**DISASTER RECOVERY PLAN – TEMPLATE**

Note: Delete this page once you complete the template.

**Who should use this template?**

Any organisation who uses information technology systems and services that wants to have a plan in place to recover technology systems in the event of a disaster.

**How to use this template**

* Make a copy of the template and save it with reference to your organisation
* All sections for consideration are as follows:
  + Mandatory: this section is core to building a disaster recovery plan and captures important information that will assist your organisation’s recovery.
  + Elective: this section may/may not be applicable depending upon your organisation’s structure and setup.
* [Placeholders] have been left within the document to indication editable sections
* <<insert content>> placeholders require information specific to your organisation
* Appendix references:
  + Appendix A contains a useful checklist that can be referenced during the development and maintenance of the Disaster Recovery Plan.
  + Appendix B contains examples of IT systems/services and potential disaster scenarios with links to IT systems/services.

**Disclaimer**

The information in this template is for general guidance only. The Digital Transformation Hub does not make any representations or warranties (expressed or implied) as to the accuracy, currency or authenticity of the information. The Digital Transformation Hub, its end users and agents do not accept any liability to any person for the information or advice given in this document.

[Insert Company Logo Here]

Disaster Recovery Plan

Version - 0.1

Effective Date: **<< Date Month Year>>**

Table of Contents

[1 Introduction 1](#_Toc97650767)

[2 Key information services and IT systems 1](#_Toc97650768)

[3 Risk Assessment 3](#_Toc97650769)

[4 Disaster Recovery Roles & Responsibilities 4](#_Toc97650770)

[5 Disaster Recovery Call Tree 5](#_Toc97650771)

[6 Communicating During a Disaster 5](#_Toc97650772)

[7 Dealing with a Disaster 6](#_Toc97650773)

[7.1 Disaster Identification and Declaration 6](#_Toc97650774)

[7.2 Disaster Recovery Plan activation and communication 7](#_Toc97650775)

[7.3 Restoring IT system functionality 7](#_Toc97650776)

[Current System Architecture 7](#_Toc97650777)

[Physical Recovery Facilities 7](#_Toc97650778)

[IT Systems 8](#_Toc97650779)

[8 Plan Testing & Maintenance 8](#_Toc97650780)

[8.1 Maintenance 8](#_Toc97650781)

[8.2 Testing 9](#_Toc97650782)

[9 Version Information and Changes 10](#_Toc97650783)

[Appendix A: Disaster Preparedness checklist 11](#_Toc97650784)

[Appendix B: Examples 12](#_Toc97650785)

# Introduction

Mandatory

This Disaster Recovery Plan (DRP) documents all of the information that describes <<Organisation’s Name>>’s ability to manage a disaster as well as the processes that must be followed to achieve disaster recovery.

**Definition of a Disaster**

A disaster can be caused by man or nature and results in <<Organisation Name>>’s IT infrastructure and systems not being able to perform as expected for a period of time. <<Organisation Name>> defines disasters as the following:

[Edit this list to reflect your Organisation]

* One or more vital IT systems are non-functional
* The office building is not available for an extended period of time however all IT systems/services are functional within it
* The building is available, but all systems are non-functional
* The building and all systems are non-functional.

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

[Edit this list to reflect your Organisation]

* Fire
* Flash flood
* Earthquake
* Cyber security incident
* Pandemic
* Power outage
* Theft
* Terrorist attack.

# Key information services and IT systems

Mandatory

This section explains the organisation’s critical data and customer-facing services. This data is referenced by the key information services in use at the organisation. Use this information to locate and restore data in the event of a disaster.

In this section it is important to explain where the Organisation’s data resides.

[List all of the key information services in your organisation in order of their criticality. Add or delete rows as needed to the table below.]

Considerations required to provide details for ***Table 1 Key information Services and IT Systems***:

* What are the key IT systems and telecommunications infrastructure your organisation depends upon to deliver its products and services?
* Outline the availability requirements based on the importance of each key IT system to the organisation. e.g. High, Medium, Low. Consider the impact to the organisation of the IT system not being available using parameters such as financial implications, compliance obligations and reputation.
* Outline Recovery Time Objective (RTO): In what amount of time would you expect this system to be restored and functioning? (**Note**: RTO refers to the maximum time taken to recover from a disaster e.g. an RTO of 8 hours means that an IT system will be back online in 8 hours).
* Outline Recovery Point Objective (RPO): The maximum amount of data you can afford to lose, stated in units of time. (**Note**: RPO refers to the maximum length of time that data can be restored from e.g. an RPO of 24 hours means that the maximum data loss in the event of a disaster will be 24 hours)

