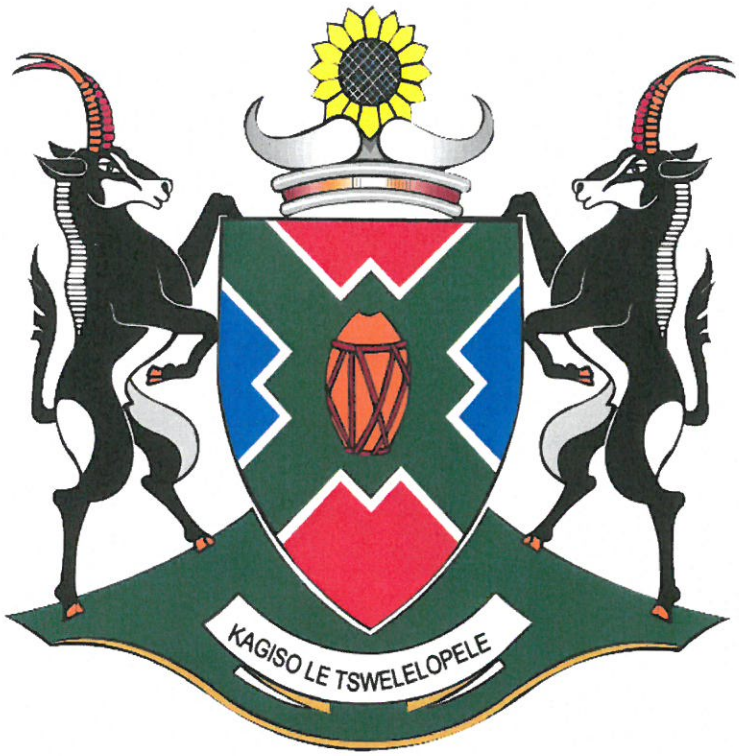
DEPARTMENT OF COMMUNITY SAFETY &TRANSPORT MANAGEMENT



INFORMATION AND COMMUNICATION TECHNOLOGY CONTINUITY PLAN

ICTCP-VERSION 1.2

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	<HoD's signature date>
Created Date	03-07-2013
Version Date	<HoD's signature date>
Version	ICTCP-VERSION 1.2

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

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer		14/07/16
Ms K. Phatudi	Governance Champion		14/07/2016
Ms M.G. Mothibedi	Departmental Risk Management Officer		14/07/2016
Mr S. Setlhare	Acting Director Legal Services		14/07/2016

Records Management Sign–Off

Name	Position	Signature	Date
Mr E Jimla	Records Manager		14/07/2016

GLOSSARY OF TERMS

ICT	Information Communication Technology
DCS&TM	Department of Community Safety and Transport Management
ICTCP	ICT Continuity Plan
HoD	Head of Department
DITO	Department Information Technology Officer
SLA	Service Level Agreements
NWPG	North West Provincial Government
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.
Server	A software program, or the specialized 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..
Filr	Software by Novell used for backup and remote access of user information
BCM	Business Continuity Management
BCP	Business Continuity Plan
Trafman	Traffic Fines Management System
eNatis	Electronic National Transport Information System
OLAS	Operator License Administration System
VMS	Vehicle Management System
DR	Disaster Recovery

Table of Contents

1. Introduction

This plan is a systematic process to prevent, predict and manage Information and Communications 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 and communications 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. 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 and 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 secure 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 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 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 is 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 and IT recovery 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 and the Availability Management and Security management processes, which 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 on the IT Service Continuity Plans and Recovery Plans.
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost – justified to do so.
- Negotiate and agree the necessary contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the Supplier Management process.

5. Purpose

The purpose of this policy is to create and maintain a Business Continuity Plan (BCP) for the IT support of critical company processes. An effective plan allows the company to minimize the adverse effect of emergencies that arise. The department has an ethical obligation to the department's workforce, shareholders, and customer stakeholders to protect the continuing operations of the business.

