THE REVOLUTIONARY GOVERNMENT OF ZANZIBAR	
Applicable Public Institution **<<insert the name of the Institution >>**	**Document Name** Disaster Recovery Plan **Document Number** <<Insert your own document reference code>>

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	<<Name of Accounting Officer>>	<<Title e.g. CEO>>	<<Signature>>	<<Date>>

Table of Contents

1. INTRODUCTION

1.1. Overview

<<Public Institution should provide here a high level description of your institution, its mission, objectives and main functions>>

The aforementioned business functions are highly dependent on information technology services including networks, systems and applications for their daily business operations.

1.2. Rationale

<<Highlight the purpose of the disaster recovery plan. An example has been provided below>>

The business functions of Public Institution are dependent on information technology services including networks, systems and applications for daily business operations. The inability of information technology services to function would immediately impact the core operations at an Institution and subsequently, the other departments, resulting in significant work backlog. This would in turn bring about inability of an Institution to respond to queries from different stakeholders, as well as failure to provide services on time.

This DRP has been developed to guide the efficient recovery of information systems supporting the Institution which is found at **<<include the address of the institution>>** It outlines the background, procedures, and contact information to recover critical networks, systems and applications.

Proper execution of this DRP will help facilitate the timely recovery of key information systems, minimizing business disruption. This DRP is an imperative component to the successful resumption of business functions at an Institution. This document also takes into consideration the broader perspective of business continuity, incorporating the elements from the Institution Business Impact Analysis. A Business Impact Analysis should be completed prior to drafting the disaster recovery plan.

This DRP is designed to assist in minimizing the effect of a disaster event, by ensuring the restoration of essential processing within the recovery time objectives **<<Include all the identified RTOs in the appendix >>** established by the Business Impact Analysis.

1.3. Purpose

The objectives of the DRP should be clearly laid out in this section. An example is provided below;

The primary objective of this DRP is to establish defined responsibilities, actions and procedures to recover the critical network, system and application environment in the event of a disaster.

The DRP is structured to attain the following key objectives:

- Recover the physical network and critical applications within Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) established and accepted by management;
- Ensure that necessary personnel and resources are prepared and understand their roles for recovery;
- Provide guidance and information to help facilitate a successful recovery process from initial activation to post-recovery; and

In order for the DRP to meet the aforementioned objectives, sufficient communication, testing, and training will need to be conducted.

1.4. Scope

This document is for the Accounting Officer (Head of Institution) at <<Insert Physical Address>>.

These rules are applicable to **<<include the name of the institution >>** Accounting Officer (Head of Institution), responsible teams for BCP/DRP and external service providers (suppliers, contractors, fire).

It applies to ICT assets owned or leased by an Institution or to devices that connect to the Institution network or reside at Institution.

2. Disaster Preparedness and Recovery Procedures

2.1. Disaster Preparedness

2.1.1. Overview of ICT environment

Public Institution should include a detailed overview of the ICT environment. The overview will include (but not limited to) the following information:

i. High level ICT organization structure
ii. The network topology of ICT
iii. List of servers, network devices and applications and their purpose
iv. Overview of available service level agreements
v. Available ICT operating procedures

2.1.2. Summary of ICT Systems

The table indexed 2(a) provides a summary of the different applications, respective hosting server, backup procedure and the support agreements in place to ensure service continuity.

2.1.3. Business Impact Analysis

A Business Impact Analysis has been performed for the ICT applications to determine the impact of any downtime and the expected timelines for recovery. This includes Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

"The RTO is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in service continuity".

"The RPO describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the maximum allowable threshold or "tolerance.""

The table indexed 2(b) provides a summary of the different information system which are used intensively by the business at the Institution and their respective Recovery Time Objective (RTO) and Recovery Point Objective (RPO). An illustrative example has been provided in the table;

In line with the above table indexed 2b (indicating RPO and RTO), the disaster scenarios have been listed together with their recovery procedures and strategy for information system, infrastructure and physical facility is defined in subsequent sections.

2.1.4. Roles and responsibilities

2.1.4.1. Disaster Recovery Task Force

In order to facilitate the efficient recovery and restoration of critical business functions, the management team from Business, Operations and key ICT staff members as well as third party service provider(s) have been assigned to Disaster Recovery Task Force (DRTF) in the Institution**.** Any contingency would be handled by two levels of task force:

a) Crisis Management Team (CMT)

b) Recovery Team (RT)

<<This section covers the detailed composition, roles, responsibilities and the action steps to be followed by each of these teams. The functions of the above teams would vary with the extent and impact of the different contingencies that could impact the operations of the different institutions. >>

The composition of DRTF is critical to successful planning and recovery of the ICT operations. It is important that the team representatives have the authority to make operational and financial decisions during a contingency.

