MUNISIPALITEIT
VAN
PRINS ALBERT

MUNICIPALITY
OF
PRINCE ALBERT

Rig alle korrespondensie aan:
DIE MUNISIPALE BESTUURDER
Privaatsak X53, Prins Albert, 6930
E-Pos / E-Mail: rekords@pamun.gov.za

Address all correspondence to:
THE MUNICIPAL MANAGER
Private Bag X53, Prince Albert, 6930
Tel: 023-541 1320, Fax: 023-541 1321

ICT DISASTER RECOVERY PLAN

TABLE OF CONTENTS

To activate this plan in the event of a real Disaster, turn to section 8: Processes

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
SME	Subject Matter Expert
ITIL	Information Technology Infrastructure Library
O/S	Operating System
CTO	Chief Technology Officer
LAN	Local Area Network
WAN	Wide Area Network
BAU	Business As Usual
Q&A	Questions and Answers
IROC	ICT Recovery Operations Centre
R & R	Roles and Responsibilities
P & P	Processes and Procedures

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.
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.
Trial-and-error	A method of multiple iterations of trying small steps or solutions, checking for errors, and then making further steps to improve the situation or solution.
Preliminary Assessment	A quick assessment, comprising a few prioritised steps of investigation, normally done by 1-2 persons, to enable a quick decision.
Comms	Communications – structured and ad-hoc. Refer to Communications Plan (Appendix A08).

1. INTRODUCTION

This document contains the < NAME> Municipality ICT Disaster Recovery Plan (DRP). The purpose of the plan is to set out the mitigation, preparation, warning, response and business continuity arrangements for the Municipality in the event of a catastrophic failure of its ICT systems.

Definition: A catastrophic failure of ICT systems means an event that significantly reduces the Municipality's ability to deliver its ICT systems and applications to the Municipality, thereby impacting its official duties. Typically, an outage to the Municipality's core functions and systems exceeding 24 hours is deemed to be a catastrophic failure.

This ICT DRP contains the following:

- Activation guidelines on who has the authority to activate this plan;

- How internal communication responses should be handled;
- How to distinguish between an ICT-related Incident and an ICT-related Disaster;
- Roles and responsibilities of the various teams associated with a catastrophic failure of ICT systems; and
- Detailed processes needed to recover critical ICT systems and applications and the technical ICT environment.

The following information is contained in the appendices:

Appendix	Contents
Appendix A: General appendices	Includes key Contact Lists, Incident Evaluation Report form, Main Data Centre(s) Floor Plans, Catalogue of ICT Services Systems & Applications, ICT Asset Register Summary. All other non –technical Recovery procedures.
Appendix B: Critical Business Functions	A table that defines the criticality of ICT related systems, services and applications, required by the Municipality based on priority. ICT Services Recovery requirements.
Appendix C: Recovery Data & Offsite procedures	Activate Recovery Data Centre procedures, Recovery Hardware Configurations, Recovery Configuration Schematics, and Recovery Data Centre Floor Plan.
Appendix D: Networks	High Level Network Diagram – Current Environment, High Level Network Diagram – DR Environment, Procedure for WAN Cutover (Include details for 3G and Wireless, VPN access, Internet access.)
Appendix E	All critical ICT Offsite Recovery Procedures, and ICT Onsite Recovery Procedures.

2. LEGISLATION

This ICT DRP was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, amongst others, were considered in the drafting of this ICT DRP:

- 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.
- Regulation of Interception of Communications Act, Act No. 70 of 2002.
- 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.
- King Code of Governance Principles, 2009.
- ISO 22301: 2012. The new international standard for Business Continuity Management System (BCMS).
- ISO 27031: 2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity.

3. OBJECTIVES OF THE PLAN

The overall objective of this ICT DR Plan is to provide the Municipality with the procedures to rapidly provide the information necessary to:

- Respond to an ICT Disaster and/or related ICT emergency situation.
- Provide formal communication and escalation procedures in the event of Disaster, with senior stakeholders and designated service providers.
- Notify necessary trained personnel.
- Assemble the ICT recovery teams.
- Recover ICT services to Municipality.