6. Scope of application

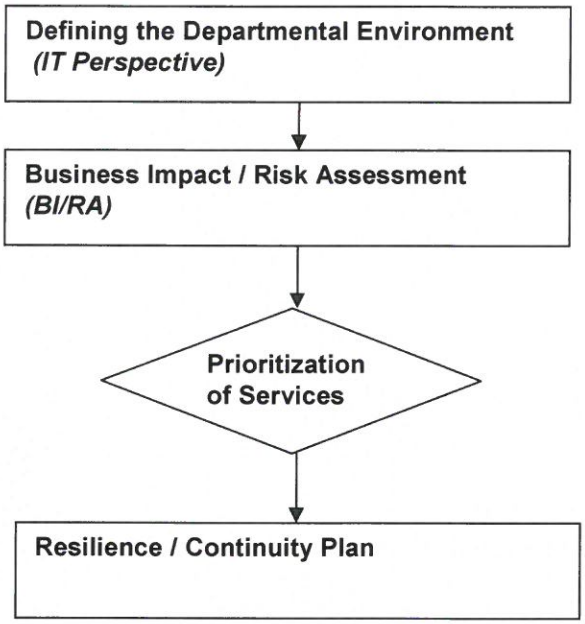
This plan encompasses all IT processes and technology within the departmental environment that supports critical business functions. However, systems hosted at Provincial IT will be catered for in their Continuity Plan. The successful implementation of this depends from commitment of senior management 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 the Office of the Premier, the departmental ICT Continuity Plan focuses on the internal ICT environment over which the department exercises control. Departmental applications that are hosted at the Office of the Premier fall to be included in the ICT Continuity Plan of the Office of the Premier; it is therefore within the responsibility of Office of the Premier to accommodate departmental systems hosted in their environment as per the signed SLA.

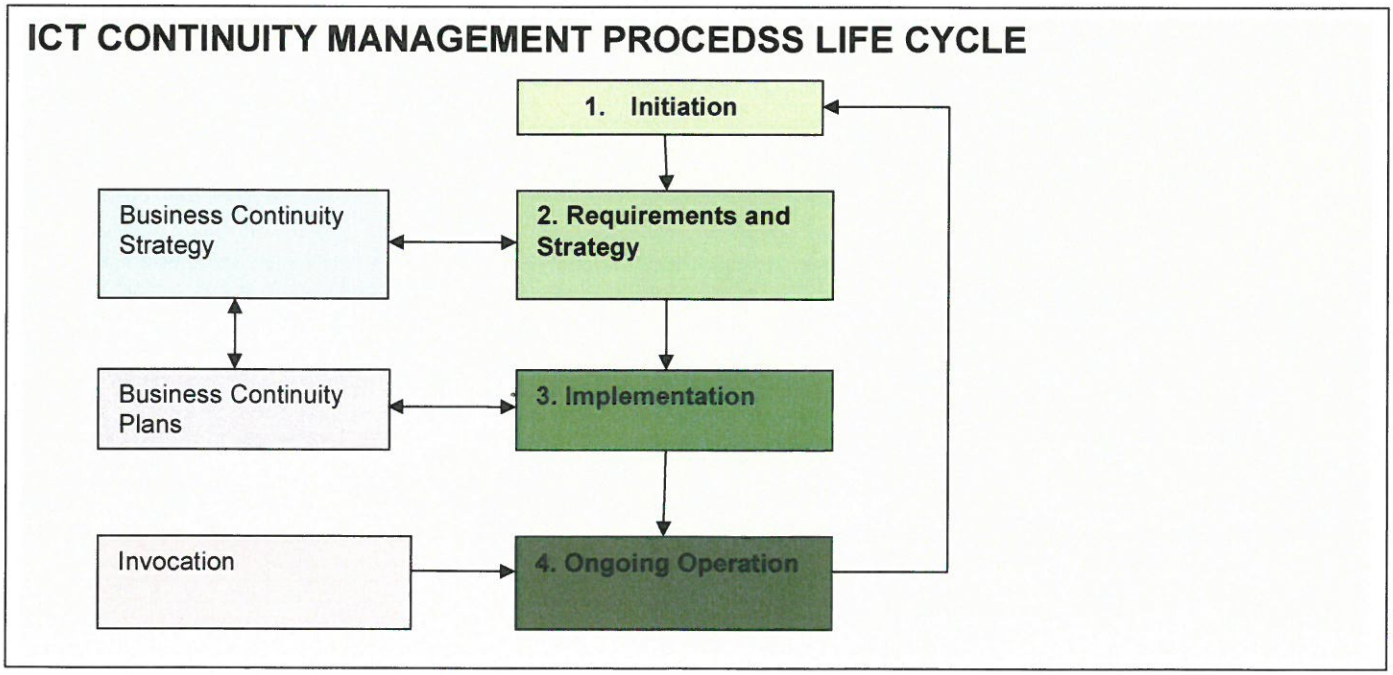
7. ICT Continuity Plan Layout

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.

HIGH LEVEL LAYOUT STRUCTURE/DIAGRAM OF THE PLAN:



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 loss of IT service 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 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 ICT Manager to ensure that the aim of IT Service Responsibilities 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 and 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 Service Continuity Plan if necessary.
- Managing the 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.
- Undertaking regular reviews, at least annually, of the Continuity Plans with the business areas to ensure that they accurately reflect the business needs.
- Negotiating 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 all the departmental ICT application systems are hosted at Office of the Premier. Amongst other services, ICT in the department in terms of network infrastructure is limited to Desktop Support, Service Level Agreement, 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 – Technical System
v) WALKER – Financial System

Key Departmental Core Business Application Systems which are also referred to in this plan with the same SLA terms as above (except for eNatis system which is a national system) include:

i) Trafman

ii) eNatis

iii) OLAS

iv) RAS

v) VMS

In the event of an incident, the plans and systems in place should ensure a resumption of service within the agreed Service Level Agreements (SLAs) ensuring compliance and customer satisfaction as well as aiding in Business Continuity. This plan shall indirectly also include departmental data stored in the following formats:

i) Doc – Word Documents

ii) xls – Excel Documents

iii) PDF – Acrobat Reader / Adobe files

iv) Ppt – Power Point Files

v) Archive Files (email files)

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

LIKELIHOOD:

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

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

From 15 - 25	Very High
From 11- 14	High
From 5 – 10	Medium
From 1 - 4	Low

11.1 Departmental Business Application System:

Location/ Hosting	Departmental ICT System	Type of Loss/ Damage	Likeli hood	Severity	Business Impact	Pre-cautions in place
SITA Building	BAS	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	5	4	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
Garona Building	PERSAL	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage	5	4	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				
Garona Building	WALKER	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
Garona Building	GroupWise	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power SLA Outage	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				
Garona Building	Remedy	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
Garona Building	Filr	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				
Garona Building	Trafman	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
TASIMA	eNatis	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				
Garona Building	CMIS	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
Garona Building	OLAS	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage	**5**	**4**	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				
Garona Building	VMS	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage • War • Theft • Terrorist Attack	5	4	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA
Garona Building	RAS	• Loss of ICT Equipments • Data loss • Fire • Flash flood • Pandemic (Virus attacks) • Power Outage	5	4	Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.	SLA

		• War • Theft • Terrorist Attack				

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)	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and money.	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.
Old Parliament Building (OLD)	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.

					money.	
Safety House	Word, Excel, PowerPoint, PDF, Email Archives and AVS system	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and money.	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.
Bojanala District	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and money.	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.
Dr Kenneth Kaunda	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of	Trend Antivirus Software installed on every user's machine. Also Filr client installed on

					departmental time. Poor service delivery in terms of time and money.	every user's machine for data backup.
Dr Ruth Mompati	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and money.	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.
Ngaka Modiri Molema	Word, Excel, PowerPoint, PDF, Email Archives	Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack	3	4	Poor decision making and inadequacy of information as a result of missing files. Business might have to re-generate data at the expense of departmental time. Poor service delivery in terms of time and money.	Trend Antivirus Software installed on every user's machine. Also Filr client installed on every user's machine for data backup.

12. Disaster Recovery Plan

12.1 Introduction

This 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.

12.2 Definition of a Disaster Recovery

This is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure 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 results 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:

- Loss of ICT Equipments
- Data loss
- Fire
- Flash flood
- Pandemic (Virus attacks)
- War
- Theft
- Terrorist Attack

12.3 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, personnel, 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.

12.4 Scope of application

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

12.5 Version Information & Changes

Any changes, edits and updates made to the DRP shall be recorded in here. It is the responsibility of the 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 indicate this.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
Ms Mogale	ICT Manager	30-06-2014	1.1	Change due to Departmental Business Merger
Ms Mogale	ICT Manager	31 -03- 2016	1.2	Annual Review
Mr Gabonnwe	Assistant Director	31 -03-2016	1.2	Annual Review

12.6 Disaster Recovery Teams &Responsibilities

In the event of a disaster, the following are key stakeholders who shall be required to restore normal functionality to the employees of the Department.

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

12.6.1 Disaster Recovery Lead

The 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 shall report to this person in the event that a disaster occurs in the Department, regardless of their business unit and existing managers. 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 Disaster Recovery Lead shall report to the Management Team.

12.6.1.1 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 all of the DR Teams.
- Organize and chair regular meetings of the DR Team leads throughout the disaster.
- Present to the Management Team on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all DRP test and author all DRP updates.
- Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the other disaster recovery teams
- Determine what first steps need to be taken by the disaster recovery teams
- Keep the disaster recovery teams on track with pre-determined expectations and goals
- Keep a record of incidents and money spent during the disaster recovery process
- Ensure that all decisions made abide by the 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 relevant parties once the disaster is over and normal business functionality has been restored.
- Provincial IT shall ensure that departmental systems hosted at their environment are included in their Plans in terms of Continuity and Disaster Recovery Plans.

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Mr Matlhako	Primary Disaster Lead / DITO	(018) 388 3219	-	0845543983

12.6.2 Disaster Recovery Team

The Disaster Management Team that shall oversee the entire disaster recovery process. They shall be the first team that shall need to take action in the event of a disaster. This team shall evaluate the disaster and shall determine what steps need to be taken to get the department back to business as usual.

12.6.2.1 Roles &Responsibilities

- Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the other disaster recovery teams
- Determine what first steps need to be taken by the disaster recovery teams
- Keep the disaster recovery teams on track with pre-determined expectations and goals
- Keep a record of money spent during the disaster recovery process
- Ensure that all decisions made abide by the 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 relevant parties once the disaster is over and normal business functionality has been restored
- After the Department is back to business as usual, this team shall be required to summarize any and all costs and shall provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information

Add or delete rows to reflect the size the Disaster Management Team of the department.

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Mr Matlhako	Primary Disaster Lead / DITO	(018) 388 3219	-	0845543983
Ms Mogale	ICT Management	018 388 2152	-	0835265507
Mr Neito	Security Service Management & Loss Control Committee Chairperson	(018) 200 8171	-	073 688 3397
Ms Ramafi	Risk Management	(018) 200 8062	-	0733890816
Ms Mpunzi	Occupational Health and Safety Management	(018) 200 8309	-	0742901428
Mr Jimla	Records Management	0183889343	-	0837574440

12.6.3 ICT Operational Committee

This team's primary goal shall be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They shall need to provide all the departmental employees in the standby facility and those working from home with the tools that their specific role requires.

12.6.3.1 Roles &Responsibilities

- Maintain lists of all essential supplies that shall be required in the event of a disaster
- Ensure that these supplies are provisioned appropriately in the event of a disaster
- Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster
- Ensure that spare computers and laptops have the required software and patches
- Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster
- Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe
- If insufficient computers/laptops or related supplies are not available the team shall prioritize distribution in the manner and order that has the least business impact
- This team shall be required to maintain a log of where all of the supplies and equipment were used
- After the Department is back to business as usual, this team shall be required to summarize any and all costs and shall provide a report to the Disaster Recovery Lead summarizing their activities during the disaster
- In the event of a disaster that does not require migration to standby facilities, the team shall determine which network services are not functioning at the primary facility
- In the event of a disaster that does require migration to standby facilities the team shall ensure that all network services are brought online at the secondary facility
- If multiple network services are impacted, the team shall prioritize the recovery of services in the manner and order that has the least business impact.

- If network services are provided by third parties, the team shall communicate and co-ordinate with these third parties to ensure recovery of connectivity. Once critical systems have been provided with connectivity, employees shall be provided with connectivity in the following order:
    - ❖ Business critical systems/users
    - ❖ All members of the DR Teams
    - ❖ All Executive and Senior Management
    - ❖ All IT employees
    - ❖ All remaining employees
- Install and implement any tools, hardware, software and systems required in the standby facility
- Install and implement any tools, hardware, software and systems required in the primary facility
- After the Department is back to business as usual, this team shall be summarize any and all costs and shall provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.
- ICT component shall ensure that Provincial IT has taken responsibility of departmental systems hosted at their location through Service Level Agreement (SLA).

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Ms Mogale	ICT Manager	018 388 2152	-	0835265507
Mr Gabonnwe	Assistant Director ICT	018 388 5685	-	0725107734
Ms Senwelo, Mr Mokgethi	ICT technicians	018 388 1673 018 381 9130	-	0767931172 0833024097
Mr Sarel van der	Provincial IT	018 388 3129	-	083 289 9121

Schyff	Manager / Networks Manager			

12.6.4 ICT Steering Committee

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

12.6.5 Roles &Responsibilities

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

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Mr O. Mosiane	Acting Head of Department	018 200 8006/1	-	0834078288
Ms Phatudi	ICT Strategic Committee Chairperson, Governance Champion & CFO	018 200 8025	-	0835174211

Ms Lehabe-Metsi	ICT Steering Committee Chairperson	018 200 8096	-	0606782107
Mr Matlhako	DITO	018 388 3219	-	0845543983
Mrs Mothibedi	Chief Risk Officer	018 200 8007	-	0835708821

12.6.6 Provincial IT Role and Responsibilities

Office of the Premier 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 Office of the Premier shall be outlined and agreed to by both two parties in the SLA.

12.6.7 Incident Reporting Procedure

In the event of the occurrence of a disaster, the 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.

13 Testing

The ICT manager shall test all IT Business Continuity Plans at least bi-annually to demonstrate the ability to achieve the BIA determined Recovery Time Objective. Conduct a lessons-learned session with all participants to capture and incorporate improvements into the plans. The ICT manager shall report all test results to the Steering Committee.

13.1 Testing Approach

- Walkthroughs
- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. The test shall be made through a checklist. This test shall provide the opportunity to review a plan

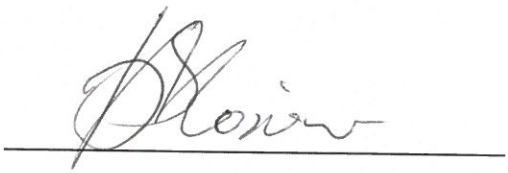
with a larger subset of people, allowing the DRP Lead, ICT manager and project manager to draw upon a correspondingly increased pool of knowledge and experiences.

14. Review of the Framework

The DRP shall be updated annually or any time a major system update or upgrade is performed, whichever is more often.

15. Approval

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



21/07/16

MR O. MOSIANE

DATE

ACTING HEAD OF THE DEPARTMENT