# Northern Cape Department of TRANSPORT, SAFETY & LIAISON

# DISASTER RECOVERY PLAN

## 2020/23

# IT Disaster Recovery Plan
# Northern Cape Department of Transport, Safety and Liaison

## 1. Background

A Disaster Recovery Plan (DRP) and Business Contingency Plan (BCP) Committee was established on 10 July 2012 in order to compile a DRP and BCP with the purpose to:

- Identify weaknesses and implement a disaster prevention programme.
- Ensure that critical business can continue with the minimal time frame in case of any disaster.
- Facilitate effective co-ordination of recovery tasks and systems.
- Monitor and evaluate on quarterly basis

The first DRP/BCP was approved on 11 April 2012. The DRP/BCP was amended to address findings of the 2013 Information System audit and was approved on 24 February 2014. The DRP was revised and approved by the HOD on 24 February 2015.

**The following Units were identified.**

| Unit | System/Responsibility | Representative | Secondi |
|---|---|---|---|
| Human Resource | Persal<br>BACS | Ms. M. Lekwene<br>053 – 839 - 1781 | Mr. BS. Marekwa<br>053 – 839 - 1795 |
| Supply Chain & Asset Management | LOGIS<br>Asset Management | Ms. A. Montwedi<br>053 – 839 - 1731 | Ms. M. Ratlle<br>053 – 839 - 1808 |
| Finance | BAS | Ms. T. Ndondo<br>053 – 839 - 1724 | Ms. L. Jampies<br>053 – 839 - 1728 |
| Financial Planning, Budgeting and | | Mr. E. Apie<br>053 839 - 1742 | Ms. G. Nakana<br>053 839 - 1726 |

| Unit | System/Responsibility | Representative | Secondi |
|---|---|---|---|
| Reporting | | | |
| Security Management | Physical Security | Mr. BM. Mjoli<br>053 – 839 - 1718 | |
| Records Management | Registry | Ms. A. Matiwane<br>053 – 839 - 1746 | Ms. A. Kleb<br>053 – 839 - 1735 |
| IT | IT Environment | Mr. TL. Aaron<br>053 – 839 - 1780 | Mr. D. Peterson<br>053 – 839 - 1770 |
| Legal Services | Legal guidance | Mr. C. Modisa<br>053 839 1789 | |
| Risk Management | Risk Management | Ms. S. Zikhali<br>053 – 839 - 1758 | Ms. C. Serati<br>053 – 839 - 1731 |

**External Stakeholders contact information.**

| Stakeholder | System | Contact person | Contact details |
|---|---|---|---|
| SITA | LAN and WAN (Datalines) | Petrus Lebotse | petrus.lebotse@sita.co.za<br>053-836 5417 / 5410<br>082 675 5654 / 076 049 9302 |
| | | Moeketsi Maishoane | Moeketsi.maishoane@sita.co.za<br>053-836 5406<br>083 376 6695 |
| Telkom | Telephone systems | Customer care | cccgov@telkom.co.za |
| | | Andrew Lamola | lamolama@telkom.co.za<br>051-4016803<br>061 425 9043 |
| Nugen | Telephone | Mr. D. Cilliers | 053 – 802 - 8900 |

| Stakeholder | System | Contact person | Contact details |
|---|---|---|---|
| | systems | | |
| Treasury | LOGIS | Samantha Pieterse. | 053-830 8283 |
| | | Leon Venter | 053-830 8378<br>073 691 3066 |
| | | Zuko Mbijekana | 053-830 8263<br>082 556 9878 |
| | PERSAL | Lebogang Mentor | 053-830 8460<br>082 359 8188 |
| | | Zuko Mbijekana | 053-830 8263<br>082 556 9878 |
| Office of the Premier | Novell Client and Novell Groupwise | Kurt Passe | kpasse@ncpg.gov.za<br>053-838 2922<br>082 825 0445 |
| | | Eggie Smit | esmit@ncpg.gov.za<br>053-838 2922 |

## 2. ASSUMPTIONS

The disaster recovery plan is based on the following assumptions:

2.1 The Public Finance Management Act No. 1 of 1999 state that the financial authority must ensure that the Department "has and maintains effective, efficient and transparent systems of financial and risk management".

