



ICT DISASTER RECOVERY PLAN

1 July 2024

Table of Contents

1. INTRODUCTION	3
2. LEGISLATION	3
3. PURPOSE	3
4. OBJECTIVES	4
5. INCIDENT VERSUS DISASTER	4
6. COMMUNICATION	5
7. ICT DR TEAM	6
8. CONTINGENCY STRATEGY	7
9. INCIDENT MANAGEMENT	8
10. INFORMATION AND COMMUNICATION TECHNOLOGY RECOVERY TEAM (ICTRT)	8
11. INSURANCE	10
12. EMERGENCY RESTORATION SERVICES	10
13. ICT SYSTEMS BACKUP AND RECOVERY STRATEGY	11
14. PREMISES AND ESSENTIAL EQUIPMENT BACKUP AND RECOVERY STRATEGY	11
15. CUSTOMER SERVICE BACKUP AND RECOVERY STRATEGY	11
16. INFORMATION AND DOCUMENTATION BACKUP AND RECOVERY STRATEGY	12
17. SEPARATION DISTANCE	12
18. ICT DISASTER TEST PLAN	12
19. BACKUP SITE EQUIPMENT REQUIREMENTS	12
20. REVIEW	13

1. INTRODUCTION

This ICT Disaster Recovery Plan is a step in the ICT development process that provides the necessary business continuity demands of Swellendam Municipality in case of a disaster. This will summarize the strategies being developed for the Swellendam Municipality and contains the strategic intentions and guidelines on Business Continuity Management in the municipality.

Therefore, Swellendam Municipality's initial strategy is to look for any potential problems within the ICT environment and take corrective action. Swellendam Municipality intends to address those issues that can be resolved to keep the exposure within acceptable levels. If a disaster occurs, Swellendam Municipality must be able to continue with its ICT activities with minimal disruption.

This ICT Disaster Recovery Plan will ensure that effective Business Continuity Management is implemented and maintained so that the municipality can recover in the event of a major disruption, crisis or disaster which threatens the ongoing existence of the municipality.

2. LEGISLATION

The following legislation, among others, was considered in the drafting of this policy/plan:

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

3. PURPOSE

The purpose of this ICT Disaster Recovery Plan - strategy is to provide contingency arrangements and services that will meet the ICT recovery demands of the Swellendam Municipality to be used in cases of a disaster.

This Plan will ensure that the interests of the municipality are secured in the event of major damage to the municipality's operations. The strategy shall support the ongoing governance, Compliance and risk initiatives and challenges faced by the municipality. This document will reflect the up-to-date status of the strategy adopted and will be reviewed and maintained regularly.

The ICT Business Continuity Strategy shall encompass ICT, data communications and voice communications equipment.

4. OBJECTIVES

The objectives of a formalised ICT Business Continuity Management strategy document are as follows:

- a) To ensure compliance with regulatory, statutory and legal requirements relative to business continuity for the Swellendam Municipality;
- b) Provide business-critical services to clients throughout a disaster or major incident;
- c) Minimise potential financial loss or legal liabilities;
- d) Utilise limited resources (human and technological) more effectively during the response, resumption and recovery phases, and
- e) Ensure the ICT Service Continuity strategy aligns with the Swellendam Municipality's risk appetite and meets the required minimum standards but does not deliver a solution that is excessive and unwarranted.

5. INCIDENT VERSUS DISASTER

Municipal 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 municipality 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.

The table below helps 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 a 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 a 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 the damage assessment report activate BCP/DRP as necessary
Denial of access to the 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.

6. COMMUNICATION

The ICT Disaster Recovery Plan will be communicated to employees of the municipality so that it does not cause undue alarm to staff. The ICT Manager will explain that it is part of the planning that all businesses should undertake. The ICT Manager will ensure that the plan is updated regularly and that copies are readily available to all employees. Care will be taken to ensure that access to the contact details for staff is restricted to a smaller number of employees.

7. ICT DR TEAM

Swellendam Municipality will have a number of people that will be able to respond to an ICT disaster if it occurs. These people will be identified and trained in the disaster recovery processes.

Membership of these teams will be based on people's strengths and weaknesses and not only on the job that they do. This will be done to ensure that, in the event of an emergency; the people will not panic but will diligently follow the prepared plan. If a situation develops that is not in the ICT continuity plan, these people must be capable of reacting to the situation.

The persons that were identified are as follows:

- a) Director Financial Services
- b) ICT Steering Committee members,
- c) ICT Manager,
- d) ICT Recovery Administrator and his team (Service provider)
- e) Disaster Manager

From the above ICT DR Team key members who carry the highest effort of responsibility and are ultimately responsible for all aspects of Disaster prevention and Disaster recovery, are:

- a) ICT DR Team Leader; and
- b) ICT Manager.