<< The section below in this document define the different roles and responsibilities for the maintenance of the DRP>>

a) Crisis Management Team

The Crisis Management Team (CMT) is the group of senior staff, which commands the resources needed to recover the operations in the event of a disaster. The roles of CMT can be assumed by Institutional ICT Steering Committee

Roles and Responsibilities of CMT

CMT Head

The CMT Head is the Accounting Officer, He/she will have overall responsibility for the response and recovery actions taken in the event of a disaster. However, he/ she will delegate the team management responsibilities to the other members of the CMT. This will entail the delegation of decision-making power and authority to make the necessary decisions during any crisis.

The CMT Head will maintain close contact with the other members of the CMT who will advise him/ her of the progress of recovery and consult with him on significant decisions.

Key responsibilities of the CMT Head include:

i. Overall responsibility for disaster declaration, response and recovery actions.

ii. Assist in decision making.

iii. Authorize crucial action steps.

iv. Visit next of kin of deceased staff (if any).

v. Brief staff of overall situation and provide overall guidance.

vi. Vet sensitive communications.

vii. Assist in crucial negotiations (financial and legal).

viii. Keep the business users informed of the status of the situation.

<< Additional responsibilities based on the business functions of the institutions should be included>>

CMT Coordinator

The key to success in developing and maintaining an effective and efficient contingency plan is the leadership provided by the CMT Coordinator, who works closely with Head of departments and members of the different teams (namely CMT and RT).

The CMT Coordinator is the Director/Head/Manager of ICT Directorate/Unit/Section. He/she is responsible for providing overall guidance during the emergency response and recovery efforts, reviewing damage assessment reports, initiating recall procedures, coordinating the activities / decisions of the CMT and RT, keeping senior management informed about recovery operations.

Key responsibilities of the CMT Coordinator include:

i. Set the DRP into motion after the CMT Head has declared a disaster

ii. Be the single point of Contact for and oversee all the DR Teams

iii. Organize, supervise and manage all DRP test and author all DRP updates

CMT Members

The CMT members are the same members of Institutional ICT Steering Committee who will manage and co-ordinate the response to, and recovery from a crisis. This role will continue through the restoration until the situation returns to normal. That is, until the ICT teams can cope with the situation without additional senior management supervision.

Responsibilities include:

i. Formalizing recovery strategy and operational requirements.

ii. Coordinating recovery at alternate site, wherever applicable.

iii. Damage Assessment.

iv. Coordinating and project manage recovery of Facility, Operations and ICT infrastructure.

v. Coordinating recovery of critical processes in different departments.

vi. Liaise with third party vendor for emergency / recovery support during crisis.

vii. Monitoring Staff Welfare.

viii. Funds Management including controlling expenditure decisions

ix. Initiating legal action, if required

<< Additional responsibilities based on the business functions of the institutions should be included>>

CMT Recovery Actions

The recovery actions of the Crisis Management Team can be classified into the following different categories:

i. Emergency actions to be taken during a disaster.

ii. Situation assessment during a disaster.

iii. Activation of disaster recovery plan in the event of a crisis.

iv. Monitoring of actions during a disaster.

v. Completion and finalization of recovery processes.

Based on the initial information obtained about the disaster, CMT would identify whether facilities have been affected or whether there is a risk of damage to premises or danger to employees. Subsequently, CMT would authorize the relevant parts of the CMT recovery actions as per the type and intensity of the disaster.

<<The contact details of all the CMT members must be provide in the table in the Appendix section 7.2 >>

b) Recovery Team (RT)

<<The Recovery team composition must be defined and should include representatives of the ICT team and third party service provider>>

The RT members must be aware of the disaster recovery plan put in place for the institution. The CMT members must be able to assist any RT with the implementation of the plan, and therefore their knowledge of the entire plan document is vital, as they play an essential role in the recovery process.

