 2** incidents. Ideally the warning should be given by the executive officer of the affected department, as soon as he receives the information from his manager (see section 5.1 above) and regards the incident as relevant.

5.4 Deploying the Crisis Committee

The **Crisis Committee** can be deployed by an executive officer, by the **BCC** (if the incident alert is received), by the **ERP Coordinator** (if aware of the incident) or by the **DRP Coordinator** (if aware of the incident), in addition to their substitutes, in many ways, including in person, by telephone, SMS, WhatsApp and/or e-mail.

	Business Continuity Management Policy		Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)		9th version

Notes:

- The **Crisis Committee** must be deployed for relevant incidents only, rated as categories 1 and 2 in the table of section 5.3 hereof.
- The effectiveness of the **BCM** is directly linked to the speed by which the response actions are defined and implemented. Thus, if necessary, both collaborators (if their managers are not available) and managers (if their executive officers are not available) can communicate relevant incidents to the **Crisis Committee**. To do so, they just need to get in direct contact with a member of the **Crisis Committee** or **BCC**.

5.5 Crisis Declaration

The crisis declaration is an administrative act that formalizes the decision by the **Crisis Committee** to rate an incident as relevant. With the crisis declaration:

- 1) The **Crisis Committee** will deploy the *Crisis Management Procedures (CMP)*, which includes communicating the incident to the Board of Directors;
- 2) The **Crisis Committee** will decide whether to call on the **BCMC** to manage the operational aspects of the incident response. At its discretion, the **Crisis Committee** can call on all the **BCMC** members or just some of its members. The **Crisis Committee** also can call on other collaborators or outside personnel to compose the **BCMC** or to compose the **Crisis Committee** itself;
- 3) If necessary, the **Crisis Committee** will appoint the **Spokesperson** and he or she will activate the **Crisis Management Communication Manual**;
- 4) If necessary, the **Crisis Committee** will decide whether internal communication is required. If so, **Human Resources** will activate the **Crisis Management Communication Manual**;
- 5) The **Crisis Committee** will define which **Crisis Management Center**, as defined beforehand in the document entitled *Crisis Management Center*, will be used and whether the use will be sporadic or full-time;
- 6) The **Crisis Committee** will authorize the deployment of the **OCPs, DRP** and/or **ERP**.

Note:

The managers and executive officers do not need to await the crisis declaration to start tackling the incidents that are affecting their departments, units, or branches.

5.6 Action in a Contingency Situation

Crisis Committee, BCMC and Spokesperson:

The **Crisis Committee**, in addition to the **BCMC** and **Spokesperson**, if those two are called on, must act according to the **PGC** and the **Crisis Management Communication Manual**.

	Business Continuity Management Policy		Issue date 11/28/2019
Prepared by: Business Continuity Coordinator		Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

Notes:

- The **Crisis Committee**, the **BCMC** and the **Spokesperson** will act at the **Crisis Management Center**.
- The **Crisis Committee** will keep the **Board of Directors** constantly informed of how the crisis is developing.
- Each incident is unique. Hence the **PGC** and the **Crisis Management Communication Manual** must be used as a frame of reference only, which may be modified or supplemented.
- For irrelevant incidents or relevant incidents not reported to the **Crisis Committee** or the **BCC**, the executive officer and manager of the affected department are the only ones responsible for ensuring the maintenance of that department, besides the physical integrity of all the people who work at or walk around the affected facilities.

IEMEs:

The **IEMEs** must act according to the procedures set out in their **OCPs**, **DRP** and/or **ERP**.

Notes:

- The **IEMEs** must know in detail, and also in advance, the **OCP**, **DRP** and **ERP**.
- Any questions about how to act in a contingency situation must be put to the immediate manager, executive officer in charge of the affected department, **BCC** or **Substitute BCC**.
- All collaborators must keep in their cellphone memory the mobile telephone numbers of their managers and colleagues. The executive officer and managers must record the number of their subordinates and colleagues.
- This **BCM** sets out response actions for the first 7 days of a contingency situation. If the incident should last longer than the estimated time, the **Crisis Committee** will seek new response actions. The guidelines on the new response actions will be given to the collaborators in time.
- Only the **Spokesperson**, as designated by the **Crisis Committee**, is allowed to provide information on the incident that is affecting the Company. Therefore, without prior permission from the **Spokesperson** or the **Crisis Committee** itself, managers and collaborators must **NOT** disclose any information on the incident to the press, investors, customers, accredited network, beneficiaries, etc.

5.7 Incident Follow-Up

The **Crisis Committee** will formally monitor the incidents with crisis declaration, with or without assistance from the **BCMC**. The incident follow-up will be documented by the **BCC**.

For irrelevant incidents or relevant incidents not reported to the **Crisis Committee** or the **BCC**, the executive officer and manager of the affected department are the only ones responsible for their follow-up.

5.8 Return to Normal Activities and Post-Crisis Report

As the incident response actions start producing the desired effect, the activities of the affected department, unit or branch will return to normality. When all the activities return to the normal standards, the **Crisis**

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.

	Business Continuity Management Policy	Issue date 11/28/2019
Prepared by: Business Continuity Coordinator	Approved by: Crisis Committee (07/01/2019) Board of Directors (11/27/2019)	9th version

Committee can **declare the end of the crisis** (e-mail issued by the chair of the **Crisis Committee**), promptly informing the **Board of Directors**.

For irrelevant incidents or relevant incidents not reported to the **Crisis Committee** or the **BCC**, the executive officer and manager of the affected department are the only ones responsible for ensuring that the operation has returned to its normal standards.

Once the **end of the crisis has been declared**, the **Crisis Committee**, with the participation of the **BCMC**, as applicable, will meet to analyze the effectiveness of the response actions taken; quantify the impacts caused by the incident; identify any lessons learnt and improve the **BCM**. The meeting will be led by the **BCC**, which will draw up the **Post-Crisis Report**, whose model is in the **PGC**.

Note:

The post-crisis meeting and the **Post-Crisis Report** will only be applicable to those **category 1 and 2** incidents and for which the **Crisis Committee** has requested the **BCC** to issue the crisis declaration.

6. SUPPLIERS AND SERVICE PROVIDERS

Whenever applicable, the contracts made with suppliers and service providers must contain clauses that secure the continuity of the Company's business.

The vital department managers are in charge of analyzing which suppliers and service providers are critical to securing the business continuity (information documented in the **OCPs** and **DRP** of the vital departments) and review the contracts made, making sure that the aforementioned mandatory clauses have been included in those documents.

7. TRIPS OR VISITS

Seeking the adequate and efficient maintenance of the Company's operations, its executive officers should travel by air or land together (e.g.: same airplane or vehicle) on trips or visits.

8. EXCEPTIONS TO THE POLICY IN CONTINGENCY SITUATIONS

The **Crisis Committee** acknowledges that in contingency situations, to enable the operation of the business or speed up its recovery / return to normality, incident response actions may be taken in breach of the guidelines and rules laid down in the Company's policies.

Thus the **Crisis Committee** undertakes to document and approve (by at least 2 executive officers) every exception to the policies in force. Once approved, the exception will be valid for that contingency situation and for that time of crisis only.

PUBLIC

The information provided in this document is the property of **OdontoPrev** and for internal use only.