Business Continuity Plan: [add date]

The purpose of a Business Continuity Plan (BCP) is to ensure the continuation of [Service Name] business during and following any critical incident that results in disruption to normal business activity.

[Service Name] recognises that risk has dimensions that include governance, strategic, legal, operational, property, financial and physical. Good management requires coordinating activities to avoid, reduce and / or manage risks to ensure continuous, safe, responsive and efficient services to our community.

To support a prompt response and recovery following unforeseen events, [Service Name] has conducted a Business Impact Analysis and developed a Business Continuity Plan to minimise the impact of such events on our objectives.

# Objectives

The objectives of the BCP process are to provide a cost-effective means of:

* Preventing or minimising the impact of events capable of disrupting business operations
* Ensuring that business units can respond to unavoidable disruptions
* Ensuring a smooth and rapid restoration of normal business operations after a disaster.

# Developing a Business Continuity Plan

The Prevention, Preparedness, Response and Recovery (PPRR) framework provides the approach to support effective business continuity planning.



* Prevention – Risk management planning
	+ Incorporates the Prevention element that identifies and manages the likelihood and / or effects of risk associated with an incident
* Preparedness – Business Impact Analysis
	+ Incorporates the Preparedness element that identifies and prioritises the key activities of a business that may be adversely affected by any disruptions
* Response – Incident Response planning
	+ Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control and minimising impacts
* Recovery – Recovery planning
	+ Incorporates the Recovery element that outlines actions taken to recover from an incident in order to minimise disruption and recovery times

# The purpose of the [Service Name] Business Continuity Plan

* Identify what type of emergency or unforeseen event could occur
* Define and prioritise [Service Name] critical business functions and the systems that support them
* Detail [Service Name] immediate response to a critical incident
* Estimate down times and outline strategies and actions to be taken to ensure [Service Name] stays in business
* Detail processes for reviewing, rehearsing and monitoring the business continuity plan

# Business Impact Analysis and Continuity Plan– [add date]

**Critical Business Activity (CBA):** Daily business activities which are critical to the organisation’s services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event /Threat** | **Critical business systems affected** | **Existing Protection strategies****(What is in place to minimise risk? )** | **Business continuity plan****(What steps will you take if this occurs ?)** | **Business continuity strategies can be effective for;** |
| **Loss of income caused by:*** **Change of Government.**
* **Change of policy direction.**
* **Inability to meet funding requirement**
* **Reputation.**
 | * Financial management systems such as payroll, asset management.
* Staff
* Partners / suppliers
* Building
* Training
* Client service delivery
 |  |  |  |
| **No or low staff numbers caused by:*** **Pandemic.**
* **Strike.**
* **Local emergency.**
* **Recruitment challenges.**
 | * Staff / staff retention
* Building
* Service delivery
* Enterprise
* Client service delivery
 |   |  |  |
| **Lack of Governance caused by:****No quorum.****Illness.****Reputation.****Travel issues.****Conflict of interest.** | * Service delivery
* Reputation
* Partners and stakeholders
 |  |  |  |
| **Litigation caused by legislative non-compliance** | * Funds
* Partners/ relationships
* Reputation
* Staff
 |  |  |  |
| **Fire**  | * Building
* Staff
* IT systems
* Funds
* Financial management systems
* Vehicles
* Service delivery
* Enterprise
 |  |  |  |
| **Flood** | * Building
* Staff
* IT systems
* Funds
* Financial management systems
* Vehicles
* Client service delivery
* Enterprise
 |  |  |  |
| **Serious accident** | * Staff
* Client service delivery
* Buildings
* Vehicles
 |  |  |  |
| **Community violence** | * Staff
* Buildings
* Client service delivery
* Vehicles
 |  |  |  |
| **Theft** | * Financial
* Reputation (stakeholders and partners)
* IT equipment and passwords
* Vehicles
* Staff
* Service delivery
 |  |  |  |
| **Power outage** | Service deliveryStaffBuildingITPhones |   |  |  |
| **Extreme Heat** | StaffService delivery |  |  |  |
| **Grief / Loss** | * Staff
* Partners
* Service delivery – if resulting in closure of service
* Travel and transport
 |  |  |  |
| **Loss of insurance / increased premiums** | * Funds / costs
* IT
* Vehicles
* Staff
* Buildings
* Reputation
 |  |  |  |
| **Eviction / lease end** | * Funds / costs
* Financial management systems
* IT
* Buildings
* Staff
* Partners / relationships with key stakeholders
* Service delivery
 |  |  | XX |
| **IT system failure/ virus** | * IT
* Partners
* Staff
* Financial Management systems/ Payroll
 |  |  |  |

