ICT DISASTER RECOVERY POLICY

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.

Terminology	Definition
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.
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.

Terminology	Definition
Test Guide	The DR Test Guide document provides guidance on the types, details, scheduling, effort and activity required for regular testing every year.
Power Cutback	An intentional situation in which the voltage in a power grid is reduced below its normal level, typically between 10-20% lower, to prevent complete power failure at the national grid.
Power Spike	Voltage spikes that occur for such a short duration of time, that may cause great damage to sensitive ICT equipment, by weakening semiconductor devices and frequently corrupting data in digital equipment.
Parallel ICT DR Test	In this test, the ICT DR Team simulate an actual ICT Disaster, by taking all relevant ICT DR Plan procedures, leaving the office, to an off-site venue or IROC, and activate VPN. The primary site is uninterrupted and critical systems are run in parallel at the alternative and primary sites.
Full Interruption ICT DR Test	This test involves all aspects of the company in response to a Disaster. All steps in the plans are performed. Systems are shut down at the primary site and all individuals who would be involved in a real emergency, including internal and if possible, external organisations, participate in the test.

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	• Almost all hardware, office infrastructure, equipment and non-electronic files are destroyed; and	Activate the BCP /ICT DRP.

Scenario	Possible causes	Impact	Recovery strategy
	failure and natural Disasters.	• Interruption of all business activities.	
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, and 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 the Municipality in the establishment, operation and continuous improvement of an ICT DR 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 the Municipality.

The policy supports the 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.
ICT DR Architecture.	• Technical Assessments; • Architecture(s) for Current Live & DR environment; and • Service details.
ICT DR Test Guide	• 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 Municipal 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 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.

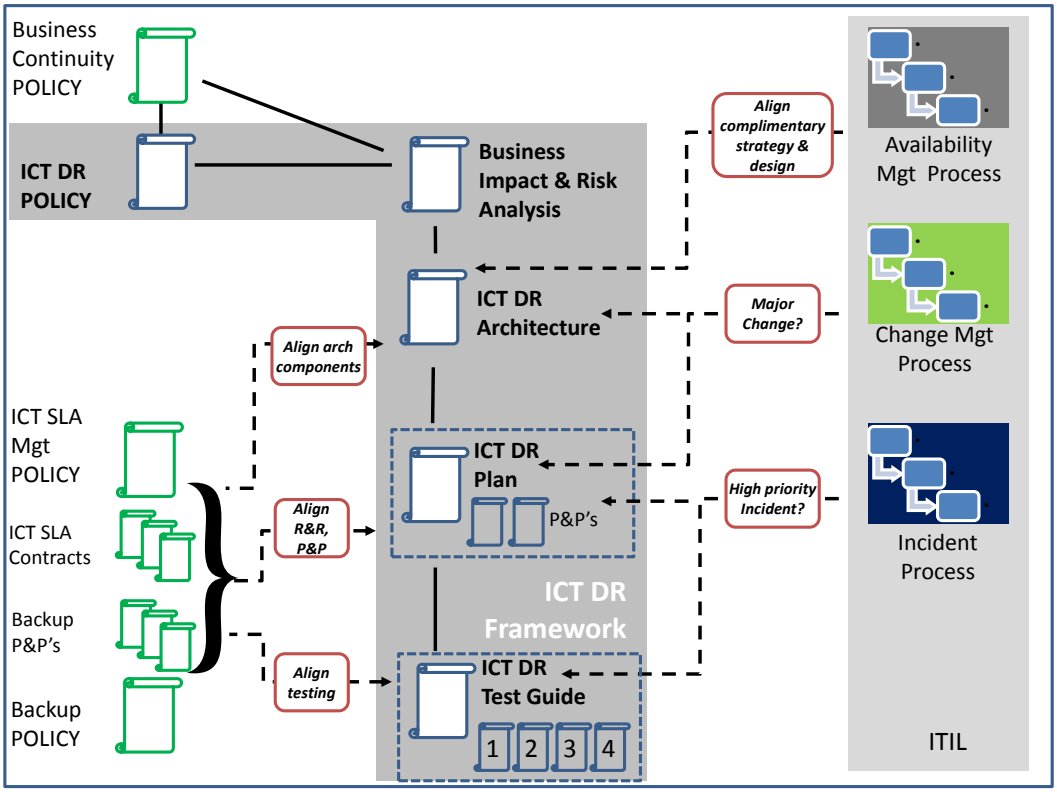

Figure 1: ICT DR Framework high level landscape

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 ICT DR 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.

