



Republic of Zambia
Office of the President
Electronic Government Division

PUBLIC SERVICE INFORMATION COMMUNICATION
TECHNOLOGY STANDARDS

Business Continuity Plan and Disaster Recovery Guidelines

1st edition 2019
© e-Government Division 2019

Foreword

The Electronic Government (e-Government) Division is responsible for formulating and enforcing standards in Information and Communication Technology (ICT) across all Ministries, Provinces and Spending Agencies (MPSAs) to facilitate the transition into a Digital Society. In view of its mandate, the e-Government Division has developed the Public Service ICT Business Continuity and Disaster Recovery Guidelines (BCDRG) to formulate procedures for Government information, applications, ICT equipment and network infrastructure.

In demonstrating Government's commitment to improving service delivery through ICTs and in providing leadership, the e-Government Division in collaboration with various stakeholders coordinated the development of the BCDRG. The guidelines will provide the means for the continuity of services provided to the Public if a disaster occurs in the Public Service.

The BCDRG shall be enforced with other existing legislation, Public Service management policies, audit procedures and Standards, administrative circulars and instructions issued by the relevant authorities.

Repercussions for violating any of the clauses specified in the guidelines shall be given in accordance with the regulations provided in Government of the Republic of Zambia (GRZ) instructions and any other law(s) that may be enacted.

I urge all MPSAs to invest in Business Continuity and Disaster Recovery Systems as they are a

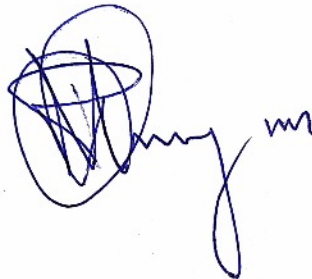


Martine G. Mtonga (Dr.)
National Coordinator
SMART Zambia Institute

Acknowledgment

The development of the Public Service ICT Business Continuity and Disaster Recovery Guidelines recognizes the need to ensure uninterrupted services by utilising ICTs that will make service delivery more friendly, convenient, transparent, efficient and cost effective. The guidelines will assist Government to guarantee availability of public services through ensuring that no major disruptions in service delivery are experienced and that ICT resources are quickly restored in the event of a disaster thereby enhancing the coordinated and collaborative approach to implementation of several initiatives under the e-Government programme.

It is for this reason that I wish to commend the e-Government Standards Task Team, Heads of ICT in Ministries, Provinces and other Spending Agencies (MPSAs) and various stakeholders for their unwavering efforts in the development of the ICT Business Continuity and Disaster Recovery Guidelines. The document will ensure that ICT resources are implemented in an effective and standardised manner.

A handwritten signature in blue ink, consisting of a large, circular scribble followed by a series of loops and a small flourish at the end.

Percive Chinyama (Mr.)
Director, Standards
SMART Zambia Institute

Table of Contents

Foreword	i
Acknowledgment	ii
Working Definitions	v
Abbreviations and Acronyms	vii
CHAPTER 1	1
1.0 Introduction	1
1.1 Objectives.....	1
1.2 Scope.....	2
CHAPTER 2	3
2.0 Guideline Statement	3
2.1 Business Continuity and Disaster Recovery Plan	3
2.2 Incident Declaration and Reporting.....	3
2.3 Disaster Recovery and Testing.....	4
CHAPTER 3	5
3.0 Communication	5
3.1 Staff Communications	5
CHAPTER 4	6
4.0 Administrative Process	6
4.1 Recovery Strategy.....	6
4.2 Service Desk	6
4.3 Public Relations	6
4.4 Funding.....	7
4.5 ICT Infrastructure and Data Loss Insurance	7
CHAPTER 5	8
5.0 Team Members' Roles and Responsibilities	8
5.1 MPSAs Level Teams	8
5.2 National Level Teams	8
5.3 Public Sector CERT.....	8
APPENDIX	10

(A) Business Continuity Plan – MPSA Template	10
(B) MPSAS Organizational Chart.....	25
(C) Disaster Impact Assessment:.....	26

Working Definitions

Applications: Also referred to as an application program or application software is a computer software package that performs a specific function directly for an end user or even another application.

Business Continuity (BC): Ongoing process to ensure that necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

Critical Information: Refers to information that is critical to the success of a particular domain area of an institution.

