dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

STRATEGIC SUPPORT SERVICES

3rd Floor Tirelo Building
Albert Luthuli Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 381 9186/9189
Fax: +27 (18) 200 8001

CONTROL SHEET FOR TRACKING DOCUMENTATION:

ISSUE / REF NR.		**FILE NO.**		
SUBJECT FOR ATTENTION	**TABLE OF CHANGES TO THE ICT CONTINUITY PLAN**			
POSITION	**NAME**	**SIGNATURE**	**DATE OUT**	**DATE BACK**
DIRECTOR SSS	**Mr. S Matlhako**		11/02/2020	
DECISION/ COMMENTS				
POSITION	**NAME**	**SIGNATURE**	**DATE OUT**	**DATE BACK**
ICT STEERING COMMITTEE: CHAIRPERSON	**Ms. F Nchoe**		17/02/2020	
DECISION/ COMMENTS				
POSITION	**NAME**	**SIGNATURE**	**DATE OUT**	**DATE BACK**
ICT STRATEGIC COMMITTEE: CHAIRPERSON	**Ms. S Mpolokeng**		17/02/2020	
DECISION/ COMMENTS				
POSITION	**NAME**	**SIGNATURE**	**DATE OUT**	**DATE BACK**
HEAD OF THE DEPARTMENT	**Ms. B Mofokeng**		6/3/2020	
DECISION/ COMMENTS				
POSITION	**NAME**	**SIGNATURE**	**DATE OUT**	**DATE BACK**
ADMINISTRATOR	**Mr. M Mokonyama**			
DECISION/ COMMENTS				

***PLEASE RETURN THE SIGNED CONTROL SHEET BACK TO THE SENDER**

dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

STRATEGIC SUPPORT SERVICES

Tirelo Building
Albert Luthuli Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 200 8001

TO : **ADMINISTRATOR**
MR M. MOKONYAMA

THROUGH : **CHAIRPERSON ICT STEERING COMMITTEE**

CHAIRPERSON ICT STRATEGIC COMMITTEE

HEAD OF DEPARTMENT

FROM : **DEPARTMENTAL INFORMATION TECHNOLOGY OFFICER**
MR S. MATLHAKO

DATE : **10 FEBRUARY 2020**

SUBJECT : **TABLE OF CHANGES TO THE ICT CONTINUITY PLAN**

1. This matter above bears reference.
2. **PURPOSE**

   This communiqué seeks the consideration and recommendation for approval of the ICT Continuity Plan below. This is in accordance with the terms of the Departmental Policy review and internal business changes.

3. The amendments have been effected following inputs called for and received from Departmental ICT Committees and officials, and are included as follows:

3.1 ICT CONTINUITY PLAN (ICTCP-Version 1.4)

POLICY VERSION	HEADING	PARAGRAPH	PAGE	INPUT
	Document name	-	Cover page	ICTCP - VERSION 1.4
	Document Detail	Table 1	(i)	Version change
	Change Records	Table 2	(i)	26-08-2018 Version 1.4 Description of change
	Stakeholder sign-off	Table 3	(i)	Replaced Governance

				Champion
ICTCP - VERSION 1.4	Stakeholder sign-off	Table 3	(i)	Replaced ICT Steering Chairperson
	Records Management Sign–Off	Table 4	(i)	Replacement of Acting Records Manager with Records Manager
	Footer	Footer	All	Version number change
	Glossary of terms	Table	(ii)	Inserted Recovery Point Objective (RPO)
	Glossary of terms	Table	(ii)	Inserted Recovery Time Objective (RTO)
	Business Application Systems Impact Assessment	11	9	Aligned the "Impact" table from 1 to 5
	Business Application Systems Impact Assessment	11	9	Removed "Severity"
	Business Application Systems Impact Assessment	11	10	Aligned the "Likelihood" table from 1 to 5
	Business Application Systems Impact Assessment	11	10	Amended ranking of likelihood and impact table
	Departmental Business Application System	11.1	11-13	Amended ratings on "likelihood" and "severity"
	Version Information & Changes	13.5	21	Amended date of change
	Version Information & Changes	13.5	21	Amended version number
	Version Information & Changes	13.5	21	Inserted reason for review
	Contact Information	13.6.2.1	24	Updated the Disaster recover team table
	Incident report procedure	14	26	Inserted a new statement on Recovery Time

				Objective
	Incident report procedure	14	27	Inserted a new statement on Recovery Point Objective
	Incident report procedure	14	27	Inserted summary of objectives
	Approval	18	28	Updated information

Regards,

Mr S. Matlhako
Departmental Information Technology Officer

11/02/2020
Date

dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Tirelo Building
Albert Luthuli Drive
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 388 3697

ICT STRATEGIC COMMITTEE

TO: **ADMINISTRATOR**
MR M. MOKONYAMA

FROM: **CHAIRPERSON ICT STRATEGIC COMMITTEE**
MS S. MPOLOKENG

DATE: **16 JANUARY 2020**

SUBJECT: **REQUEST FOR APPROVAL OF THE REVIEWED ICT CONTINUITY PLAN**

1. This matter above has reference.

2. PURPOSE

To request the Administrator to approve the reviewed ICT Continuity.

3. BACKGROUND

In the 2018/19 Audit findings, it was found that the ICT Disaster Recovery Plan (DRP) was in place, however it was noted that the plan was not comprehensive due to the following:
"The time objective and recovery point objective as informed by the department Business Impact analysis for Trafman system were not included". Management response on the audit finding was for the Strategic Support Services to review the ICT Continuity plan to include the Recovery point and time objective.

The lack of adequate disaster recovery processes may lead to the Department not being able to successfully restore and/ or recover systems and related data within reasonable timelines and in line with expectations from various lines of business.

Strategic Support Services effected the review the ICT Continuity Plan in order to include the Recovery Point and Time Objective in line with the Audit Action Plan. The plan was circulated to all the Departmental officials for input and later sent to the Departmental Legal Services for legalese.

Further, the plan was presented and shared with the ICT Governance Structures (ICT Steering and Strategic Committee) for input and recommendations. The ICT Governance Structures have engaged on the plan and are satisfied with the content of the plan and the amendments made. At this stage the ICT Strategic Committee is making a recommendation for the approval of the ICT Continuity Plan by the Accounting Officer.

It is against this background that the Administrator is requested to approve the ICT Continuity Plan.

Hope this is in good order.

Regards,

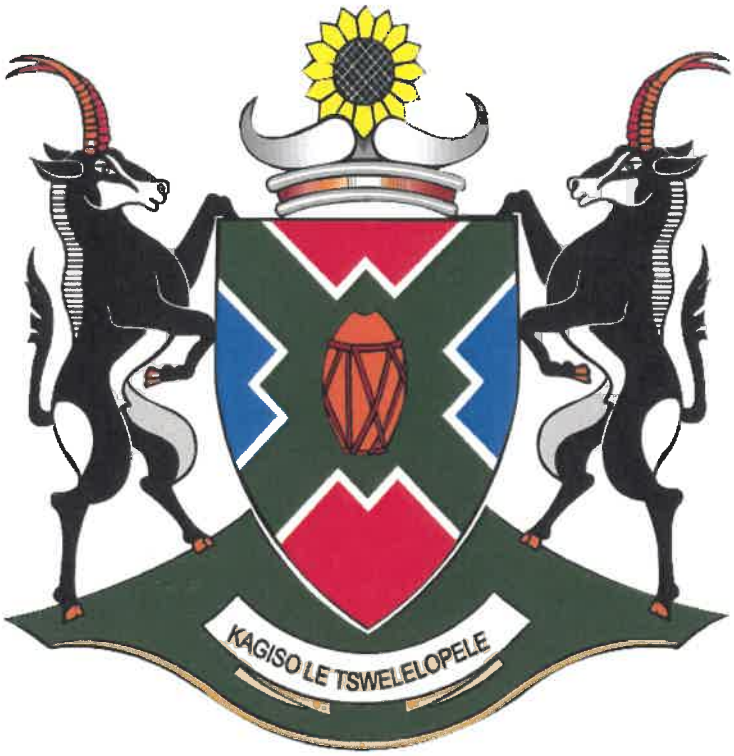
MS. S. MPOLOKENG
CHAIRPERSON ICT STRATEGIC COMMITTEE

17/02/2020
DATE

CC CHAIRPERSON ICT STEERING COMMITTEE

RESTRICTED

DEPARTMENT OF COMMUNITY SAFETY & TRANSPORT MANAGEMENT



INFORMATION AND COMMUNICATION TECHNOLOGY CONTINUITY PLAN

ICTCP-VERSION 1.4

Document Details

Author	Directorate Strategic Support Services
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	ICT Continuity Plan
Sensitivity	Internal Use Only
Effective Date	01 April 2018
Created Date	03-07-2013
Version Date	<Date of Accounting Officer's signature>
Version	ICTCP-VERSION 1.4

Change Record

Modified Date	Author	Version	Description of Changes
26-09-2014	Directorate Strategic Support Services	1.1	Departmental Business Change
31 -03-2016	Directorate Strategic Support Services	1.2	Annual Review
26 – 03 - 2018	Directorate Strategic Support Services	1.3	Annual Review
	Directorate Strategic Support Services	1.4	Review

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer		
Ms F. Nchoe	Chairperson: ICT Steering Committee		17/02/2020
Ms S. Mpolokeng	Chairperson: ICT Strategic Committee & Governance Champion		17/02/2020
Ms M.G. Mothibedi	Departmental Chief Risk Officer		26/02/2020
Mr P. Namate	Director Legal Services		27/02/2020

Records Management Sign–Off

Name	Position	Signature	Date
Ms M. Malatji	Records Manager		04/05/2020

GLOSSARY OF TERMS

AVS	Abnormal Vehicle System
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Assessment
DCS&TM	Department of Community Safety and Transport Management
DITO	Department Information Technology Officer
DR	Disaster Recovery
eNatis	Electronic National Transport Information System
Filr	Software by Novell used for backup and remote access of user information
Accounting Officer	Head of Department
ICT	Information Communication Technology
ICTCP	ICT Continuity Plan
Information Systems	A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.
Information Technology(I.T.)	The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
NWPG	North West Provincial Government
OLAS	Operator License Administration System
Recovery Point Objective (RPO)	Describes the acceptable amount of data loss measured in time.
Recovery Time Objective (RTO)	is the duration of time and a service level within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity
Server	A software program, or the specialised computer on which that program runs, that provides a specific kind of service to client software

	running on the same computer or other computers on a network..
SLA	Service Level Agreements
Trafman	Traffic Fines Management System
Vis Majore	Is an act of God. Results from natural causes such as a hurricane, tornado, or earthquake and without the intervention of human being.

Table of Contents

1. Introduction

This plan is a systematic process to prevent, predict and manage Information Communication Technology (ICT) disruption and incidents which have the potential to disrupt ICT services and is planned to result in a more resilient IT service capability aligned to wider departmental requirements.

ICT Business Continuity describes the daily Information Communication Technology (ICT) activities that are undertaken to enable the department to perform its key functions and deliver its ICT services.

"Business Continuity is the term applied to the series of management processes and integrated plans that maintain the continuity of the critical processes of an organization, should a disruptive event take place which impacts the ability of the organization to continue to provide its key services"- According to ENISA (2008: 8). ICT systems and electronic data are crucial components of the processes and their protection and timely return is of paramount importance.

2. Background

Research indicates that IT Service Continuity evolved from ICT Disaster recovery which began to develop in the mid- to late 1970s as computer centre managers began to recognize the dependence of their organizations on their computer systems. At that time most systems were batch-oriented mainframes which in many cases could be down for a number of days before significant damage would be done to the organization.

In recent years, Information Communication Technology (ICT) has become integral to many of the essential activities carried out by organizations. The advent of the Internet and other electronic networking services together with the current and developing capabilities of systems and applications has also meant that those organizations have become more and more dependent on reliable, safe and secured ICT infrastructures.

At the same time the need for Business Continuity Management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has become steadily more prevalent in developed and developing economies. Failures of supporting

ICT services (including information security issues such as systems intrusion and malware infections) are recognized as having the potential to impact the continuity of business operations.

As a result managing ICT and related continuity and other security aspects forms an essential component of business continuity requirements. In addition it is often the case that critical business functions that require business continuity are usually dependent upon ICT. This dependence means that disruptions to ICT services can constitute strategic risks to the reputation of an organization and its ability to operate effectively.

IT Service Continuity is essential for many organizations in the implementation of Business Continuity Management and Information Security Management. It is also essential as part of the implementation and operation of information security management as well as business continuity management as specified in ISO/IEC 27001:2013 and ISO 22301:2012 respectively.

It is therefore critical to develop and implement continuity for the ICT services to help ensure business continuity.

3. ICT Continuity Goal

To support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities can be resumed with required, and agreed, business timescales. As technology is a core component of most business processes, continued or high availability of ICT services are critical to the survival of the business as a whole. This shall be achieved by introducing risk reduction measures and recovery options.

4. Objectives

- Maintain a set of IT Service Continuity Plan that support the overall Business Continuity Plan (BCPs) of the department.
- Complete regular Business Impact Analysis exercise to ensure that all continuity plans are maintained in line with changing business impact and requirements.

- Conduct regular Risk Analysis and management exercises, particularly in conjunction with the business, the Availability Management and Security management processes, to manage IT services within an agreed level of business risk.
- Provide advice and guidance to all other areas of the business and IT on all continuity and recovery related issues.
- Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets.
- Assess the impact of all changes incurred by the implementation of the IT Service Continuity Plans and Recovery Plans.
- Ensure that proactive measures to improve the availability of services are implemented whenever it is cost – justified to do so.

5. Purpose

The purpose of this plan is to create a conducive environment where IT service Continuity is maintained to sustain Departmental business processes. The effectiveness of this plan shall allow the Department to minimize the adverse effect of emergencies that arise. The department has an ethical obligation to the workforce, and stakeholders to protect the continuing operations of the business.

6. Scope of application

This plan encompasses all IT processes and technology within the departmental environment that supports critical business functions. However, systems hosted at Provincial IT will be catered for in their Continuity Plan. The successful implementation of this depends from commitment of senior management and the support of all departmental officials within all spheres of the department and the respective suppliers.

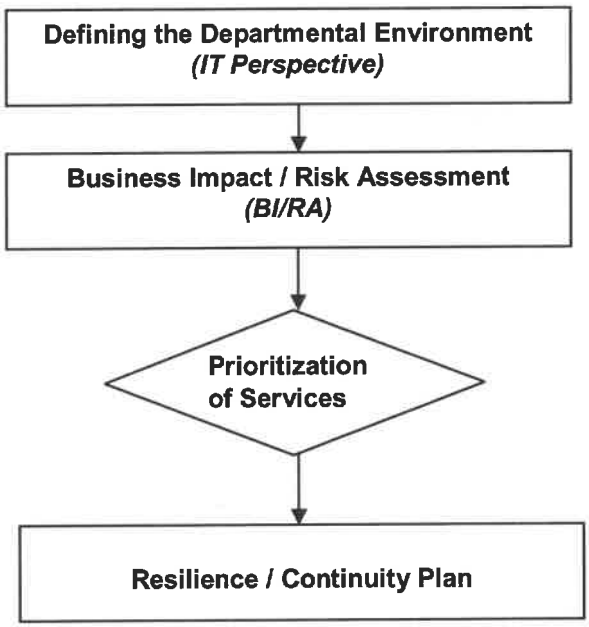
Due to the fragmented nature of the responsibilities over ICT between the Department and Provincial IT, the departmental ICT Continuity Plan focuses on the internal ICT environment, over which the department exercises control. Departmental applications that are hosted at Provincial

IT fall to be included in the ICT Continuity Plan of Provincial IT; it is therefore within the responsibility of Provincial IT to host and/or accommodate departmental systems in their environment as per the signed SLA.

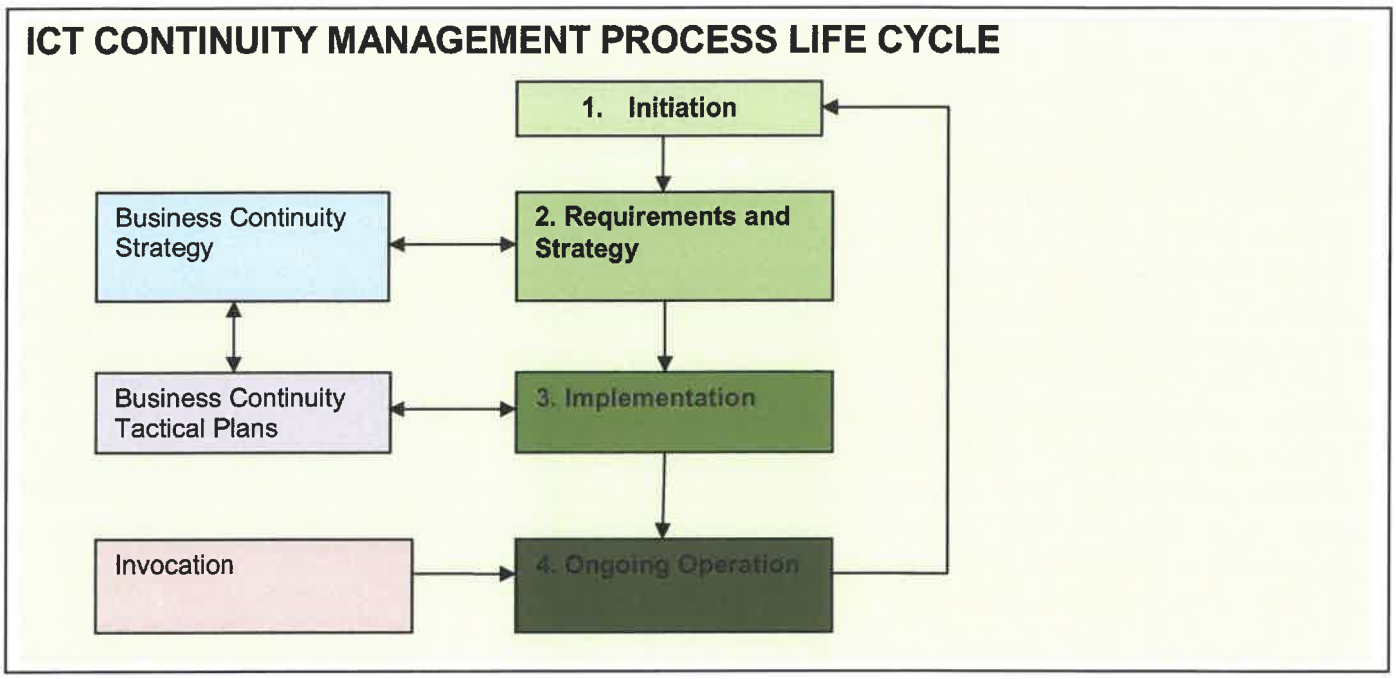
7. ICT Continuity Plan Layout

This plan is based on Impact Awareness method. It shall define the environment, conduct Impact Assessment and Prioritize events according to the business impact and deliver the plan and outline a recovery plan. The plan shall acknowledge the existing departmental policies and strategies.

GENERAL PLAN LAYOUT STRUCTURE/DIAGRAM:



8. ICT Service Continuity Management Process



8.1 Key Activities:

- **Initiation**
  - Policy setting
  - Scope
  - Initiate a project

- **Requirements and Strategy** (Business Continuity Strategy)
  - **Business Impact Analysis (BIA)** - To quantify the impact of loss that IT services would have on business.
  - **Risk Assessment (RA)** - Identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified.
  - **IT Service Continuity Strategy –** Production of overall strategy that must be integrated into Business Continuity Management Strategy. It can produce the two steps identified

above, and is likely to include the elements of risk reduction as well as selection of appropriate and comprehensive recovery options.

- **Implementation** (Business Continuity Tactical Plans)
  - Develop IT Service Continuity Plans
  - Develop IT Plan, Recovery plans and procedures
  - Organization Planning
  - Testing Strategy

- **Ongoing operation** (Invocation)
  - Education (awareness and Training)
  - Review and Audit
  - Testing
  - Change Management

9. Roles and Responsibilities

It is the responsibility of DITO and team to ensure that the aim of IT Service is met. This shall include such tasks and responsibilities as:

- Performing Business Impact Analysis for all existing and new services.
- Implementing and maintaining the ICT continuity process in accordance with the overall requirements of the department's Business Continuity Management process, and representing the IT Services function within the Business Continuity Management process.
- Ensuring that all ICT Continuity plans, risks and activities underpin and align with all BCM plans, risks and activities are capable of meeting the agreed and documented targets under any circumstances.
- Performing Risk assessment and risk management to prevent disasters where cost-justified and where practical.
- Developing and maintaining the department's ICT continuity strategy.

- Assessing the potential service continuity issues and invoking the ICT Service Continuity Plan where necessary.
- Managing the ICT Service Continuity Plan while it is in operation, including fall –over to a secondary location and restoration to the primary location.
- Performing post mortem review of service continuity tests and invocations, and instigating corrective actions where required.
- Developing and managing the ICT continuity plans to ensure that, at all times, the recovery objectives of the business can be achieved.
- Ensuring that all IT service areas are prepared and able to respond to an invocation of the continuity plans, i.e. ensuring readiness and security of the secondary site
- Undertaking regular reviews, at least annually, of the Continuity Plan with the business areas to ensure that they accurately reflect the business needs.
- Defining and managing contracts with providers of third-party recovery services.
- Assessing changes for their impact on Service Continuity and Continuity Plan.

10. Overview of the Departmental Environment in IT Perspective

The department does not own any network infrastructure, as such departmental ICT application systems are housed at Provincial IT. Amongst other services, ICT in the department in terms of network infrastructure is limited to Desktop Support, Management of the Service Level Agreement with Provincial IT, and Configuration Management etc. ICT in the department shall ensure that departmental data is secured from user End-Point and also ensure IT Service Continuity from technical support perspective.

The following are transversal systems which are indirectly referred to in this plan, and shall be managed through Service Level Agreement (SLA):

i) Basic Accounting System (BAS) – Financial System
ii) GroupWise – Email System

iii) PERSAL – Personnel Salary System

iv) Filr – File Backup System

v) Remedy System – Incident Management System

vi) WALKER – Financial System

vii) SharePoint Portal System – M&E Reporting System

viii) Natis –National Traffic Information System

Key Departmental Core Business Application Systems which are also referred to in this plan include:

i) Trafman - Departmental System

ii) VMS – Provincial Treasury System

iii) eNatis - National System

iv) OLAS / RAS – National System

v) AVS – National System

In the event of an incident, the ICT Continuity Plan and all relevant SLAs should ensure a resumption of services. This plan shall indirectly also include departmental data stored in the following formats:

i) Doc(x) – MS Word

ii) Xls(x) – MS Excel

iii) PDF – Acrobat Reader / Adobe

iv) Ppt(x)– MS Power Point

v) Acc(x) - MS Access

vi) Archive Files (email)

11. Business Application Systems Impact Assessment

The above mentioned Business Application System shall be assessed as follows:

Likelihood	Severity				
	Negligible(1)	Minor(2)	Moderate(3)	Major (4)	Extreme (5)
Rare(1)	Low	Low	Low	Low	Medium
Unlikely (2)	Low	Low	Medium	Medium	High
Possible (3)	Low	Medium	Medium	High	High
Likely (4)	Low	Medium	High	High	Very High
Almost certain(5)	Medium	High	High	Very High	Very High

Criteria and Risk categories for the identification and classification of Risk:

IMPACT:

SCORE	RATING	DESCRIPTION
1	Insignificant	Little impact.
2	Minor	No material impact on achievement of the departmental strategies or objectives.
3	Moderate	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.
4	Major	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.
5	Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation.

LIKELIHOOD:

SCORE	RATING	DESCRIPTION
1	Rare	The risk shall probably not occur, i.e. less than once in 100 years. (Probability = 0 -1% p.a.)
2	Unlikely	The risk could occur at least once in the next 10 – 100 years; (Probability = 1 – 10% p.a.)
3	Moderate	The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50 % p.a.)
4	Likely	The risk is almost certain to occur once within the next 12 months. (Probability = 10-50% p.a.)
5	Almost Certain (Common)	The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)

Risk Assessment ratings are the product of likelihood and impact and are ranked as follows:

20-25	Critical
From 15 – 19	Major
From 10- 14	Moderate
From 5 – 9	Minor
From 1 – 4	Insignificant

11.1 Departmental Business Application System:

Location/ Hosting	Departmental ICT System	Type of Loss/ Damage	Likelihood	Severity	Business Impact	Pre-cautions in place
SITA	BAS	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	PERSAL	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	WALKER	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA

Garona Building	GroupWise	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	Remedy	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	Back up system	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	Trafman	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental	SLA

		as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage			plan.	
Road Traffic Management Corporation (RTMC)	eNatis	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA
Garona Building	OLAS	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage	3	5	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	SLA

Other Departmental Data in the format outlined above. *(Within the control of departmental ICT capacity)*

Location/ Hosting	**Departmental ICT System**	**Type of Loss/ Damage**	**Likelihood**	**Severity**	**Business Impact**	**Precautions in place**
Old Parliament Building (NEW)	MS Word, MS Excel, MS PowerPoint, MS Access, PDF, Email	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made*	3	4	Significant impact on achievement of strategic objectives and targets relating to the	Antivirus Software installed on every user's machine. Back up

	Archives	*circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage			departmental plan.	system installed on every user's machine for data backup.
Old Parliament Building (OLD)	MS Word, MS Excel, MS PowerPoint, MS Access, PDF, Email Archives	*Vis majore/ acts of God* such as, lightning, Fire, Flash flood. *Man-made circumstances* such asSoftware/Networ k Failure, and Terrorist attack, Labour unrest, Espionage	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.
Tirelo Building	Word, Excel, PowerPoint, PDF, Email Archives and AVS system	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.
Safety House	Word, Excel, PowerPoint, PDF, Email Archives and AVS system	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure,	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on

		and Terrorist attack, Labour unrest, Espionage				every user's machine for data backup.
Bojanala District	Word, Excel, PowerPoint, PDF, Email Archives	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.
Dr Kenneth Kaunda	Word, Excel, PowerPoint, PDF, Email Archives	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour unrest, Espionage	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.
Dr Ruth Mompati	Word, Excel, PowerPoint, PDF, Email Archives	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software /Network Failure, and Terrorist attack, Labour	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.

		unrest, Espionage				
Ngaka Modiri Molema	Word, Excel, PowerPoint, PDF, Email Archives	*Vis majore/ acts of God* such as lightning, Fire, Flash flood. *Man-made circumstances* such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage	3	4	Significant impact on achievement of strategic objectives and targets relating to the departmental plan.	Antivirus Software installed on every user's machine. Back up system installed on every user's machine for data backup.

11.2 DEPARTMENTAL SERVICE PRIORITY

In the event of limited services, the Department shall prioritize core functions and some key business systems. Following are Departmental business mission critical systems in descending order:

1. Key Business Application System
   - PERSAL
   - WALKER
   - BAS
   - Ms Office Productivity Suite
   - Groupwise

2. Core Business Application Systems
   - Trafman
   - eNaTIS
   - AVS
   - OLAS/RAS
   - VMS

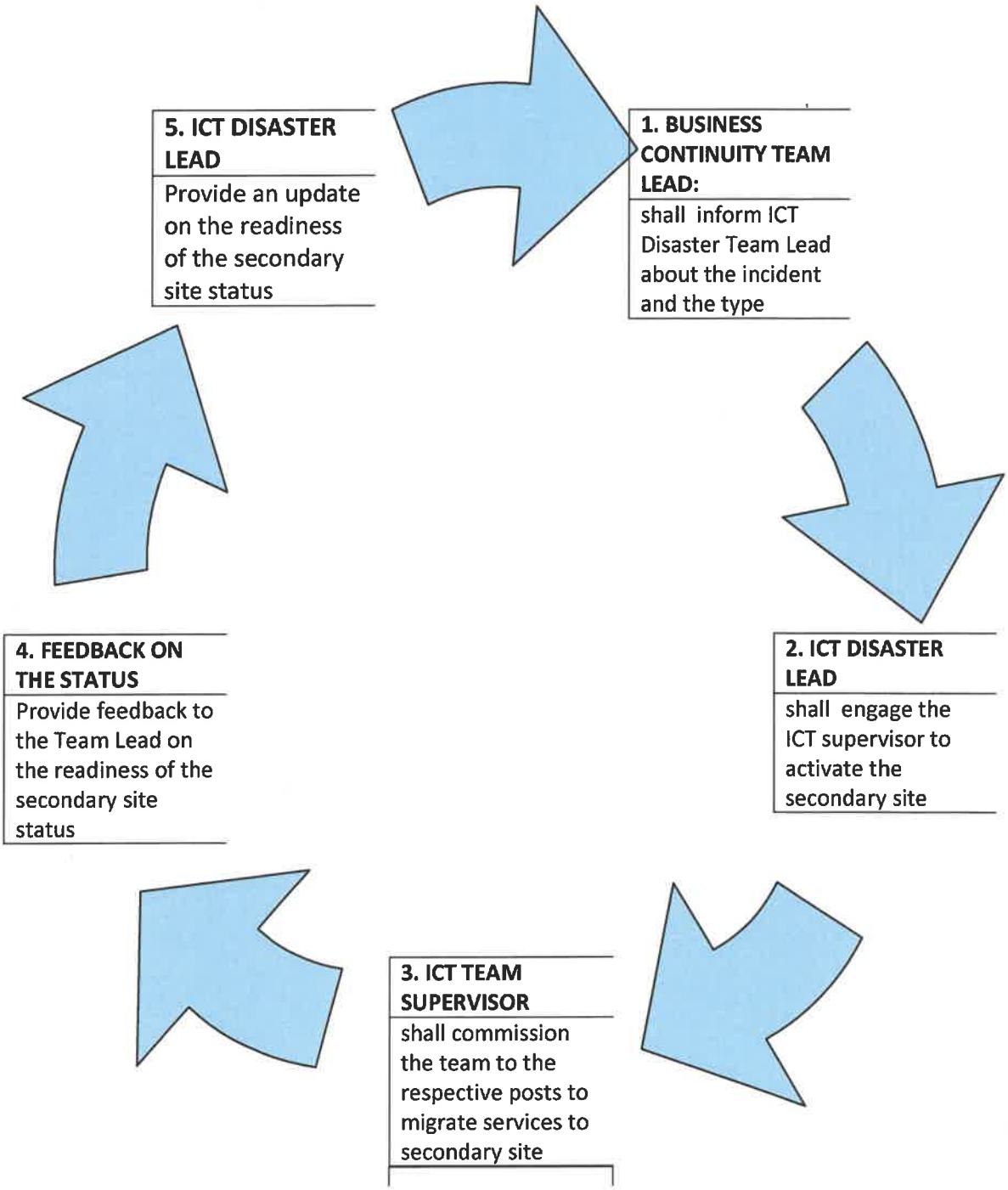
12. INVOCATION PLAN

During disaster, invocation shall follow the following process:

- ICT Disaster Team Lead shall be informed about the incident and the type.
- Team lead shall commission ICT team to the respective posts
- ICT team supervisor in conjunction with representation from Business Continuity team / Lead shall execute the migration of services to the secondary site
- ICT team supervisor shall engage the relevant ICT officials

Below is a diagram outlining the invocation process:

Fig.1 INVOCATION PROCESS DIAGRAM



13. ICT Disaster Recovery Plan

13.1 Introduction

This ICT Disaster Recovery Plan captures, in a single repository, all of the information that describes the Department's ability to withstand ICT disaster as well as the processes that must be followed to achieve disaster recovery.

13.2 Definition of ICT Disaster Recovery

This is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructural services which are vital to the Department after a natural or human-induced disaster. It focuses on the IT or technology systems that support business functions.

