

IT Disaster Recovery Plan

In the event that a disaster destroys all or part of the organisation, the information presented in this plan, guides the organisation through the recovery of IT facilities, including data restores for user data, organisation shared data, MIS, financial, EPOS, entry and VLE systems.

All disaster recovery plans assume a certain amount of risk, the primary risk being human error of manually saving data to incorrect storage locations. Organisations must consider the compromises between the amount of time, effort, and money spent in the planning and preparation of a disaster and the amount of data loss you can sustain and remain operational following a disaster.

Contents:

- Overview
- Salvage Operations at Disaster Site
- Designate Recovery Site
- Purchase New Equipment
- Begin Reassembly at Recovery Site
- Restore File and Email Data from Backups
- Restore of MIS, Financial, Entry, EPOS, VLE Systems
- Move Back to Restored Permanent Facility
- Disaster, Risks and Prevention
- Exclusions
- Disaster Recovery Routines

Overview

Following the disaster, a planned sequence of events needs to begin, and IT personnel need to be notified to initiate the recovery process. The Organisation must take necessary measures to ensure that the IT personnel are provided with resources to meet their needs. This plan calls for the appointment of a person in the organisation, whose job will be to liaise with the IT personnel throughout the course of the recovery process.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. Any storage media/devices should be identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

At the same time, a survey of the disaster scene is done by the appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use a cold site; this is a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. The repairing or rebuilding of the primary site may take months, the details of which are beyond the scope of this document.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The Organisation will rely upon emergency procurement procedures.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore File Data from Backups

In the event of the organisation being full-cloud and providing users have been following correct procedures of cloud storage, data recovery of personal and shared data is not required. All data is stored in the cloud.

In the event of the organisation being on-prem and providing users have been following correct procedures of storing files in specific network locations, data recovery of personal and shared data can be undertaken by the IT Support Provider. Recovery of user data relies upon the use of backups stored in air-gapped locations away from the organisation. This may be in the form of encrypted storage drives or server to cloud backup. In this scenario, the IT Support Provider will work with the organisation, to restore data to a secure temporary location. Furthermore, following the reconstruction of the main site, the IT Support Provider will work with the organisation, to restore all data to the new site. See Move Back to Restored Permanent Facility section for more information.

Restore of MIS, Financial, Entry, EPOS, VLE Systems and data.

The organisation is to liaise with all third-party providers.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Cold Site, physical restoration of the server room (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Cold Site are to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the Cold Site.

Disaster, Risks and Prevention

The threat of fire in the organisation, especially in comms (servers, switch) rooms, is very real and poses the highest risk factor of all the causes of disaster mentioned here. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. Not to be forgotten are the hydrogen gas producing batteries in the Uninterruptible Power Supplies where a spark could ignite a fire and explosion.

The computers within the facility also pose a quick target for arson from anyone wishing to disrupt Organisation operations.

The Organisation is fitted with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building.

Hand-held fire extinguishers are required in visible locations throughout the building. Staff are to be trained in the use of fire extinguishers.

The Organisation is built primarily of non-combustible materials. The risk to fire can be reduced when new construction is done, or when office furnishings are purchased, to acquire flame resistant product.

Type	Description	Managed By	Backup Provider	Frequency	Additional Info
Org Teacher/Pupil Shared Data	On-Prem Server Shared Storage	IT Support Provider	N-Able Cove Cloud-to-Server Backup	Daily	
Org Teacher/Pupil Individual Data	On-Prem Server Personal Storage	IT Support Provider	N-Able Cove Cloud-to-Server Backup	Daily	
MIS	SIMS	Local Authority	Local Authority	Daily	Managed by third party
Financial	Oracle	Local Authority	Local Authority	Daily	Managed by third party

