Business Continuity

&

Recovery Plan

Template

This is an example plan. Please ensure you update this plan template so that it’s suitable for your organisation.

# Introduction

Physical locations, assets, data and staff are critical to the operation of an organisation and the service it provides to its service users. Therefore, there’s a need to be able to restore service operations, following a ‘disaster’, as soon as it’s possible.

The purpose of a plan is to maximise the ability of the organisation to recover from such a disaster, if one occurs. For this purpose, a disaster would be anything threatening the continuity of the organisation’s core business. This includes:

* a fire
* a bomb (terrorism)
* an explosion (gas)
* a pandemic
* severe weather conditions

In a disaster situation there’s an initial sense of shock, followed by a team spirit with everybody wishing to help. The team spirit will exist not only from the staff, but also from the general public.

This team spirit of co-operation will last for a few days, but a lack of interest will set in if people see that they’re not being given any direction or assistance. For example, the inability to carry out services (supervising users through group work, one to one support, payment of staff) will lead to stress and complaints.

Getting the ‘essentials’ back up and running speedily should be the priority.

Responsibility for this program has been given to <Organisation> management. Your co-operation with these efforts will help us to maintain a program that accomplishes its goals.

Thank you,

<Name>, <Position>.

<Signature>

## Responsibilities

It’s the responsibility of the <role>, to ensure that disaster recovery plans are in place and available for all sites. These plans are to be checked, distributed and tested on a regular basis, but at least annually.

Copies of this plan, and up to date site information sheets, are located <location>. ‘Controlled’ copies are reissued by:

* <role>
* <role>
* <role>
* all caseworkers
* <role>
* all administrators
* <role>

Depending on the site and nature of the disaster, various members of staff from different functions will form the 'Disaster Recovery Team’, who’ll each be assigned specific tasks.

In the event of a major terrorist activity, the whereabouts of staff potentially visiting or travelling through the affected area on business, should be reviewed.

## Initial safety actions for staff

1. Ensure that all staff and visitors have been evacuated from the building to a safe area.
2. Liaise with the emergency services (if in attendance).
3. Identify the number of potential casualties.
4. Ensure no staff or members of the general public enter any area classed as unsafe.

Contact with the following emergency services should be made.

1. <Role>, <Name> - <Contact Number>.
2. <Role>, <NAME> - <Contact Number>.

## Temporary Measures

### Alternative location principles or possibilities

If a particular building is not usable, alternative options should be reviewed. For example:

* another office – ensure it’s fit for purpose and carry out risk assessments as required for different offices/building
* working from home and provide remote services (may be limited)
* local court buildings
* other similar service provider accommodation (Social Services)
* local authorities, charity organisations
* portable buildings
* rent or lease of local office/shop units
* arranging transportation for service users to access our services an alternative office

## Business process principles

Team seniors should draw up a list of priorities for work with staff, assessing what can be achieved when and by who.

Following consultation with the <role> this should be communicated to:

* service users
* courts
* probation services
* partnership agencies

Where data information has been temporarily lost as a result of a disaster, encrypted backups held offsite should be used to restore information lost on the previous business day.

Where necessary, a contracted IT company should be able to assist with restoring data onto servers over time. Client information through online systems should be available.

In the event of complete internet failure, an additional wireless router with local area network (LAN) connectivity should be obtained and plugged into the main router for internet access.

A hard copy backup of contacts and client contacts should be kept and updated monthly by staff.

## Business Resumption

This details the process that determines when and how the organisation returns to ‘normal’ operation. This would change depending on the nature of the disaster, so it’s difficult to outline.

Generally, the management team will draw up a solution and develop an implementation plan. It’s important to stress that it may take considerable time to rebuild or relocate to a new building.

## IT Recovery

The responsibility of IT recovery lies solely with the IT Provider.

Major incidents are to be reported to them through the Office Manager. Telephony services will be the responsibility of the Office Manager.

## Contact with service users

Contact arrangements may need to be re-established and co-ordinated by the individual caseworkers for each project.

Signs or notices on disaster sites can direct users to a new location or give temporary contact details, identifying ‘business as usual’ details.

Use of announcements on social media and in the local press or on local radio stations may assist in increasing the awareness of temporary arrangements.

## Staff Counselling

Staff counselling may be needed and where this cannot be provided from within the organisation’s own staff, external help will be sought. Individual assistance will be co-ordinated by the CEO.

All staff directly involved will be contacted to understand if any assistance is required.

It should also be recognised that staff not directly involved in the incident may also need specific help.

## Communication

Incorrect statements may be made to the press and general public, and rumours may start. This will give the impression of a general state of disorganisation and will reflect badly on the service for years to come. Therefore, all communications, and delivery of such messages, will be the responsibility of the <role> or the <role>.

### Media Contact

This will be handled by the <role> or the <role>.

Staff, courts (Crown and Magistrates), probation services, service users and the public will need to know:

* what has happened
* what we’re doing about it
* what actions are being implemented to provide services to the public
* regular updates on the situation and how it may affect them

Contact with the following media services should be made.

1. BBC Radio: <Region> – <phone number>.
2. Local paper: <Name > – <phone number>.

## Testing and Exercises

We will conduct testing and exercises annually to evaluate the effectiveness of our preparedness program, make sure employees know what to do and find any missing parts.

There are many benefits to testing and exercises. These include to:

* train personnel – clarify roles and responsibilities
* reinforce knowledge of procedures, facilities, systems and equipment
* improve individual performance – as well as organizational co-ordination and communications
* evaluate policies, plans, procedures and the knowledge and skills of team members
* reveal weaknesses and resource gaps
* comply with local laws, codes and regulations
* gain recognition for the emergency management and business continuity program

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and the <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this policy: annually by the <role>.

Next review date: <date month year>.