4. AIM OF THE PLAN

The aim of the plan is to minimise the impact to the Municipality in the event of a catastrophic failure of ICT systems, through:

- Minimising and supporting the number of decisions that must be made during a crisis.
- Minimising the need to perform crisis actions by trial-and-error when a crisis occurs.
- Minimising the need to develop new procedures, programs or systems during an ICT crisis.
- To provide documented procedures, programs and systems necessary to assist the Municipality during a crisis.

- To enable the Municipality to proactively prepare itself for the activation of this ICT DR Plan recovery of ICT Systems.
- To provide a best practice ICT DRP framework.

5. SCOPE

This ICT DRP provides the Municipality with a structured approach to DR, comprising of a set of detailed procedures, processes and systems, to support the Municipality in the event of a failure of its ICT systems.

This plan further provides the Municipality with a combined set of responsibilities for the ICT DR Team. These responsibilities are supported by the set of operating procedures to be carried out by the ICT DR Team, in the event of a declaration of an ICT Disaster.

5.1 ICT DR Framework

This plan is supported by a set of documents that supports the development and continuous improvement of this ICT DR Plan. These documents are suggested in order of priority and recommended sequence of development. International best practice recommends that these documents must go through continuous cycles of improvement and review, to enhance the Municipality's ability to deal with Disaster more effectively.

		YR1	YR2	YR3
ICT DR Policy.	• Broad policy, principles, high level framework & obligations.	X	X	X
ICT Risk & Impact Analysis.	• Risk & Vulnerability Analysis; and • Business Impact Assessment.	X	X	X
ICT DR Plan.	• Actionable Plan in event of Disaster incl. teams, processes & forms/templates.	X	X	X
ICT DR Architecture.	• Technical Assessments; • Architecture(s) for Current Live & DR environment; and • Service details.	X	X	X
ICT DR Test Guide.	• Tiered Test plan.	X	X	X

5.2 Storage

Copies of this ICT DR Plan, in both digital and hard copy format, must be stored in secure locations, to be defined by the Municipality's ICT Steering Committee. Each member of the ICT DR Team will be issued a digital, as well as a hard copy, of this plan. A protected master copy must be stored at the following locations:

- Municipality Document Management System (<location>)
- Backup Data Centre (<location>)
- Offsite Storage Facility (<location>)

The sequencing of ICT DR development can be demonstrated at a high level by the following the implementation roadmap, towards eventual testing in preparation for audit requirements and continuous improvement of the Municipality's DR capability.