Critical Database: Refers to a database that contains data that is critical to the business operations of an institution.

Disaster Recovery: This is a process of restoring to original status, damaged infrastructure, in this case ICT infrastructure, after a disaster.

Email: This is a computer service used for sending and receiving messages electronically over computer networks. An email user will be identified on the network by an email address with which he sends and receives messages.

Government Information: Key information that is of strategic significance to the Government as a whole.

Help and Service Desk: Is the communications center that provides a single point of contact between the provider of a service and the end user. Critical Business Function.

Network Infrastructure: Is the hardware and software resources of an entire enterprise network that provides the communication path and services between users, processes, applications, services and external networks or the internet.

Recovery Time Objective: Is the targeted duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity.

Risk Management: This is a process that includes identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected.

Stakeholders: A person or institution with an interest and can affect or be affected by the institution's actions.

Security Incident: In information operations, it is an assessed event of attempted unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Abbreviations and Acronyms

BCDR	Business continuity and Disaster Recovery
BCM	Business Continuity Manager
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
DR	Disaster Recovery
GRZ	Government of the Republic of Zambia
ICT	Information and Communication Technology
ID	Identity
IP	Internet Protocol
IR	Information Resource
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
MPSA	Ministry Province and Spending MPSAs
PC	Personal Computer
PDA	Personal Digital Assistant
QoS	Quality of Service
RACI	Responsible Accountable Consulted and Informed
RTO	Real Time Objective
SMS	Service Management System
SPOC	Single Point of Contact

Document Information

File Name	Public Service Business Continuity and Disaster Recovery Guidelines
Document Description	Provides compliance requirements for Guidelines Governing Business Continuity and Disaster Recovery, in Government
Original Authors	ICT Standards Technical Task Team
Creation Date	August, 2018
Last Update	None
Report Number	1
Version	Version 1.0 (F)

Document Approval

NAME (SZI STANDARDS REVIEW COMMITTEE)	TITLE	DATE
Dr. Martine G. Mtonga	National Coordinator	
Mr. Percive Chinyama	Director - Standards	

Document Distribution

NAME	TITLE	ORGANISATION
Dr. Martine G. Mtonga	National Coordinator	SMART Zambia
Mr. Percive Chinyama	Director - Standards	SMART Zambia
Mr. Milner Makuni	Director - EGovernment	SMART Zambia
Stakeholders	Directors and Managers	MOCT and ZICTA All
Heads of ICT	Heads of ICT	All MPSAs

Document History/Record of Updates

DATE	AUTHOR/S	VERSION	DESCRIPTION
August, 2018	ICT Standards Technical Task Team	Issue 1.0 (F)	Produced by SZI

CHAPTER 1

1.0 Introduction

The Government and its citizens expect that critical government services will continue to function in the event of a disruption or major disaster. The Ministries, Provinces and Spending Agencies (MPSAs) are exposed to potential risks that could disrupt or destroy critical business functions and/or service delivery. The guidelines have been developed in support of a comprehensive programme for Government business continuity, disaster recovery, and overall business sustainability.

The guidelines outline Government's strategy to plan and respond to a major crisis to ensure:

- a) Public service functions and services continue to operate as near to normal performance as possible; and
- b) That MPSAs can respond effectively to a disruption and restore essential services to the public as quickly as possible.

1.1 Objectives

The objective of this document is to provide guidelines for the recovery of ICT systems and services within the set 'Recovery Time Objective' (RTO). In view of attaining this objective, MPSAs shall ensure that:

- a) Sufficient resilience is in place for critical services;
- b) An up to date continuity plan reflects current business requirements;
- c) Internal and external parties have the 'Responsible, Accountable, Consulted and Informed' (RACI) Matrix in the Continuity Plan;
- d) Business critical information is available to the business in line with minimum required service levels; and
- e) Service continuity tests have verified the effectiveness of the plan.

1.2 Scope

This document provides Business Continuity and Disaster Recovery Guidelines for MPSAs.

The guidelines and procedures contained in this document shall accordingly apply to all MPSAs' employees, contractors and consultants in relation to GRZ system continuity and Disaster Recovery.

The Business Continuity and Disaster Recovery Guidelines will also apply to all Public ICT systems currently in existence and to any new business systems that will be acquired in future, at all levels of sensitivity, whether maintained in-house or commercially.