<<The table should be populated with the contact details of all the Recovery team members as per Appendix section 7.3>>

The roles and responsibilities of the RT are as follows:

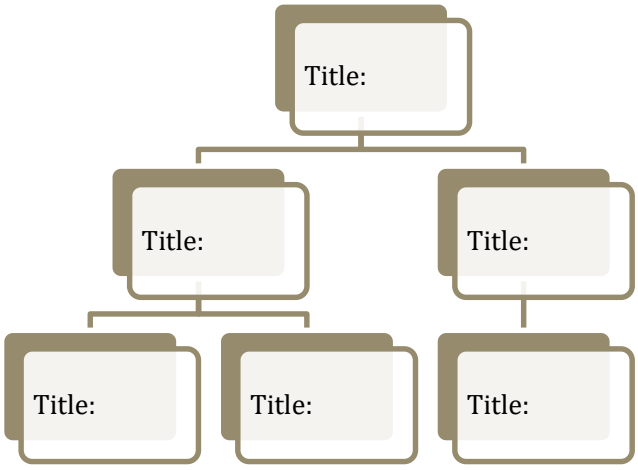
i. Formalizing recovery strategy and operational requirements

ii. Coordinate recovery of the premises and infrastructure so that normalcy can be restored at an earliest.

iii. Perform scheduled DR testing to ensure if the process is reliable in case of disaster.

2.1.5. Call Tree

In the event of a major disruption, it is important that employee or security personnel who detects the incident, informs Management/ any CMT Member who will in turn inform other members. The call tree provided below guides the communicators and helps ensure that all critical members from DRTF are informed about the event.

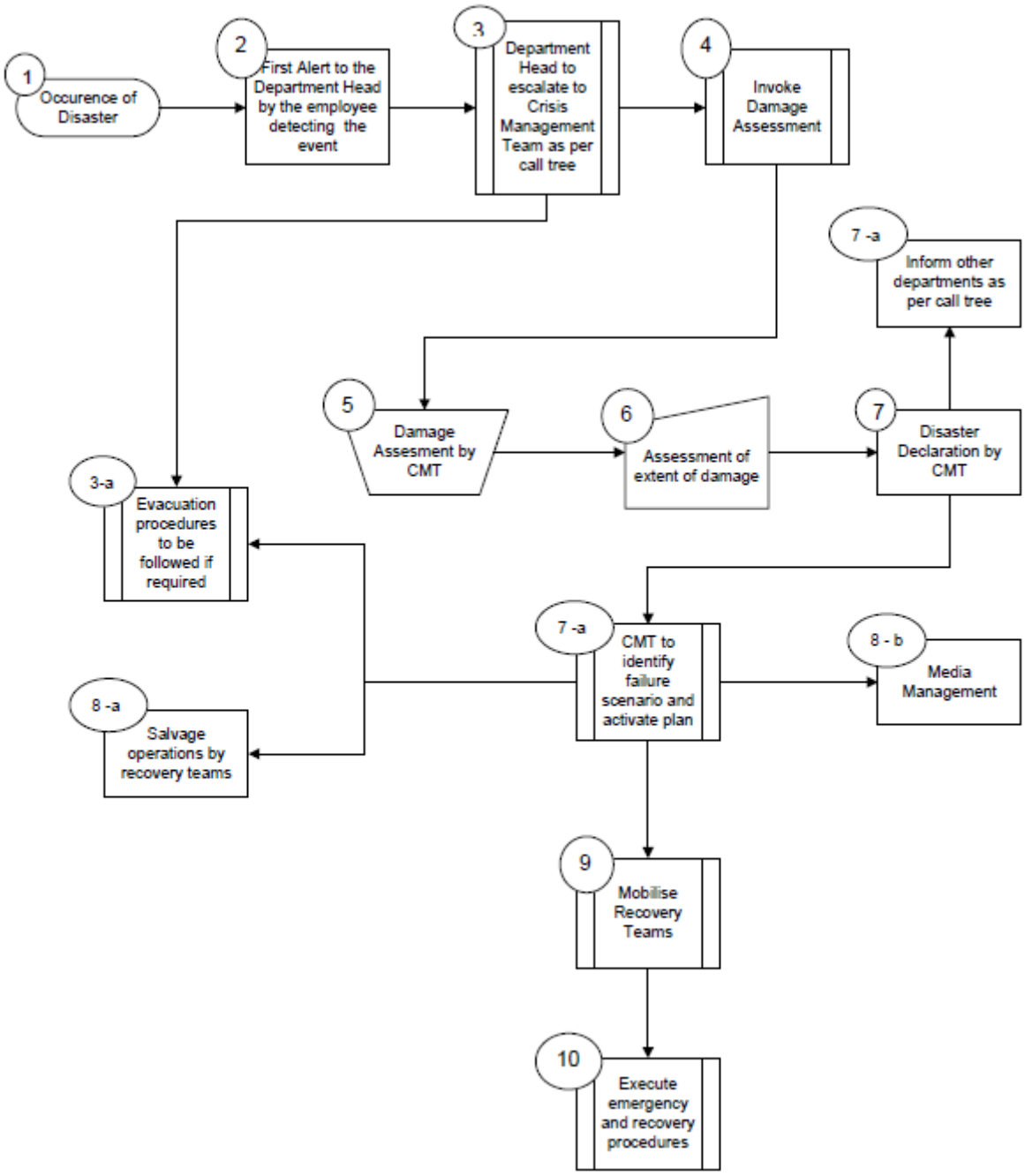


<< The title and names of nominated persons should be provided in the above call tree>>

2.2. Disaster Recovery

2.2.1. Activity flow in case of disaster

<<Include the name of the public institution >> shall include an activity flow to follow in the event of a disaster. An illustrative example has been provided in the diagram below.



