CEDERBERG MUNICIPALITY

Cederberg Municipality

CEDERBERG

- Clanwilliam
- Citrusdal
- Lamberts Bay
- Elands Bay
- Graafwater
- Leipoldtville
- Wupperthal
- Elandskloof
- Paleisheuwel

ICT DISASTER RECOVERY POLICY

JANUARY 1, 2015

CEDERBERG MUNICIPALITY
2A – VOORTREKKER STREET – CLANWILLIAM - 8135

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

Glossary of Terminologies

Terminology	Definition
Business case	A formal requirement in order for a specific business function to perform its required task, such as to implement a project initiative.
Line manager	Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks.
Main Site	Municipal Head Office and assumed in some case to be the location of the Municipality Main Data Centre
Maximum Tolerable Outage	The amount of time the identified critical business function may be unavailable before the Municipality is severely impacted.
ICT Recovery Operations Centre	The offsite command centre that gets established, by approval within the framework of the ICT DRP, for the purpose of ICT recovery operations & necessary relocation of identified resources.
Simulation Lite	A simulation DR test conducted by 2-3 individuals, usually the ICT Manager, the ICT DR Team Leader and an assistant.
Procurement	The external acquisition of services, assets and consumables, whether by outright purchase, hire, licensing or outsourcing.

Terminology	Definition
Recovery Point Objective	The worst data loss that the Municipality is willing to accept. In other words, this is the point from which recovery of lost data must take place.
Service	A Service delivered to the municipality by ICT or by 3rd parties. Examples: email, Internet, printing.
Contract	An agreement (which may be verbal or in writing) entered into with the intention of creating legally binding consequences. The contract includes all annexures, schedules, etc., as well as any agreed amendments.
Incident	Typically impacts a specific service or server. Examples of Incidents include a compromised service resulting from a hacking attack or the partial loss of an office area due to a burst water pipe.
Disaster	A significant or unusual Incident that has long-term implications. An example of a Disaster would be the loss of a building due to a fire.
Fit-for-purpose	An approach or solution that is pragmatic, by tailoring the scope of a piece of work, effort or solution to the prioritised elements, which can be better understood and operated.
Disaster (formal definition as per The Disaster Management Act)	The Disaster Management Act (Act No. 57 of 2002) defines a Disaster as a progressive or sudden, widespread or localised, natural or human-caused occurrence which: • Causes or threatens to cause: ○ Death, injury and/or disease. ○ Damage to property, infrastructure and/or the environment. ○ Disruption of life, within the community. • Is of a magnitude that exceeds the ability of those affected by the Disaster to cope with its effects using only their own resources.
Test Plan	The DR Test Plan document provides guidance on the types, details, scheduling, effort and activity required for regular testing every year.

Incident versus Disaster

Business functions are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, hardware failure, denial of access to the building, partial damage to offices) to severe (e.g. equipment destruction, fire). Vulnerabilities may be minimised or eliminated through technical, management, or operational solutions as part of the entities risk management effort. However, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service disruption by focusing on effective and efficient recovery solutions.

In the context of this document and the documents listed in the Scope section, an Incident is distinguished from a Disaster.

The table below, lists examples to help differentiate between Incidents and Disasters to assist in determining when the plan should be activated and when normal recovery will suffice.

Scenario	Possible causes	Impact	Recovery strategy
Destructive loss of building. *	Fire, explosion/ bomb, sabotage, flood, structural failure and natural Disasters.	• Almost all hardware, office infrastructure, equipment and non-electronic files are destroyed; and • Interruption of all business activities.	Activate the BCP /ICT DRP.
Loss of infrastructure.	Loss of power, flood, lightning, theft.	• Major loss of ICT Services; and • Core infrastructure is impacted and non-functional.	Activate ICT DRP.
Partial loss of building. *	Localised fire, explosion, bomb, sabotage, flooding, power surge.	• Destruction of facilities and equipment in the affected area; • Possible damage to some areas of the building; and • Interruption of some business activities	Depending on damage assessment report activate BCP/DRP as necessary .
Denial of access to building.	Public disturbances, civil unrest, closure by authorities, bomb threat.	• Staff cannot gain access to the building; • Limited, if any, impact on infrastructure; • Possible disruption of business activities; and • Critical systems can still be accessed remotely.	• Access systems remotely; and • Perform business activities remotely for a limited time.

1. INTRODUCTION

This policy guides Cederberg Municipality in the establishment, operation and continuous improvement of an ICT Disaster Recovery Framework: a system of five inter-dependant 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 Cederberg Municipality.

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

1.1 ICT DR Framework

This ICT DR framework consists of five key documents, and resides in a broader landscape of relevant process within the Municipality. The five main ICT DR documents are listed as follows:

Document	Summary
ICT DR Policy.	• Broad policy, principles, high level framework & obligations.
ICT Risk & Impact Analysis.	• Risk & Vulnerability Analysis; and • Business Impact Assessment.
ICT DR Plan.	• Actionable Plan in event of Disaster incl. teams, processes & forms/templates.
Definition of ICT DR Architecture.	• Technical Assessments; • Architecture(s) for Current Live & DR environment; and • Service details.
ICT DR Test Plan.	• Tiered Test plan.

Table 1: ICT DR Framework documents

Some key relationships may apply, to other important ICT documents and processes as listed below, but are not limited to that which is shown below:

- Backup and Recovery Policy;
- Incident Management process;
- Change Management process;
- Availability Management; and

- Service Level Agreement Management Policy.

2. 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.

3. OBJECTIVE OF THE POLICY

The objective of this document is to guide the Cederberg Municipality management to define the ICT DR policy so that an effective sustainable ICT DR Plan can be constructed, to enable the 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 Municipality, consumers, licensees, stakeholders and staff by minimising the impact of significant interruption to the 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.

4. THE AIM OF THIS POLICY

The aim of this policy is to ensure that the 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 Cederberg Municipality's Corporate Governance of ICT Policy.

5. 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 municipalities 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 Municipality.

The policy applies to everyone in the municipality, including its service providers/vendors. This policy is regarded as being crucial to the operation and availability of ICT systems of the Municipality. Municipalities must customise their own ICT Disaster recovery controls and procedures by adopting the principles and practices put forward in this policy.

To give full effect to the DR planning and preparation in the Municipality, the broader group of ICT DR documents are included in the planning process (see Section 1.1).

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

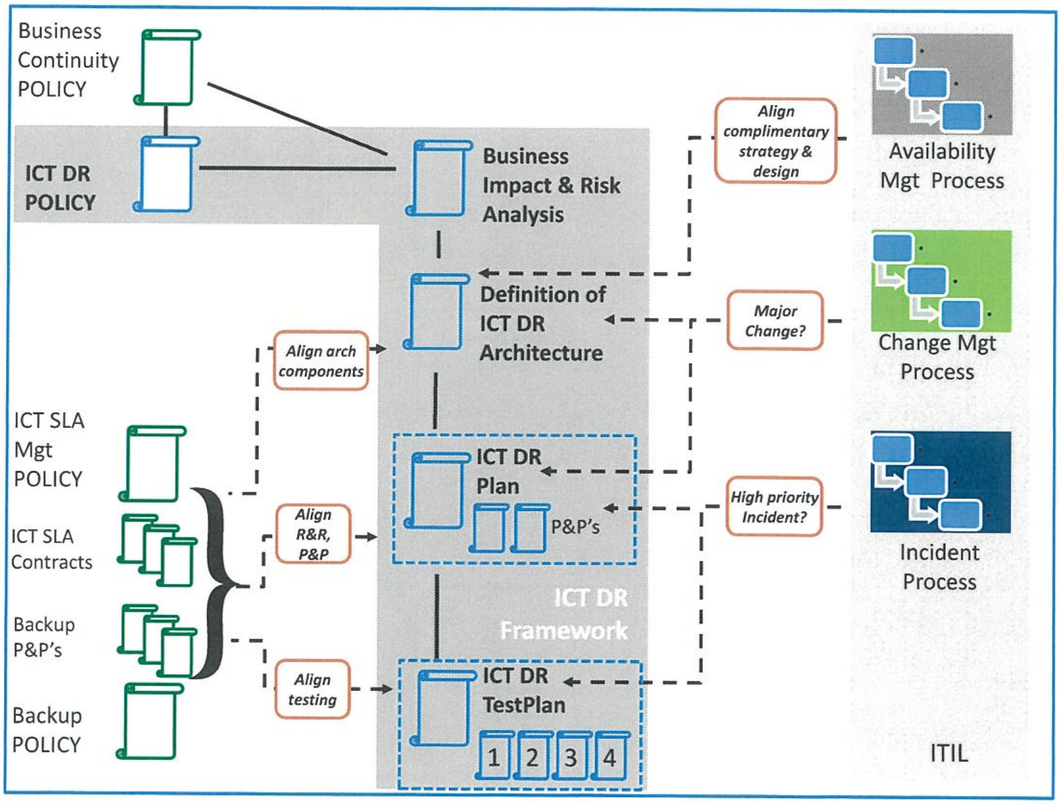

Figure 1: ICT DR Framework high level landscape

Note: Key dependencies will need to be managed continuously, specifically to the identification of critical services (in the event of critical service failures), supplied by external service providers, as governed and directed by the Service Agreement Policy.

This DR policy and its inter-related documents gives full effect to the management of Disaster recovery in the Municipality, as demonstrated in the high level landscape of inter-related documents (for more detail, refer to the Definition of ICT Architecture and the ICT DR Plan).

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978); or
- Punitive recourse against a service provider in terms of the contract.

7. CONFIDENTIALITY AND NON-DISCLOSURE

This document is confidential and must be treated as such. Distribution and usage of this document is subject to the signed confidentiality clause stipulated in employee contracts.

8. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council.

9. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personal responsibilities and accountability to the Management with regards to the Corporate Governance of ICT.