CHAPTER 2

2.0 Guideline Statement

The following guideline statements describe the requirements to be complied with by the MPSAs at all times:

2.1 Business Continuity and Disaster Recovery Plan

All MPSAs shall prepare a **Business Continuity and Disaster Recovery** (BCDR) Plan for approval by the responsible officer. The plan will include requirements for disaster management including mitigation, preparedness, response and recovery measures. See Appendix B.

2.2 Incident Declaration and Reporting

In an event of an ICT incident the following will be undertaken:

- a) Users shall report to the ICT unit;
- b) The ICT unit shall undertake an assessment to determine the extent and severity of the incident;
- c) The ICT unit shall notify the responsible Officer and the Head of the Institution;
- d) The internal disaster recovery team at the MPSAs shall attempt to restore the services;
- e) If the restoration fails, the e-Government Division shall be notified through the office of the responsible Officer and the Head of the Institution;
- f) In response to the notification, the e—Government Division shall trigger appropriate actions to avert the incident; and
- g) The e-Government Division shall determine when an ICT incidence is a disaster or not and report accordingly to the relevant authorities.

2.3 Disaster Recovery and Testing

All MPSAs should consistently perform functional disaster recovery tests for all systems that support critical business functions. The individual MPSA's functional disaster recovery testing verifies whether the MPSA can recover systems to meet the two key recovery objectives outlined below:

- a) Recovery time - the target time required for the recovery of an ICT system after a disruption.
- b) Recovery point - the point in time to which an MPSA must restore the systems, services and data after a disruption, for example, restoring data to the end of the previous day's processing.

The MPSAs in collaboration with the e-Government Division and /or solution providers, shall provide adequate training to staff with specific disaster recovery roles and responsibilities to equip them with the requisite knowledge and skills needed to manage the recovery of a system after a disruption. Active participation in disaster recovery tests and theoretical training is a key tool for developing staff skills and experience.

MPSAs that have outsourced some services to other service suppliers and vendors shall ensure that these partners provide a full and rapid recovery of systems.

CHAPTER 3

3.0 Communication

During a crisis situation, communication with all affected parties – from staff to citizens to media – is vital. The information provided to all audiences must be accurate and timely taking into consideration the possible impacts of such disclosure. The responsible officers in MPSAs shall issue notifications to relevant stakeholders to improve appropriate public response to future emergencies and disasters through education and awareness programmes.

Any estimate of the timing to return to normal working operations should be announced with care. It is also very important that only authorised personnel deal with media inquiries.

3.1 Staff Communications

If a member of staff learns of a potential disaster, the employee should immediately contact the Head of ICT or the officer in Charge of BCDR. Once a crisis has occurred, the following chart and plan section will be used to communicate with all parties:

A normal service outage shall be announced by the service desk team of the MPSA after the responsible officer has been notified using the following media;

- a) SMS to designated recipients;
- b) Email to designated recipients;
- c) Emergency meeting;
- d) Phone to designated recipients; and
- e) Social media with appropriate controls.

A critical outage shall be announced by designated service desk team members to approved contacts, to contact designated recipients. The MPSAs will then communicate to the e-Government Division Help and Service Desk located at the e-Government Division using the appropriate media as outlined in the Service Charter.

CHAPTER 4

4.0 Administrative Process

The administrative process shall consist of the segments listed below;

4.1 Recovery Strategy

The e-Government Division shall provide a guide for MPSAs Disaster Recovery Strategy and Business Continuity Plan that shall be communicated to the various government agencies and shall validate the MPSA's strategy.

Individual MPSAs shall develop a detailed and comprehensive Business Continuity Plan and Disaster Recovery plan for each critical business function and or office location. Reference is made to the Business Continuity Plan and Disaster Recovery Templates provided by the e-Government Division.

4.2 Service Desk

The ICT Service Desk shall be a primary point of engagement between users and an ICT department. It should be kept informed of user's day-to-day issues relating to ICT. The service desk manages incidents (service disruptions) and service requests (routine service-related tasks) along with handling user communications for things like outages and planned changes to services. The ICT service desk has a broad scope and is designed to provide the user with a single place to go for all their ICT needs.

The guideline requires establishment of a help/service desk at MPSA level to handle queries for the various MPSAs.

