Business Continuity Plan – model template

# Introduction

The objectives of this Business Continuity Plan (BCP) are to:

* define and prioritise the critical business functions required in order to remain functioning post business interruption
* identify key actions and contacts for use in the immediate response to a business interruption
* outline strategies and actions to be taken preventatively, through the incident and in the recovery
* to deliver services
* highlight how review and update of this plan will be undertaken on a regular basis.

The scope of the BCP applies to, [e.g.] the whole organisation OR, xxx location/region.

Definitions:

* [if required}

# Potential threats and actions

The following proactive strategies have been identified and will be put into place to reduce the risk of crises occurring or to minimise the impact if there is a business interruption:

| **Item** | **Potential threat and impact on the business – description** | **Likelihood** | **Consequence** | **Risk level** | **Preventative action** | **Contingency plans** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | *e.g. fire or flood affects office location* | *low* | *high* | *high* | *Setup IT systems to enable staff in critical functions to work from any location**Insurance cover reviewed annually* | *Transfer critical functions to work from home or other office**Suspend non-critical functions**Insurance claim to cover losses* |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |

# Business continuity team

Members of the business continuity team are outlined below, including their broad areas of responsibility.

This is example content and individual organisations should review for their circumstances

| **Role** | **Alternate** | **Key responsibilities** |
| --- | --- | --- |
| Chief Executive Officer | Chief Financial Officer | * Activate the Business Continuity Plan
* Oversee incident response and recovery
* Communicate with key stakeholders as needed
* Provide important information for distribution to staff and public
* Keep Board and staff apprised of any changes to situation.
 |
| Chief Financial Officer | Chief Executive Officer | * Liaise with insurers
* Support CEO in immediate response
 |
| Operations Manager | Second in charge | * Review impacts to business and customers
* Report to and liaise with CEO on decisions required
* Develop and implement alternate resource plans
 |
| IT Manager | IT officer | * Review impacts to business if IT is affected
* Report to and liaise with CEO on decisions required
* Develop and implement alternate resource plans
 |
| HR Manager | HR officer | * Support other managers with alternate resource plans if required
* Oversee internal communications with staff
 |
|  |  |  |

# Emergency contact information

Contact list - internal

| **Person** | **Contact number/s** | **Email** | **Role** |
| --- | --- | --- | --- |
|  |  |  | Chief Executive Officer |
|  |  |  | Board Chair |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contact list – external

| **Key contacts** | **Organisation name and Contact person (if known)** | **Contact number/s** |
| --- | --- | --- |
| Emergency services (Police, Fire, Ambulance) |  |  |
| Security |  |  |
| Insurance |  |  |
| IT support |  |  |
| Phones/internet |  |  |
| Electricity |  |  |
| Gas |  |  |
| Bank/s |  |  |
| Regulators or funders |  |  |
| Lawyer |  |  |
| Public Relations firms |  |  |

# Incident response plan

This business continuity plan is activated by the CEO or Board Chair.

Emergency evacuation procedures should be posted in several different locations at each site.

This is example content and individual organisations should review for their circumstances

This example is intended to become an initial checklist for short term actions rather than the full plan for how to respond to the incident.

| **Item** | **Have you:** | **Done?** | **Comments** |
| --- | --- | --- | --- |
| 1 | Assessed the incident? |  |  |
| 2 | Evacuated if necessary? |  |  |
| 3 | Accounted for all staff, volunteers, customers, visitors? |  |  |
| 4 | Activated the business continuity plan? |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 5 | Identified and begun treating any injuries? |  |  |
| 6 | Contacted emergency services? |  |  |
| 7 | Communicated with parties as required:* internally (with staff)
* Board
* Customers
* other external parties
* media (if required)
 |  |  |
| 8 | Met with the incident leadership team? |  |  |
| 9 | Allocated specific roles and responsibilities? |  |  |
| 10 | Engaged outside providers as required, e.g.:* Security
* Insurance
* IT support
* Phones/internet
* Electricity
* Gas
* Bank/s
* Regulators or funders
* Lawyer
* Public Relations firms
 |  |  |
| 11 | Identified critical activities that have been disrupted? |  |  |
| 12 | Begun to implement contingency actions? |  |  |
| 13 | Complied with any regulatory/compliance requirements (e.g. data breach, notify funder)? |  |  |
| 14 |  |  |  |
| 15 |  |  |  |

# Recovery plan

This is example content and individual organisations should review for their circumstances

IT recovery checklist:

| **Item** | **Have you:** | **Done?** | **Comments** |
| --- | --- | --- | --- |
| 1 | Brought email systems back online and tested? |  |  |
| 2 | Brought server/s back online and tested? |  |  |
| 3 | Brought each database system and application back online and tested, e.g.:* Financial system
* CRM system
* HR system
* etc
 |  |  |

Incident recovery checklist:

| **Item** | **Have you:** | **Done?** | **Comments** |
| --- | --- | --- | --- |
| 1 | Contacted the insurer? |  |  |
| 2 | Brought IT and other systems back online? |  |  |
| 3 | Undertaken a lessons learned reflection on the incident and what you should update in this plan? |  |  |
| 4 | Kept staff informed? |  |  |
| 5 | Kept other stakeholder informed? |  |  |
| 6 | Reassessed your financial position after the incident? |  |  |
| 7 | Reassessed strategic and business priorities as appropriate? |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

# Review

At least once a year, management will review and test the BCP, such as through role play with relevant stakeholders of a risk event scenarios; and address any lessons learned through an update of the BCP.