2.3. Communication Plan

2.3.1. Declaration of disaster

CMT Head will be responsible to declare the disaster and the level of disaster. Based on the intensity of an event, the initial report of the Crisis Management Team (CMT) and the

expected time to recover normal operations, the CMT Coordinator will meet, analyze facts, intensity of the event and CMT Head will declare a disaster.

A preliminary announcement is used to communicate, responsively and accurately, to the following key departmental Heads / Managers at various units of the institution, immediately following the disruption;

<<Include a list of all the units of the institution>>

Details such as nature of the DR event, services affected, steps taken to restore services, expected downtime etc. will be communicated.

2.3.2. Media management plan

Apart from authorized spokesperson **<<e.g. Public Relation Officer>>** of the institution, no other person should speak to the press in the event of a disaster.

Depending upon the media's responsiveness and in anticipation of their usual quick response, the CMT Head is responsible to inform the department of Media Relations of all happenings during a disaster. This would help the spokesperson to effectively manage the media. The spokesperson interfaces with the media, employees and public for release of official statements concerning the contingency and the ability of the organization to continue operations. This person serves as the only authorized source for publicity and press releases. During the state of chaos immediately following a disaster.

It is crucial that all questions and comments be coordinated through this spokesperson for consistency and clarity purposes.

2.3.3. Disaster Declaration

When declaring a disaster, care must be taken not to disclose unnecessary critical or sensitive information to the public. A sample disaster declaration is shown below;

<<"...A <fire, power outage, etc.> has temporarily disrupted operations at the Data Center <mention the location/site>. The Data Center building has experienced some damage. Officials of the <<include the name of the institution>> are evaluating the extent of the damage and probable cause. The Disaster Recovery Plan has been activated and is progressing according to schedule. Additional information will be provided when details are available...."">>

If it is immediately known that employees or vendor employees have been injured, this should be included in the preliminary announcement to the media. This announcement should have a classifying statement that, "The exact extent of the injuries and the names of the employees injured are unknown at this time." Any announcement to the media should also contain the name and telephone number of the Public Relations Officer who is available to answer any questions that media may have.

Notes for the Public Relations Officer

i. Never accept a cold call from a reporter: Instead, get their name, organization, subject of the interview and the reporter's deadline and advise that you will call them back

ii. Do not volunteer negative information

2.3.4. Important instructions

First Point of Contact

If any employee or vendor suspects that there is a potential or actual disaster in progress, he/ she needs to first inform one of the following and subsequently the respective team lead.

Name	Department	Email Address	Contact Numbers

<<Complete the above table with the names of the identified first point of contact>>

Event Reporting

Report the following information to Physical security / CMT / Administration team,

i. Your name

ii. Description of the event

iii. Preliminary information of damages and injuries if any

iv. Any information regarding attempted or actual contacts with CMT members, other employees, fire brigade, police etc.

v. Extension/Mobile number and location where you can be reached

<<Complete the table below with the details of the emergency contact services>>

Emergency Service Listing

Service	Contacts Details	Contact Numbers
Police Stations		
Ambulance		
Fire Services		

2.3.5. Procedure for damage assessment and salvage

If a detailed damage assessment and salvage operation is required, the procedure is as follows:

a) Make a detailed assessment of the damage and list down the assets with a unique control number (salvage number). The sheet should also contain the location and work area where the asset was placed along with quantity and if possible the asset number from asset list.

b) Search the site systematically. Fill in a Damage Assessment Sheet as referred below for each Business Unit / Rack etc. All items must be logged on the sheets, filling in as many of the entries in each row as possible. For example, try to obtain and record model number, serial number and asset number. These details will be required for identification and insurance purposes.

c) Incomplete details can be input later by reference to the off-site asset register.

d) The Sheet comprises a number of columns which must be completed as follows:

   i. Salvage Control No. - a sequential identifier for each salvaged item.

   ii. Location/Work Area should contain the location/work area - it must be possible to cross-reference this to the site plan.

   iii. Quantity - self-explanatory.

   iv. Item Type e.g. Server hardware, network switch etc.

   v. Model and Serial No. - Self-explanatory.

   vi. Asset Reference Number should correspond to the central asset register.

   vii. Condition should indicate whether the item is recoverable, a total loss or status unknown - tick the relevant column.

   viii. Destination should contain the destination of the item when or if it is removed from the Disaster Site, e.g. Salvage Company or alternative site(s).

   ix. Remove Sheet Ref. should contain the reference of the corresponding Asset Removal Form.

   x. Comments should contain any additional information, as appropriate.

e) Employ other team members away from the affected site, matching the tabulated items in the Sheets to the Assets Inventory, ticking them off on the Register, and completing any details missing from the Sheets.

f) An Asset Removal Form as referred below must be filled in for any item removed from the Primary Site after approval received from the Crisis Management Team (CMT) coordinator. The 'Released by:' 'Transport by:' and 'Received by:' entries must be signed off.

g) Disaster Recovery Test report should be prepared and signed as per sample report **Appendix 7.8**

h) Sample Damage Assessment Form, Asset Removal Form, Test Result Report Form, List of all Hardware and Applications sample report forms are provided in **Appendix *7.4*** *up to* ***7.8***

i) Note: The completed Damage Assessment sheets, Asset Removal Forms and Recovery Test Reports must be securely stored; they are vital documents for recovery management and insurance purposes.

2.4. Disaster Recovery Scenarios

2.4.1. Disaster Level I: Failure impacting single department

Significant malfunction of/ disruption to primary infrastructure supporting operations of a single department

Failure Scenario	**<<Insert the possible type of failure e.g. Failure of network >>**
Possible Cause	**<<Insert the possible root cause>>**

Information systems impacted	**Processes impacted**	**Departments impacted**

<<The above table should be completed to reflect the chosen failure scenario>>

2.4.1.1. Pre-Events

Action Steps	**Responsibility**	
	Dept / Team	**Person(s)**
Maintain adequate Service Level Agreement (SLA) - Vendor i. Faults / failures / repairs are set right within <> hours of being informed. ii. Replacement should be provided within <> hours of being informed of any fault / failure / repairs.	CMT	
Keep redundant router/ switch or any appliance	RT	
Periodically check all the cabling and networking components in the existing Wide Area Network (WAN) setup.	RT	
Update the cabling diagram of the WAN set up.	RT	
Maintain Service Outage Register. Register should contain at the least following: i. Description of problem / error, ii. Time of outage, iii. Time & person informed, iv. Time of service resumption,	RT	

v. Solution applied.		
Ensure that Closed Circuit Television (CCTV) Surveillance Cameras are well managed and feeds are readily available on needs.		
Restrict access to CCTV Control rooms to only authorized personnel.		

2.4.1.2. Detection & Escalation

Action Steps	**Triggers**	**Responsibility**	
		Dept / Team	**Person(s)**
Inform Vendor	Users unable to access WAN	RT	
Inform CMT Coordinator	Diagnosis by vendor	CMT	

2.4.1.3. Recovery

Action Steps	**Responsibility**	
	Dept / Team	**Person(s)**
Ensure that repairs / replacement are done within set time limit (<> hours as per SLA) and escalate the matter to the higher authority of vendor about the failure in case of delayed recovery.	CMT	
Identify cause of failure and rectify the same.	Vendor	
Update Service Outage Register with regard to following: i. Time of service resumption ii. Solution applied.	RT	

<<Other scenarios that can affect a single department must be elaborated and included in this section. Examples of such scenarios include:

- **Loss of business applications (due to software issues)**
- **Hardware/ server failures**
- **Connectivity outage>>**

2.4.2. Disaster Level II: Failure impacting multiple sites

Significant malfunction of/ disruption to critical primary infrastructure, supporting operations at multiple sites. For e.g.: failure of any of the critical primary servers or data storage systems.

Failure Scenario	**<<Insert the possible type of failure e.g. Failure of multiple devices>>**
Possible Cause	**<<Insert the possible root cause>>**

Information systems impacted	**Processes impacted**	**Departments impacted**

2.4.2.1. Pre-Events

Action Steps	**Responsibility**	
	Dept / Team	**Person(s)**
Maintain adequate SLA - Vendor i. Faults / failures / repairs are set right within 6 hours of being informed. ii. Replacement should be provided within 6 hours of being informed of any fault / failure / repairs.	CMT	
Back up of application server, database on a regular basis	RT	
Maintain Service Outage Register. Register should contain at the least following: i. Description of problem / error ii. Time of outage iii. Time & person informed iv. Time of service resumption v. Solution applied.	RT	
Ensure that Closed Circuit Television (CCTV) Surveillance Cameras are well managed and feeds are readily available on needs.	RT	
Restrict access to CCTV Control rooms to only authorized personnel.	RT	

2.4.2.2. Detection & Escalation

Action Steps	Triggers	Responsibility	
		Dept / Team	Person(s)
Inform vendor	Users unable to access server	RT	
Inform CMT Co-coordinator	Diagnosis by GOC/ ICT Officers	CMT	

2.4.2.3. Emergency

Action Steps	Responsibility	
	Dept / Team	Person(s)
In case of server failure (perform existing recovery strategy such as recovery from backup tapes)	RT	
Inform vendor about the failure.	RT	
Update Service Outage Register with regard to: i. Description of problem / error ii. Time of outage iii. Time & person informed	RT	

2.4.2.4. Recovery

Action Steps	Responsibility	
	Dept / Team	Person(s)
Ensure that repairs / replacement are done within set time limit (<> hours) and escalate the matter to the higher authority of the vendor about the failure in case of delayed recovery.	CMT	
Identify cause of failure and rectify the same.	Vendor	
Update Service Outage Register with regard to following: i. Time of service resumption ii. Solution applied	RT	
Once the servers start working, test it before making it live.	RT	

2.4.3. Disaster Level III: Premises Unavailable

Total shutdown of data centers, as a result of fire, building collapse etc.

The plan addresses the following types of Level III disasters, which affect the access of employees to the work premises:

i. Fire

ii. Power Outage

iii. Theft

Key Objectives:

1. To ensure safety of employees
2. To recover operations as quickly as possible
3. Work in close co-ordination with the Civic Authorities, as in a building wide disaster, the resources of the institution may not be equipped to handle the impact.

A. Failure Scenario	**Fire**

2.4.3.1. Pre-Events

Action Steps	**Responsibility**
Provide adequate fire safety measure i.e., gas fire extinguishers, fire exits, clear exit marking, fire alarms etc.,	CMT Coordinator and RT
Conduct fire safety drill on regular basis.	CMT Coordinator and RT
Fire extinguishers should be periodically examined (e.g. Gas level, expiry dates) and tested to ensure that they would be useful in case of fire.	CMT Coordinator and RT
Employees should be demonstrated the use of the fire extinguisher.	CMT Coordinator and RT
Ensure that Closed Circuit Television (CCTV) Surveillance Cameras are well managed and feeds are readily available on needs.	CMT Coordinator and RT
Restrict access to CCTV Control rooms to only authorized personnel.	CMT Coordinator and RT

2.4.3.2. Emergency

Action Steps	Responsibility
In case of a small fire, attempt to extinguish fire with hand held fire extinguishers, otherwise raise an alarm.	RT
Inform Fire Brigade / police either based on first-hand information or independent detection depending on the initial assessment of the situation.	RT
If the event occurs during normal office hours, then based on the extent of Fire, start full / partial evacuation by announcing the event to all staff and raising fire alarm (if it has not gone on already) or by manual means.	RT
While evacuating, if time permits, guide people and carry important papers. Put important papers (if any) in fireproof safe.	RT
<<Insert public institution name>> should ensure that funds are sufficiently available to address the recovery requirements when responding to a disaster situation.	Accounts
If the fire is spreading or if it is at critical location like Server Room, all users of the system should logout and switch off their terminals. The ICT Officer should then shut down the server. If the time does not permit a proper shutdown, it should be directly switched off by the ICT Officer. The users and ICT Officer should try to save critical hardware and data. The criticality for various types of items are as follows: 1. Previous day's backup, 2. Server, 3. Other Hardware items	IT Officer/ RT
The main power supply should be switched off.	RT

Gather at (Emergency Assembly Point)

2.4.3.3. Recovery

Action Steps	Responsibility
Co-ordinate with Civic Authorities to help control fire, evacuate trapped people etc.	RT
Take a Roll Call / Head Count.	RT
Investigate any missing member of staff / visitors.	RT
Information about missing person(s) is to be given to RT members.	RT

In case of injury, call ambulance and arrange for first aid.	RT
Inform family members and relatives of the employees about safety of the employees present.	RT
RT coordinator to ask employees other than RT members to leave premises.	RT
RT to arrange movement of employees to reach their homes, if the vehicles parked in parking area have been affected during the fire.	RT
Arrange for basic amenities like food, water and accommodation for employees who have to remain for recovery operations.	RT
When the situation is back to normal, follow up with the vendors for repair/ replacement of the hardware/servers.	RT
Check critical data availability in restored database	RT

If event occurs in off-peak office hours (when only skeletal staff is present), then inform Civic Authorities and RT members, and evacuate people. RT will then decide who should reach the site for damage assessment and when the recovery procedures should start.

