OVERBERG

DISTRICT MUNICIPALITY

ICT DISASTER RECOVERY PLAN
2025/26 -2026/27

Council Resolution No:	……
Date:	……
Municipal Manager:	……
Executive Mayor	……
Reference No:	……
Municipal Code No:	……

Table of Contents

Glossary of Abbreviations

Abbreviation	Definition
BCMS	Business Continuity Management System
BC	Business Continuity
DR	Disaster Recovery
DRP	Disaster Recovery Plan
HR	Human Resources
ICT	Information and Communication Technology
MTO	Maximum Tolerable Outage
RTO	Recovery Time Objective
RPO	Recovery Point Objective
ITIL	Information Technology Infrastructure Library
RACI	Responsible, Accountable, Consulted, Informed
IROC	ICT Recovery Operations Centre
BAU	Business As Usual
VM	Virtual Machine

1. INTRODUCTION

This plan guides the Overberg District Municipality in the establishment, operation and continuous improvement of an ICT DR Framework: a system of five inter-dependent documents that co-exist to support the most important document i.e., the ICT DR Plan.

This plan provides background information on what ICT Disaster recovery is, as well as the role of this ICT plan, to provide governance and controls to manage the ICT Recovery capability of the Overberg District Municipality.

The plan supports the Overberg District Municipality's ICT Governance Policy and was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

2. LEGISLATION

The plan was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this plan:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- Copyright Act, Act No. 98 of 1978.
- Electronic Communications and Transactions Act, Act No. 25 of 2002.
- Minimum Information Security Standards, as approved by Cabinet in 1996.
- Municipal Finance Management Act, Act No. 56 of 2003.
- Municipal Structures Act, Act No. 117 of 1998.
- Municipal Systems Act, Act No. 32, of 2000.
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
- Promotion of Access to Information Act, Act No. 2 of 2000.
- Protection of Personal Information Act, Act No. 4 of 2013.
- The Disaster Management Act, Act No. 57 of 2002; Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT standards were leveraged in the development of this plan:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014.
- Control Objectives for Information Technology (COBIT) 5, 2012.
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE PLAN

The objective of this document is to guide Overberg District Municipal management to define an effective and sustainable ICT DR Plan that will enable the Overberg District Municipality to enact an orderly and timely recovery from a Disaster or disruptive incident.

The controls within this plan seek to achieve the following objectives:

- Provide guidance on developing all related ICT DR documents and prioritise the reason for the inter-relationships.
- Protect the operations of the Overberg District Municipality, consumers, licensees, stakeholders and staff by minimising the impact of significant interruption to the Overberg District Municipality through the effective implementation and maintenance of ICT DR arrangements and solutions.
- Recover the critical prioritised operations and services, in a controlled manner to meet the requirements of the department, law, regulation or other factors; and
- Ensure that business continuity is an essential part of business planning and future development, and that this plan be integrated into an overall municipal Disaster Management Plan at a later stage of business continuity being improved.

4. THE AIM OF THIS PLAN

The aim of this plan is to ensure that the Overberg District Municipality conforms to standardised ICT Disaster recovery governance and controls, in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that the risks associated to the management of effective ICT DR, are mitigated. This plan supports the Overberg District Municipality's Corporate Governance of ICT Policy.