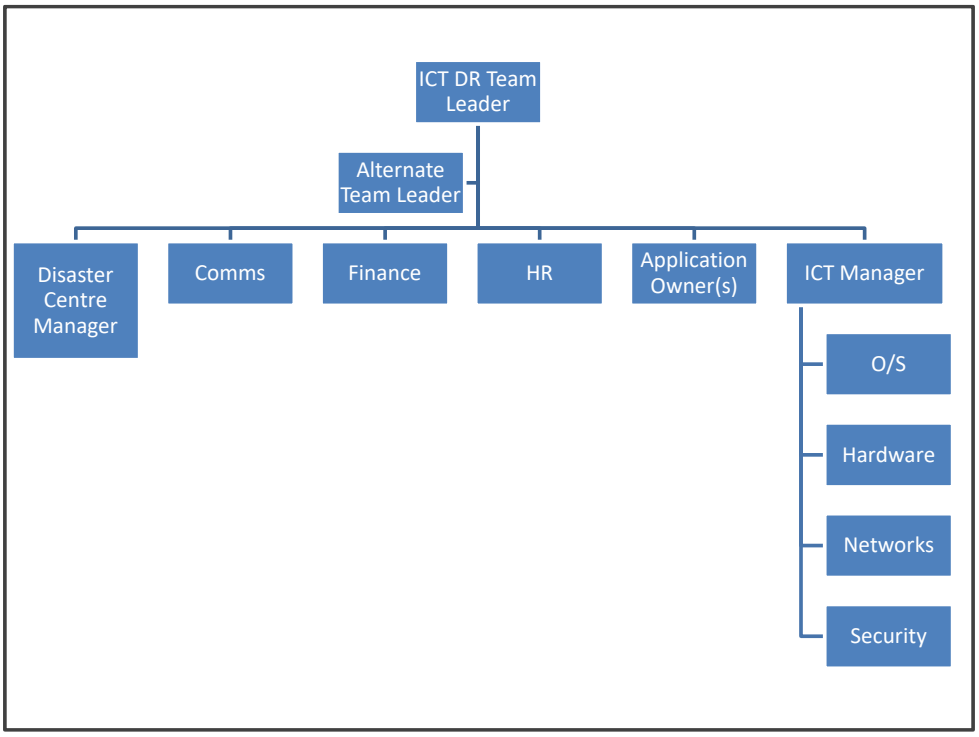
Actions - Year One	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Assemble ICT DR Team. Assign owners to customise documents.Obtain signoff. Print & handout new Versions.												
Communicate Status, IC DRP to Line Managers & Muncipal Mgt .												
Facilitate Bus Impact & Risk Analysis with Line Managers .												
Convene 2 x Reqmts meeting to handover new requirements to ICT Manager.												
Strategy: Review Recovery Approach & Technology Architecture.												
Define initiatives for Technology Upgrades, business case & costs to address gaps. Request proposals.												
Implement Technology initiatives.												
Address gaps in ICT DR Plan and Definition fo Architecture documents and update.												
Testing - Refer to ICT DR TestPlan document.												
Identify gaps & assign tasks to improve ICT DR Plan.												
Review, audit preparation.												

6. ROLES & RESPONSIBILITIES

6.1 Section overview

This section covers the roles and responsibilities required to manage the ICT Recovery process should an ICT Disaster occur. It further describes the structure of the ICT DR Team and the roles and responsibilities for each member of the team.

The figure below depicts the structure for the ICT DR Team within the Municipality.



The table below summarises the roles and responsibilities of the various members of the Municipality's ICT DR Team.

Role	Name	Responsibilities
Team lead	*<name>* *Corporate Services Director* *or* *Municipal Manager* *or* *Delegated Official*	• Assume overall responsibility for the management of the plan • Knowledge of computer operations, systems, etc. • Retrieve the off-site backup tapes • Establish infrastructure at IROC • Advise the alternate site of a Disaster alert prior to a Disaster being declared • Advise the alternate site of a declared Disaster • Advise the alternate site of a stand down from alert if recovery is not to be effected at the site or the Disaster is not declared • Communicate with alternate site management and personnel • Alert key internal & external stakeholders, and service providers. • Authority to declare a Disaster • Oversee the recovery • Communicate with *National Treasury*, *Provincial Treasury* and the *Provincial Department of Local Government* • Update staff on status of Disaster • Liaise with service providers • Manage transport requirements • Oversee facilities and security • Damage assessment
Alternate lead	<name> *Delegated Official*	• Full authority to act if team leader is not available
ICT Team Manager	*<name>* *ICT Manager or* *Delegated Official*	• Co-ordinate ICT activities across the technical system capability roles for O/S, Hardware, networks, security, databases, Applications, etc. • Co-ordinate 3rd party activities, and Service Level management
Comms	*Delegated Official*	• Co-ordinate, qualify and manage all internal and external communications
Disaster Centre Manager	*Delegated Official*	• Co-ordinate and integrate all relevant operations and escalation between the ICT DR Team and Disaster Centre operations
Finance	*<name>* *Acting Chief Financial Officer*	• Approve necessary procurement for DR • Provide the funding of continuity and restoration activities • Communicate with insurance companies
HR	*<name>* *HR Manager*	• Process & authorise overtime expenses • Authorise movement of people
Applications	*<name>* *Applications Manager or* *Delegated Official*	• Recovery of *application* components, modules
Operating System	*<name>* *ICT Technician/Engineer or* *Delegated Official*	• Recovery of O/S, Virtualisation & database components
Hardware	*<name>* *ICT Technician/Engineer or* *Delegated Official*	• Recovery of hardware components

Role	Name	Responsibilities
Networks	*<name>* *ICT Technician/Engineer or* *Delegated Official*	• Recovery of LAN, WAN and other networking infrastructure
ICT Security	*<name>* *ICT Technician or* *Delegated Official*	• Recovery of key operation of Security systems and processes (Access, Firewalls etc.)

