UWEZO UGANDA

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

[Approved by the Board on 27th June 2023]

Table of contents

Contents

UWEZO UGANDA

VISION

A society in which all children are learning and realising their full potential.

MISSION

We are committed to demonstrating how to improve learning outcomes and keeping communities and leaders focused on learning through assessment, research, innovations, partnerships, and advocacy.

DISASTER RECOVERY PLAN

1.0 Introduction

The quantity of data and information technology infrastructure exposed to catastrophes seems to grow as firms depend increasingly on technology and electronic data for day-to-day operations. Every year, calamities, unpreparedness, and lost productivity cause organisations to lose money and incur expenditures. That is where a catastrophe recovery strategy comes into play. The purpose of this policy is to establish procedures for recovering critical IT systems and data in the event of a disaster or major outage. The policy is intended to minimise the disruption of business operations and to ensure the preservation of vital information and systems.

2.0 What is a Disaster Recovery Plan?

A disaster recovery plan, often known as a DRP, is a written process or method designed to restore critical information technology systems and services if an unforeseen event disrupts them. The purpose of a DRP is to safeguard a company's reputation and lessen the negative effects a catastrophic event, such as a power loss, data breach, or natural disasters such as earthquakes or floods, may cause to day-to-day business operations.

Here are the major goals of a disaster recovery plan.

- To minimise interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimise the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

3.0 Scope of the policy

This policy applies to all IT systems that support Uwezo Uganda operations; including the server, the common folder, Sophos firewall, Internet radio converter, Kaspersky password manager and data stored on Dropbox used by Uwezo Uganda.

4.0 Types of disasters covered

The policy is designed to prepare Uwezo Uganda for a wide range of potential disasters, including:

- **Natural Disasters**: These include events such as earthquakes and floods. These types of disasters can cause damage to buildings, equipment, and infrastructure, and can disrupt power and communication networks.
- **Power Outages**: These can be caused by a variety of factors, including natural disasters, equipment failure, and human error. Power outages can cause data loss, damage to equipment, and disruption to business operations.
- **Cyber Attacks**: These can include malicious software (malware), phishing scams, and hacking. Cyber attacks can cause data loss, damage to IT systems, and disruption to business operations.
- **Human Error**: These can include accidental deletion of files, misconfiguration of systems, and mishandling of equipment. Human error can cause data loss and disruptions to business operations.
- **Terrorism**: These include physical attacks, cyber-attacks, and disruptions to critical infrastructure. Terrorism can cause damage to buildings, equipment, and infrastructure, and can disrupt power and communication networks.

5. 0 Systems and data covered

This policy typically covers a wide range of systems and data, including:

Server: This is the backbone of Uwezo Uganda's IT infrastructure, and it stores the data under the Common folder, configures the domain and has the Aruti application. A disaster recovery plan should include procedures for protecting servers, as well as procedures for restoring them in the event of a disaster.

Network infrastructure: This includes the routers, switches, hubs, and other network equipment that are essential for connecting systems and data.

Applications: These are the software programs that Uwezo Uganda uses to support its operations

Data: This includes all the information that Uwezo Uganda stores, including programs data, financial data, communications data and sensitive information.

Cloud-based services: Uwezo Uganda uses cloud-based services for storage, email, and other applications.

User devices: This includes desktops, laptops, and mobile devices that employees use to access systems and data.

RISK ASSESSMENT

Risk Category	Risk Description	Likelihood	Impact	Critical Systems/Data	Priority	Current Control	Control Effectiveness	Risk Level	Risk Mitigation Plan
Natural Disaster	Flooding	Low	High	• Server • Network infrastructure	• Low	• Dropbox	Backups done regularly	Low	Implement weekly backups of all data onto dropbox & external hard drives and have all office assets insured.
	Earthquakes	High	High	• User devices	• Low • Medium		Yearly insurance of office assets done	Medium	The external hard drives should be secured in a fire proof location such as a safe or metallic cabin.

Risk Category	Risk Description	Likelihood	Impact	Critical Systems/Data	Priority	Current Control	Control Effectiveness	Risk Level	Risk Mitigation Plan
						• Asset insurance policy			
Cyber Attack	Ransomware, phishing scams, and hacking	High	High	Servers, Applications, User devices and cloud-based services	High	Firewall and antivirus software	Regular updates and subscription for antivirus	Medium	Implement regular software updates, train staff on use of password managers, use of multi factor authentication, regular monitoring of network & system logs in the firewall and devices

Risk Category	Risk Description	Likelihood	Impact	Critical Systems/Data	Priority	Current Control	Control Effectiveness	Risk Level	Risk Mitigation Plan
Power Failure	Loss of power	Low	Medium	All IT systems	Medium	UPS and backup generator	Testing of UPS	Low	Implement regular testing of UPS and communicating with building manager of prolonged power shortage
Human Errors	Accidental deletion of data or misconfiguration of systems	Medium	Medium	Server and User devices	Medium	Server	Regular checking of data storage locations and system configurations	Low	Train staff on usage of IT systems and data storage locations.

6.0 Backup and Recovery

6.1 Regularly backing up critical data and systems
Uwezo Uganda will regularly back up all critical data and systems to ensure that it can be recovered in the event of a disaster.

6.2 Types of backups
There will be use of a combination of full, incremental, and differential backups to ensure that all critical data and systems are properly protected. (Full back up is back up system that saves a copy of an entire data set, while Incremental back up involves back up of the data that has changed since the previous back up. Differential back up involves back up of all the files that have changed since the previous full back up. The difference between incremental and differential backup is that, while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup). Full backups will be performed on a weekly basis, while incremental and differential backups will be performed on a more frequent basis (possibly daily) to ensure that recent changes are captured.

1.3 Backup media and devices
There will be a variety of backup media and devices, such as external hard drives provided to each Uwezo Uganda Unit, cloud-based storage to ensure that backups are stored in multiple locations. The external hard drives containing the weekly full back up shall be securely kept in a fire proof location such as safe or metallic cabin.

6.4 Backup schedule: Backups will be performed on a regular basis, with full backups performed on a weekly basis and incremental and differential backups performed on a daily basis but not so frequently in that backing up becomes a burden.

6.5 Procedures for restoring backups in the event of a disaster
In the event of a disaster, we shall follow a detailed set of procedures to restore backups and recover critical data and systems. These procedures will include steps for identifying the specific backups that need to be restored, as well as the specific steps for restoring the backups.

6.6 Testing and verifying backups
Regular tests and verifying of backups to ensure that they can be successfully restored in the event of a disaster. This will include running restore tests on a quarterly basis and verifying that the backups can be successfully restored to a test environment.

6.7 Documenting
Documentation of the backup process, including the types of backups performed, the backup schedule, and the procedures for restoring backups in the event of a disaster.

6.8 Review and update
A review and update of the backup and recovery plan shall be done on a biannual basis to ensure that it remains relevant to the organisation's changing needs and to ensure that the backups and recovery procedures are up-to-date.

7.0 Business Continuity Plan

7.1 IT Infrastructure

System or Process	Dependencies	Critical Data	Critical Personnel	Critical Suppliers and Vendors
Server	Network infrastructure, Electrical power	Organisation records, Staff files, Financial records, Aruti	IT personnel	Sybyl, Logik Technologies, Network service provider
Sophos Firewall	Server, Internet service provider	VPN, Office internet connection	IT personnel	ICT Beacon
Telephone System	Network infrastructure, Electrical power	Office communication	All Staff	Logik Technologies
Xero Financial software	Internet	Financial records, Invoices, Reports	Accounting department	Xero support
Salesforce System	Internet	Organisational data on payments, requisitions, imprests, contracts etc	All staff	Salesforce support

7.2 Communication

Effective communication is a crucial component of a disaster recovery plan as it ensures that all stakeholders are informed and updated throughout the recovery process. This section outlines the procedures for disseminating information about the disaster and recovery efforts, key contacts for employees to reach out to, procedures for communicating with suppliers and other external stakeholders, and a communication plan for the different stages of disaster recovery.

7.2.1 Procedures for Disseminating Information

In the event of a disaster, the following procedures will be followed to disseminate information about the disaster and recovery efforts:

The IT officer will activate the disaster recovery plan and inform the Procurement / HR Associate.

The Procurement / HR Associate will convene a meeting to assess the situation and determine the next steps.

The IT officer will provide regular updates to the Procurement / HR Associate and keep a record of all decisions and actions taken.

Procurement / HR Associate will communicate with all employees through email, whatsapp, or company meetings to keep them informed of the situation and the recovery efforts.

7.2.2 Key Contacts for Employees

In the event of a disaster, staff can reach out to the following key contacts for information and support:

IT Officer: Vincent Kalibbala, vkalibbala@uwezouganda.org, +256-706327072

Procurement / HR Associate: Judith Nyakaisiki, jnyakaisiki@uwezouganda.org , +256-783783233

8.0 Roles and Responsibilities of Employees during a Disaster

The roles and responsibilities of employees during a disaster will vary depending on the specific duties of each position and the needs of the organisation during the disaster event. However, some general responsibilities for each role during a disaster might include:

Executive Director

1. Ensure that all critical systems and processes are operational
2. Oversee disaster recovery efforts
3. Ensure that employees are safe
4. Communicate with external stakeholders such as Board members and partners
5. Make decisions about business operations during the disaster

Senior Programs Officer

1. Ensure the continuity of key programs and services
2. Work with other departments to maintain critical systems and processes
3. Communicate with external stakeholders regarding program disruptions

Procurement & Human Resources Officer

1. Obtain resources and supplies necessary for disaster recovery efforts
2. Ensure that contracts and agreements with suppliers are in place to support recovery efforts
3. Ensure that employee safety is a priority during the disaster
4. Manage payroll and benefits during the disaster event
5. Provide support to employees who have been affected by the disaster

Accountant

1. Maintain financial records during the disaster
2. Assist with the preparation of financial reports related to the disaster

Accounts & IT Assistant

1. Assist the accountant with maintaining financial records during the disaster
2. Provide support for financial reporting as needed
3. Ensure that critical IT systems are operational
4. Restore systems and data as necessary
5. Work with other departments to ensure the continuity of critical systems and processes

Administrative Assistant

1. Ensure that administrative processes are maintained during the disaster
2. Manage logistics during the disaster, such as transportation and temporary shelter for employees
3. Provide support to other departments as needed.