4.3 Public Relations

The designated spokesperson will develop an official statement for relevant stakeholders. Depending upon the type and severity of the event, the statement may be issued in the following ways:

- a) Through local media i.e. Radio, Print, TV, etc;

- b) Scheduled citizens may be called or e-mailed and or
- c) Notice may be posted at the affected facility(ies).

The spokesperson shall provide for timely, accurate and coordinated public information during a multi-MPSAs crisis.

4.4 Funding

The MPSAs shall make provision for allocation of resources according to their BCDR plans. The e-Government Division shall be responsible for making provision for resources for backup and recovery for critical disasters on common ICT platforms. Resources shall also be accessed from the Disaster Management and Mitigation Unit (DMMU) when a critical ICT system disruption has been declared as a National disaster.

4.5 ICT Infrastructure and Data Loss Insurance

All MPSAs shall take out insurance for the critical ICT Infrastructure and data to minimise eventual huge costs in case of a disaster. They shall ensure a cost-benefit analysis is conducted based on a risk assessment report.

CHAPTER 5

5.0 Team Members' Roles and Responsibilities

A key part of any MPSA's response to a disruption is providing the necessary resources for the Institution to continue delivering critical business functions.

5.1 MPSAs Level Teams

At MPSA level two teams shall be formed as detailed below:

a) Business Continuity Plan Coordination Team

This team is responsible for drafting and finalising the MPSA's BCDR Plan. This includes developing a BCDR work plan outlining the steps necessary to draft the plan and ensuring that each step is completed.

b) Business Continuity Plan Response Team

This team is responsible for responding in the event of a disaster. This includes assessing potential disaster to the MPSA's ICT systems and enacting the MPSAs Business Continuity and Disaster Recovery Standards. This also includes taking lead responsibility for ensuring that the MPSA can function effectively during a crisis and can resume business operations as quickly as possible.

The members and roles of these two teams are outlined in the Business Continuity and Disaster Recovery Templates at annex B.

5.2 National Level Teams

At National level the Public Sector Computer Emergency Response Team (CERT) shall be responsible for coordinating Business Continuity and Disaster Recovery.

5.3 Public Sector CERT

This team is responsible for:

- a) Assessing potential damage to the MPSA's ICT systems and enacting the MPSAs Business Continuity and Disaster Recovery Standards;

- b) Ensuring that the MPSAs can function effectively during a crisis and can resume business operations as quickly as possible;
- c) Serving as a trusted focal point for coordinating computer incidences and disasters;
- d) Developing a capability to support incident reporting;
- e) Developing an infrastructure for coordinating responses;
- f) Participating in Cyber Watch functions;
- g) Helping MPSAs develop their own incident management capabilities;
- h) Facilitating Cyber drills and Exercises in the Public Service;
- i) Making security best practices & guidance available to MPSAs; and

APPENDIX

(A) *Business Continuity Plan – MPSA Template*

Business Continuity and Disaster Recovery Plan

Template for MPSAs

Provided by e-Government Division

(Table of Contents)

[This document provides an example of a business continuity and Disaster Recovery plan for MPSAs]

I. INTRODUCTION

A. Purpose of the Plan

The plan is designed to help MPSAs recover from a disruption in service. Specifically, this plan provides policy and guidance to ensure that the **[MPSA Name]** can respond effectively to a disruption and restore essential services to the public as quickly as possible.

B. Objectives of this Plan

The objectives of this Business Continuity Plan are to:

- Identify advanced arrangements and procedures that will enable **[MPSA Name]** to respond quickly to an emergency event and ensure continuous performance of critical business functions.
- Protect essential Government information, applications, ICT equipment, and network infrastructure.
- Reduce and mitigate disruptions to business operations.
- Identify teams which would need to respond to a crisis and describe specific responsibilities.
- Facilitate effective decision-making to ensure that **[MPSA Name]** operations are restored in a timely manner.
- Identify alternative courses of action to minimise and/or mitigate the effects of the crisis and shorten **[MPSA Name]** response time.
- Quantify the impact of any kind of emergency in terms of money, time, services, and work force.
- Recover quickly from an emergency and resume full service to the public in a timely manner.

C. Authority for this Plan

The Plan will be enforced by the Permanent Secretary or CEO of the MPSAs and all functional departments/units will be required to adhere to the contents of the plan.