6.2 SERVICE PROVIDERS AND THIRD PARTIES

Critical Service Providers must be identified in this ICT DR Plan. The requirements for resources and tools, by Service Providers, in the event of a declaration of an ICT Disaster, must be included in the signed SLA between the Municipality and the Service Provider. (Appendix A02: Contact Lists)

7. ACTIVATION GUIDELINES

7.1 Section overview

This section explains

- Guidelines on how to identify an Incident, with the potential to be declared a Disaster, are provided;
- How communications should be handled in terms of key procedures and samples of typical communications content;
- Who has the authority to activate this plan?

7.2 Communications

The members of the ICT DR Team must follow the communications notification process described in Appendix A08 in order to communicate a failure of ICT systems to all key stakeholders.

7.3 Incident Management

This section provides guidance on how to identify high priority Incidents that have the potential to be classified as a Disaster.

7.3.1 Priority levels

The figure below provides a process summary on how an Incident must be managed. This process is in alignment with ITIL best practice.

It is important to establish priority levels so that the appropriate action can be taken. The priority levels must be determined using the Incident priority matrix identified in the table below: The Incident priority matrix is used to prioritise Incidents as and when they occur to ensure that the appropriate remediation actions are taken.

Incident priority			Severity level		
			3 - Low Issue prevents the user from performing a portion of their duties.	2 - Medium Issue prevents the user from performing critical time sensitive functions.	1 - High Service or major portion of a service is unavailable.
Impact	3 - Low	**One or two personnel** have degraded service levels but still processing within SLA requirements.	3 - Low	3 - Low	2 - Medium
	2 - Medium	**Multiple personnel in one physical location** affected. Degraded service levels experienced. Not processing within service level agreement (SLA) or able to perform only minimum level of service. Cause of Incident falls across multiple functional areas.	2 - Medium	2 - Medium	**1 - High**
	1 - High	Personnel from multiple Departments are affected. Public facing service is unavailable.	**1 - High**	**1 - High**	**1 - High**

7.3.2 Incident handling

The ICT Manager may decide to do a preliminary assessment of an Incident and send the information to any member of the ICT DR Team at any time.

The member/members of staff concerned must:

- Ensure safety of workers, visitors and stakeholders and take names of any injured;
- If possible, assess the priority of the Incident;
- Notify the ICT DR Team of the Incident, the initial assessment findings and any known injured; and
- Notify emergency services, if required.

Until the ICT DR Team can take control of the situation, the staff member/members must:

- Keep in continuous communication with the ICT DR Team in order to update information with regard to the status of the Incident and the on-going condition of any known injured;
- Communicate with any ICT DR Team member attending the scene and brief them accordingly;
- Assist with any recovery tasks defined by the ICT DR Team.

After being informed about a high priority Incident, Disaster, the ICT Manager must:

- Ensure that the staff member on site has performed all initial actions considered appropriate to stabilise the situation and to keep them fully briefed;
- Analyse the nature of the Incident and make an initial decision about the severity of the Incident and the response required;
- Contact the appropriate ICT DR Team members and summarise the Incident based on the information available, while acting as the primary coordinating team member, until the Incident is closed;
- Confirm the status of the Incident with the other ICT DR Team members by agreeing on the priority and the immediate recovery actions required;
- Communicate with management, and brief them on the Incident and its impact on business processes;
- Ensure any internal and external communications to staff; customers and stakeholders are channelled to the ICT DR Team for further action. The ICT DR Team must be involved as soon as possible and no other staff should speak to the media during an Incident.

