OVERBERG

DISTRICT MUNICIPALITY

ICT MIGRATION & DISASTER RECOVERY POLICY/PLAN 2020/21 -2022/2023

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

1. 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

2. INTRODUCTION

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

The policy 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.

3. LEGISLATION

The policy 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 policy:

- 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 policy:

- 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.

4. OBJECTIVE OF THE POLICY

The objective of this document is to guide Overberg District Municipal management to define the ICT DR policy so that an effective sustainable ICT DR Plan enable the Overberg District Municipality to enact an orderly and timely recovery from a Disaster or disruptive incident.
The controls within this policy 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 policy be integrated into an overall municipal Disaster Management Plan at a later stage of business continuity being improved.

5. THE AIM OF THIS POLICY

The aim of this policy 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 policy supports the Overberg District Municipality's Corporate Governance of ICT Policy.

6. APPLICATION & SCOPE OF POLICY

The ICT DR policy 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.

This ICT DR Policy has been developed to guide and assist the Overberg District Municipality to be aligned with internationally recognised best practice DR controls and procedures. This policy further recognizes that municipalities are diverse and therefore

adopts the approach of establishing principles and practices to support and sustain the effective control of Disaster recovery in the Overberg District Municipality.

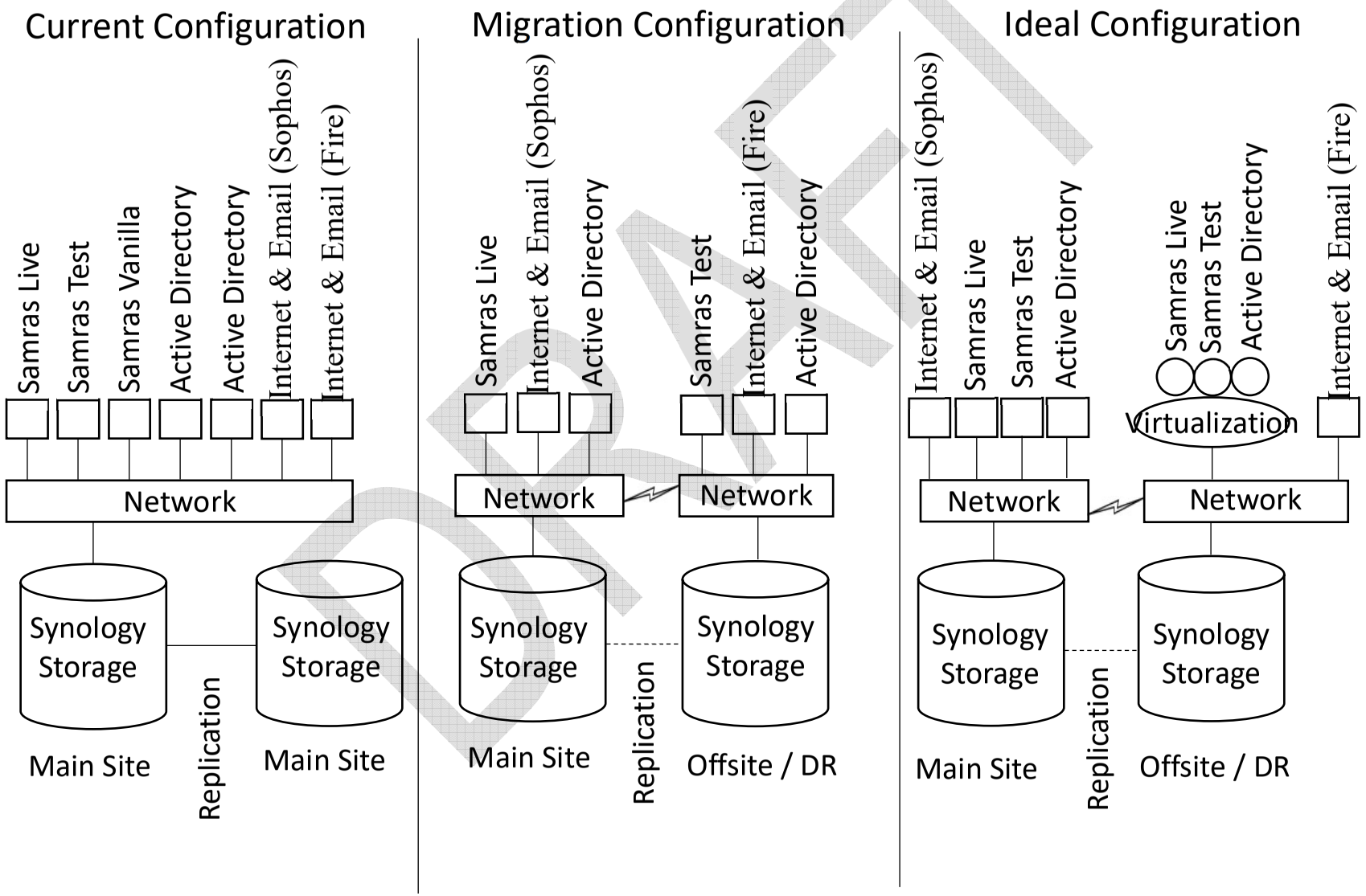
The policy applies to everyone in the Overberg District Municipality, including its service providers/vendors. This policy is regarded as being crucial to the operation and availability of ICT systems of the Overberg District Municipality.

To give full effect to the DR planning and preparation in the Overberg District Municipality, the broader group of ICT DR Documents are included in the planning process (see Section 7).

