



**Business Continuity Plan <<Template>>.**

<<Your Company Name>>

Empower humans. Enhance brands.

Table of contents

[Plan Overview 3](#_Toc15045792)

[Plan Overview 3](#_Toc15045793)

[Plan Management 4](#_Toc15045794)

[Ownership 4](#_Toc15045795)

[Naming Convention 4](#_Toc15045796)

[Storage 4](#_Toc15045797)

[Site Incident Management Team 5](#_Toc15045798)

[Overview 5](#_Toc15045799)

[SIM Team Details 5](#_Toc15045800)

[SIM Team Meeting Places 5](#_Toc15045801)

[Business Continuity Plan Standards 6](#_Toc15045802)

[Facilities Maintenance & Emergency Procedures 6](#_Toc15045803)

[Staff Emergency Communications Plan 6](#_Toc15045804)

[Customer Communications & Escalation Plans 6](#_Toc15045805)

[BCP Pre-planned responses & solutions 7](#_Toc15045806)

[Site IT Operational Documentation 7](#_Toc15045807)

[Incident Management Overview 8](#_Toc15045808)

[How Are Incidents Managed? 8](#_Toc15045809)

[Initial Incident Response Procedures 8](#_Toc15045810)

[Document Control Page 10](#_Toc15045811)

[Document Identification 10](#_Toc15045812)

[Referenced Documents 10](#_Toc15045813)

[History 10](#_Toc15045814)

Plan Overview

Plan Overview

This Business Continuity Plan (**BCP**) provides the framework, standard tools and supporting documentation required to address incidents that arise from the following common threats to your business.

* IT and/or voice services unavailable
* Building – unavailable e.g. fire, flood, etc.
* Workforce unavailable
* Interrupted power supply
* Terrorist bomb threat
* Local threats and risks <<Please remove any items not relevant to your site or add any other threats you have identified>>
  + Severe weather - typhoons, hurricanes, tornados, monsoon, winter storms, etc.
  + Earthquakes
  + Active shooters
  + Etc........

Plan Management

Ownership

* **<<JOB TITLE>> (Business Continuity Plan Owners)** are accountable for ensuring that the Standard Business Continuity Plan is managed in compliance to with any Global Business Continuity Management Policy and/or customer contractual requirements

<<SITE NAME>> Business Continuity Plan Owner is <<First Name Last Name>>

<<POSITION OR TITLE>>

<<EMAIL ADDRESS>>

* **Site Business Continuity Plan Custodian** is the person nominated by the <<BUSINESS CONTINUITY PLAN OWNER”S JOB TITLE>> to manage the deployment, maintenance and testing of the BCP to ensure your business and people are protected and that your contractual obligations are being met.

<<SITE NAME>> Business Continuity Plan Custodian is <<First Name Last Name>>

<<POSITION OR TITLE>>

<<EMAIL ADDRESS>>

Storage

This BCP and all supporting documentation should be stored in the <<FOLDER NAME>> folder on <<FILE LOCATION>> which can be accessed via the following link <<LINK TO FOLDER>>

Site Incident Management Team

Overview

The Site Incident Management Team (SIM Team) are the people responsible for managing incidents at the local level. Any member of the SIM Team can declare an incident and activate this plan.

All SIM Team members should have at least one alternate. All members should provide contact details that enable contact both inside and outside of normal office hours (home phone or personal mobile).

SIM Team roles are listed in the table below. This list is not definitive – If there are other associates who have key skills and experience that could help management of an incident then please add them to the Team e.g. communications specialists, Fire Marshalls, First Aid Coordinators, etc.

SIM Team Details

|  |  |  |  |
| --- | --- | --- | --- |
| **CMT Role** | | **Role Holder** | **Contact Details** |
| **Incident Manager** | Primary |  |  |
| First Alternate |  |  |
| Second Alternate |  |  |
| **Facilities Management** | Primary |  |  |
|  | Alternate |  |  |
| **Operations Management 1** | Primary |  |  |
|  | Alternate |  |  |
| **Operations Management 2** | Primary |  |  |
|  | Alternate |  |  |
| **Operations Management 3** | Primary |  |  |
|  | Alternate |  |  |
| **HR** | Primary |  |  |
|  | Alternate |  |  |
| **Work Force Management** | Primary |  |  |
|  | Alternate |  |  |
| **IT Support** | Primary |  |  |
| Alternate |  |  |

SIM Team Meeting Places

The team will meet at <<DESIGNATED CRISIS COMAND CENTER LOCATION NAME>>, known as the Crisis Command Center. The Crisis Command Center should have appropriate communications and restricted access to enable confidentiality regarding the incident.

You should identify at least one internal and one external Crisis Command Center:

* Internal– A location on the site to be used if incident does not require evacuation of the facility.
  + **Location**: <<Insert details of location>>
* External – A location outside of the site to be used if your access to the facility is denied.
  + Location: <<Insert details of location>>

Business Continuity Plan Standards

If your BCP uses referenced standards. All standards should be stored in the <<NAME OF FOLDER>> folder on <<LOCATION>> which can be accessed via the following link:

<<LINK TO FOLDER>>.

The standard components required are:

Facilities Maintenance & Emergency Procedures

Maintenance and emergency procedures are a critical tool for ensuring the safety and welfare of your staff and for protecting and ensuring the availability of critical assets located within the facility.

Ensuring the site is safe, secure and operating efficiently reduces the probability of incidents and equipment failures and the impact of any associated outages.