II. [MPSA Name] OPERATIONS

A. [MPSA Name] Mission and Key Activities

Mission:

XXX [Insert as applicable]

Key MPSAs activities include:

- XXX [Insert as applicable]
- XXX [Insert as applicable]

B. Team Roles & Responsibilities

BCDR Sponsor: XXX [Insert as applicable]

BCDR Coordinator: XXX [Insert as applicable]

The MPSAs have created two business continuity and disaster recovery teams:

- BCDR Coordination Team
- BCDR Response Team

For emergency contact information for members of all teams, see separate calling tree lists.

BCDR Coordination Team

This team is responsible for drafting and finalising the MPSAs Business Continuity Plan. This includes developing a BCDR work plan outlining the steps necessary to draft the plan and ensuring that each step is completed. This team will finalise the questions to be asked as part of the Business Impact Analysis (BIA) process. Each team member will fill out a BIA

questionnaire and will also assign staff within his/her own division to answer BIA questions, as necessary. This team will meet periodically to review BCDR progress, will revise work plan as necessary, and will edit and approve the final plan.

	<i>Team Members</i>	<i>Role / Responsibilities</i>	<i>Contact Information</i>
1.	BCDR Coordinator Permanent	Draft work plan necessary to develop the BCDR. Draft BIA questions for staff to answer. Conduct interviews with all staff members. Compile information and draft BCDR.	work phone
2.	BCDR Sponsor Deputy Director	Assist Coordinator to draft BCDR work plan and draft BIA questionnaire. Complete BIA questionnaire. Assign other staff as necessary to complete BCDR. Send out periodic emails to all staff providing project updates.	work phone
3.	PSA Director	Review and approve initial BIA questionnaire. Review work product throughout BCDR. Send out occasional emails to all MPSAs staff underscoring importance of project thanking staff for their work on developing BCDR.	work phone
4.	Designated Spokesperson/PRO	Review on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for completing communications section of plan.	work phone
5.	Head ICT	Review on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for drafting Business Continuity and Disaster Recovery Plan.	work phone

6.	Field Manager/ICT Officer/Sub-Sector Representative	Review on-going work as member of this team. Complete BIA questionnaire and identify staff needed to complete specific tasks. Has primary responsibility for drafting recovery steps for field office section of the plan.	work phone
7.	Consultant	Has lead responsibilities for ICT systems service provision through a contract or a SLA.	work phone

BCDR Response Team

This team is responsible for responding in the event of a disaster. This includes assessing potential damage to the MPSAs ICT Infrastructure and enacting the MPSAs' Coordinating Center. This also includes taking lead responsibility for ensuring that the MPSA can function effectively during a crisis and can resume business operations as quickly as possible.

	<i>Team Members</i>	<i>Role / Responsibilities</i>	<i>Contact Information</i>
1	MPSA Director	Determine if event is severe enough that BCDR should be enacted. Operates from the MPSA Coordination Center. Initiates call tree process of contacting all staff.	work phone
2	BCDR Sponsor Deputy Director	Acts as back-up to MPSA director if director is unavailable.	work phone
4	Designated Spokesperson / PRO	Has lead responsibility for implementing communications strategy contained in this plan.	work phone
5	BCDR Coordinator	Has lead responsibility for ensuring that BCDR is properly enacted and steps are followed as appropriate.	work phone
6	Head ICT	Conducts initial assessment ICT for MPSA following the event. Has lead responsibility for implementing sections of plan dealing with of ICT and network elements.	work phone

7	Contracts and Procurement Manager	Has lead responsibility for dealing directly with vendors and suppliers of ICT equipment	work phone
8	Field Manager, ICT Officer/Sub-Sector Representative	Has lead responsibility for implementing plan as it relates to field office.	work phone
9	Consultants	Has lead responsibilities for ICT systems service provision.	work phone

C. Plan Activation Procedures

The ability to execute this plan following an event with little or no warning will depend on the severity of the emergency and the number of MPSAs systems that have been affected by the incidence.

D. Identification of Potential Disaster Status

Criteria for determining whether a particular emergency situation requires that emergency actions be taken or the BCDR be enacted include:

- Is there an actual or potential loss of ICT infrastructure/network?
- Is there an actual or potential loss of critical data?
- XXXX [Insert as applicable]
- XXXX [Insert as applicable]

E. Direction and Control

[Explanation: During a disaster/disruption, it is imperative to have a clear chain of command and delegation of authority. Describe the chain of command and authority that will exist during an event. NOTE: insert organizational charts to explain the chain of command.]