B. Failure Scenario	**Power Outage**

2.4.3.4. Pre-Events

Action Steps	**Responsibility**
Prepare a list of critical and non-critical electricity consuming equipment.	RT
Maintain UPS for all servers and other critical components.	RT
Maintain the following generators: i. Non-critical generator used for general lighting during office hours and ii. The critical generator for the key components.	RT
Test UPS and generators periodically.	RT
Maintain adequate capacity generators.	RT
Store of adequate quantity of diesel.	RT
Ensure that Closed Circuit Television (CCTV) Surveillance Cameras are well managed and feeds are readily available on needs.	RT
Restrict access to CCTV Control rooms to only authorized personnel.	RT

2.4.3.5. Emergency

Action Steps	Responsibility
Save all work being currently carried out.	RT
Switch on the generators.	RT
Rescue any staff that may be trapped in the lifts due to power outage.	RT
Shut down non-critical equipment.	RT

2.4.3.6. Recovery

Action Steps	Responsibility
Liaison with Electricity Provide and wait for power supply to resume.	RT
Switch over to the primary power supply after normal power supply restored.	RT

C. Failure Scenario	Theft

2.4.3.7. Pre-Events

Action Steps	Responsibility
Maintain an ICT Inventory Register for the following: i. IT hardware ii. Software iii. Electronic Data iv. Back up media (tapes)	CMT
Carry out physical checking of all above inventory periodically (e.g. every <> months).	CMT
Restrict access to server rooms to only authorized personnel.	CMT
Ensure that Closed Circuit Television (CCTV) Surveillance Cameras are well managed and feeds are readily available on needs.	CMT
Restrict access to CCTV Control rooms to only authorized personnel.	CMT

Maintain physical access register in all server rooms and other key locations. Such log should be reviewed at regular intervals to identify any unauthorized access.	CMT
The off-site back up must be maintained with proper physical security and the access to off-site back up should also be restricted to authorized personnel.	CMT
Critical data should be maintained in encrypted forms.	CMT
There should be a 'Confidentiality clause' in all the SLA agreements with service providers.	CMT
Physical security should maintain a separate registers for employees and visitors. It should log the name, address, contact, incoming and outgoing time, any articles being carried along with and remarks.	Physical Security Guard

2.4.3.8. Emergency

Action Steps	**Responsibility**
Inform all the employees about the theft.	RT
Inform the nearest police station about the theft.	RT
Block all the exits of the premises. If at all it is necessary for someone to leave the premises, he/she should be thoroughly checked for the stolen data/ hardware/ software etc.	Physical Security Guard

2.4.3.9. Recovery

Action Steps	**Responsibility**
Physically check all the visitors and employees inside the premises.	Physical Security Guard
Assist the police investigation by providing various trails like access registers, OS audit trails etc.	RT
Follow up with the police department regarding the theft.	RT
When the situation is back to normal, follow up with the vendors for procurement of the hardware/servers.	RT
Check critical data availability in restored database.	RT

3. IMPLEMENATION, REVIEWS AND ENFORCEMENT

This document will come into operation once tabled and agreed in management meeting, and approved in its first page.

This document is subject to review at least once every three years. Any other minor reviews will be done as per requirement from management.

4. ACRONYMS

BIA	Business Impact Analysis
CCTV	Closed Circuit Television
CMT	Crisis Management Team
DRTF	Disaster Recovery Task Force
GOC	Government Operation Center
MTPD	Maximum Tolerable Period of Disruption
PTO	Recovery Time Objective
RPO	Recovery Point Objective
RT	Recovery Team

5. RELATED DOCUMENTS

i. IT Service Management Procedures Ref No: **<<insert document title>>**
ii. Information Security Risk Assessment Ref No: **<<insert document title>>**

6. DOCUMENT CONTROL

REVISION	NAME	COMMENT	DATE
Rev. 1.0		Creation of Document	<INSERT DATE>

----------***For Government Control Only***----------

Sample Name: **Disaster Recovery Plan Sample**
Sample Reference: **eGAZ/EXT/SAM/001**
Sample Version: **1.0**
Sample Effective Date: **March 2022**
Sample Creation: **Zanzibar e-Government Agency**
Sample Changes: **None**

