# Business Continuity Plan Template

| **Version** | **Approved By** | **Revision Date** | **Description of Change** | **Author** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

## Purpose

The purpose of this Business Continuity Plan (BCP) is to outline the steps which enable <business name> to prevent, prepare, respond and recovery from disruptions or outages that would prevent the company from providing their services or business critical operations. The aim is to restore such services to maintain business functionality and productivity in the shortest time possible.

It also covers the response to disasters (natural or man-made) that would render the practice and resources found at <business address> unusable.

The owner of the Business Continuity Plan is <insert role/name> and this plan is to be stored at <location> and reviewed, tested and updated as required but annually as a minimum.

This plan assumes that you understand your business, its processes and its dependencies. It is a basic BCP and should be tailored to the complexity of your practice.

Before completing this BCP it is also recommended that you complete a Risk Assessment and a Business Impact Analysis of your business to identify gaps that need to be addressed in this BCP.

This BCP can refer to other documentation. For example, your Disaster Recovery Plan (if applicable), SLAs and contracts with Vendors, the Risk Assessment and Business Impact Assessment documents.

It is up to you to determine your appetite for how detailed you need your BCP to become.

The objectives of this document are to:

* Perform and document a Risk Assessment
* Define and Prioritise business critical functions and vital services
* Detail the business response to a critical incident
* Identify strategies to minimise impact and maintain business continuity on critical incidents
* Regularly review, update and test the plan

# Procedure – The Business Continuity Plan

# Risk Assessment

Before you can plan how to keep your business continuously operating, you will need to understand what risks could prevent it. Understand the seriousness of the impact to your business and the likelihood of it occurring, whilst also understanding if the risk can be removed, minimised or mitigated. There are several templates you can use to manage your risks but we have included a table below to get you started. We also recommend using the standard risk matrix as per the image below.



Date last reviewed:

Person Responsible:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | Impact | Likelihood | Consequence | Priority | Preventative/Mitigation Actions |
|  |  |  |  |  |  |

# Business Impact Analysis

Once you have completed or reviewed your Risk Assessment, the next step is to review those risks that are critical to the operation of your business (i.e. if they ceased to operate, the impact to the business would be significant). These risks should have a Recovery Time Objective, that is, the time from initial incident to the time the critical function must be fully operational in order to avoid serious consequences like financial loss, reputational impact, legal implications and so on. This may or may not be a separate document. The table below is a basic BIA, however we encourage you to find a BIA that suits the needs and complexity of your business.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Critical Business Function | Description | Priority to the Business | Impact of Loss | RTO |
|  |  |  |  |  |

# Incident Response

Review & Rehearse

Review the Incident, the Response, the Recovery

Identify areas of potential weakness or opportunities for improvement

Implement changes

Regularly audit and test the plan

Regularly provide training

Recover

Monitor service delivery and business operations

Communicate Progress internally

Review Recovery Effort

Communicate Externally\*

Disaster/Significant Event Closure

Respond

Declare Disaster/Significant Event

Kick-off recovery effort

Implement backup options

Communicate Plan internally

Communicate Externally\*

Relocate\*

Triage

Initiate IRT

Assess Impact

Review Actions

Review Roles & Responsibilities

Initial Comms

Incident

## Triage

When an event occurs, the role of the BCP Team is to determine whether or not the incident has interrupted business continuity through an initial assessment and triage. If the disruption is significant (for example, no water for more than 4 hours or ransomware activated on the network), then the Business Continuity Plan shall be followed, and the Incident Response Team will be required to meet to determine the next steps. If the disruption is not classified as significant, then it will follow the regular incident management process (for example, logging a helpdesk ticket).

## Respond

### Declaring a ‘Disaster’ or significant event

This plan becomes effective when there is a significant disruption to business continuity.

Significant disruption means that one or more vital services are currently unavailable without a resolution time or a resolution time greater than 4 hours (Vital Services are listed in the appendix). The Incident Response Team must meet to determine the next steps and which roles to bring into the recovery effort.

A Disaster means that there needs to be an effort to recover vital technology, infrastructure and systems due to the primary site no longer being fit for purpose due to natural or human-made event. This might be a natural disaster, a fire, an epidemic, or ransomware. The BCP does not cater for disasters like nuclear war or terrorism.

During this time, the Incident Response Team will also be responsible for communicating the assessment, the plan and progress of the incident. The IRT will also be responsible for developing a Restoration Priority List, which will identify facilities, vital records and equipment needed for resumption activities that could be operationally restored and retrieved quickly. If there are sites and/or records that have been damaged in the event, they will also develop a Salvage Priority List identifying sites and records which could eventually be salvaged.

### Communication

Throughout the process, there must be a strong communication plan to ensure people are aware of the progress, the plan and the resolution to prevent rumour and chaos.