7.1 Crisis Control

In the context of Crisis Control, the ICT DR Team Leader and the ICT Manager with the recovery team shall:

- a) Report to the Municipal Manager on the risks identified;
- b) Provide a focal point for Swellendam Municipality to ensure the media and public receive the correct and non-contradictory information;
- c) Ensure staff and relevant departments are made aware of the problems and the remedial action taken; and
- d) Ensure that the Recovery Coordinator and Recovery Teams have the resources and support necessary to perform their duties.

7.2 Crisis Management

The team's core responsibility is to ensure that incidents that arise and escalations of incidents into crises or disasters are well managed and communicated in a manner that protects the organization's reputation.

Oversee the execution of the ICT Disaster Recovery Plan, Emergency Responses and Crisis Control.

7.3 Business Continuity Management

The main responsibility of the recovery team is to manage the response and recovery efforts until the resumption of normal business operations. These teams will operate at a tactical level and are comprised of Senior Management. In the event of a disaster, the team shall operate from a central point of command and be responsible for the following:

- a) Invoking the relevant Disaster Recovery Plans and procedures.
- b) Selecting an alternative central point of command when necessary;
- c) Command and control all recovery processes and actions until the resumption of normal business operations;
- d) Ensuring that recovery efforts are executed and will include the selection of alternative relocation options for staff, i.e. alternative off-site locations;
- e) Updating the Municipal Manager on the progress of all business continuity and recovery efforts;
- f) The Recovery teams shall also be responsible for the following pre-incident planning functions:
- g) Ensuring that all applicable risk management policies, practices and procedures are enforced and complied with, to prevent the occurrence of disruptions and minimize their impact when they occur;
- h) Ensuring the development, maintenance and testing of recovery plans addressing all "disaster" scenarios (including the maintenance of the overall ICT recovery program and its supporting infrastructure).

7.4 Damage Assessment

The responsibilities of the ICT Manager and his teams are to:

- a) Evaluate the initial status of the damaged functional area and estimates both the time to reoccupy the facility and the recoverability of any remaining equipment;
- b) It also has interfaces with affected external parties such as emergency service providers, and insurers.

8. **CONTINGENCY STRATEGY**

The contingency strategy aims to recover operations with minimal if any, impact on the services supplied to the Municipality customers. The contingency strategy focuses on resolving issues relating to information technology, suppliers and services offered to Swellendam Municipality customers and, where appropriate the public.

Specifically, the contingency strategy focuses on:

- a) Immediate welfare of staff employed at the service site
- b) Assessing the workload requirements for Business Units
- c) Establishing priorities for, and allocating the use of, technological and human resources
- d) Delegating responsibilities for critical recovery procedures of each functional service area
- e) Central control of recovering operations
- f) Availability of data and relevant applications
- g) Communicating the status of the event to the Municipal Manager.

9. INCIDENT MANAGEMENT

The configuration of Incident Management may vary with each emergency, depending on the type of specialist skills required. In the event of a disruption, whether from a predicted source or elsewhere, it will be activated.

The purpose of Incident Management is to determine whether the nature and extent of the disruption warrants deploying/activating the relevant ICT Disaster Recovery Plan and if so should:

- a) Implement the selected procedures, securing the required resources where appropriate;
- b) Identify, and where appropriate adapt, the relevant continuity procedures to ensure that the business continues to operate as near to normal manner as possible for the duration of the disruption;
- c) Identify, and where appropriate adapt, the relevant recovery procedures to ensure that the business recovers from disruption in a timely and controlled manner once the root cause of the disruption has been eliminated;
- d) Communicate with all parts of the organisation affected by the disruption on a regular basis regarding progress and the actions taken;
- e) Organise, once recovery actions have been completed, a thorough review of its management of the disruption so all relevant lessons from the experience can be learned and incorporated into procedures and training programmes.

10. INFORMATION AND COMMUNICATION TECHNOLOGY RECOVERY TEAM (ICTRT)

The ICTRT will consist of senior representatives from the main business and support units. The ICTRT Leader will be the ICT Manager and will be responsible for taking overall

charge of the process and ensuring that the municipality returns to normal working operations as early as possible.