Details of the procedures can be found in the Facilities Emergency procedures document which is held in the <<FOLDER NAME>> folder which can be accessed at the following link:

<<LINK TO FOLDER>>

Staff Emergency Communications Plan

Staff are your most critical asset so being able to communicate with them during an incident is perhaps the most important part of your BCP. You can replace premises and technology but without the people who know how to operate the services you do not have a business.

As reports will constantly change it is not required to produce the staff contact details until an incident occurs, but you should ensure that staff maintain current details in any applications that will be used to generate the reports.

Customer Communications & Escalation Plans

The Customer Communications & Escalation Plans (CCEP’s) outlines:

* Communications procedures to be used for any BCP or security incident impacting the customer services. This should include:
  + Contact details
  + Means of reporting
  + Reporting schedule including required frequency of reporting & escalation trigger points
* Tactical response to address service outage. This should include
  + Contact procedures and escalation triggers for reporting customer service outages
  + Any agreed operational workarounds in the event of customer service outages

<<LINK TO SITE BCP SHAREPOINT FOLDER>>.

CCEP details should be verified as part of the Business Review process at least quarterly.

BCP Pre-planned Responses & Solutions

No two incidents will ever be exactly the same, but the actions that you take in response to a specific type of incident will typically be quite similar.

There are 3 principle threats:

* Loss of premises
* Loss of IT services
* Loss of workforce

Site IT Operational Documentation

BCP Custodians should work with IT resources to ensure they have access to current IT Operational Documentation detailing the key infrastructure. Documentation should be held in the <<FOLDER NAME>> folder which can be accessed at the following link:

<<LINK TO FOLDER>>

Incident Management Overview

How Are Incidents Managed?

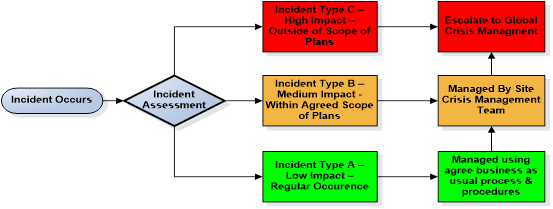
Site Incident and Global Crisis Management Teams (SIM Team & GCM Team) provide leadership in the event of a crisis or incident where a pre-defined level of impact has occurred or is expected.

These teams are individuals who have been selected to manage the incidents based on:

* A pre-identified group of skill sets;
* Their organizational knowledge; and
* Their decision making capability.

All team members should receive training in relation to their roles which includes incident management and the use of this plan to enable an effective and timely response.

An overview of the Crisis Management Process can be seen in the diagram below.



Most incidents will be managed by the SIM Team using this plan and the procedures listed below. However a small number of incidents may need to be escalated to the GCM Team (see Plan Overview at start of document for details of how to activate GCM Team).

Initial Incident Response Procedures

Initial priorities in response to a business continuity incident are as follows:

|  |  |
| --- | --- |
| **Priority** | **Issue** |
| **1.** | **People:** Staff *and visitor safety should always be the first priority.*  Aside from your duty of care to your people and guests, a real issue for continuity is the availability of skilled and trained staff to deliver your services.  Ensure that all staff and other third parties known to have been on the site are in a place of safety either on or off the site  Confirm that if evacuation was required that the procedure was correctly followed and that all persons were either accounted for or have been reported to the Emergency Services as missing. |

|  |  |
| --- | --- |
| **2.** | **Security of Assets:** *Ensure that information and other* ***i****mportant assets are secure*  If appropriate, confirm that secure areas are locked or are being monitored to ensure that assets are secured (data and physical assets).  In the event of evacuation confirm that entrance points are being observed and any unauthorized entry has been reported to the SIM Team to enable appropriate action. |
| **3.** | **Operations:** *Consideration of the operational interests of customers*  Confirm with operations leads that any client/stakeholder agreed plans/responses have been activated e.g. agreed prioritization of services, etc.  Determine the impact to Customer Services and draft an initial statement for each customer detailing:   * Service impact * Actions taken * Actions planned * Any items requiring client/stakeholder action or authorization of next actions |
| **4.** | **Communication:** *This is critical element of the response to a BCP incident.*  A poor communications strategy in the event of an incident can have a major impact on   * Associate welfare and support of the business * Relationships with customers * Your business’ reputation   Staff  Draft and issue an initial communication to staff to reassure them and to provide any initial instructions and guidance to ensure their safety and welfare.  Media & Other Third Parties  Emphasize to staff that they are not authorized to speak about the incident to any third party and to avoid being drawn into discussion with members of the press or broadcast media. Provide them with a suitable reference point for any such enquiries e.g. Crisis Leader or other SCMT member.  Customers  Follow the agreed procedures as documented in the in the Customer Communications & Escalation Plan (see Section 5 of this plan). |
| **4.** | **Incident stabilization:** *Ensure the incident is under control so you can plan for recovery.*  Initiate the appropriate planned responses referenced in the following section of this BCP assigning actions as appropriate and establishing the timeframes for required progress updates and internal and external communications. |

Document Control Page

Document Identification

|  |  |  |  |
| --- | --- | --- | --- |
| **Title** |  | | |
| Version: | 0.0 | Creation Date: | DD Month YYYY |

Referenced Documents

|  |  |
| --- | --- |
| **Number** | **Description** |
|  |  |
|  |  |
|  |  |

History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



Empower humans. Enhance brands.