2.2 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 IT Disaster Recovery Plan the focus will remain on computerised systems only.

2.3 The Department is dependent on external stakeholders for example Treasury, SITA etc for most of their systems such as Transversal, NTCM, NLTIS and ENATIS.

2.4 The DRP is dynamic and should constantly be tested and revised as circumstances change.

2.5 The safety of officials is of prime importance and their safeguarding will take priority over concerns regarding ICT equipment.

## 3. List of Abbreviations

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
RPO - Recovery Point Objective
NTCM – National Traffic Contravention Model
NLTIS – National Land Transport Information System
ENATIS - Electronic National Transport Information System

## 4. Objectives

The primary objective of the DRP is to develop a logical and easily understood plan that will assist the Department to recover as fast and effectively as possible from a disaster that interrupts business operations and systems as well as ensuring continuation of services in preventing possible disasters.

Secondary objectives are:

- To ensure that responsible officials understand their duties in implementing a DRP under different circumstances.
- To minimize confusion, errors and expense to the Department.
- To reduce risks or loss of services.
- To provide ongoing protection of Departmental assets and records.
- To guarantee the continued viability of this Plan.
- To ensure that the necessary response team is in place to communicate processes to normal operations

## 5. SCOPE

A disaster will influence all aspects of service delivery within the Department.

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 continues basis to ensure that the plan is practical with regard to execution.

All the other systems for example BAS, PERSAL and LOGIS are provided by Treasury and the other web-based systems is hosted and administered by National Department of Transport.

The DRP and BCP will therefor address backup equipment for example routers and switches to be utilized as replacements if faulty routers or switches cause downtime.

## 6. IDENTIFICATION OF KEY IT BUSINESS FUNCTIONS

6.1 Transversal Systems.

6.2 Internal Departmental Systems.

6.3 Telephone Systems.

6.4 Computer Hardware and User Backups.

6.5 Network equipment.

## 7. THE ROLE OF IT IN RELATION TO EACH BUSINESS FUNCTION.

7.1 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.

7.2 Telephone systems - Availability of a remote site with telephone communication network if disaster occurred.

7.3 Computer hardware and user backups – Ensure that all users have backup facility. Availability of an off-site backup of user backups is still a challenge.

7.4 Network Equipment – 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.

## 8. PRE- DISASTER ACTIONS TO ENSURE READINESS

8.1 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. All PERSAL transactions are currently centralized and captured at Provincial Office.

| Site | Users | System | Alternative site |
|---|---|---|---|
| Ocean Echo Building – 3rd floor – Kimberley | 5 | PERSAL | No alternative site |
| Ocean Echo Building – 5th floor– Kimberley | 10 | PERSAL | No alternative site |
| Ocean Echo Building – 3th floor– Kimberley | 31 | BAS | No alternative site |
| Ocean Echo Building – 3rd floor– Kimberley | 19 | LOGIS | No alternative site |
| Ocean Echo Building – 2nd Floor - Kimberley | 13 | NLTIS | Alternative site |

8.2 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.

8.3 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 and traffic station with a shared drive available for user backups.

8.4 Network Equipment – Minimum stock level of network equipment should be in place to ensure availability of network in case of a disaster. **2** routers and **3** 24 port switches should be in stock to serve as backup equipment.

## 9. WHAT CONSTITUTES A DISASTER?

A disaster will occur due to natural disaster for example floods, fire, earthquakes and tornadoes or power failures and faulty data lines.

A DRP involves the timely recovery of information technology assets and services after a disaster such as a fire or multiple hardware failure occurs.

A BCP is broader that a DRP in that it plans for contingency measures in the entire organization's business processes to prevent disasters.