10. EXCEPTIONS

10.1 This policy does not include the Business Continuity Plan or the Business Continuity Management System, which are typically created in larger or mature municipalities, who have the resources, management and intent to drive such comprehensive frameworks.

10.2 This policy does not apply to broader BC-type components for business processes such as emergency response, financial, HR, Media, logistics and Marketing.

11. GENERAL POLICY

11.1 The Municipality must initialise a DR workshop by identifying and inviting key Municipal stakeholders, ICT Department members, key external Service Providers, Line or Department Managers and the Municipal Manager.

11.2 The five key ICT DR documents must be shared with the workshop attendees at least 5 days before the workshop, for prior reading.

11.3 An ICT DR Team Leader must be appointed, along with an Alternate Leader.

11.4 A provisional ICT DR Team must be defined according to the roles and responsibilities of the ICT DR Plan.

11.5 A high level plan must be reviewed, by delegating specific documents, sections and activities to the ICT DR Team.

11.6 The ICT DR Plan is a critical document to be utilised by the municipality in the event of a Disaster. The ICT DR Plan helps guide recovery processes to the return of normal operations (termed as “Business As Usual” or BAU).

11.7 Any decision to implement an offsite Recovery Data Centre must consider a minimum radial distance of 6 km from the main Data Centre.

12. POLICY: External Policies and Processes

12.1.1 This policy will also make reference to other documents that will have inter-dependency, in the life-cycle of the ICT DR documentation.

12.1.2 These inter-dependencies must be explicitly documented, be updated regularly, and Municipal Committee informed via reporting of key status and changes.

12.1.3 These other policy and processes include, (but are not limited to):

- Business Continuity Policy (part of a BCMS);
- Incident Management Policy and process;
- Change Management Policy and process;
- Availability Management Policy; and
- SLA Management policy.

13. POLICY: ICT Business Impact and Risk Analysis

13.1 A formal impact and risk assessment shall be undertaken by/with Line Managers to determine the requirements for the Disaster recovery plan, from Municipal operations.

13.2 The ICT Manager must attend a minimum of 50% of all impact and risk analysis assessment meetings, with Line and/or Department Managers.

13.3 The ICT Manager must advise on the process and answer any key discrepancies in the development of the Impact and Risk analysis.

13.4 The individuals performing the business impact & risk analysis, must summarise the ICT system recovery requirements, to be communicated to the ICT Manager and the ICT team (including the MTO, RTO and RPO requirements.

13.5 The recovery requirements should categorise the Municipal operations or systems in levels of priority.

13.6 The ICT Manager and Line Managers, in consultation with the Municipal Manager, agree a document on key strategic decisions for ICT Recovery, for both onsite and offsite operations.

13.7 The Business Impact and Risk Analysis must be reviewed:

- Once a year; or
- Whenever there is a key identification that additional planning is required to cater for improved Disaster recovery to support the business.

13.8 The Municipality must prioritise an adequate and specific ICT DR strategy, and implementation of ICT availability controls, to cater for the significant risk of power grid failure in South Africa. The impact of loss of power (See Section 8.3: Loss of key dependencies, "ICT Business Impact and Risk Analysis") could be a realistic time period between a few hours and 2-3 weeks. The Municipality, as matter of policy, must implement:

- A suitable power generator to support a minimum of critical ICT servers, databases and prioritised operations.
- Adequate storage of diesel in close proximity to the power generators as a contingency to prevent catastrophic loss of ICT services in the event of a power failure.
- Evaluation of the probability of damage due to 'power cutbacks', and 'power spikes', that may impact critical equipment in the Data Centre and patch panels.
- Using this evaluation, the Municipality must justify the implementation of additional power line filtering, voltage clamping and UPS equipment (for very sensitive equipment and/or critical applications) to reduce the degree of impact.
- Physical testing of all power generators, diesel levels and UPS systems must occur at least every 3 months, in addition to scheduled ICT DR annual tests. These power tests must be prescribed by the ICT Manager in the ICT DR Test Guide document. The "Parallel" and "Full Interruption" ICT DR tests must specify whether or not a generator and UPS should be included in such tests.
- All technical details pertaining to power availability and DR strategy, such as: diesel generators, diesel tanks, UPS, wiring diagrams, and configuration summary, must be included in the ICT Disaster Recovery Architecture document.