A disaster can be caused by man or nature and result in the department not being able to perform all or some of their regular roles and responsibilities for a period of time. In this document a disaster is defined as follows:

- One or more vital systems are non-functional
- The building is available but systems are non-functional
- The building and all systems are non-functional

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

Vis majore / acts of God such as lightning, Fire, Flash flood,

Man-made circumstances such as Software / Network Failure, and Terrorist attack, Labour unrest, Espionage.

13.3 Purpose

The purpose of this DRP document is in twofold: first to capture all of the information relevant to the Department's ability to withstand a disaster, and second to document the steps that the department shall follow if a disaster occurs.

Note that in the event of a disaster the first priority of the ICT unit is to prevent the loss of data.

This DRP takes all of the following areas into consideration:

- Data Storage and Backup Systems
- End-user Computers
- IT Documentation

This DRP does not take into consideration any non-IT resources, Human Resources and real estate related disasters. For any disasters that are not addressed in this document, shall be documented in the Business Continuity Plan.

13.4 Scope of application

This plan is confined to user data recovery in the format as outlined above.

13.5 Version Information & Changes

Any changes, edits and updates made to the DRP shall be recorded in here. It is the responsibility of the ICT Disaster Recovery Lead to ensure that all existing copies of the DRP are up to date. Whenever there is an update to the DRP, the Department requires that the version number be updated to include the change.

Role of Person Making Change	Date of Change	Version Number	Notes
ICT Manager	30-06-2014	1.1	Change due to Departmental Business Merger
ICT Manager	31 -03- 2016	1.2	Annual Review

Assistant Director	31 -03-2016	1.2	Annual Review
ICT Manager	26 – 03 - 2018	1.3	Annual Review
ICT Manager		1.4	Review to address inadequacy of the plan

13.6 ICT Disaster Recovery Teams &Responsibilities

In the event of a disaster, the following are key internal stakeholders who shall be required to restore normal ICT business systems functionality to the users of the Department.

- ICT Disaster Recovery Lead(s) (DITO)
- ICT Disaster Recovery Team (ICT Unit)
- ICT Steering Committee
- ICT Operational Committee

13.6.1 ICT Disaster Recovery Lead

The ICT Disaster Recovery Lead shall oversee the entire disaster recovery process and is responsible for making all decisions related to the Disaster Recovery efforts. He/she shall be the first person to take action in the event of a disaster. This person shall evaluate the disaster and shall determine what steps need to be taken to get the department back to business as usual.

This person's primary role shall be to guide the disaster recovery process and all other individuals involved in the disaster recovery process and a report through a supervisor shall be made available to this person in the event a disaster occurs in the department. All efforts shall be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead shall not be a member of

other Disaster Recovery groups in the Department. The ICT Disaster Recovery Lead shall report to the ICT Steering Committee.

13.6.1.1 Roles and Responsibilities

- Make the determination that a disaster has occurred and trigger the DRP and related processes.
- Be the single point of contact for and oversee the ICT DR Team.
- Organize and chair regular meetings of the ICT DR Team throughout the disaster.
- Present to the ICT Steering Committee on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage ICT DRP test and author ICT DRP updates.
- Set the ICT DRP into motion after the Disaster has been declared.
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the ICT disaster recovery team
- Determine what first steps need to be taken by the ICT disaster recovery team
- Keep the ICT disaster recovery team on track with pre-determined expectations and goals
- Keep record of incidents and expenditure during the disaster recovery process
- Ensure that all decisions made within ICT environment abide by the ICT DRP and policies set by the Department
- Get the secondary site ready to restore business operations
- Ensure that the secondary site is fully functional and secure
- Create a detailed report of all the steps undertaken in the disaster recovery process

- Notify the Department through proper channels once the disaster is over and normal business functionality has been restored.

Contact Information

Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Primary ICT Disaster Recovery Lead / DITO	(018) 388 3219	-	0845543983/0614937231

Provincial IT shall ensure that departmental systems hosted at their environment are included in their ICT Continuity and Disaster Recovery Plan.

13.6.2 ICT Disaster Recovery Team

The Team shall be the first to take action in the event of a disaster. It shall assess the disaster and determine what steps need to be taken to get the department back to normal business operations.

13.6.2.1 Roles &Responsibilities

- Operationalize ICT DRP after the Disaster Recovery Lead has declared a disaster
- Assist in determining the magnitude and class of the disaster
- Assist in determining what systems and processes have been affected by the disaster
- Execute the necessary steps which are guided by the ICT Disaster Recovery Lead towards expected goals.
- Assist in keeping a record of expenditure during the disaster recovery process
- Ensure that all decisions made abide by the ICT DRP and policies set by the Department during operations
- Assist in getting the secondary site ready to restore business operations

- Assist in drafting a detailed report of all the steps undertaken in the disaster recovery process
- Provide a summarized report of all activities that includes all costs related to the disaster recovery.

Contact Information

ICT Disaster Recovery Team of the department.

Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Primary ICT Disaster Lead / DITO	018 388 3219	-	0845543983/0614937231
ICT Manager	018 388 5685	-	0725107734
Assistant Director Infrastructure Support	018 388 1673	-	0767931172
ICT System Administrator	018 388 2877	-	0833750340
ICT Technicians	018 388 5580 / 5042 / 3819130	-	0712120759 0833024097 0797049276
Provincial IT Manager / Networks Manager	018 388 3129	-	083 289 9121

13.6.3 ICT Operational Committee

This committee's primary goal shall be to assist on providing users with the necessary ICT resources needed to perform their roles as quickly and efficiently as possible. It shall need to assist in providing the departmental users in the standby facility and those working from home with relevant resources.