| **# \*** | **Key information service/ IT systems** | **Availability requirements** | | | **Data backups** | | **SLA provided by supplier e.g. 95% uptime** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Availability  (H, M, L) | Recovery Time Objective  (hours) | Recovery Point Objective  (hours) | Frequency  (hours) | Backup location |  |
| 1 | E.g. Email and collaboration systems |  |  |  |  |  |  |
| 2 | e.g. SharePoint |  |  |  |  |  |  |
| 3 | e.g. CRM |  |  |  |  |  |  |
| 4 | e.g. Website |  |  |  |  |  |  |
| 5 | e.g. File servers |  |  |  |  |  |  |
| 6 | e.g. VoIP or phone services |  |  |  |  |  |  |
| … | … | … | … | … | … | … | … |
| … | … | … | … | … | … | … | … |

Table 1: Key Information Services and IT Systems

\* This number is to be referenced in ***Table 2 Disaster Recovery Scenarios.***

# Risk Assessment

Mandatory

There are a number of potential disruptive threats which can occur at any time and affect normal organisational operations. A wide range of potential threats which could impact on <<Organisation Name>>’s IT systems and services are included in this section.

The focus here is on the level of disruption to operations which could arise from each type of disaster from a risk assessment perspective. Potential disasters have been assessed as follows:

Probability: 1=Very Low, 5=Very High.

Impact: 1= Minor inconvenience, 5= Critical impact.

| **Potential Disaster scenario** | **IT systems impacted \*** | **Probability Rating** | **Impact Rating** | **Description of potential consequences and remedial actions** |
| --- | --- | --- | --- | --- |
| Flood / Fire /Loss of building access |  |  |  |  |
| Electrical power failure |  |  |  | e.g. Redundant UPS array with standby generator tested weekly and remotely monitored. |
| Cyber security incident |  |  |  |  |
| Loss of communications network services |  |  |  |  |
| Loss of Internet connectivity at primary site |  |  |  |  |
| Third party supplier impacted |  |  |  | e.g. Contingency plans identified and documented in <<xxx>> location |
| … |  |  |  |  |
| … |  |  |  |  |

Table 2: Disaster Recovery Scenarios

\* **Note**: Column ‘IT systems impacted’ to be populated with the relevant numbering of information services affected from ***Table 1 Key Information Services and IT Systems***.

# Disaster Recovery Roles & Responsibilities

Mandatory

In the event of a disaster, different groups will be required to assist <<Organisation Name>> to restore normal functionality to the operations of the organisation. The different groups and their responsibilities are as follows.

The lists of roles and responsibilities in this section reflect the likely tasks that employees will have to perform.

[Please note that the following teams will vary depending on the size of your organisation. Some teams/roles may be combined or may be split into more than one team.]

[Edit this list to reflect your organisation]

| **Role** | **Responsibility** |
| --- | --- |
| Disaster Recovery Lead(s) | * Make decisions related to the Disaster Recovery efforts * Work with the technical representative to determine IT systems/processes affected by the disaster * Initiate the DR call tree * Communicate the disaster to affected stakeholders (e.g. employees, authorities, partners, customers, vendors, media) * If applicable, get the secondary site ready to restore operations and ensure that the secondary site is fully functional and secure * Guide the Disaster Recovery process * Following recovery, provide a summary of the activities undertaken during the disaster. |
| Senior Leadership Team | * Make decisions that will impact the organisation. This can include decisions concerning:   + Rebuilding of the primary IT facilities (where applicable)   + Significant hardware and software investments and upgrades   + Other financial and operating decisions. * Depending upon the IT systems impacted:   + Ensure that payroll occurs and that employees are paid as normal where possible   + Communicate with banking partners as required in regards to finance matters that may be impacted. |
| Technical Representative  (This representative may be an individual internal/external to the organisation) | * Work with the Disaster Recovery Lead to coordinate the aspects of technology that have been impacted. This may include:   + Network infrastructure for data and voice internal/external to the organisation   + Physical server infrastructure   + IT systems and applications   + Other technical operational requirements. |

Table 3: Disaster Recovery Roles and Responsibilities

# Disaster Recovery Call Tree

Mandatory

In a disaster recovery or business continuity emergency, time is critical so <<Organisation Name>> will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

The Disaster Recovery Team Lead calls all the other stakeholders.

**Note**: It is important that these contact details are kept updated. Also ensure you store these phone numbers in your phone contact list.

| **Contact** | **Work** | **Mobile** | **Home** |
| --- | --- | --- | --- |
| Disaster Recovery Lead(s) |  |  |  |
| Technical Representative |  |  |  |
| Senior Leadership Team Representative |  |  |  |

Table 4: Disaster recovery call tree

# Communicating During a Disaster

Mandatory

In the event of a disaster <<Organisation Name>> will need to communicate with various stakeholders to inform them of the effects on the organisation’s operations and timelines. The <<insert name>> Team will be responsible for contacting all of <<Organisation Name>>‘s stakeholders.