7.4 Disaster declaration guidelines

- The Incident causes a major, prolonged or indefinite disruption to business.
- The Incident is of sufficient magnitude with regard to:
    - The scale and impact to normal operations.
    - The severity of impact to Municipal standards for quality of operations.
- The Incident has met and/or exceeded the threshold of Disaster declaration criteria for appropriate major public sector entities on a local, regional, national or international level.
- Not declaring the Incident a “Disaster” poses a direct threat to the sustainability of the business.
- The Incident is so severe that it poses a threat to surrounding businesses and the community at large.

7.5 Authority to activate

The ICT DR Team Lead or his delegated official, has the exclusive authority to activate this plan by the process of declaring an ICT Disaster. The Corporate Services Director or his delegated official will assume the role of ICT DR Team Leader. See Appendix A15 for details of the delegated authority.

To activate this plan in the event of a real Disaster, turn to

Section 8: Processes

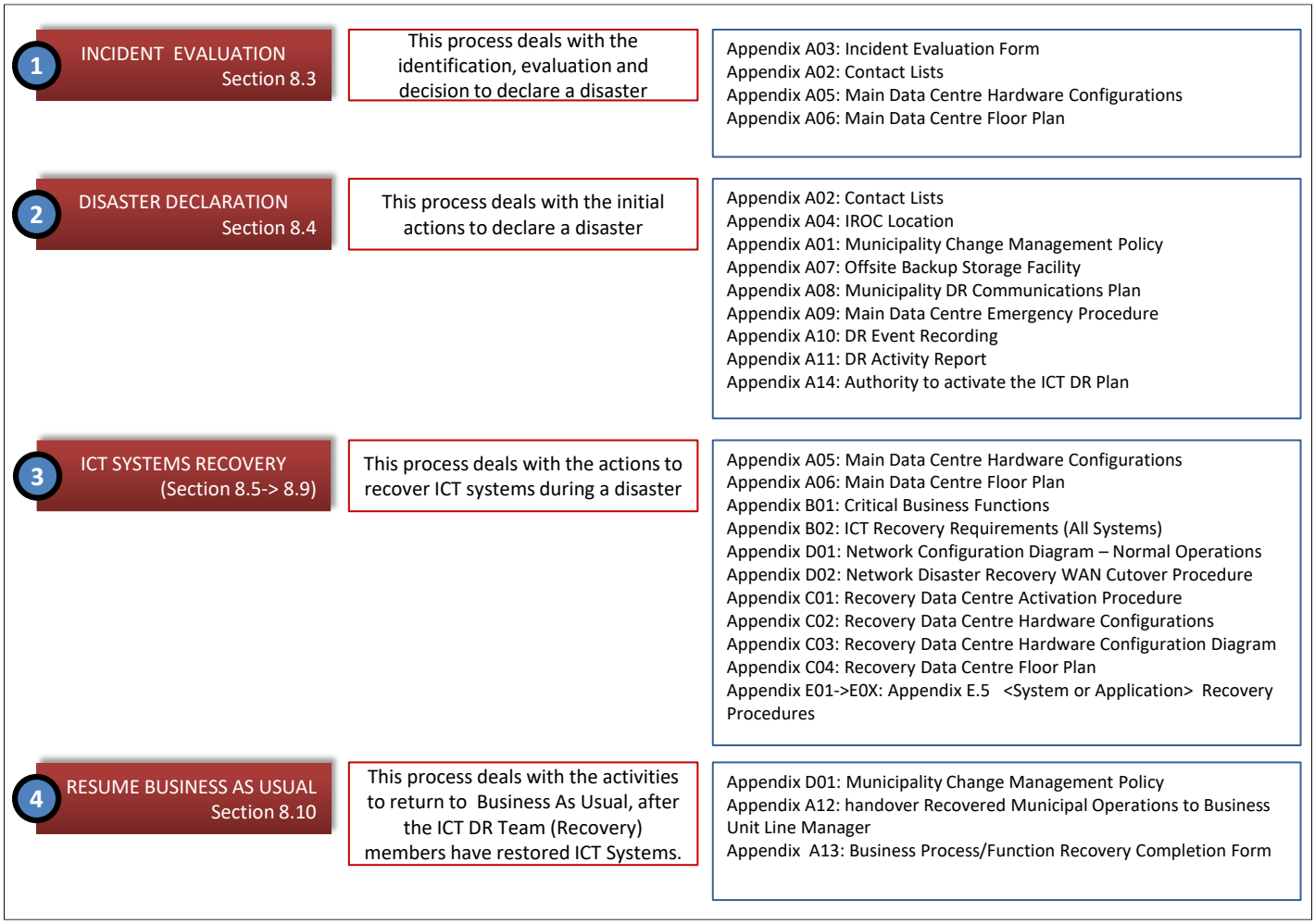
8. PROCESSES

8.1 Section Overview

The processes section defines the actions that need to be performed by members of the ICT DR Team to recover the Municipality to its regular state of operations, in the event of a Disaster occurring.

8.2 Overall process

The figure below, summarises the overall process flow, and the supporting documentation which need to be referenced in the event of a declaration of a Disaster, for the Municipality.



8.3 Evaluation of a High Priority Incident

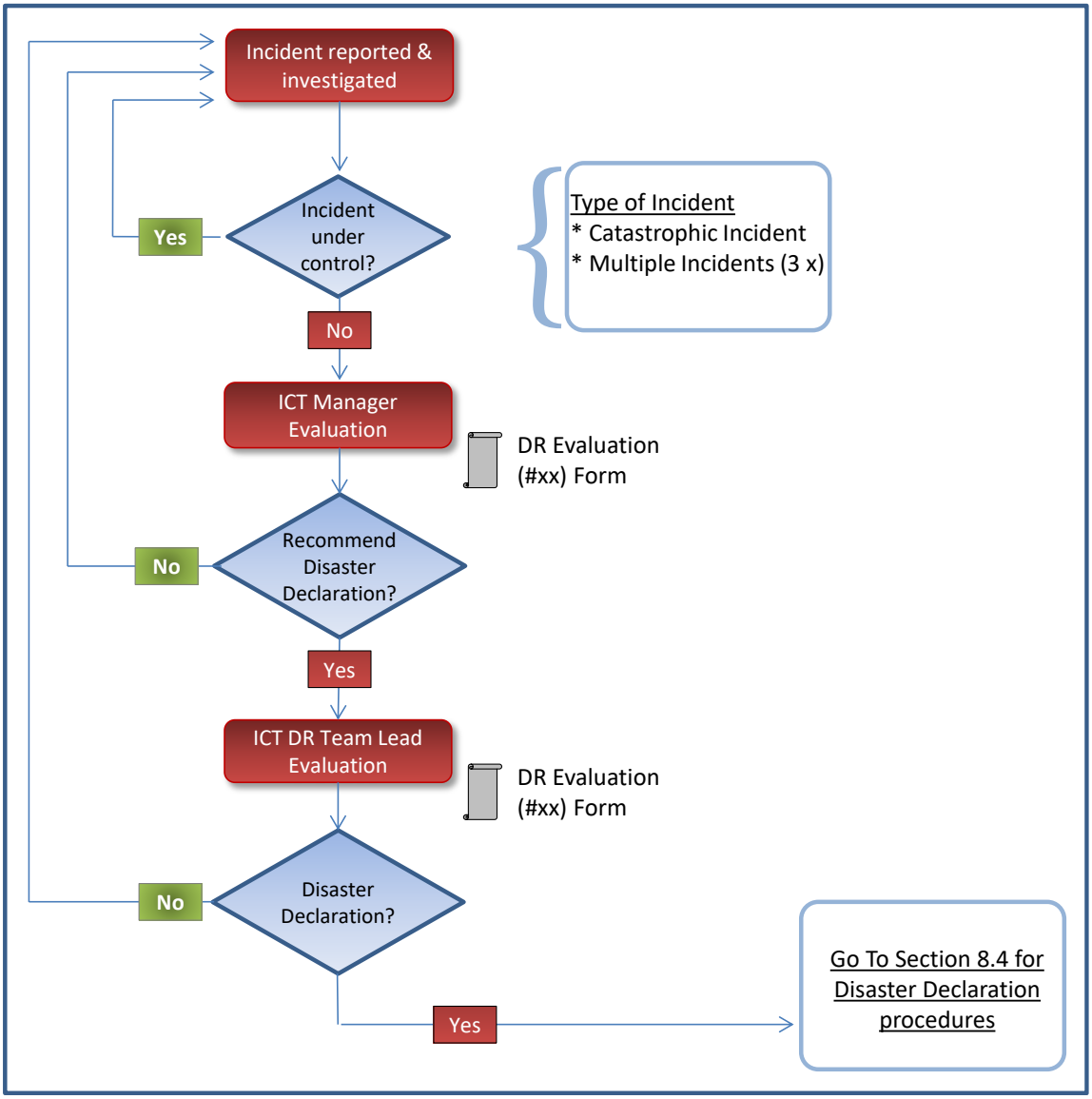
After being informed of a serious Incident(s), *the ICT Manager* must evaluate the Incident for impact, and recommend the declaration of a Disaster, to the *ICT DR Team Leader*, if necessary (Please use the template Appendix A03: Incident Evaluation Form – Part 1). Types of high priority Incidents are defined as:

- Multiple Incidents with a high impact to the stability of ICT systems, occurring within a 6 hour period; or
- High priority classification of an Incident, as guided in Section 6.4.1.

After the *ICT DR Team Leader* reviews the initial Incident information and the Incident Evaluation Form, the ICT DR Team Leader then completes the form (i.e. Part 2). The completed Incident

Evaluation Form is used to support or decline the decision to declare a Disaster and in the event of a declaration of a Disaster, the information pertaining to the declaration of a Disaster, should be shared with the ICT DR Team, and other key stakeholders.

The Evaluation of a High Priority Incident process is depicted as follows:



8.4 Disaster declaration

8.4.1 Disaster declaration procedure

The sequenced high level steps required in declaring a Disaster are:

No	Type of Activity	Activity Step
1	Comms	Communicate to the ICT DR Team the intention to declare a Disaster, with supporting ICT DR Incident Evaluation Form.
2	TEAM	Convene the ICT DR Team at a known location.
3	TEAM	The ICT DR Team determines if the situation requires escalation, based on inputs from the severity status and damage assessment provided by the ICT DR Team Leader & ICT Manager.
4	TEAM & Comms	If a Disaster is not declared, the ICT DR Team advises, through the ICT DR Team Leader to Municipal Management and/or Manager, that the team will then continue to address the emergency until it is brought under control.
5	TEAM & Comms	If a Disaster is declared, the ICT DR Team supports the ICT DR Team Leader to: • Declare a Disaster. • Activate a full ICT DR Plan process.
6	Comms	Contact key management to inform that a Disaster has been declared: • Municipal Manager/Municipal Management • Communicate with National Treasury, Provincial Treasury and the Provincial Department of Local Government
7	Comms – 3rd party	Contact 3rd party stakeholders:
8	Comms-3rd party	Confirm the relocation site for usage by any designated staff or operations.
9	Comms-internal	Co-ordinate ICT Recovery with representatives for Municipal *operations and functions*.
10	Comms-3rd party & procedure	If a technology issue is experienced at the 3rd Party, escalate through the escalation process (see Section 9). Place ICT Recovery team members on standby until Incident are resolved.
11	Comms-3rd party	Communicate at regular intervals with 3rd party Account Manager & Executive, to determine if issue can be resolved within SLA levels of X hours.
12	Comms-internal	If an Incident Is not expected to be resolved within **X** hours, contact the Municipal Manager as an escalation to the Municipal operations representatives.
13	Comms-internal	Contact key Stakeholders (internal Technology issue):
14	Comms & TEAM	If technology issue is deemed to extend past **Y** hours, inform the ICT Recovery Team at a designated ICT DR site.
15	Comms & logistics	Notify the Municipality through the Municipal Manager, of current status of issues, and to prepare planning of logistics for temporary solutions of designated personnel and operations, along with required provision of technical services (e.g. network access via 3G etc.).

