<Organisation Name>

Business Continuity Plan [Template]

(Major Cyber Security Incident)

<Document Version & Date>



Copyright © 2021 <Organisation Name>

This document is based on a template document provided by Real World Technology Solutions.

Real World Technology Solutions grants permission for the template document to be modified in any manner <Organisation Name> wishes, provided this acknowledgement remains in place.

Document Owner: <Person’s Name>

Contact: <Person’s email and/or mobile telephone>

**How to use this template document**

This is a template document. It contains suggested or recommended content.

It is content that can be freely added to, moved, modified, or deleted.

Do not feel obliged to use the content as is if it does not suit your organisation.

You should read and adopt, adapt or remove, as appropriate!

What to do:

1. This document uses generic text for certain items that need to be updated by the organisation. These template text items are formatted in red with angle brackets (e.g. <Organisation Name> representing the organisation’s name), and should be updated to replace the template text with appropriate text specific to the organisation.
2. Using global replace, change <Organisation Name> to the organisation’s name
3. On the front page and in the page headers, change the Document Title to remove
“ [Template]” from the title, if present
4. On the front page and in the page footers, update the <Document Version & Date> to a new version of this document after your editing, and as you edit it in the future; e.g. V1.5 2025-05-05
5. Edit the document header to include the organisation’s logo, or remove the <Organisation Logo> template text
6. Find any other template text items and update them with the appropriate text for the organisation
7. Sometimes <there will be additional usage guidance formatted in blue like this comment> – it provides guidance and a reminder that the content can be freely edited to make it appropriate for your organisation
8. Review all the content and change anything as required to meet the organisation’s requirements and circumstances – sections and text can be modified, moved, deleted or added
9. Update the Contents table after updates by clicking on “Contents” and “Update Table…”; you may occasionally be prompted and can “Update entire table”
10. When ready, delete these instructions on this page and update the Contents again
11. Save the updated document

Contents

[1 Introduction 5](#_Toc88123697)

[1.1 Scope 5](#_Toc88123698)

[1.2 Prerequisites and Associated Documents 5](#_Toc88123699)

[1.3 Printed! 5](#_Toc88123700)

[2 Executive Summary 6](#_Toc88123701)

[2.1 Purposeful 6](#_Toc88123702)

[2.2 Activation and Management Authority 6](#_Toc88123703)

[3 Business Activities Details 7](#_Toc88123704)

[3.1 Essential Functions, Services and Activities 7](#_Toc88123705)

[3.2 Non-Essential 7](#_Toc88123706)

[4 Execution 8](#_Toc88123707)

[4.1 Initiation 8](#_Toc88123708)

[4.2 Response 8](#_Toc88123709)

[4.3 Recovery 8](#_Toc88123710)

[4.4 Restoration 8](#_Toc88123711)

[4.5 Completion 8](#_Toc88123712)

[5 Alternates 9](#_Toc88123713)

[5.1 Physical Relocation 9](#_Toc88123714)

[5.2 Virtual Relocation 9](#_Toc88123715)

[5.2.1 Service Name 9](#_Toc88123716)

[5.2.2 Service Name 9](#_Toc88123717)

[5.2.3 Service Name 9](#_Toc88123718)

[6 Post-Incident 10](#_Toc88123719)

[7 Rehearsal, Review and Revision 11](#_Toc88123720)

# Introduction

This is the Business Continuity Plan for <Organisation Name>. It defines what must happen to maintain continuity of <Organisation Name>’s essential business activities during a major cyber security incident.

## Scope

This Plan is focussed on cyber security. Whilst there are many other events that can impact <Organisation Name>, including fire, flood, civil disturbance, etc, this Plan does not explicitly cover them. Nevertheless, the Plan does have aspects that are common to any event that can compromise the continuity of normal operations, and therefore can be helpful in a broader set of business continuity planning activities.

