# Disaster Recovery Plan

*Zevin Alifi*

# Table of Contents

# 1 Purpose

The best disaster recovery plans are designed with the express intention of minimizing the damage that a disaster event would cause to the organization and their resources. Additionally, it must minimize the interruptions that it would cause to business functions. These functions come in the varieties of business operations as well as financial functions. Downtime can be extremely costly to an organization in their customer base, as during the period of downtime they are not receiving the services that the organization provides and may lose interest or trust.

In light of this, the recovery must be as swift as possible, which is a primary goal of this response plan. Disaster scenarios that are accounted for include physical disaster scenarios such as fires, floods, tornadoes, and power outages. This additionally extends to technical disasters such as a data breaches or application failures. The Disaster Recovery Plan is designed to be malleable in the event of non-defined disasters as well. The following document will be given to all parties employed by the organization so that they can account for a disaster scenario. It must be followed to specification unless an exception is stated. Should anyone on staff have concerns about the contents of this document, they are encouraged raise them to your superiors for further modification.

# 2 Disasters

The category of the disaster can drastically change the appropriate response plan. It is important to have an understanding of all of them and the associated resources at risk before the disaster takes place so that it can be properly addressed by all the parties involved. Below will be a categorized list of potential disasters.

### Floods

Floods are a threat to any company equipment that is located on the first floor and the data contained on them. It could pose a physical risk to staff depending on the scale of the flood.

### Fires

Fires are a threat to the company equipment nearby relative to the fire itself, and have the capability of spreading and damaging more, including the building itself if improperly handled. Smoke inhalation in an enclosed space can additionally cause physical damage to the lungs or suffocation and the fire itself can pose a physical risk to staff.

### Electrical Failure

Electrical failure typically is a threat to the data contained on company equipment. It also poses a physical risk to staff in proximity of the source of the electrical failure.

Communications Loss

Attacks on the communication services can take the form of an internal act of sabotage, which can be difficult to identify while they are happening. on the organization or from an external, malicious hacker. It can vary in gravity based on how much the organization's functions are undermined. It poses no physical risk, however it can affect customer relations, data integrity, or affect the status of employment for several members of staff.

# 3 Action

## 3.1 Preventative

Being prepared for a disaster that disrupts data functions requires a backup strategy to be put in place for key business processes. Full mirrors of the data for the following are necessary to resume functions as quickly as possible during the recovery process, during a disaster they will be deployed as replacement for company functions.

- Email
- Purchase history
- Finances
- Website, front-end and back-end
- IT Operations

Smoke alarms are to be installed in the buildings. Halocarbon-based Fire extinguishers are nearby essential equipment. Evacuation points are established as the front entrance, the entrance to the parking lot, and a fire escape. Standby generators are ready to be deployed and all mission critical devices are connected to a dual parallel redundant Universal Power Supply system.

## 3.2 During incident

- All staff, regardless of their role should have access to this disaster recovery plan and be familiar with the content within.
- Personnel has responsibility to declare when a disaster is occurring or otherwise is expected to occur.

  *Communication between all employees is a vital part of taking action. It is the responsibility of any personnel to report an incident.*
- Evacuation through means of the front door, parking lot, or fire exit depending on the availability and proximity of each
- Identify what resources are at risks related to the disaster

  *One must classify what stored important company data is at risk. This data includes email services, websites, customer information, etc.*
- Disable hardware if accessible

  *Natural disasters such as floods are a threat to physical hardware and require the devices to be immediately shut off whenever feasible.*
- Report incident to a department manager.

  *9/11 should also be contacted if the building is at risk (e.g Fire Department)*
- Assign responsibilities in emergency response to employees

# 4 Restoration

## 4.1 Recovery

- Notify all staff of procedure
- Public Relations will be responsible for the official statement to end users.

  *Communicate the disaster, reassure that all customer data is safe, make statement about what steps are being taken to resume operations.*
- Restore primary organization services through off-site backups
- In event of a hospitalization, contact and notify the family of the staff in question
- If it is expected to incur a Service repair fee from damages, contact Insurance for assistance.
- Assess the resulting Financial Impact

  *Check for loss of revenue, financial documents, etc.*
- Review incident with Legal Department
- Assess damages to physical hardware, contact workstation and server suppliers for each identified resource that has been damaged
- Restore the rest of organization functions once all threats have been neutralized

# 5 Resources

## 5.1 Primary Contacts

Contact information for staff such as their number will be provided. Management team must maintain physical copies of the lines of communication to each employee and service.

| Staff Name | Title/Role | Phone Number | Email |
|---|---|---|---|
| Andrew Hopkins | Management | 480-856-3521 | ahopkins@yahoo.com |
| Nathan Vance | Legal Team | 480-252-1214 | nathanvance@yahoo.com |
| Saul Vetterlein | Media Team | 480-112-4146 | svetterlein31@yahoo.com |

## 5.2 External Contacts

| Service Provider | Title/Role | Phone Number | Email |
|---|---|---|---|
| Grimswood Electric | Power Company | 1800-205-5230 | supportline@grimswo.od |
| Server Supply | Server Maintenance | 1800-377-8823 | service@serversupply.com |
| Lenovo | Workstation Service | 1332-600-6293 | contact@lenovosupport.com |
| Nexsurance | Insurance Provider | 1245-322-1112 | next@insuran.ce |