The purpose of the ICT Recovery Team is to determine the nature and extent of the disruption and should:

- a) Co-ordinate the allocation of resources;
- b) Co-ordinate the management of the undisrupted business;
- c) Manage communication with Municipal Manager, associates and staff;

ICT recovery requires many types of resources. Those resources may include the following:

10.1 People

- a) Recovery team members
- b) Security guards
- c) Cleaning staff
- d) Drivers
- e) Temporary employees
- f) Supporting vendors

10.2 Supplies

- a) Replacement office supplies
- b) Recovery supplies
- c) Computer printer paper, cartridges etc.
- d) Health and Safety
- e) Water
- f) Sanitary

10.3 Equipment

- a) Replacement production equipment
- b) Additional production equipment
- c) Replacement computer equipment
- d) Additional computer equipment
- e) Special recovery equipment
- f) Furniture

11. INSURANCE

An important strategy to be considered is the maintenance of insurance to cover emergency losses, such as non-performance claims by clients, loss of income, or civil authority actions.

12. EMERGENCY RESTORATION SERVICES

Swellendam Municipality is allowed to procure goods and services under emergency per the procurement regulation without following the normal procurement process. The following are conditions under which the emergency procurement process may be utilised.

Emergency procurement is a procedure used by agencies to procure goods or services that are urgently needed and the procurement cannot be delayed by following the normal competitive procurement procedures.

Emergency procurements are authorized when:

- a) There exists a threat to public health, welfare or safety.
- b) Circumstances outside the control of the municipality and create an urgency of need, of which the delay does not permit the time involved in using more formal, competitive procedures.

The conditions warranting Emergency Procurement include the existence of one or more of the following:

- a) The possibility of human injury or death,
- b) The prevalence of human suffering or deprivation of rights,
- c) The possibility of damage to property, or suffering and death of livestock and animals,
- d) The interruption of essential services, including transportation and communication facilities or support services critical to the effective functioning of the Municipality as a whole,
- e) The possibility of serious damage occurring to the natural environment,
- f) The possibility that failure to take necessary action may result in the Municipality not being able to render an essential community service,
- g) The prevailing situation, or imminent danger, should be of such a scale and nature that it could not readily be alleviated by interim measures, to allow time for the formal tender process.

Emergency Procurement must not be used in respect of the following:

- a) To circumvent normal procurement procedures;
- b) As a result of insufficient stock levels for items that are used daily.
- c) As a result of working programs not properly planned;

The accounting officer must record the reasons for any deviations in terms of sub-regulation (1)(a) and (b) and report them to the next meeting of the council and include them as a note to the annual financial statements.

13. ICT SYSTEMS BACKUP AND RECOVERY STRATEGY

One of the most important aspects of ICT continuity planning is the choice of an appropriate strategy for the backup and recovery of ICT-based systems. Consideration should be given to the impact on the municipality's ICT systems of potential severe damage to premises or communications systems.

14. PREMISES AND ESSENTIAL EQUIPMENT BACKUP AND RECOVERY STRATEGY

Many unexpected events can affect premises and essential equipment vital to the continuation of normal business activities. This plan has therefore been developed to ensure continued service to customers in the event of a disaster affecting either the organisation's premises or its essential equipment.

The Municipality agreed on backup and recovery strategies for premises and essential equipment as follows:

Premises

Name of premises	Agreed backup and recovery strategy
Swellendam Municipality Head Office (IT services)	All personal computers will be configured in such a way that all important data is backed up centrally at the Head Office server room and alternative server room.

15. CUSTOMER SERVICE BACKUP AND RECOVERY STRATEGY

It is critical to be able to continue to provide an adequate level of service to the organisation's customers throughout an emergency, and this area has therefore been

treated as a high priority when considering the preferred backup and recovery strategy.

16. INFORMATION AND DOCUMENTATION BACKUP AND RECOVERY STRATEGY

It is necessary to identify the dependencies that the organisation has on digitized information and to develop workable strategies for continuing an adequate level of business operations during a serious disruption, even though, in certain circumstances, access to such information may become difficult or even impossible.

17. REPLACEMENT PROCESS FOR FIREWALL

The firewall has an automatic failover in the event the firewall failed. The automatic switchover is managed by the IT Manager and IT Service Provider. Regular backups are made of the firewall.

18. SEPARATION DISTANCE

Alternative business sites to the server room will be the old server room in the Main Building. Backups are automatically synchronized every night to these sites from the Server room.

19. ICT DISASTER TEST PLAN

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

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

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

This part of the policy will only be implemented once a DR site has been established.

20. BACKUP SITE EQUIPMENT REQUIREMENTS

A backup site will later be established when enough funds are available at a location more than 6 kilometres away from the Municipal Main Offices with the necessary communication infrastructure and equipment to take over the complete functionality

of the ICT systems in the case of a disaster, but only on a small scale until the Main site has been restored to its normal operations.

21. REVIEW

The ICT Disaster Recovery Policy must be approved by Council and be reviewed annually.