This Plan covers these operations of <Organisation Name> at these locations:

* <These activities> at <Location>
* <These activities> at <Location>
* <These activities> at <Location>

## Prerequisites and Associated Documents

This Plan has certain prerequisite preparations, including:

* Perform a Risk Assessment of the cyber security risks, threats and vulnerabilities in the organisation
* Perform a Business Impact Analysis (BIA) of the organisation’s activities to understand and prioritise the organisation’s functions, services and activities
* Create formal Plans as listed below

The outputs from these and other prerequisite activities are various associated documents. They are an essential part of the overall preparation for Business Continuity and other activities within <Organisation Name>. The documents include:

* <This is an example list of documents – add, delete, modify as needed>
* Business Continuity Policy
* Business Continuity Overview
* Business Continuity Planning Guide
* Business Continuity Requirements
* Cyber Security Incident Response Plan
* Cyber Security Incident Recovery Plan
* Cyber Security Incident Communications Plan
* IT Risks Register
* <Other relevant documents>

This Plan is executed in conjunction with related Plans as indicated throughout this document.

## Printed

This Plan and all associated Plans that are needed during a major cyber security incident **must be printed**, ensuring the **latest version** is always the one available in printed form. This is required because cyber security incidents commonly make access to electronic files problematic or impossible.

# Executive Summary

This Business Continuity Plan for <Organisation Name> defines what must happen to maintain continuity of <Organisation Name>’s essential business activities during a major cyber security incident, including managing the following types of incidents:

* Ransomware
* Distributed Denial of Service (DDoS)
* Trojan Horse
* Worm
* Various virus and malware infections
* Online intrusion
* Data breach
* External and internal unauthorised access

## Purposeful

Whilst anticipating various types of incidents and planning to manage them as effectively as possible, there can be no guarantee that essential functions will be available during a major incident.

The purpose of this Plan is to methodically work to provide continuity of essential functions, as much as possible, when a major cyber security incident occurs. Other relevant Plans and procedures will also be invoked to manage a major incident. The Plan has the following overall goals:

* Act as soon as a major cyber security incident is detected
* Protect essential functions, services and high-value data as much as possible and isolate them from further impact where possible
* Stop the incident from progressing and having increasing impact
* Communicate with stakeholders internally and externally
* Invoke alternate operations to provide essential functions and services where these have been reduced or stopped in their normal form of provision
* Identify the root cause of the incident and eliminate it or prevent it from having further effect
* Recover essential functions and services as normal operations
* Recover all remaining functions and services as normal operations

## Activation and Management Authority

This Plan will be activated under the authority of <Organisation Group or Person>.

The Plan is executed under the overall management and authority of <Organisation Cyber Security Manager>.

The Cyber Security Incident Communications Plan provides for the regular communication of information to <Organisation Group or Person>.

# Business Activities Details

Overall business priorities during the Response, Recovery and restoration of normal operations are:

* <Main Function>
* <Main Service>
* <Primary Activity>

These are mapped out in more detail below.

## Essential Functions, Services and Activities

This Business Continuity Plan covers the following essential business functions, services and activities:

<This table is a bare example of what might be useful – add, delete and modify sections as needed, and then add appropriate content>

|  |  |  |  |
| --- | --- | --- | --- |
| Priority | Function/Service/Activity | Resources | Owner |
| High |  | People, technology | Person |
| Medium |  |  |  |
| Low |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

The Owners of the various essential functions, services and activities are responsible for the execution of actions to respond, recover and restore these to normal operations. They act under the authority of the <Organisation Cyber Security Manager> and will keep the <Organisation Cyber Security Manager> informed as the incident progresses.

## Non-Essential

Functions, services and activities not listed above are considered non-essential and are recovered and restored after those classed as essential.

# Execution

This Plan will be invoked when a major cyber security incident is declared. This declaration is made by <Organisation Group or Person> on advice from <Organisation Cyber Security Manager>. Declaring that this Business Continuity Plan is invoked is based on the nature of the incident and its effects on the organisation.

Once a major cyber security incident has been declared and this Plan invoked, it is managed as detailed here.

## Initiation

The <Organisation Cyber Security Manager> will invoke the Cyber Security Incident Communications Plan and the Cyber Security Incident Response Plan. These Plans provide the detail of how to communicate and initially respond to and manage the incident.

