



the denc

Department:
Environment & Nature Conservation
NORTHERN CAPE PROVINCE
REPUBLIC OF SOUTH AFRICA

Private Bag X6102, Kimberley, 8300, Metlife Towers, T-Floor, Tel: 053 807 7300, Fax: 053 807 7328

DEPARTMENT OF ENVIRONMENT AND NATURE CONSERVATION

**DISASTER RECOVERY PLAN
25 NOVEMBER 2012
CORPORATE SERVICES UNIT**

"A PROSPEROUS AND EQUITABLE SOCIETY LIVING IN HARMONY WITH OUR NATURAL RESOURCES"

Table of Contents

DEPARTMENT OF ENVIRONMENT AND NATURE CONSERVATION	1
1. CONCEPTUAL BACKGROUND	2
1.1 INTRODUCTION.....	2
1.2 LEGISLATIVE REQUIREMENTS.....	3
2. POLICY STATEMENT AND APPLICATION SCOPE.....	4
2.1 POLICY STATEMENT.....	4
2.1.1 DISASTER RECOVERY SCOPE.....	4
2.1.2 PLAN ASSUMPTIONS.....	5
2.1.3 BUSINESS CRITICAL SYSTEMS FOR THE DENC.....	5
2.1.4 IDENTIFICATION OF KEY IT BUSINESS FUNCTIONS.....	5
2.1.5 IDENTIFICATION OF KEY STAKEHOLDERS PER BUSINESS FUNCTION.....	6
2.1.5.1 INTERNAL STAKEHOLDERS.....	6
2.1.5.2 EXTERNAL STAKEHOLDERS.....	6
2.1.6 THE ROLE OF IT IN RELATION TO EACH BUSINESS FUNCTION.....	7
2.1.7 PRE-DISASTER ACTIONS TO ENSURE READINESS.....	7
2.1.7.1 TRANSVERSAL SYSTEMS.....	7
2.1.8 ACTION PLAN IN TERMS OF DIFFERENT KEY BUSINESS FUNCTIONS AFTER DISASTER OCCURRED.....	8
PREVENTATIVE MEASURES (BCP).....	10
ACTION PLAN.....	10
2.2 APPLICATION SCOPE.....	11
3. POLICY FRAMEWORK.....	12
3.1 IDENTIFICATION AND CONSULTATION OF STAKEHOLDERS.....	12
3.2 TIMEFRAMES.....	12
3.3 IMPLEMENTATION STRATEGY.....	12
The implementation date for this policy is	12
3.4 FINANCIAL IMPLICATIONS.....	12
3.5 COMMUNICATION.....	13
3.6 COMPLIANCE, MONITORING AND EVALUATION (M&E).....	13
3.7 POLICY REVIEW.....	13
3.8 POLICY IMPACT.....	13
3.9 INTERIM MEASURES.....	14
4. ADOPTION OF POLICY.....	15

1. CONCEPTUAL BACKGROUND

1.1 INTRODUCTION

The Department of Environment & Nature Conservation recognizing its operational dependency on computer systems, including the Local Area Network (LAN), Servers, Internet and email and the potential loss of data and operational control that may occur in the event of a disaster; authorized the preparation, implementation and maintenance of a comprehensive disaster recovery plan.

The purpose of the disaster recovery plan is to provide a written of how the Department of Environment & Nature Conservation is to deal with potential disasters, especially the technology infrastructure critical to business functioning of the Department of Environment & Nature Conservation. Disasters are events that make the continuation of normally function impossible and the DRP consists of the precautions taken so that the effects of the disaster will be minimized and the Department of Environment & Nature Conservation will be able to either maintain or quickly resume mission-critical functions.