### Internal Communication

The main form of communication for updating staff would be email, telephone and secure messaging services where applicable. In the event that staff do not receive any updates, they should contact their line manager.

### External Communications

Where it is deemed necessary, external communication may be required as interested parties are affected by the incident. The IRT are designated as the contact with customers, couriers, the media, regulatory agencies, government agencies and other external stakeholders & organizations following a disaster declaration.

## Recover

Once (backup) services have been restored and verified as fully operational, the business will move into a recover or monitoring phase. If the services restored are backups, then the effort to restore the primary services will continue.

You should identify how long you will run on backup services before the backup becomes the primary service. After a period of monitoring the effectiveness and operationality of the business, there will need to be a point in time where the incident is formally closed and a review of the incident be conducted, to find areas for improvement. Monitoring should be of the services you have restored, your staff and the impact the incident has had on your external stakeholders.

## Review & Rehearse

In order to ensure your BCP is fit for purpose, it is always a good idea to have test runs, to be sure people know what to do in the event of a significant incident – think of it like a fire drill. It will also give you an opportunity to find any gaps or risks that weren’t previously visible and confirm the risks and business impact analysis you have already conducted, especially if new staff have come onboard. This can take the form of training and education of the BCP, or an actual run through of restoring backup data and testing communication methods and these should be recorded in tables like those below.

This plan is intended to represent the most up to date risks, business impacts and business continuity plans for <business name>. As such, it should be reviewed annually as a minimum (ideally quarterly) or when there has been a reasonable movement in staff onboarding, offboarding or role changes.

Training Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| Training Date | Type of Training | Attendees | Comments |
|  |  |  |  |

Rehearsal Schedule

|  |  |  |  |
| --- | --- | --- | --- |
| Rehearsal Date | Type of Rehearsal | Person Responsible | Comments/changes made |
|  |  |  |  |

# Appendices

## Incident Response Team

The table below describes the team that will be brought into an incident if it occurs. The roles and responsibilities will depend on the type of incident or outage.

|  |  |  |
| --- | --- | --- |
| **Role** | **Primary Contact**  | **Alternative Contact** |
| IRT Team Leader | NameContact Details | NameContact Details |
| IT & Infrastructure |  |  |
| Communications & PR |  |  |
|  |  |  |
|  |  |  |

## Key Contacts – Internal

The below table identifies the key contacts who should be alerted in the event of an incident, outage or disaster. This will be different for every business but there should be representation in management, IT and communications.

|  |  |  |
| --- | --- | --- |
| **Role** | **Primary Contact**  | **Alternative Contact** |
| Executive | NameContact Details | NameContact Details |
| IT and Infrastructure |  |  |
| Communications & PR |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Key Contacts – External

The below table identifies the external parties which may or may not need to be notified in the event of an incident, outage or disaster. These are emergency services (police, ambulance, fire), utility companies (i.e water and sewerage, gas, electricity, phone and internet), your suppliers (medical supplies, deliveries) and your interested parties (media, insurance, medical providers, interest groups). You may not have all of the above, every business is different, but once you have reviewed your businesses risks and impacts, this table will be easier to fill out.

|  |  |  |
| --- | --- | --- |
| **Role** | **Primary Contact**  | **Alternative Contact** |
| Police, Ambulance, Fire | 000 |  |
| Water & Sewerage |  |  |
| Gas & Electricity |  |  |
| Australia Post |  |  |
| Insurance |  |  |
|  |  |  |
|  |  |  |

## Business Critical/Vital Services Functions

The table below describes the business critical or vital services that the business needs to have operational to continue to provide their services. If you have life saving or life monitoring equipment, these should be placed on the Each of these items should have a document outlining the following:

* Name and Description of the service
* Ownership with primary and secondary contacts
* Support and service contacts and contracts (if applicable)
* A summary of the business continuity controls
* Monitoring method for normal operations
* Incident response plan or alternate service plan
* The recovery process
* The test schedule
* Associated Risks on your risk register

Critical services can be Water or Electricity, IT systems, Phone and Internet, Building integrity.

## Alternate Site

Some business continuity plans outline an alternate site if their site is no longer usable (for example, due to a flood or fire, or a cyber incident that has compromised the network). Here is where you would outline the plans for using the alternate site, and who is able to work from the alternate site and who can work from home/out of office.

|  |  |
| --- | --- |
| **Alternate Site**  | **Primary Contact**  |
| Address |  |
| Utilities |  |

## Event Log

When an incident occurs that require the Incident Response Team to be called into action, it’s best to keep an Event Log to track the activities that occur post incident.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date**  | **Time** | **Action** | **Person Responsible** |
|  |  |  |  |