The initial priorities embodied in these Plans are to:

* Make an initial assessment of the incident
* Engage and communicate internally with personnel required to manage the incident
* Determine the scope of effect of the incident
* Initiate scope containment and isolation activities
* Communicate with <Organisation Group or Person>

The <Organisation Cyber Security Manager> will direct the execution of the response and recovery activities starting from the invocation of this Business Continuity Plan until restoration of normal operations and completion of this Plan.

## Response

The Cyber Security Incident Response Plan will be initiated as soon as any cyber security incident is detected. This should happen regardless of whether this Business Continuity Plan is invoked or not. If this Business Continuity Plan is invoked, it provides the overall context for execution of all other Plans.

## Recovery

The Cyber Security Incident Recovery Plan will be invoked by the <Organisation Cyber Security Manager> when a cyber security incident is in progress and the state of response warrants recovery actions to begin. This should happen regardless of whether this Business Continuity Plan is invoked or not.

## Restoration

Once essential operations have been recovered, they will resume as normal operations. Other non-essential operations can then be recovered and restored.

## Completion

The execution of this Business Continuity Plan will conclude when <Organisation Group or Person> deems that its purpose has been fulfilled and essential operations, and any specific non-essential operations, are restored. After <Organisation Group or Person> declares the Plan has been executed to completion, the <Organisation Cyber Security Manager> will ensure all post-incident activities are performed.

# Alternates

This Plan provides for the relocation of essential functions, services and activities if these cannot be effectively performed in the usual place of business. These relocations may be physical or virtual.

<These sections may or may not be needed – add, modify and delete as appropriate>

## Physical Relocation

On the advice of the <Organisation Cyber Security Manager> and operational and business personnel, and on the final authority of <Organisation Group or Person>, business operations may be physically relocated. The alternate physical location during response and recovery is:

* <Name and Address of alternate location>
* <Contact Details>
* <Person or Role> will be the liaison with <Alternate Liaison Person>

Transportation arrangements for relocation will use:

* <Name and Address of Transportation Provider>
* <Contact Details>
* <Person or Role> will be the liaison with <Transportation Provider Person>

Liaising with <Organisation Cyber Security Manager>, <Person or Role> will provide overall coordination and management of relocation activities.

## Virtual Relocation

On the advice of the <Organisation Cyber Security Manager> and operational and business personnel, and on the final authority of <Organisation Group or Person>, various business functions and capabilities may be virtually relocated. The alternate virtual locations during response and recovery are:

### Service Name

* <Service Provider>
* <Contact Details>
* <Person or Role> will be the liaison with <Service Provider>
* <Service, function, activities to be migrated>

### Service Name

* <Service Provider>
* <Contact Details>
* <Person or Role> will be the liaison with <Service Provider>
* <Service, function, activities to be migrated>

### Service Name

* <Service Provider>
* <Contact Details>
* <Person or Role> will be the liaison with <Service Provider>
* <Service, function, activities to be migrated>

# Post-Incident

After this Plan has been executed and the major incident resolved with normal operations restored, these additional activities are required:

* <This list contains some <example activities>, as well as activities that should be included – add, delete and modify as needed>
* <Contact insurance re any insurance claims>
* <Compensate customers, clients and beneficiaries, if appropriate>
* <Contact creditors and debtors to discuss any relevant matters arising from the incident>
* <Apply for assistance from government or other relevant organisation, if appropriate>
* Determine consequential short-, medium- and long-term effects and any required actions
* Update this Plan and other related documents with lessons learned during the incident
* Provide a written report on the incident and execution of this Plan to <Organisation Group or Person> within seven days

# Rehearsal, Review and Revision

This Plan (and associated Plans) must be rehearsed and reviewed from time-to-time. The <Organisation Cyber Security Manager> will activate a rehearsal of the Plan <at least once annually>. This rehearsal will be made as realistic as possible without interrupting normal operations.

The <Organisation Cyber Security Manager> will appoint a person to act as the “monitor” of the rehearsal. That person will observe and record the activities and progress of the rehearsal, including feedback and comments from participants that can be used to improve this and related Plans. This person should not actively participate in the activities, if possible.

After each rehearsal, the performance of the Plan will be discussed and reviewed, and the Plan updated as needed.

Modifications to this Plan are approved by <Organisation Group or Person>.

As noted in Section 1.3 above (Printed!), **always print the latest copies of all relevant Plans**!