This DR policy 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.

7. ANNEXURE A MIGRATION / DISASTER RECOVERY PLAN

DIAGRAM:



CURRENT CONFIGURATION

The current configuration consists of the following:

- Two Active Directory servers
- Three SAMRAS servers (Live, Test and Vanilla)
- Two Synology backup devices
- One Sophos device for internet / email access
- One ADSL internet router for internet / email access (backup)

These servers are connected to the network via CAT 6 network cable using Gigabit Power over Ethernet (PoE) switches. Bytes estimate that the SAMRAS Vanilla system will be phased out by June 2018. Backups are configured to start in the evening. The server stores its backups on the storage system. In turn, this storage system replicates to another storage system early morning, using the same CAT 6 network cable and Gigabit PoE switch as mentioned above. The equipment mentioned above are all in the same building.

IN THE EVENT OF A DISASTER:

SAMRAS Scenario 1:
If one of the SAMRAS server fails/is lost during disaster, Bytes will do the necessary configuration to make the SAMRAS Test system work like the live system. A new server will be procured via the SCM processes and be configured as the new SAMRAS Test system.
Recovery Time: 6 working days

SAMRAS Scenario 2:
If both SAMRAS server fails/are lost during disaster, we will procure a new server via the deviation process. The server and backups will be taken to Bytes in Cape Town to do the required installations and uploads of data. After that, the new server will replace the old one. The second (test) server will be procured via the normal SCM process and be configured by Bytes to run as a test server.
Recovery Time: 6 working days

Active Directory Scenario 1:
If one Active Directory server fails/is lost during disaster, the second one is configured to automatically take over and continue the work.
Immediate Recovery

Active Directory Scenario 2:
If both Active Directory servers fail/are lost during disaster, we will procure a new server via the deviation process. IT will configure the new server with the required software in order for users to be able to log into their computers/laptops.
Recovery Time: 6 working days

Internet Scenario:

If the Sophos device fails, IT will reconfigure the network to use the ADSL router to provide internet to the users. When TWK Communications replaces the Sophos router, it will be configured to be the main internet supplier.
Recovery Time: 2 working days

Testing of the Disaster Recovery Plan in the Current Configuration is not financially feasible.

Migration Configuration

As part of getting ready for the ideal configuration, two servers will be moved to an offsite / DR location. This includes the following equipment:

- One Active Directory server
- The SAMRAS Test server
- The secondary Synology backup device
- One ADSL internet router for internet / email access (backup)

Both sets of equipment (the main site and DR site) will connect to the network via a wireless link. The backup schedule remains unaffected. The two Synology backup devices will replicate using the wireless link.

IN THE EVENT OF A DISASTER:

SAMRAS Scenario 1:
If one of the SAMRAS server fails/is lost during disaster, Bytes will do the necessary configuration to make the SAMRAS Test system work like the live system. A new server will be procured via the SCM processes and be configured as the new SAMRAS Test system.
Recovery Time: 6 working days

SAMRAS Scenario 2:
If both SAMRAS server fails/are lost during disaster, we will procure a new server via the deviation process. The server and backups will be taken to Bytes in Cape Town to do the required installations and uploads of data. After that, the new server will replace the old one. The second (test) server will be procured via the normal SCM process and be configured by Bytes to run as a test server.
Recovery Time: 6 working days

Active Directory Scenario 1:
If one Active Directory server fails/is lost during disaster, the second one is configured to automatically take over and continue the work.
Immediate Recovery

Active Directory Scenario 2:
If both Active Directory servers fail/are lost during disaster, we will procure a new server via the deviation process. IT will configure the new server with the required software in order for users to be able to log into their computers/laptops.
Recovery Time: 6 working days

Internet Scenario:
If the Sophos device fails, IT will reconfigure the network to use the ADSL router to provide internet to the users. When TWK Communications replaces the Sophos router, it will be configured to be the main internet supplier.
Recovery Time: 2 working days

Testing of the Disaster Recovery Plan in the Migration Configuration is not financially feasible.

IDEAL CONFIGURATION

The ideal configuration consists of the following:
Main Site:

- The SAMRAS Live server
- The SAMRAS Test server
- One Active Directory Server
- The primary Synology backup device

DR Site:

- One Virtualization server
- The secondary Synology backup device

The virtualization server is one physical server that will be capable of hosting the SAMRAS Live, SAMRAS Test and Active Directory servers. The two Synology backup devices will replicate using the wireless link.

IN THE EVENT OF A DISASTER:

Scenario:
If any physical server fails/is lost during disaster, its virtual counterpart will be turned on and the required configuration will be performed by IT and/or Bytes to ensure that the users can continue working. For example: If SAMRAS Live fails, the virtual SAMRAS Live will be turned on and configured. A new server will be procured via the SCM processes and be configured to replace the lost server.
Recovery Time: 6 working days

Internet Scenario:
If the Sophos device fails, IT will reconfigure the network to use the ADSL router to provide internet to the users. When TWK Communications replaces the Sophos router, it will be configured to be the main internet supplier.
Recovery Time: 2 working days

TESTING OF DR PLAN

Testing will be done annually although connectivity is an important activity, any issues regarding connectivity will be reported by the end-users when occurs.
The following will be tested:

- Network connectivity (Active Directory)

- SAMRAS connectivity
- Internet connectivity (Fire brigade ADSL)
- Test of SAMRAS functionality by the different user departments