- Lines of succession will be maintained by all senior officers reporting to the MPSAs Director to ensure continuity of essential functions. If possible, successions should be provided to a depth of at least three staff where policy and directional functions are involved.

- The MPSAs Director or designated back-up (successor) may order activation of the MPSAs business continuity plan.
- See Appendix **XXX [Insert as applicable]** for Delegations of Authority and the MPSAs organizational chart.

F. Communications Plan

During a crisis situation, communication with all affected parties – from staff to citizens through various media is vital. The information provided to all audiences must be accurate and timely.

In particular, any estimate of the timing to return to normal working operations should be announced with care. It is also very important that only authorised personnel deal with media inquiries.

G. Citizens Contact:

The Communication Manager or designee will develop an official statement to the citizens. Depending upon the type and severity of the event, the statement may be issued in the following ways:

- a) Through SMS notification
- b) Staff/citizen(s) may be called or e-mailed
- c) Through local media
- d) Notice may be posted at the affected facility(ies)

The MPSAs Director may direct callers to the MPSAs web site (if available) for additional information and updates.

H. Management and Staff Contact:

The MPSAs Director or designee will develop an official statement for Head of ICT and staff. In general, the employee call tree involves the following:

- MPSAs Director calls:
 - Head of ICT
 - Communications Manager ●
 - XXXX [Insert as applicable]**

- XXXX [Insert as applicable]

Media Contact:

Once an event occurs, the Communications Manager will develop official “public statements” to respond to questions frequently asked by the media and the public. The communications director will provide these statements to the MPSAs Director or designee for review and approval before providing the statements to any external parties.

The Communications Manager will develop statements to respond to the following questions:

- What happened?
- When did it happen?
- How is state government affected by this incident?
- What corrective measures are being taken to ensure that this doesn’t happen again?
- How will this event affect the MPSAs’ service to the public?

Depending on the nature of the crisis, determine if a technical expert or a public official with specific jurisdiction is required to provide clarity to the situation and/or disseminate information to the media.

III. CRITICAL BUSINESS FUNCTIONS

[Explanation: Provide the following information for each of the MPSAs’ identified Critical Business Functions (CBFs).]

A. CBF #1 – XXX [Insert as applicable]

1. Description of Business Function

2. Recovery Time Objective (RTO)

XXX [Insert as applicable]

3. Priority Level (relative to other business functions) - 1

4. Key Staff

XXX [Insert as applicable]

5. Key processes

#	<i>Business Processes</i>	<i>Point of contact and contact information</i>	<i>Recovery priority and rationale</i>

6. Key Dependencies

#	<i>Upon which activities is this business process dependent?</i>	<i>Point of contact and contact information</i>	<i>Recovery Time Objective for the dependency</i>

7. Vital Records

<i>Description</i>	<i>Where</i>	<i>Contact</i>

8. ICT INFRASTRUCTURE TO AID DISASTER RECOVERY

In order to execute this business function, the following minimum facilities are

<i>Description</i>	<i>Where</i>	<i>Contact</i>

B. CBF #2 –

XXXXX [Insert as applicable]

IV. RECOVERY PLAN

This section includes the MPSAs plan to ensure continuity of operations in case the MPSA’s ICT function is not available. Examples might include:

1. A breach has occurred in the network and the server has been shut down due to a computer virus or any other security breach
2. The server gives out and must be replaced
3. WAN malfunction

A. Recovery Procedure

The recovery procedure consists of

- 1.XXXXX
- 2.XXXXX
- 3.XXXXX

The recovery procedure depends upon the length of time the ICT system is anticipated to be out. If it is anticipated that restoration will take place in two days or less, processes that do not require the affected ICT systems shall be completed manually. If it is anticipated that failure will exceed two days, manual procedures manual procedures shall be implemented until computer systems become available.

When computer systems are available, all business processes will continue as normal, and all manual/paperwork will need to be recorded in the systems retroactively.

