|  |  |
| --- | --- |
| Policy No: 1.17 | Policy Name: Business Continuity |

|  |  |
| --- | --- |
| Applies to: | Version: |
| Specific responsibility: | Date Approved: |
|  | Review Date: |

# Purpose

The purpose of this policy is to describe the systems and processes that will ensure that [Service Name] is well equipped to respond to numerous potential disruptions or breakdowns to key operational areas; this is so that [Service Name] can provide a safe environment for staff, clients and others, as well as support service and business continuity.

This policy applies to all [Service Name] staff, students, visitors, clients and Board members.

# Policy statement

In cases of major, unexpected disruptions to critical service or business processes, [Service Name] identifies the core functions and critical systems within its operations, determines acceptable estimated downtimes and establishes current continuity, contingency and recovery plans.

The business continuity plan is informed by [Service Name] Risk Management Policy and plan; it is also related to the Fire Safety, Incident Management, Critical Incidents, IT and Emergency Response Policies.

The [Board / Management Committee] approves the business continuity plan as part of a suite of risk management plans, including the risk management plan, emergency response procedures, fire drills and evacuation procedures.

# References

Work Health and Safety Act 2011

Workers Compensation Act 1987

Workplace Injury Management and Workers Compensation Act 1998

Workers Compensation Legislation Amendment Act 2012

Work Health and Safety Act 2011 (Cwlth)

Work Health and Safety Regulations 2017 (Cwlth)

# Definitions

**Critical incident** is a negative occurrence which may have the potential to disrupt regular business operations.

**Business continuity** is the ability of an organisation to maintain regular operations during and after an incident, emergency or disaster has occurred.

**Business Impact Analysis** is a process to determine and evaluate the potential effects on regular business operations if an incident, emergency or disaster were to occur.

# Procedure

**Identify critical activities/resources and undertake a business impact analysis**

* Identify your **critical business activities and resources**—these are the activities and resources without which your service could not continue.
* Undertake a **business impact analysis and estimated recovery time goal—**for each critical business activity and resource, assess the effects that not having that activity or resource would have on your organisation. Then, estimate how quickly your organisation would require that activity or resource back to ensure the continuity of services and organisational functioning.

An example of the first two steps of this process may appear as outlined in Table 1.

Table 1: Business Impact Analysis.

|  |  |  |
| --- | --- | --- |
| Critical activity/resource | Business impact analysis | Recovery time estimation |
| Community centre (CC) building.  Why is it critical?  All services are centre based and provided by the CC building.  All resources are located in the CC building, | In case of fire or another crisis resulting in the loss of a building,  no services could be provided;  there could be losses of property, IT, data and records. | **Immediate:** safe evacuation procedure.  **Interim:** One week to locate an interim service location and resume providing services to clients.  **Longer term:** A longer time frame to repair the CC building, depending on the extent and nature of the damage. |

**Apply the PPRR model and develop the business continuity plan**

Develop a plan for each of the critical activities you identified in this document and what your organisation can do to:

* **Prevent** the likelihood of the occurrence—this may not be possible with all risks (e.g., unexpected weather events), but it may be possible to prevent others, such as equipment failures through an effective Asset Management Policy.
* **Prepare** for the event, even if it is unlikely—for example, you can ensure that you have data backup systems to manage an IT failure, as well as adequate insurance against fire, flood and theft.
* Develop an **emergency response** **strategy** if the worst occurs—for example, in the event of a fire or flood that destroys the building, ensure that you have evacuation procedures and arrangements to use an alternative venue from which your service can operate, data backups for your policies, procedures and client files and other strategies. It is best to split the actions into an immediate response checklist (see Table A1) and then have an action plan for interim arrangements that can enable the service to operate even if at a reduced capacity, while the full recovery plan is being implemented.
* Implement **recovery planning**—for each critical activity, develop a detailed recovery plan that has documented roles, responsibilities and time frames (refer to your business impact analysis and recovery time objective to inform your recovery plan). Have a copy of the plan off the premises and ensure that it is regularly updated and that all staff have a copy. There are many elements of this plan that can and should be regularly rehearsed (e.g., the way that fire drills and evacuation procedures are regularly conducted).

To use the previous example of a disaster resulting in the loss of a building through fire, the beginning steps of developing a business continuity plan using the PPRR model may appear as in Table 2.

**Table 2: Business Continuity Plan.**

|  |  |  |  |
| --- | --- | --- | --- |
| Prevention | Preparedness | Emergency response plan | Plan recovery |
| * Building maintenance checks and audits building to ensure that it is safe and in good repair. * Smoke alarms and sprinklers are tested. | * Regular fire drills and evacuation procedures are held. * Adequate building and contents, as well as public liability, insurance is organised. * Data safety and cloud backup procedures are established. * Arrangements exist for using an alternative venue as a temporary service home in the event of a disaster. | * Evacuation procedure implemented. * Immediate response checklist implemented. * Insurance claims lodged. * Trauma counselling immediately offered to all staff and clients. | * Staff to move to an alternative premise as an interim measure with all functional computers in one week. * Additional laptops to be purchased for all staff who do not have a computer. * Assessment of damage is undertaken in one week. * Building repairs commence in accordance with the damages assessment report. |

This is a summary example to demonstrate a straightforward implementation of the PPRR model. However, the final version of the business continuity plan requires more details about the strategies, as well as time frames and the allocation of responsibilities against each item.

**Review and currency of the business continuity plan**

The [Board / Management Committee] and the [Service Manager] have a joint responsibility to ensure that:

* the business continuity plan is always current
* the preventative and preparedness measures are implemented and up to date
* all staff, volunteers and other persons whom the plan my affect are regularly briefed about the business continuity plan and that they have copies of all relevant documents.

# Related documents

Emergency Procedures Policy

# Review

|  |  |  |
| --- | --- | --- |
| **Reviewing and approving this policy** | | |
| Frequency | Person responsible | Approval |
| [How often will this policy be reviewed] | [Position of person responsible for reviewing policy] | [position of person/group who approves this policy] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy review and version tracking** | | | |
| Review | Date approved | Approved by | Next review date |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |