

WEST RAND DISTRICT MUNICIPALITY



DATA BACKUP PROCEDURE

<u>NAME AND POSITION</u>	<u>DATE</u>	<u>SIGNATURE</u>
M E Kolozi MUNICIPAL MANAGER	10/12/2024	

CONTENTS

1.	INTRODUCTION	1
2.	DEFINITIONS.....	1
3.	PURPOSE AND SCOPE.....	1
4.	Roles and Responsibilities.....	2
5.	PROCEDURE	3
6.	PROCEDURE REVISION	4

1. INTRODUCTION

ICT aim to highlight to the user how and when the backup is run and what is actually backed up. This Procedure provides good advice on how staff can ensure their work data is stored safely.

2. DEFINITIONS

The definitions are described in the table below

TERM	DEFINITION
WRDM	Shall mean West Rand District Municipality
Back-Up data	To back up data is to copy it to another medium or other facility so that, if the active data is lost, it can be recovered in a recent if not completely current version. Backup is primarily intended for disaster recovery, and the assumption is that in most cases the Backed-up data will not be read.
To archive data	To move them to another medium for long term storage. Archive is intended for the storage of data that do not need to be kept immediately accessible, but which may possibly be needed at some point in the future.
The distinction between backup and archive	Is not absolutely clear if data are backed up, and then subsequently the original, more accessible copies are deleted, the backed-up copies effectively become an archive.
The Backup Process	Does not include the physical Operating System of such device, but rather the important Data on it.

3. PURPOSE AND SCOPE

The purpose of this procedure is as follows:

- ✓ To safeguard the information assets of WRDM.
- ✓ To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- ✓ To permit timely restoration of information and business processes, should such events occur.
- ✓ To manage and secure backup and restoration processes and the media employed in the process.

This procedure applies to all servers in Information and Communication Technology (ICT), including all Network Attached Storage Devices (NAS).

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.

Backup retention periods are in contrast to retention periods defined by legal or business requirements.

System backups are not meant for the following purposes:

- ✓ Archiving data for future reference.
- ✓ Maintaining a versioned history of data.

4. ROLES AND RESPONSIBILITIES

4.1.1 ICT Manager

- Identify critical systems and data to be backed up
- Oversee the backup process
- Regularly validate backup jobs
- Determine frequency and retention of backup
- Ensure backup schedule is adhere to

4.1.2 Service provider

- Provide advice on backup and storage services
- Manage and maintain backup systems
- Verify all backup jobs
- Provide report of jobs success / failure.
- Perform file restore operations are required.
- Performs DRP test quarterly

4.1.3 Network Administrator

- Maintain applications and system software
- Regularly validate backups
- Restore, recover and test data from backup systems

4.1.4 ICT Steering committee

To ensure timeous review of the ICT policies

To advise on amendments and implementation of the policies

To recommend reviewed ICT policies to serve at other committees of council prior to approval

4.1.5 Internal audit

To assess business processes within ICT

To assess the efficacy of risk management efforts

To evaluate internal controls and provide improvement recommendations

To assess governance risk and compliance within ICT.

5. PROCEDURE

Systems will be backed up according to the schedule below:

5.1 User data saved in “my documents” will be redirected to 107EOC file server under “userdata” then backed up daily, (Mon.-Sun.) stored and automatically pushed to an off-site storage location via encrypted ftp protocols.

5.2 The Munsoft/Payday System will be backed up by a service provider (Munsoft) on a daily basis and will be stored off-site.

5.3 User to use OneDrive to backup laptop or computer data for ease of data restoration in case the device is lost.

5.4 The Virtual Machine Servers will have its VM data regularly backed up as follows:

- ✓ Backups of virtual machine data will be taken from Mon-Sun. These backup files will be stored on-site on the Backup Server and off-site.
- ✓ File and folder full backup will be taken on Mon-Sunday. These backup files will be stored off-site.

5.5 Backup Media described below:

- ✓ Currently all backups will be written to Disk, a RAID5 Set in the WRDM-Backup Server.
- ✓ Daily backups will be stored on-site in an encrypted format on a Server in a physically secured area.
- ✓ Daily backups will be maintained for one week.
- ✓ Weekly backups will be stored on-site on a Server, in a physically secured area. Weekly backups will be maintained for a period of three weeks.

5.6 Backup Review

On a daily basis, backup notification are sent to specific personnel in ICT for the following purposes:

- ✓ To check for and correct errors and escalate issues of concern.

5.7 Pro-active

ICT will identify problems and take corrective action to reduce any risks associated with failed backups:

- ✓ Restore tests will be done quarterly in order to verify that backups have been successful.
- ✓ ICT will maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this Procedure for auditing purposes.

5.8 Data Recovery

- ✓ In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.
- ✓ In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.
- ✓ In the event that the local Financial, Hr and payroll system is lost, the systems can be started from a remote site hosted by the service provider within 2 hours.

5.9 Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made to WRDM ICT Helpdesk.

6. PROCEDURE REVISION

The procedure will be reviewed biennial.