DISASTER RECOVERY PLAN

Date of adoption: 23 May 2017
Council resolves to adopt the under-mentioned revised policy as the Information Technology Policy of the DR BEYERS NAUDE LOCAL Municipality

TABLE OF CONTENTS

1. INTRODUCTION

This is a systematic process to prevent, predict and manage Information and Communication Technology (ICT) disruptions and incidents which have the potential to disrupt the municipality ICT services. It is planned to result in a more resilient ICT service capability aligned with the objectives of Sarah Baartman District Municipality (BNLM)

ICT Business Continuity describes the daily ICT activities that are undertaken to enable the municipality 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 disruption event take place which impacts the ability of the organization to continue to provide its key services, the ICT systems and electronic data are crucial components of the processes and their protection and timely return is of utmost importance.

2. DEFINITION OF A DISASTER

A disaster can be caused by people, natural occurrence or technical catastrophe. This would result in BNLM's employees not being able to perform all or some of their roles and responsibilities. BNLM defines disasters as the following:

- The building is accessible but one or more vital systems are non-functional;
- The building is not accessible for a period of time but all systems are functional within it; and
- The building and all systems are non-functional

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

- Fire
- Flash flood
- Pandemic (Virus Attacks)
- Power Outage
- War
- Theft
- Terrorist Attack

3. PURPOSE

The purpose of this Disaster Recovery Plan (DRP) document is twofold: first to capture all of the information relevant to the municipality's ability to withstand a disaster, and second to document the steps that the municipality will follow if a disaster occurs.

In the event of a disaster the first priority of the ICT Unit is to prevent the loss of data.

The second priority of the ICT Unit will be to enact the steps outlined in this DRP to bring all of the municipality's groups and departments back to business-as-usual as quickly as possible. This includes:

- Preventing the loss of the municipalities' resources such as ICT hardware, software and data.
- Minimizing downtime related to ICT
- Keeping the business running in the event of a disaster

The BNLM DRP takes all of the following areas into consideration:

- Network Infrastructure
- Servers Infrastructure
- Telephone System
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems
- ICT Documentation

This DRP does not take into consideration any non-ICT, personnel, records and real estate related disasters.

4. DISASTER RECOVERY TEAM AND RESPONSIBILITIES

In the event of a disaster, the following are key participants who shall be required to restore normal functionality to the employees of the municipality:

- Director: Finance and Corporate Services (Disaster Recovery Lead)

- ICT Unit (Technical Team)
- ICT Service Providers (Relevant to the Disaster)

The Disaster Recovery Team will be responsible for assessing damage specific to any network and server infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the municipality as well as telephony and data connections with the outside world. They will also be responsible for providing the physical server infrastructure required for the municipality to run its ICT operations and applications in the event of a disaster. They will be primarily responsible for providing baseline functionality.

4.1Role and Responsibilities

- In the event of a disaster that does not require migration to standby facilities, the team will determine which network services and servers are not functioning at the primary facility
- If multiple network services and servers are impacted, the team will prioritize the recovery of services in the manner that will minimize the impact on the municipality by addressing the high priority areas first.
- If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
- In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility
- Once critical systems have been provided with connectivity, employees will be provided with connectivity
- Install and implement any tools, hardware, software and systems required in the secondary facility
- Re-install and implement any tools, hardware, software and systems required in the primary facility
- After BNLM is back to business as usual, this team will provide a detailed report to the Disaster Recovery Lead summarizing their activities during the disaster including costs incurred.

5. DATA STORAGE AND BACKUPS

This section explains where all of the municipality’s data resides as well as where it is backed up to. This information is used to locate and restore data in the event of a disaster.

The municipality server and network rooms are located on the 1st floor. The Data Backups are stored on the 2nd floor in a locked fire proof safe.

The marking of the tapes is just as important. The ICT Unit must mark the label on the tape and not on the cover to avoid tapes being placed in incorrect cases.

The documentation of tapes is important. When removing tapes from the safe, it must be documented into the Backup Tape log book. This will prevent any confusion regarding tape and dates used.

Data is backed-up in the following manner:

5.1 Windows System:

The windows system is backed-up daily, weekly, monthly and yearly by using back-up tapes as follows:

- There is a series of 20 tapes to back-up Mondays to Thursday's differential data for the month.
- There is a series of 5 tapes to back-up full weekly data on Fridays for the month.
- There is a series of 12 tapes to back-up full monthly data on the last Friday of each month.

Backup Solution Windows machines					
	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
Week 1	Differential	Differential	Differential	Differential	Full
Week 2	Differential	Differential	Differential	Differential	Full
Week 3	Differential	Differential	Differential	Differential	Full
Week 4	Differential	Differential	Differential	Differential	Full
Week 5	Differential	Differential	Differential	Differential	Full
Last Friday of the month			**Full Monthly**		
Yearly - Last Friday of the year			**Full Yearly**		

5.2 Linux Server

The Linux server is backed-up daily, monthly and yearly by using back-up tapes as follows:

- There is a series of 25 tapes to back-up Mondays to Fridays full data for the month.
- There is a series of 12 tapes to back-up full monthly data on the last Friday of each month.

Backup Solution Linux machine					
	Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
Week 1	Full	Full	Full	Full	Full
Last Friday of the Month			**Full Monthly**		
Yearly Backup			**Full Yearly**		

The procedure to back-up the PROMUN Server is attached as Annexure A.

The above back-up tapes are rotated in a manner to ensure that all data backed-up is up to date.

The backup tapes are rotated daily and signed off by the allocated ICT Personnel as “back-up completed” in the Back-up Register. The Systems Administrator will ensure that the back-up was successful and will sign off Back-up Register.

5.3 Data back-up in order of Priority

The servers are backed-up in the following order of priority:

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)

1	User Data and Network Groups	Confidential,	Daily at 7:00 pm	Backed up to External HDD
2	PROMUN Finance System application	Confidential	Daily at 9:00 pm	Backed up to tape drives
3	SYNTELL database	Confidential	Daily at 7:00pm	Backed up to External HDD
4	GIS APP Server	Public	Daily at 7:00pm	Backed up to External HDD
5	MunAdmin	Confidential	Daily at 7:00pm	Backed up to External HDD

6. RESTORING ICT FUNCTIONALITY

Should a disaster occur, the municipality will implement the DRP. This section will be referred to frequently during the implementation of the DRP, as it provides the Disaster Recovery Team with the necessary information that defines the manner in which the municipality's information system will be recovered.

6.1 Restore Scenarios

The restore procedures are equally important to the backup procedures. It is from these restores that any work will be recovered. *Listed below are some scenarios where recovery is required. It also explains the recovery procedure.*

Windows 2008 File Server/Exchange 2008 Windows systems

- <u>Disk failure</u>

The Systems Administrator must notify the Director: Finance and Corporate Services immediately

The Systems Administrator must notify users of the possible downtime and brief reason thereof

The disk needs to be replaced and a restore needs to be performed immediately by the Disaster Recovery Team

- File corruption

  The Systems Administrator must notify the Director: Finance and Corporate Services immediately

  The Systems Administrator must notify the relevant users or department(s) of the affected file and the estimated time of recovery

  The Disaster Recovery Team must restore last successful backup

- Problems caused by a user

  The Systems Administrator must notify the Director: Finance and Corporate Services immediately.

  The Disaster Recovery Team must immediately address the problem

- Theft of the Server

  The Systems Administrator must notify the Director: Finance and Corporate Services immediately

  The Systems Administrator must notify users of the possible downtime and brief reason thereof

  The Systems Administrator must notify Asset Management immediately to initiate the insurance claim process

  The Disaster Recovery Team must procure a new server immediately

  The Disaster Recovery Team must setup and configure the new server with the same Redundant Array of Inexpensive Disks (RAID) configuration.

  The Disaster Recovery Team must restore the last successful backup

Linux Server (PROMUN Server)

- Sever failure

  The Systems Administrator must notify the Director: Finance and Corporate Services immediately

The Systems Administrator must inform the Senior Manager: Finance as well as the financial system service provider (RDATA)

The Systems Administrator must notify users of the possible downtime and brief reason thereof

The server needs to be replaced and/or restored from full system back-up tape immediately by the Disaster Recovery Team

- Disk failure

  The Systems Administrator must notify the Director: Finance and Corporate Services immediately

  The Systems Administrator must inform the Senior Manager: Finance as well as the financial system service provider (RDATA)

  The Systems Administrator must notify users of the possible downtime and brief reason thereof

  The Disaster Recovery Team will replace the failed disk immediately and restore the data lost by using the backup tape (if there is any data loss).

- PROMUN data or design files corruption.

  The PROMUN system can be corrupted when the following happens:

o When a machine shuts down while users are busy.

o The above can be caused by someone switching off the machine or a power failure with no UPS.

o Incorrect database shutdown.

- Hard disk failure.

  In the event of any of the above occurrences, the following is required:

The Systems Administrator must notify the Director: Finance and Corporate Services immediately

The Systems Administrator must inform the Senior Manager: Finance as well as the financial system service provider (RDATA)

The Systems Administrator must notify users to log off of the system, possible downtime and brief reason thereof

The data and design files need to be restructured and/or restored from full system back-up tape immediately by the Disaster Recovery Team

The procedure to restore data on the PROMUN Server is attached as Annexure A.

- Theft of the Server

The Systems Administrator must notify the Director: Finance and Corporate Services immediately

The Systems Administrator must notify users of the possible downtime and brief reason thereof

The Systems Administrator must notify Asset Management immediately to initiate the insurance claim process

The Disaster Recovery Team must procure a new server immediately

The Disaster Recovery Team must setup and configure the new server with the same Redundant Array of Inexpensive Disks (RAID) configuration.

The Disaster Recovery Team must restore the last successful backup

7. CURRENT SYSTEM ARCHITECTURE

The municipality’s ICT Infrastructure Architecture is depicted in the diagram below:

ADD DIAGRAM HERE!

ICT Systems

The municipality utilizes the following ICT Systems:

No.	ICT System	System Description
1	Microsoft Server 2012 R2 Standard	Domain Controller for user creation and Group Policies

2	W2k8 Active Directory (Dynamic Host Configuration Protocol (DHCP),Domain Name System (DNS))	W2k8 Active Directory is the system used to manage the users and computers connected to the municipal domain (bnlm.gov.za)
3	PROMUN Finance System	Linux Server hosts the municipal Finance System (PROMUN)
4	ESET Antivirus	ESET Endpoint Antivirus Server hosts the municipal antivirus software
5	Centos Firewall	Linux Firewall Server protects the programs on the Linux Server from external network attacks.
6	Internet Proxy	Internet Proxy controls the internet traffic.
7	Routers and Switches	Routers and Switches enable network connectivity of the municipality
8	Cisco Call Manager	Cisco Call Manager is the Telephone Management System Server that manages the telephones of the municipality.
9	Geographic Information System App Server	Geographic Information System App Server hosts the GIS application of the municipality
10	Performance Management System Server	Performance Management System Server hosts the Performance Management System application of the municipality

8. PLAN TESTING AND MAINTENANCE

While efforts were made to develop this DRP as complete and accurate as possible, it is essentially impossible to address all possible problems at any given time. Additionally, over time the DRP needs of the municipality will evolve. As a result of these factors, this plan will need to be tested on an annual basis to identify errors and omissions that will then be factored into future DRP’s.

8.1 Maintenance

The DRP will be updated annually or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the municipality in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

- Ensuring that call trees are up to date
- Ensuring that all team lists are up to date
- Reviewing the plan to ensure that all of the instructions are still relevant to the municipality
- Making any major changes and revisions in the plan to reflect municipal shifts, changes and goals
- Ensuring that the plan meets any requirements specified in new laws
- Other municipal specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the municipality, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

8.2 Testing

BNLM is committed to ensuring that this DRP is functional. The DRP should be tested annually in order to ensure that it is still effective. Testing the plan will be carried out as follows:

1) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the Systems Administrator to draw upon a correspondingly increased pool of knowledge and experiences. Employees should be familiar with procedures, equipment, and offsite facilities (if required).

2) **Simulations-** A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a

reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

3) **Parallel Testing**- A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

4) **Full-Interruption Testing**- A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

9. REVIEW

This ICT Disaster Recovery Plan shall be reviewed at least annually.

ANNEXURE A: PROMUN BACK-UP AND RESTORATION PROCEDURE

PROMUN System Back-up

A scheduler like NT's called cron will read the crontab file and at a set time will duplicate the data to tape.

What does the backup include?

The entire system excluding raid1 is backed up every day. This includes all PROMUN system files, all data files and all print files as well as all user and system utility files.

How does the backup take place?

Cron tab runs the nightly procedure which consists of the following steps:

1. A “shutdown” command is executed at 22:00 Sunday to Friday.
2. At 23:00 a clean-up is done using a script called CYPCLEAN which copies files recursively from /home/prints to the appropriate daily directories.
3. At 1:00 a script called WBACKUP runs the CPIO backup onto the small tape.
4. At 3:30 the ufsback script runs a command – ufsdump and this backs up all the data onto the large tape.

When does the backup take pace?

How does the scheduling work? The entries in the crontab file are lines of six fields each. The fields are separated by spaces or tabs. They have the following values:

- Minute (0-59)
- hour (0-23)
- day of the month (1-31)
- month of the year (1-12)
- day of the week (0-6 where 0 = Sunday).

The actual backup commands or dump commands are stored in the cron file. Crontab just schedules these commands.

To access crontab type the following:-

crontab –l	to list
crontab –e	to edit
crontab backup	will schedule the backup as specified
crontab –r backup	will remove a scheduled back

RESTORATION OF DATA FROM TAPES

- Make sure that all users are off the system.
- Make sure the right tapes are in place to do the restore.
- Use the following command as an example to restore from the large tape (ufsback):

Firstly change directory into the folder that you want to restore to.

To extract use ufsrestore ivfs /dev/rmt/1h *

- 1 = raid
- 2 = home
- 3 = var
- 4 = usr
- 5 = opt
- 6 = / (root)

To restore something on raid replace the * above with 1 for raid.

Eg ufsrestore ivfs /dev/rmt/1h 1

Change directory to the desired directory within the dump volume.

To add files to a list to be restored use the command – add.

Wild card characters can be used for this.

Files are marked for restore with an asterisk (*).

Files can also be removed from the extraction list with the delete command.

When all files are selected extract them from the dump volume using the extract command.

This will then be displayed;

```
Extracted requested files

You have not read any volumes yet.

Unless you know which volume your files are on you

Should start with the last volume and work towards the first.

Specify next volume #: 1

Extract file ./.filename

Add links

Set directory mode, owner, and times.

Set owner/mode for ‘.’? [yn] n
```

To restore from the little tape (CPIO) do the following:

Log on as root

Go to root (cd /)

If restoring from raid the next step is not necessary.

Forward the tape cpio –itvc –C65536</dev/rmt/0hm

Make a new or temp directory eg: mkdir temp

Go to this directory e.g. cd temp

Wildcards may be used when using CPIO but may never be used if using TAR

To restore enter the following commands:

```
   Cpio –idvcu –C65536 “PROMUNdata/DIV/SAL/Data/*” </dev/rmt/0h
```

(no slash is required in front of PROMUN data)

Notes: -u = unconditionally overwrite existing file

-I = extracts files from the standard input

-c = read or write header information in ASCII character form for portability

-d = create directories as needed

-v = verbose (print a list of file names)