The DRP preparation process includes several major steps as follows:

- Identify systems and applications currently in use
- Analyse Business Impact and determination of critical recovery time frames
- Determine recovery strategy
- Document Recovery Team Organisation
- Document Recovery Team Responsibilities
- Develop and document Emergency Procedure
- Document Training and Maintenance Procedures

LIST OF ABBREVIATIONS

DENC	:	Department of Environment & Nature Conservation
HOD	:	Head of Department
CIO	:	Chief Information Officer
DRP	:	Disaster Recovery Plan
ERT	:	Emergency Response Team
IT	:	Information Technology
SLA	:	Service Level Agreements
LAN	:	Local Area Network
PFMA	:	Public Finance Management Act

SITA : State Information and Technology Agency
ICT : Information Communication and Technology
WAN : Wide Area Network

1.2 LEGISLATIVE REQUIREMENTS

- **Section 51 of the Public Finance Management Act no1 of 1999**
- **Treasury Regulation**



2. POLICY STATEMENT AND APPLICATION SCOPE

2.1 POLICY STATEMENT

The mission of the Disaster Recovery Plan is to establish defined responsibilities, actions and procedures to recover the Department of Environment & Nature Conservation's computer, communication and network environment in the event of an unexpected and unscheduled interruption. The plan is structured to attain the following objectives:

- Recover the physical network;
- Recover the applications;
- Minimize the impact on the business units in the DENC

2.1.1 DISASTER RECOVERY SCOPE

A disaster will influence all aspects of service delivery within the DENC. In this regard DENC business impact assessment will have to be done to establish how all functions will be influenced such as sufficient personnel; transport; the budget; physical accommodation; security etc. This plan will however only address the recovery of systems under the direct control of the IT support services. The plan will be tested on a continuous basis to ensure that backups (user data) are not corrupt.

All the other systems for example BAS, PERSAL and LOGIS are provided by Treasury. The DRP and BCP will therefore address backup equipment for example routers and switches to be utilized as replacements if faulty routers or switches cause downtime.

The DRP was written with the following objectives:

- To ensure the safety of all DENC employees throughout the emergency condition, disaster declaration, and recovery process.
- To reestablish the essential organization related services provided by DENC within their required recovery time frames.
- To suspend all non-essential activities until normal and full organization functions have been restored.
- To mitigate the impact to DENC's customers through the rapid implementation of effective recovery strategies as defined herein.
- To reduce confusion and misinformation by providing a clearly defined command and control structure.
- To consider relocation of personnel and facilities as a recovery strategy of last resort.



2.1.2 PLAN ASSUMPTIONS

The DRP was developed under certain assumptions in order for the plan to address a broad spectrum of disaster scenarios. These assumptions are:

- Section 51 of the Public Finance Management Act no1 of 1999 stipulates that the financial authority must ensure that the DENC “has and maintains effective, efficient and transparent systems of financial and risk management”.
- A disaster can be seen as the failure of computerised systems under different circumstances e.g. fire, but it is not limited to computerised and network connected systems only. For the purpose of the ICT Disaster Recovery Plan the focus will remain on computerised systems only.
- The DENC is dependent on external stakeholders for example Treasury, SITA etc for most of their systems such as Transversal systems.
- The DRP is dynamic and should constantly be tested and revised as circumstances change.
- The safety of officials is of prime importance and their safeguarding will take priority over concerns regarding ICT equipment.
- DENC's recovery efforts are based on the premise that any resources required for the restoration of critical organization functions will reside outside of the primary facility.
- Any vital records required for recovery can be either retrieved or recreated from an off-site location and moved to the recovery facility

2.1.3 BUSINESS CRITICAL SYSTEMS FOR THE DENC

The Department of Environment & Nature Conservation is located in Kimberley and housed in 2 buildings, viz. Metlife/ PostOffice Building and Sasko Building. The total number of employees for DENC is 214 employees. Business critical systems that are utilized by the DENC include the following:

- Persal for salary administration
- BAS for financial accounting
- Novell 6.5 for directory services
- GroupWise 7 for email and calendar services.

2.1.4 IDENTIFICATION OF KEY IT BUSINESS FUNCTIONS

The following key systems are available within the DENC:

- Transversal Systems, e.g. BAS, PERSAL
- Telephone Systems
- Computer Hardware and User Backups
- Network equipment
- Server equipment

2.1.5. IDENTIFICATION OF KEY STAKEHOLDERS PER BUSINESS FUNCTION

2.1.5.1 INTERNAL STAKEHOLDERS

The following table is indicative of the internal stakeholders as well as their functionality in relation to business functions:

Component	System/Responsibility	Representative	Contact Details
Human Resource	Persal	V.Fredricks	053 807 7378
Finance	BAS	W. Ditshetelo	053 807 7343
Finance	LOGIS	C. Mackay	053 807 7344
Security	Physical Security	L. Morule	053 807 7318
Records Management	Registry	A. Pienaar	053 807 7351
ICT	Network (Lan)	P.Mabija	053 807 7388
	Server environment	D.Vos	053 807 7361
	Novell Client and Novell Groupwise	L.Modimoeng	053 807 7361
CFO	Financial Management	B.Mashobao	053 838 2924
Website	Website Content	F.Etty	053 807 7360
	Website Access	F.Etty	

2.1.5.2 EXTERNAL STAKEHOLDERS

Stakeholder	System	Contact person	Contact details
SITA	LAN and WAN (Datalines)	Zanele Nkenkana	zanele.nkenkana@sita.co.za 053-836 5408 082 372 0690
		Moeketsi Maishoane	Moeketsi.maishoane@sita.co.za 053-836 5406 083 376 6695
Nugenl	Telephone systems	Cecil Steenbok	053 – 807 7333
Telkom			
Transversal Systems	BAS	Bangile Jonney	053-830 8371
		Ettiene Ockhuis	053-830 8375
	PERSAL	Lebogang Mentor	053-830 8460
		Zuko Mbijekana	053-830 8263
	LOGIS	Zuko Mbijekana	053-830 8263

2.1.6 THE ROLE OF IT IN RELATION TO EACH BUSINESS FUNCTION

Transversal Systems: Ensure minimum required access to all transversal systems. These include the availability of a remote site to access transversal systems, backup equipment to access systems and sufficient network connectivity to allow access to the transversal systems.

Telephone systems: Ensure the availability of a remote site with telephone communication network if disaster occurred.

Computer hardware and user backups: Ensure that all users have backup facility. Availability of an off-site backup of the user backups.

Network Equipment: Ensure the availability of a remote recovery site with sufficient data bandwidth to accommodate all systems in case of a disaster. Sufficient levels of emergency network equipment in case of a damaged network site e.g. Routers & switches.

2.1.7 PRE-DISASTER ACTIONS TO ENSURE READINESS

2.1.7.1 TRANSVERSAL SYSTEMS

BAS, PERSAL and LOGIS

PC's available at other sites and laptops in different directorates will be utilized in case of disaster. The following is a list of BAS, PERSAL and LOGIS users at various offices with alternatives in case of disaster.


Site	Users	System	Alternative site
MetLife-Tower	Virgil Fredericks	PERSAL	Sasko
MetLife-Tower	Itumeleng Ratikoane	BAS	Sasko
MetLife-Tower	Carmen Cloete	LOGIS	Sasko

Telephone Systems

Telephone system should function properly at recovery site. 10 Pin codes should be available and not in use to allow immediate telephone access in case of a disaster.

Computer hardware and user backups

PC's available at other sites and laptops in different directorates will be utilized in case of a disaster. Servers are installed at each district office with a shared drive available for user backups. Users are currently doing their own backups onto their external hard drives.



Network Equipment

Minimum stock level of network equipment should be in place to ensure availability of network in case of a disaster. The router at the Sasko building will be used to connect all the transversal services to SITA. A spreadsheet exists with a list of IP addresses for transversal servers and Laptops that will be connecting to them.

2.1.8 ACTION PLAN IN TERMS OF DIFFERENT KEY BUSINESS FUNCTIONS AFTER DISASTER OCCURRED

In order to provide the DENC with guidance in case of a disaster this document provides an overall guidance in case of a disaster. Specific actions may however vary depending on the nature of the disaster especially under circumstances where human lives have been affected or jeopardized by the disaster.

Under most circumstances the disaster will come under the attention of the security personnel of buildings or any other official who will inform the HOD. The HOD will brief the Executive Managers and Senior Managers.

In an event where the DENC experience any form of disaster that influence the functioning of IT and related systems the following steps needs to be taken to ensure a well coordinated response:

After a disaster the Executive Manager Corporate Services should convene an Emergency Response Team (ERT). The size and compilation of the ERT will vary depending on the extent of the disaster but to attend to the IT recovery process the following members should be included:

- IT Manager – Responsible for IT.
- Physical planning official – Responsible for office accommodation and assessment of buildings.
- Finance representative - If BAS AND LOGIS are influenced.
- Human Resource representative – If PERSAL is influenced.
- Physical Security Representative – If security issues are at stake.
- Other members can also be included depending on the nature of the disaster.