7. APPENDICES

7.1. Contact Details of Third party Vendor

Supplier		
Address		
Primary Contact	Name:	
	Fax:	
	Office Tel:	
	Mobile:	
	Email:	
Backup Contact	Name:	
	Fax:	
	Office Tel:	
	Mobile:	
	Email:	

<<Include the contact details of all suppliers>>

7.2. Contact Details of CMT

Crisis Management Team and Contact Details			
Name	**Designation**	**Role**	**Contact Details**
		CMT Head	
		CMT Coordinator	
		CMT Member	
		CMT Member	
		CMT Member	
		CMT Member	

7.3. Contact Details of RT

Name	Designation	Role	Contact Numbers	
			Office	Mobile
		RT Head		
		RT Member		
		RT Member		

7.4. 7.4 Sample Asset Removal Form

<<Include the name of the public institution >> Asset Removal Form

Location/Work Area: _____

Salvage Control No(s):_____

Asset No(s): _____

Description: _____

Reason for Removal: _____

Destination Location: _____

Additional Information: _____

_____

_____

Requested by:_____ _____ _____

Name Signature Date

Approved by: _____ _____ _____

Name Signature Date

Removal Control No.: _____

Released by: _____ _____ _____

Name Signature Date

Transport by: _____ _____ _____
Name Signature Date

Received by: _____ _____ _____
Name Signature Date

Additional Information: _____
_____
_____

7.5. Sample Damage Assessment Sheet

<<Include the name of the public institution >> Damage assessment Sheet

Salvage Control No.: _____

Location/ Work Area: _____

Quantity: _____

Item Type: _____

Model and Serial No: _____

Asset Reference Number: _____

Condition: ☐ Recoverable ☐ Total Loss ☐ Unknown

Destination: _____

Asset Removal Sheet Ref:
_____

Prepared by: _____ _____ _____
Name Signature Date

Reviewed by: _____ _____ _____
Name Signature Date

Approved by: _____ _____ _____
Name Signature Date

7.6. Sample application list form

a summary of the different applications, respective hosting server, backup procedure

Application	Description	Server Name	Backup/ Redundancy	Supported By(Internal/Third Party Vendor)

7.7. Application RTO an RPO sample form

a summary of the different information system which are used intensively by the business at the Institution

Application	Description and Purpose	Outage Impact (High, Medium, Low)	Department	RTO	RPO
SunSystems	Financial management Reporting (debtors, management account, local sales) Cheque printing Archiving	**High -** Unable to generate financial statements	Finance and accounts	4 hours	3 hours

7.8. Test Result Sample Form

Index 7.8: Test Results Sample Form

<<INSERT ORGANIZATION'S LOGO & NAME>>

Disaster recovery tests

Date: _____ Office/Location: _____

Data loss and backup recovery				
Ref.	Task	Result	Performed by	Sign off
1.	How long did the recovery process take?			
2.	Where RPO and RTO objectives met?			
3.	What unexpected issues hindered the recovery process if any			
4.	What improvements could be made to speedup recovery?			

Failed backups				
Ref.	Task	Results	Performed by	Sign off
1.	<<outline steps performed in performing backup from the secondary site>>			
2.				

Onsite threats and physical dangers				
Ref.	Task	Results	Performed by	Sign off
1.	Test evacuation drills in case of fire			
2.	Emergence procedures in case of natural disasters eg. Pandemic disease, earthquakes			
3.	Call tree tests			

Workforce interruptions				
Ref.	Task	Results	Performed by	Sign off
1.	Testing IT systems & platforms that facilitate remote work			
2.	Testing the procedures that will help to maintain critical operations			
3.	Testing the business's ability to relocate operations			

Utility Outages				
Ref.	Task	Results	Performed by	Sign off
1.	Assessing whether the outage eg. electric power is localized to the building or widespread.			
2.	Communication with the utility provider to report the outage			
3.	Inspection of backup power sources, if deployed, to ensure they're working properly			

Hardware failure				
Ref.	Task	Results	Time Frame	Sign off
1.	Does hardware need replacement?			
2.	How fast was the new equipment deployed?			
3.	Are there vendor relationships that can ensure same-day replacement?			
4.	How did efficient was the new deployed equipment?			

Network interruption outages				
Ref.	Task	Results	Time Frame	Sign off
1.	Testing for unexpected surges in network traffic			
2.	Mock tests that replicate the effects of a crippling network attack			
3.	Network health testing that identifies potential problems in specific parts of the network			
4.	Readiness tests that ensure that IT teams are able to rapidly respond			