# Insurance

Insert - link to see Insurance Policy and Procedure, Policy number, contacts

# ‘Business as usual’ Planning

|  |  |  |  |
| --- | --- | --- | --- |
| Rank | Type | Address | Equipment available |
| 1 | Staff work from home to deliver services | Various – see staff contact list | IT, Phones ,office equipment  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

# Knowledge security and IT backup strategy

Insert - IT officer needs to develop an IT protection, business as usual and recovery plan

# Emergency Action Plan

## Emergency Contacts

|  |  |
| --- | --- |
| **Name** | **Phone Number** |
| Police |  |
| Fire |  |
| Ambulance |  |
| Rural Fire Service |  |
| Hospital |  |
| Insurance |  |
| Bank |  |
| IT support |  |
| Accounting System (Xero / MYOB etc) |  |
| Telephone/internet services provider |  |
| Accountant |  |
| Govt Contact |  |
| Tradies / suppliers – Electrical, plumbing |  |
| Staff support - EAP |  |

Insert - An up to date list of Staff and Board contact numbers will be maintained by [staff position].

## Evacuation drill schedule

Insert -

* How often is the evacuation drill held?
* Who is responsible?
* Link to emergency evacuation procedure and evacuation plan.

## Emergency team roles and responsibilities

Insert

* who are they, what is their role?

##

## Incident response Checklist [add date] \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A copy of the incident response checklist is kept near each telephone, in every vehicle and in the Go Pack

|  |  |  |
| --- | --- | --- |
| **Steps** | **√** | **Decision log** |
| **First response** |  | **Actions taken** | **Name of person leading the action.** |
| 1. **Ensure safety of those immediately affected**
 |  |  |  |
| 1. **Initiate evacuation procedure if applicable**
 |  |  |  |
| 1. **Ensure communication can be maintained**
 |  |  |  |
| 1. **Contact emergency services if required**
 |  |  |  |
| 1. **Identify further risk to person or property**
 |  |  |  |
| 1. **Identify critical business activities that have been disrupted?**
 |  |  |  |
| 1. **Report to line manager**
 |  |  |  |
| **Manager / Emergency management team** |
| 1. Start a log of actions taken
 |  |  |  |
| 1. Convene your emergency response team
 |  |  |  |
| 1. Inform staff and Directors
 |  |  |  |
| 1. Decide on course of action
 |  |  |  |
| 1. Communicate decisions to staff and Key stakeholders
 |  |  |  |
| 1. Provide public information to maintain reputation and business
 |  |  |  |
| 1. Arrange debriefing
 |  |  |  |
| 1. Review Business continuity plan
 |  |  |  |
| **Other** |  |  |  |

## Emergency Kit

An emergency kit or “Go Pack” is prepared for each site. It is kept next to the First aid kit. It is to be taken from the building as part of any evacuation or serious incident.

|  |  |
| --- | --- |
| GeneralContents of “Go Pack” | * Business continuity plan / incident response checklist
* List of employees with contact details
* List of Board members with contact details
* Details of IT provider
* Contact details for members
* Contact details for suppliers
* List of funding contracts held and contact details
* Contact details for Local council
* Contact details for landlord
* Contact details for insurer
* Building site plan
* IT back up – payroll and other essentials
* USB backup of passwords
* Stationery/message pads/textas/ pens and pencils
 |
| Emergency Supplies | * Spare keys
* Portable First Aid Kit
* Torch with spare batteries
* Emergency hats and vests for wardens
 |

#### Who is responsible for maintaining the kit?

Insert - How often will it be checked – by whom?

# Reviewing and monitoring the business continuity plan.

#### How often will the plan be reviewed?

1. Every 6 months aligned to review of the [Service Name] risk management plan.
2. Following an incident so that learning’s can be recorded and improvements made via the [Service Name] continuous improvement procedure.

#### How?

The Emergency management team and representatives from the WHS committee will review the Business continuity plan. It is then forward to the Managers meeting for input before changes are documented, approved by the [Service Manager] and communicated to all staff.