Disaster Recovery Policy

Template

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

## Overview

Since disasters happen so rarely, management often ignore the disaster recovery planning process. It’s important to realise that having a contingency plan in the event of a disaster gives <Company Name> many advantages.

This policy requires management to financially support and attend to disaster contingency planning efforts. Disasters are not limited to destructive weather conditions. Any event that could likely cause an extended delay of service should be considered.

## Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Company Name>. The plan will describe the process to recover IT systems, applications and data from any type of disaster that causes a major outage.

## Scope

This policy is directed to those who are responsible for ensuring the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan. It does not provide requirement around what goes into the plan or sub-plans. These can only be developed from an in-depth look into the individual circumstances of the organisation.

## Policy

### Contingency Plans

The following contingency plans must be created:

1. Computer emergency response plan - who is to be contacted? When and how? What immediate actions must be taken in the event of certain incidents?
2. Succession plan - describe the flow of responsibility when normal staff are unavailable to perform their duties.
3. Data study - detail the data stored on the systems, its criticality and its confidentiality.
4. Criticality of service list - list all the services provided and their order of importance.
5. It also explains the order of recovery in both short-term and long-term timeframes.
6. Data backup and restoration plan - make reference to:
   * the data that’s backed-up
   * the media to which it’s saved
   * where that media is stored
   * how often the backup is done

It should also describe how that data could be recovered.

1. Equipment replacement plan - describe what equipment is required to begin to provide services. List the order that’s necessary, and note where to purchase the equipment.
2. Mass media management - who is in charge of giving information to the mass media? This includes the press, newspapers, radio and television.
3. Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it’s important to practice them to the fullest extent possible. Management should set aside time to test the implementation of the Disaster Recovery Plan. Table top exercises should be conducted at least annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

Review of this document: annually by <role>.

Next review date: <date month year>.