Use the table below to identity the communication requirements and contacts of relevant stakeholders.

| **Stakeholders**  **[Edit this section to reflect your Organisation]** | **Communication content (examples only)**  **[Edit this section to reflect your Organisation]** | **Contact details** |
| --- | --- | --- |
| Internal Stakeholders (e.g. staff, board members, etc) | e.g. Implications of the disaster and impacts on IT systems and applications i.e. what services have been impacted | <<insert process to be used to communicate with stakeholders>> |
| External stakeholders (e.g. authorities, clients, supporters, etc) | e.g. Anticipated impact on services, security of client information, actions being taken and anticipated timelines | <<insert process to be used to communicate with stakeholders>> |

**Table 5: Stakeholder Communications**

# Dealing with a Disaster

Mandatory

If a disaster occurs at <<Organisation Name>>, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organisation.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

[Edit this list to reflect your Organisation]

1. Disaster identification and declaration
2. Disaster Recovery Plan activation and communication
3. Restore IT operations.

## Disaster Identification and Declaration

Mandatory

Since it is almost impossible to predict when and how a disaster might occur, <<Organisation Name>> must be prepared to find out about disasters from a variety of possible avenues that would provide information that an incident has occurred. These can include:

[Edit this list to reflect your Organisation]

* Firsthand observation
* System alarms and network monitors
* Environmental and security alarms
* Security incident notification
* End users
* 3rd Party vendors
* Media reports.

Once the Disaster Recovery Lead has determined that a disaster had occurred, they must officially declare that the organisation is in an official state of disaster.

## Disaster Recovery Plan activation and communication

Mandatory

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the Disaster Recovery Plan by triggering the Disaster Recovery Call Tree. The nature and impact of the disaster should be communicated, expected duration of the disaster and actions taken currently.

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to a representative of the Senior Leadership Team.

The organisation’s senior leadership must be notified first, once it is established that a disaster has occurred. For other communications required, refer to **Section 6 Communicating During a Disaster.**

## Restoring IT system functionality

Mandatory

Should a disaster actually occur and <<Organisation Name>> need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which <<Organisation Names>>’s information services and IT systems will be recovered.

This section will contain all of the information needed for the organisation to get back to its regular functionality after a disaster has occurred. It is important to include all Standard Operating Procedures documents, run-books, network diagrams, software format information etc. in this section.

### Current System Architecture

Elective

In this section, include a detailed system architecture diagram. Ensure that all of the Organisation’s IT systems and their locations are clearly indicated.

<<System Architecture Diagram>>

### Physical Recovery Facilities

Elective

Consider where alternative physical premises may be required to house IT systems and service infrastructure in the event of a disaster. If this is a requirement, identify what these facilities are and how they will be used in a disaster recovery scenario.

### IT Systems

Mandatory

Please list all of the IT Systems in your organisation in order of their criticality. Next, list each system’s components that will need to be brought back online in the event of a disaster. Add or delete rows as needed to the table below.

Based on ***Table 1 Key Information Services and IT systems***, identify the restoration of IT systems and dependencies required.

|  |  |  |
| --- | --- | --- |
| Rank | IT system | System components (in order of importance) |
| 1 |  | …  …  … |
| 2 |  | …  …  … |
| 3 |  | … |
| 4 |  | … |
| 5 |  | … |
| 6 |  | … |

**Table 6: IT System Restoration.**

# Plan Testing & Maintenance

Mandatory

While every effort will be made to construct this Disaster Recovery Plan as complete and accurate as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the organisation will change. As a result of these two factors this plan will need to be tested periodically to discover errors and omissions and will need to be maintained to address them.

## Maintenance

Mandatory

The Disaster Recovery Plan will be updated <<indicate frequency>> or any time a major IT system/service update or upgrade is performed, whichever is more often. The <<identify responsible role>> will be responsible for updating the entire document, and so is permitted to request information and updates from other staff and departments within the organisation in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

[Edit this list to reflect your organisation]

1. Update the DR call tree

2. Update of the disaster recovery role and responsibility details

3. Review the plan to ensure that all instructions are still relevant to the organisation

4. Make any major changes and revisions in the plan to reflect organisational shifts, changes in the IT environment and goals

5. Ensure that the plan meets any requirements specified in new compliance obligations

6. Other organisational specific maintenance goals.

## Testing

Mandatory

<<Organisation Name>> is committed to ensuring that this Disaster Recovery Plan is functional. The Disaster Recovery Plan should be tested every <<indicate frequency>> in order to ensure that it is still effective.