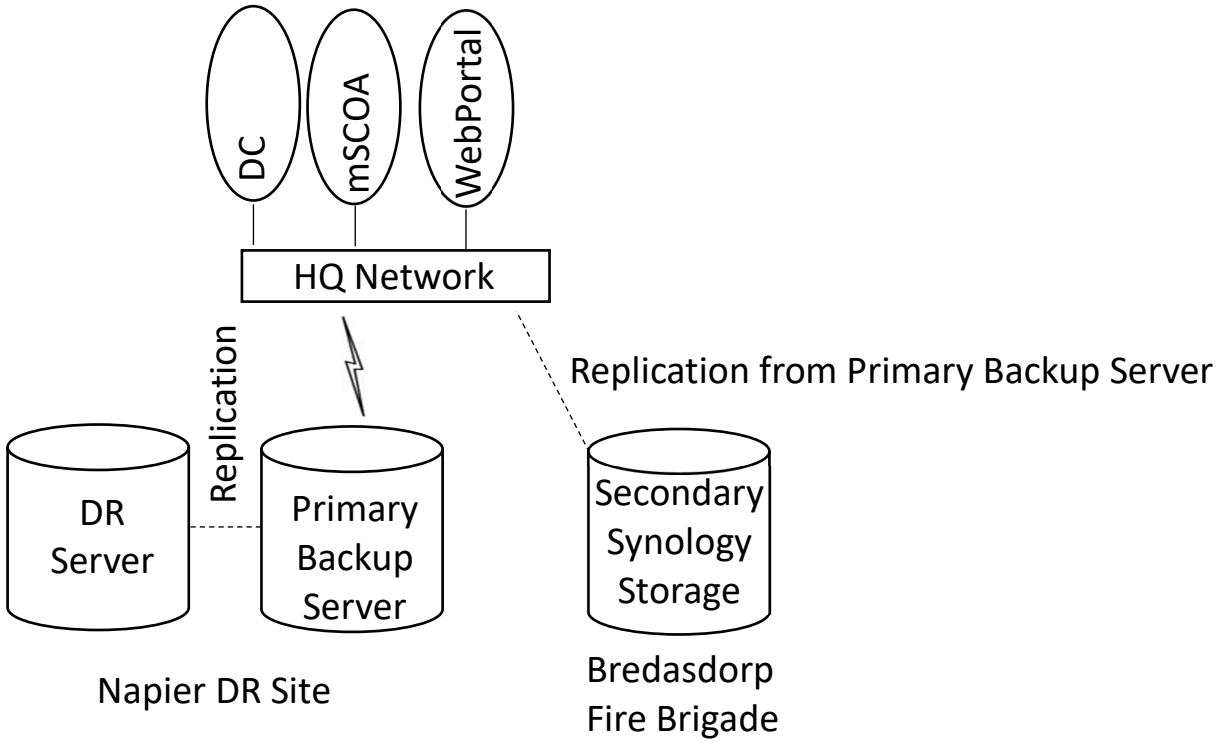
5. APPLICATION & SCOPE OF PLAN

The ICT DR plan will become a part of business continuity frameworks (such as BCMS – see Legislation Section) but focuses on a “fit for purpose” ICT DR approach that guides the authorised personnel, to recover internal and external ICT systems in the event of a Disaster.

The plan applies to everyone in the Overberg District Municipality, including its service providers/vendors. This plan is regarded as being crucial to the operation and availability of ICT systems of the Overberg District Municipality.

This DR plan and its inter-related documents gives full effect to the management of Disaster recovery in the Overberg District Municipality, as demonstrated in the high-level landscape of inter-related documents.

6. ICT SERVER INFRASTRUCTURE



7. CURRENT CONFIGURATION

The current configuration consists of three host servers with virtual machines (VM) connected to them, namely:
DC: Primary Active Directory, Vanilla Samras, PayDay and PayDay UAT
mSCOA: Samras Web and Samras Web UAT
WebPortal: SamrasPLUS and Secondary Active Directory

The host servers are connected to the network via CAT 6 network cable using Gigabit Power over Ethernet (PoE) switches. Backups are configured to start every hour between 07:00 and 17:00 and in the evening. The server stores its backups on the Primary Backup Server. The Backup Server also replicates to both the DR server and secondary Synology storage once the backup is completed.

7.1 IN THE EVENT OF A DISASTER:

VM server failure scenario:
If one of the Virtual Machines fails/is lost during disaster or cyberattack, IT will start up the virtual equivalent on the disaster recovery server. Repairs and/or data restoration will be done on the faulty Virtual Machine and will be powered on once concluded.
RTO: 10 minutes

Host server failure scenario:
If an entire host fails, then all VMs hosted on that host server will be powered on in the DR server. Repairs and/or data restoration will be done on all affected VMs and will be powered on once concluded. If the host is not repairable, a new host will be procured using the SITA transversal tender.
RTO: 30 – 60 minutes

8. DISASTER NOTIFICATION

Steps to be taken in the event of a server failure:

1. An email will be sent to employees notifying them of a server failure.
2. The replica of the failed server will be started in the DR environment to allow users to continue to work.
3. Repairs and/or data restoration will be performed on the failed server.
4. Once the failed server is restored, any changes made to the DR server environment will be copied back to production.
5. The production server will be brought back online.
6. An email will be sent to employees notifying them that the original server is back online.

9. TESTING OF DR PLAN

Testing of the DR Plan will be done twice a year.
The Recovery Point Objective (RPO) is one hour, as backups are done hourly.
The following will be tested:

- Network connectivity (Active Directory)
- Integrity of backup data