## 10. ACTION PLAN I.T.O. DIFFERENT KEY BUSINESS FUNCTIONS AFTER DISASTER OCCURRED.

This document will provide the Department with 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 Senior Managers.

In an event where the Department 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.
Facility Management Official – Responsible for office accommodation and assessment of buildings.
Finance representative – Responsible for BAS.
Finance representative responsible for LOGIS
Human Resource representative – Responsible for PERSAL.
Directorate: Transport Operations – Representative for NLTIS.
Directorate: Transport Regulations – Representative for NTCM.
Physical Security Representative – Responsible for security issues.
Records Manager – Responsible for Registry.
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 Senior Manager (Corporate Services) should contact the HOD and inform 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 2.
- 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.

## 11. RECOVERY POINT OBJECTIVE (RPO)

The Recovery Point Objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure. The RPO is expressed backward in time from the instant at which the failure occurs, and can be specified in seconds, minutes, hours, or days.

Once the RPO for a given computer, system, or network has been defined it determines the minimum frequency with which backups must be made. This, along with the recovery time objective (RTO), helps administrators choose optimal disaster recovery technologies and procedures.

For example, if the RPO is one hour, backups must be made at least once per hour. In this case, external, redundant hard drives may prove to be the best disaster recovery solution. If the RPO is five days (120 hours), then backups must be made at intervals of 120 hours or less. In that situation, tape or recordable compact disk (CD-R) may be adequate.

As mentioned previously the Department does not have any systems that require backups. Backups for transversal systems are done by Treasury and other systems for example NTCM, NLTIS etc are National web-based systems.

Users are responsible to do backups of normal user data to either servers or external hard disks or CD's and DVD's. The RPO for user data is five days (120 hours) and therefor users should ensure that backups are done at intervals of 120 hours or less.

## 12. DISASTER RECOVERY PLAN

**Recovery overview:**

This DRP and BCP only address backup equipment for example routers and switches to be utilized as replacements if faulty routers or switches cause downtime. Alternative sites for transversal systems and NTCM, NLTIS and are currently available and active.

This plan will therefore not address post recovery verification, procedures for maintaining service in recovery mode, procedures for restoration to a permanent site etc.

| Threat | Steps | Instruction |
|---|---|---|
| Natural disasters, Floods, Fire, earthquakes and Tornadoes | Identification of alternative sites as disaster recovery sites. | Sites will be identified by Infrastructure and Facilities Management. For the purpose of this document and in the interim other Departmental buildings will be used where available in the different towns. Where other offices are not available other Departments will be requested via the HOD to host essential services. |
| | Evacuate affected | If the emergency requires |

| | | |
|---|---|---|
| | facility. | evacuation of employees, execute evacuation plans contained in Emergency procedure plan. |
| | Go to staging areas | Follow building evacuation instructions |
| | Determine length of outage. | Review written and verbal damage reports from ERT and estimate time the facility will be uninhabitable. |
| | Select disaster level. | HOD/ERT should declare the disaster level based on the estimated duration of the outage, L1 – Less than 48 hours, L2 – 48 hours to 6 weeks, L3 – 6 weeks and longer. |
| | Activate alternative facilities | Contact alternative facilities identified by the facilities unit. Confirm their availability and alert them of resettlement of equipment. |
| | ERT establish command centre | ERT should be the first to arrive at alternative facility to setup and organize the command centre prior to the arrival of essential personnel. |
| | Establish situation desk. | At the command centre establish a dedicated line with an operator to handle all incoming calls. |