14. POLICY: ICT DR Plan

14.1 The Municipality shall develop a comprehensive ICT Disaster recovery plan.

14.2 The ICT DR Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.

14.3 All staff must be made aware of the ICT DR Plan and their own respective roles.

14.4 The ICT DR Plan is to be kept up to date every 3 months, to take into account changing circumstances.

14.5 A single ICT DR Team is to be appointed, with key roles and responsibilities, to own the process of recovery in the event of Disaster. Note that these roles will require various senior managers and representatives of the Municipality

14.6 The DR Plan must contain all relevant information, templates and procedures in order for the ICT DR Team to be informed (prior to, and during a Disaster) on how to recover the key ICT systems and applications.

15. POLICY: ICT DR Architecture

15.1 The ICT Manager must delegate, and co-ordinate a team of senior technical engineers to document the ICT technical architecture and its components.

15.2 The document must represent the:

- Current live ICT environment; and
- Current ICT Disaster Recovery architecture with attention to components.

15.3 All sections of this document must be updated:

- Every 6 months;
- Every time a configuration change impacts the ICT architecture;
- Every major Change Management activity that impacts architecture directly or indirectly;
- With sufficient detail on future necessary improvements depicted with the necessary schema, tables, gap analysis, functional notes and key DR functionality proposed changes; and
- With an updated relevant DR Roadmap that illustrates the active and proposed project activities, with relevance to DR capability and improvement.

16. POLICY: ICT DR Test Plan

16.1 All senior members of the Municipal Management, key stakeholders and service providers, must be informed of the annual DR Test Plan within 1 month of the start of the new fiscal year.

16.2 The ICT DR Plan must be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.

16.3 Within any calendar year, the following test requirements are considered to be minimal:

- Follow the Implementation Plan as provided in the ICT Test Plan;
- At least one Simulation Lite test; and
- At least one other test as defined in the Test Plan.

17. POLICY: ICT DR Team

17.1 The core team of highest priority, is the ICT DR Team (of approximately 10+ roles) of which the key roles that carry the highest effort of responsibility, ultimately responsible for all aspects of Disaster prevention and Disaster recovery, are:

- ICT DR Team Leader; and
- ICT Manager.

17.2 The structure, roles and responsibilities of the ICT DR Team is defined in the ICT DR Plan. These roles must be delegated to key individuals within the Municipality as advised and guided by the ICT DRP.

17.3 This team does not exist as a day-to-day ongoing business entity, but the members come together as a virtual team, to orchestrate all matters relating to an actual or potential Disaster. The team is responsible for the ongoing task of Disaster recovery planning, maintenance of the ICT DR Plan, including the implementation of Disaster prevention activities.

17.4 The ICT Manager and Test team must take considerable care during any test, that possible impact to business operations is investigated prior to the start of the text and checked with Line Managers and Applications Owners.

18. IMPLEMENTATION ROADMAP

Actions- Year One	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Convene a KickOff workshop with key personnel to introduce the 5 main documents. Delegate responsibilities.												
Conduct Business Impact/Risk Analysis with Line Managers & Application owner(s)												
Prepare an initial draft of Definition of DR Architecture document by base-lining the current environment.												
Review gaps between the Municpal requirements for DR and the ICT DR Plan & Defn of ICT Arch documents. Update documents.												
Drive initiatives to upgrade DR capability (systems, documents, awareness, RACI.												
Address gaps in ICT DR Plan and Definition fo Architecture documents and update using as-built information.												
Testing - (see ICT DR TestPlan) .												
Identify gaps & assign tasks to improve ICT DR Plan.												
Review policy, audit preparation.												

Actions- Years Two and Three	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Convene a annual DR KickOff workshop with key personnel. Check responsibilities & assign roles.												
Review the Business Impact and Risk Analysis (Line Managers & App Owners).												
Review and improve Definition of ICT DR Architecture.												
Review gaps between Municpal requirements and the ICT DR Plan & Defn oif ICT Arch documents. Update documents.												
Drive initiatives to upgrade DR capability (systems, technology, awareness, RACI).												
Testing - (see ICT DR TestPlan) .												
Identify gaps & assign tasks to improve ICT DR Plan.												
Review policy, audit preparation.												