The ERT will assess the situation, determine the extent and severity of the situation and based on the assessment the team will determine whether it can be classified as “routine recovery” or whether it should be declared a formal disaster and the HOD should be informed accordingly. In case of a “routine recovery” the team should draft a recovery effort based on the resources available within one day and put in place recovery equipment and systems within 3 working days.

In case of an IT disaster the Corporate Services Manager contacts the HOD and informs him/her of the disaster. The HOD contact different Disaster teams and provide them with the following information:

- Brief overview of disaster
- Location and times to meet
- Time schedules
- Additional information as required
- Level of security and impact also needs to be announced by HOD

ERT needs to take the following steps to ensure contingency of systems:

- Supervise, coordinate, communicate and prioritize recovery activities.
- Take into consideration the DRP and put systems in place where it has been provided for.
- Liaise with other stakeholders to get systems into place such as: SITA; Telkom; Treasury etc. Contact information on page 7.
- Hold regular meetings with heads of components.
- Heads provide HOD with updates and only HOD and Media Liaison officials communicate with media.
- Identify and obtain additional resources to assist with disaster recovery effort.
- Do final assessment of the recovery status and determine when IT services can resume at minimum required level.
- Treasury Regulation Chapter 16A6.4 makes provision for deviation from normal Supply Chain Management procedures in case of an emergency.



PREVENTATIVE MEASURES (BCP) ACTION PLAN

Risk Areas	Subject	Action Plan	Time Frame	Responsibility
1. Transversal Systems PERSAL/BAS	1.1 Maintenance of Computers	Maintain equipment as reported on Helpdesk System	According to IT Action Plan	IT
	1.2 Ensure minimum required access to all transversal systems.	<ul style="list-style-type: none"> Identify critical posts Identify alternative sites per offices in case of disaster. 		Finance / HR
	1.3 Ensure WAN access	Ensure that SLA with SITA exists and are renewed every 3 years. SLA provide for more than 98% WAN uptime	Every 3 Years	IT Legal Services
	1.4 Ensure backup equipment for Network e.g. Routers and Switches.	<ul style="list-style-type: none"> Costing of additional Routers x2; Switches x 3; Purchase 2 x routers and 3 x switches 	2 nd quarter 2 nd quarter	IT, Finance IT, Finance
2. Internal Systems - NUGEN, website	1.5 Physical access and training.	In-house training to ensure multi-skilling of transversal system users.	Ongoing	Finance / HR
	1.6 Ensure backup printers are in place	<ul style="list-style-type: none"> Identify backup Dot Matrix and Laser printers Test functionality of printers 		SCM/IT SCM/IT
	2.1 Maintenance of Computers	Maintain equipment as reported on Helpdesk System	According to IT Action plan	IT
	2.2 Ensure Network Access	Maintained networks	Quarterly inspections of network sufficiency	IT
3. User Backups	2.3 Ensure backup Network equipment especially Routers en Switches	<ul style="list-style-type: none"> See 1.4 Purchase Data storage solution 	2 nd quarter 2 nd quarter	IT, Finance
	3.1 Ensure Backup Facilities for all users.	<ul style="list-style-type: none"> Develop template to rate data to be backed up. Install backup Novell Network servers 	Needs to be procured.	Record Management IT

Risk Areas	Subject	Action Plan	Time Frame	Responsibility
		<ul style="list-style-type: none"> Connect users to novell directory service for automatic backup system Met-Life Tower Sasko	Servers need to be procured	IT IT IT, Finance
	3.2 Backup Servers / Regular Off Site Backups	<ul style="list-style-type: none"> Test & copy files to DVD/Bluray & Tape Maintain a register for monthly backups 	Monthly Procure Tapes and DVD/Blurays	IT
	3.3 Ensure security of servers	<ul style="list-style-type: none"> Install servers in secure network rooms. Install fingerprint access control, CCTV cameras, fire suppression, climate control and generator at Midas server room. 	Completed	IT
4. E-mail	4.1 Ensure Network Access	See 2.2	Completed	IT/Lefatshe

2.2 APPLICATION SCOPE

This policy will apply to all officials of the Department of Environment and Nature Conservation.