| | | |
|---|---|---|
| | Create Technology shopping list | Once the technology requirements of the office are known, create a requirements list for the support staff. |
| | Obtain emergency approval from HOD. | Order emergency equipment via emergency application. |
| | Retrieve vital records from backup facility. | Retrieve vital records from alternative locations. |
| Power Failures | Determine level of outage. | ERT should declare the disaster level based on the estimated duration of the outage, L1 – Less than 48 hours, L2 – 48 hours to 6 weeks, L3 – 6 weeks and longer. |
| | Avail power generator. | Power generator backup to be taken to office for network and critical functions only. |
| | Fuel procured for time of emergency | Emergency procurement obtained from HOD to procure fuel for generator. |
| Faulty Data lines | Determine cause of network downtime | IT Unit to troubleshoot network equipment to establish cause of network downtime.<br>If cause is faulty router or switches it should be replaced with backup network equipment stored in IT container |
| | Determine duration of network downtime | IT Unit should report faulty data line at SITA call centre |

| | | |
|---|---|---|
| | | and obtain clarity on the duration of network downtime. |
| | Configure equipment for users to capture data on transversal systems at alternative sites. | If equipment is not available at alternative sites IT will provide temporary equipment and configure it to access the network.<br>The IT Unit should liaise with Treasury to link the users with the necessary LU's and setup the transversal printing settings to enable printing on the temporary equipment. |

## 13. TESTING OF THE DRP

The ERT will be responsible to test the DRP bi-annual and report the test results to the DRP Committee.

Testing will focus on the following:

- Testing of DRP backup network equipment (routers, switches and fibre converters).
- Test restoring of user backups.
- Test capturing of data on transversal systems at alternative sites.
- Evaluate effectiveness of ERT members to ensure speedy and successful recovery process.

## 14. PLAN STORAGE

The DRP will be distributed to members of the DRP Committee. Members of the ERT must however sign for receipt of a copy of the DRP.

Copies of the DRP will also be stored in the Ocean Echo Building server room.

**APPROVED / NOT APPROVED**

**Mr. M. P. DICHABA**
**HEAD OF DEPARTMENT**

**DATE:** 26/06/2020

## 9. PREVENTATIVE MEASURES (BCP)

### 9.1 Action plan

| Risk Areas | Subject | Action Plan | Time Frame | Responsibility |
|---|---|---|---|---|
| 1. **Transversal Systems** PERSAL/BAS/ LOGIS | 1.1 Maintenance of Computers | Maintain equipment as reported on Helpdesk System | According to strategic plan | IT |
| | 1.2 Ensure minimum required access to all transversal systems. | • Identify critical posts<br>• Identify alternative sites per offices including regional offices and traffic stations in case of disaster. | • Completed<br>• Completed | Finance / HR<br>IT |
| | 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<br>Legal Services |
| | 1.4 Ensure backup equipment for Network e.g. Routers and Switches. | • Purchase 1 x router and 6 x 24 port switches | • Completed<br>• Completed | IT<br>IT |
| | 1.5 Training. | • In-house training to ensure multi-skilling of transversal system users. | Ongoing | Finance / HR |
| | 1.6 Ensure backup printers are in place for LOGIS | • Identify backup Dot Matrix and Lazer printers<br>• Test functionality of printers | • Completed<br>•Ongoing | SCM/IT<br>SCM/IT |
| 2. **User Backups** | 2.1 Ensure Backup Facilities for all users. | • Develop template to rate data to be backed up.<br>• Install Novell Netware servers at 10 Traffic Stations and 5 Regional Offices.<br>• Install shared drive for backups for:<br>- Enatis sites<br>- NTCM sites | Completed<br>Completed<br>Completed. | Record Management<br>IT<br>IT |
| | 2.2 Backup Servers / Regular Off | • Test & copy files to DVD's | Monthly | IT |

| | | | | |
|---|---|---|---|---|
| | Site Backups | • Maintain a register for monthly backups | | |
| | 2.3 Ensure security of servers | • Install servers in secure network rooms.<br>• Install fingerprint access control, CCTV cameras, fire suppression, and climate control at Ocean Echo Building and ENatis server rooms. | Completed<br>Completed | IT<br>IT |
| | 2.4 Backups at remote Sites | • Encourage users to do backups to removable storage media. | Monthly | IT |