13.6.3.1 Roles &Responsibilities

- Assist in maintaining a lists of all essential supplies that shall be required in the event of a disaster;
- Assist in ensuring that these supplies are provisioned appropriately in the event of a disaster;
- Assist in ensuring that secondary site is adequately equipped with ICT resources so that work is not significantly disrupted in a disaster;
- When the Department is back to normal operations, this committee shall assist in summarizing all costs and activities embarked on during the disaster, and provide a report to the ICT Disaster Recovery Lead;
- If multiple network services are impacted, the committee shall assist in prioritizing the recovery of services in the manner and order that has the least negative business impact;
- Once the ICT systems on the primary site are readily configured, users shall be allocated with resources in the following order:
  - ❖ Business critical systems/users
  - ❖ All Executive and Senior Management
  - ❖ All IT officials
  - ❖ All remaining departmental users

13.6.4 ICT Steering Committee

The ICT Steering Committee shall make any business decisions that are out of scope for the ICT Disaster Recovery Lead. Decisions such as constructing a new data center, relocating the primary site etc. should be made by the Executive Management. The ICT Disaster Recovery Lead shall ultimately report to this committee.

13.6.4.1 Roles &Responsibilities

- Ensure that the ICT Disaster Recovery Team Lead is held accountable for his/her role
- Assist the ICT Disaster Recovery Team Lead in his/her role as required

- Make recommendations that shall impact the Department. This can include decisions concerning:
  - ❖ Rebuilding of the primary facilities
  - ❖ Rebuilding of data centers
  - ❖ Significant hardware and software investments and upgrades
  - ❖ Other financial and business decisions

13.6.5 Provincial IT Role and Responsibilities

Provincial IT shall ensure that all the departmental systems hosted at their location are planned for in terms of Continuity and Disaster Recovery Plan. Service Levels rendered by Provincial IT shall be outlined and agreed to by both two parties in the SLA.

14. Incident Reporting Procedure

In the event of the occurrence of a disaster, the ICT DR Lead shall call the ICT manager who will subsequently engage the ICT team and the respective stakeholders to Identify mitigation actions to ensure the easiest and most timely recovery. Also the ICT manager shall perform a technical, natural, and man-made risk assessment. Records of disaster Incident shall be maintained.

Senior Management shall be responsible for the review and approval of the following:

- Recovery Time Objective

RTO includes:

- ❖ the time for trying to fix the problem without a recovery
- ❖ the recovery tests and the communication to the users

- Recovery Point Objective

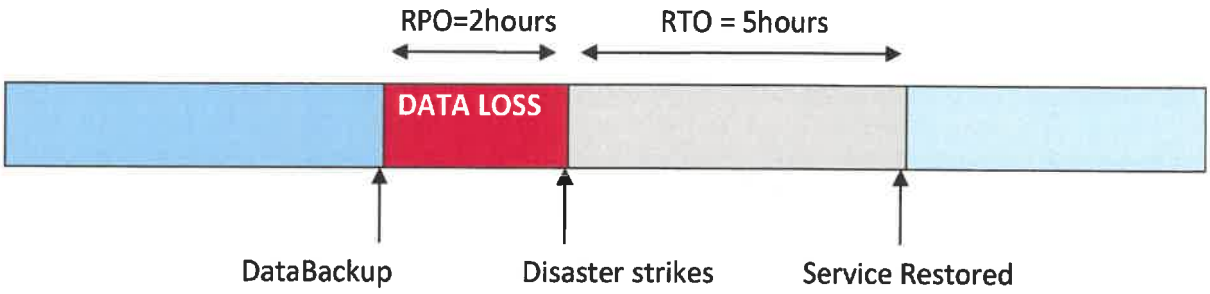
When the data Backup is performed at 09:00am and the System crashes at 11:00am without new backup. The loss of the data captured between 09:00am and 11:00am will be lost. Data loss is acceptable because of the 2 hours RPO. The restored system will continue with data at the point in time of 09:00am. All data in between will have to be manually recovered through other means.

Summary

RTO and RPO approved by senior management remain as objectives. Deviation from the objectives should be monitored.

RPO = 2 hours - the department cannot suffer loss of data made in more than two (2) hours time.

RTO = 5 hours - the department cannot accept the service not being available for more than five (5) hours.



15. Testing

The ICT DR Lead shall be responsible to ensure that test of ICT Continuity Plan take place at least annually, to demonstrate the ability to achieve the determined Recovery Time Objective. ICT DR Lead is responsible for conducting lessons-learned sessions with all participants to capture and incorporate improvements into the plan. The ICT DR Lead shall report all test results to the ICT Steering Committee.

15.1 Testing Approach

- Walkthroughs - identify key areas that need to be tested and ensure that all areas are covered by the test plan.
- The test shall be made through a checklist. Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test shall provide the opportunity to review a plan with a larger subset of people, allowing the ICT DRP Lead, ICT manager and project manager to draw upon a correspondingly increased pool of knowledge and expertise.

16. Review of the Plan

This plan shall be reviewed after a period of three (3) years or as and when there is a major change.

17. Limitations / Disclaimer

The full operationalisation of the plan is dependent on the existence of the approved Departmental Business Continuity Plan. Therefore, some sections of this plan will not be possible to implement until the approval and coming into effect of the Departmental Business Continuity Plan.

18. Approval

This ICT Continuity Plan is agreed to by the Accounting Officer.

06/03/2020

MS. B MOFOKENG **DATE**

HEAD OF DEPARTMENT