3. POLICY FRAMEWORK

3.1 IDENTIFICATION AND CONSULTATION OF STAKEHOLDERS

This policy document was distributed to staff members within the department and their feedback and inputs are included where changes were suggested and motivated. Information sessions were also held as part of the consultation process. The recognized Labour Unions are not excluded in the process as they do have shop stewards within the department, and them being part of the departmental staff, thus had the opportunity to participate in the process. Furthermore, it needs to be mentioned that the department cannot negotiate with the Unions (Organized Labour) as a separate entity on this policy. Especially, because there are matters of mutual interests that must be dealt with in the formal structures created for this purpose, such as the Provincial Bargaining Council.

3.2 TIMEFRAMES

In August 2007 a draft of this policy was reviewed by the departmental legal services and policy unit who submitted their comments on the policy. After incorporating those comments a second draft was send to the policy and planning unit on the 14-18 February 2008 to align and re-check the policy. 02- 14 April 2008, the policy unit used the soft copies of this policy to align it with the provincial template. The final draft was reviewed by the Corporate Policy unit on June 14, 2012.

3.3 IMPLEMENTATION STRATEGY

It is the responsibility of each Head of department to ensure that this policy is carefully followed within the department. All managers should make members of their employees aware of the obligation to familiarize themselves with and follow this policy.

An implementation plan will be drafted which will outline how and when this policy will be implemented. The plan will be drafted two months after the implementation date of this policy. In order to ensure adequate implementation of this policy the human resource unit will compile an infrastructure investment (in terms of human capital) and policy management plan. The plan will be updated on an annual basis and will contain details on future guidelines for this policy. The financial implications if any will be indicated on the plan in order to ensure that funds are available or availed.

The implementation date for this policy is _____

3.4 FINANCIAL IMPLICATIONS

This policy will be funded by the Human Resource Unit. The budget for the financial year is



3.5 COMMUNICATION

- IT Manager – Responsible for IT.
- Physical planning official – Responsible for office accommodation and assessment of buildings.
- Finance representative - If BAS AND LOGIS are influenced.
- Human Resource representative – If PERSAL is influenced.
- Physical Security Representative – If security issues are at stake.
- Other members can also be included depending on the nature of the disaster.

3.6 COMPLIANCE, MONITORING AND EVALUATION (M&E)

ERT needs to take the following steps to ensure contingency of systems:

- Supervise, coordinate, communicate and prioritize recovery activities.
- Take into consideration the DRP and put systems in place where it has been provided for.
- Liaise with other stakeholders to get systems into place such as: SITA; Telkom; Treasury etc. Contact information on page 7.
- Hold regular meetings with heads of components.
- Heads provide HOD with updates and only HOD and Media Liaison officials communicate with media.
- Identify and obtain additional resources to assist with disaster recovery effort.
- Do final assessment of the recovery status and determine when IT services can resume at minimum required level.

Treasury Regulation Chapter 16A6.4 makes provision for deviation from normal Supply Chain Management procedures in case of an emergency.

3.7 POLICY REVIEW

This policy will be reviewed when the need arises or in case of the occurrence of extenuating circumstances (political mitigation, or pronouncement by legislation and/or regulations). The contact person for this policy will be required to submit all relevant information pertaining to this policy in conjunction with a signed memo with all amendments (addition or omission) during the third quarter annually.

The exception, the Policy development unit will be conducting all extenuating reviews throughout the year, therefore it is paramount that any new information received be submitted to this unit, in order to coordinate the review process of this policy.

3.8 POLICY IMPACT

The wish of the DRP is to plan to address a broad spectrum of disaster scenarios, especially IT related disasters.

3.9 INTERIM MEASURES

This is an interim document for this Department until such time that a provincial policy has been developed.

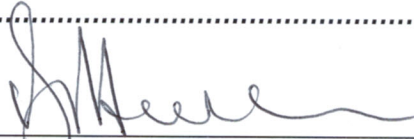
A handwritten signature in black ink, appearing to be 'SMA', located at the bottom right of the page.

4. ADOPTION OF POLICY

Approved / ~~Not Approved~~

Comments:

.....
.....
.....



HEAD OF DEPTMENT

2012/12/25

DATE