Dependencies

This plan is dependent upon having the designated backup data center, XXXX, XXX & XXXX **[Insert as applicable]**

Recovery Steps – Summary

- Step 1 – Contact BCDR Response Team and arrange for a meeting.
- Step 2 – BCDR Response Team meets and reviews plan steps.
- Step 3 – Assess damage to ICT infrastructure, ICT functionality or data
- Step 4 – Contact ICT and determine when ICT services will be available.

- Step 5 – Contact staff/citizens, etc. and inform them of possible delays.
- Step 6 – Establish communication with staff/citizens for alternative solution for business process(es)
- Step 7 – Announce alternative business process(es) solutions to media outlets.
- Step 8 – Notify and update citizens as systems become available.
- Step 9 – Resume normal operations.

Recovery Steps - Detail

<i>Step #</i>	<i>Step</i>	<i>Step Detail</i>	<i>Additional Resources</i>	<i>Responsibility</i>	<i>Date Completed</i>
1	Contact BCDR Response Team members and arrange for a meeting	Contact team members and arrange a meeting.	Telephone BCDR Response Team contact information	BCDR Coordinator Back up: - BCDR Sponsor - Head ICT	
2	BCDR Response Team meets and reviews plan steps; activates recovery process	Meet with BCDR Response Team members and assess the situation. Review the plan and determine whether or not all steps need to be taken. Based on the situation, do other steps need to be implemented? If so,	Meeting location Telephone	BCDR Sponsor Back up: - BCDR Coordinator - Head ICT	

<i>Step #</i>	<i>Step</i>	<i>Step Detail</i>	<i>Additional Resources</i>	<i>Responsibility</i>	<i>Date Completed</i>
		assign responsibility.			
3	Assess damage to MPSAs ICT Infrastructure and data	Walk through MPSAs ICT System, if possible. assess extent of damage to the equipment. (See Appendix	Telephone	Head ICT Back up: - BCDR Sponsor -MPSAs Director	
4	Prepare DR Site to take over ICT Systems operations	Arrange the details of how and when to relocate equipment or systems or activation of systems at DR	DR Site	Head ICT Back up: - BCDR Sponsor - MPSAs Director	
5	Review operating procedures	Ensure that all required equipment and software is present and in working order. Ensure all required support supplies are present.		Head ICT Back up: - BCDR Sponsor - MPSAs Director	
6	Contact staff/citizens, equipment, vendors, etc. to inform them of possible	Contact citizens and notify them of MPSAs ICT system switch to DR and Inform	Citizen Contact Information Telephone	Communications Manager Back up: - BCDR Sponsor -Head ICT	

<i>Step #</i>	<i>Step</i>	<i>Step Detail</i>	<i>Additional Resources</i>	<i>Responsibility</i>	<i>Date Completed</i>
		staff/citizens of possible service delays.			
7	Notify and update users as systems become	Maintain communication with outside users to update them of systems status. Update staff and users as systems become	ICT system access	Communications Manager Back up: - BCDR Sponsor - BCDR Coordinator	
8	Resume Normal Operations	When all systems have been restored, resume normal	ICT System	MPSAs Director Back up: - BCDR Sponsor - Head ICT	

(B) MPSAS Organizational Chart

**(This chart can be used to show delegation of authority or
MPSAs can insert separate chart showing lines of
authority.)**

(C) Disaster Impact Assessment:

[Explanation: This table is intended for completion during a disaster or disruption in order to assist you in assessing the impact of the event upon each of your critical business functions. This table should be left blank during the plan writing and used only during the disaster. Please note that in this table we are interested in outage estimates rather than recovery time objectives.]

DESCRIPTION OF DISASTER/DISRUPTION:

DATE:			DATE Response TEAM MOBILIZED:					
BUSINESS								
FUNCTION NUMBER	BUSINESS FUNCTION	STATUS LEVEL (SEE TABLE BELOW)					ASSESSMENT CARRIED OUT BY	COMMENTS
		1	2	3	4	5		

THE FOLLOWING STATUS LEVELS SHOULD BE APPLIED:

LEVEL	DESCRIPTION
1	Is likely to seriously affect normal business operations for over four weeks
2	Is likely to seriously affect normal business operations between one and four weeks
3	Is likely to seriously affect normal business operations for over a week
4	Is likely to seriously affect normal business operations for less than one week
5	Is likely to seriously affect normal business operations for less than two days