Testing the plan will be carried out as follows:

[Edit this list to reflect your organisation and select which method(s) your organisation will employ to test the Disaster Recovery Plan]

1. **Walkthroughs:** Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses.

This test provides the opportunity to review a plan with a larger group of people, allowing the Disaster Recovery Lead to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

1. **Simulations:** A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation and other necessary utilities should be thoroughly tested in a simulation test.

Validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyse the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases are applied.

1. **Parallel Testing:** A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current date should agree with those reports produced at the alternate processing site.
2. **Full-Interruption Testing:** A full-interruption test activates the total Disaster Recovery Plan. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous Disaster Recovery Plan phases cannot be overstated.

Any gaps in the Disaster Recovery Plan that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

# Version Information and Changes

Mandatory

Any changes, edits and updates made to the Disaster Recovery Plan will be recorded in here.

It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the Disaster Recovery Plan are up to date. Whenever there is an update to the Disaster Recovery Plan, <<Organisation Name>> requires that the version number be updated to indicate this.

| **Version** | **Change Description** | **Reviewed By** | **Approved By** | **Date** |
| --- | --- | --- | --- | --- |
| 1.0 | … | … | … | … |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix A: Disaster Preparedness checklist

A reference checklist to be used during development and maintenance of the Disaster Recovery Plan:

* Does your organisation have all key organisational documents, contact information and records of technologies and facilities collected and saved both electronically and in hard copy?
* Does your organisation have a plan for how to communicate internally and externally during and after a disaster impacting IT systems/applications?
* Does your organisation have a plan for the continuity of primary operations after a disaster/emergency?
* Does your organisation have a plan for data backup and the backup of equipment and devices?
* Are the staff members and key volunteers in your organisation aware of all the disaster preparedness plans and trained accordingly?
* Does anyone in your organisation know the procedures to recover technologies after a disaster/emergency?

(Adapted from: Content from Tech Soup Disaster Preparedness courses).

# Appendix B: Examples

The following are example IT systems/technical infrastructure that may be impacted by a disaster. They are provided as examples of the key information services and IT systems to be captured as part of a Disaster Recovery Plan.

**Table 1. Key Information Services and IT Systems Examples.**

| **# \*** | **Key information service/ IT systems** | **Availability requirements** | | | | **Data backups** | | **SLA provided by supplier e.g. 95% uptime** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **Availability**  **(H, M, L)** | **Impact** | **Recovery Time Objective**  **(hours)** | **Recovery Point Objective**  **(hours)** | **Frequency**  **(hours)** | **Backup location** |  |
| 1 | Email system | H | Client communication affected | 2-4 | 4 | 4 | M365 cloud | 99.95% |
| 2 | Customer Relationship Management (CRM) system | H | Client data collection and client service provision affected | 2-4 | 4 | 4 | CRM system backups (cloud) | 95% |
| 3 | VoIP or phone services | H | External communication affected, primarily impacting clients | 4 | -- | -- |  | 99% |
| 4 | File servers | M | Internal documentation access impacted | 8 | 8 | 8 | Local backup server; offsite backup | -- |
| 5 | Finance system | M | Can resort to manual operations; may slow operations but not stop processes | 24-48 | 24 | 24 | Local backup server; offsite backup | -- |

Linked to the example information services and IT systems above, potential disaster scenario examples are outlined in the table below. These are linked to the IT systems that may be impacted with examples of consequences and remedial actions.

Note that the ratings for the disaster scenario parameters of probability and impact are stated below

Probability: 1=Very Low, 5=Very High

Impact: 1= Minor inconvenience, 5= Critical impact

**Table 2. Disaster Recovery Scenarios Examples.**

| **Potential Disaster scenario** | **IT systems impacted \*** | **Probability Rating** | **Impact Rating** | **Description of potential consequences and remedial actions** |
| --- | --- | --- | --- | --- |
| Flood / Fire /Loss of building access | 4. File servers  5. Finance system | 2 | 3 | e.g. Manual workarounds for finance processes, offsite data backups for file servers to be restored to procured cloud environment. |
| Electrical power failure | All systems | 1 | 4 | e.g. Loss of access to all IT systems on premise and cloud. Redundant UPS array with standby generator tested weekly and remotely monitored. Staff able to work remotely to access IT systems not on-premises. |
| Cyber security incident | 4. File servers  5. Finance system | 3 | 3 | e.g. resort to manual finance processes |
| Loss of communications via network services | VOIP or phone services |  |  | e.g. DNS, Azure Active Directory impacted, functionality on LAN affected. |
| Loss of Internet connectivity at primary site | Email system  CRM system |  |  | e.g. Secondary internet link established. |