16	Comms Procedure	Initiate Procurement processes: Initialise process for finance approvals for procurement. Contact required vendors for procurement of necessary ICT equipment. Initiate the process to submit insurance claims for damaged or lost equipment.

8.4.2 Disaster declaration guidelines

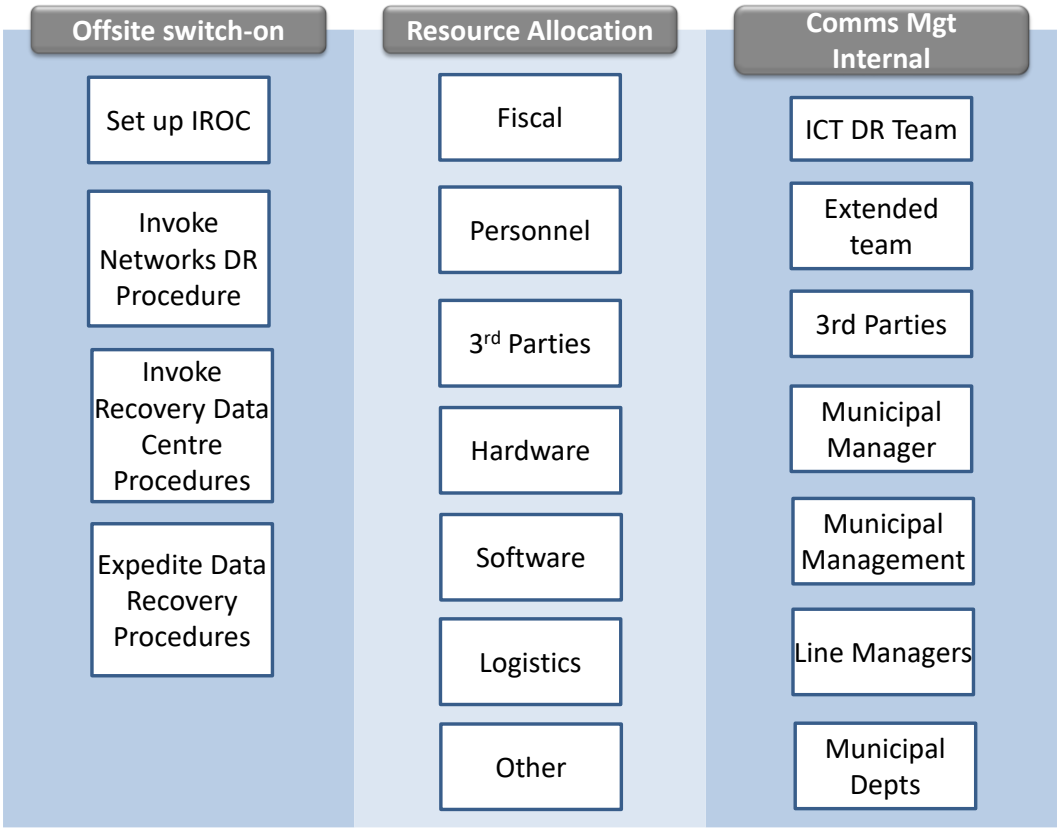
Refer to Section 7.4.1, for guidelines for declaring a Disaster.

8.5 Main Recovery Processes

The Main Recovery processes will work within the context of

- Offsite Switch-on
    - SET up IROC
    - Invoke Network Recovery Procedure
    - Invoke Recovery Data Centre Procedure
    - Expedite the Data Recovery procedures that were initialised in the Disaster Declaration
- Resources (may require procurement and/or rentals)
    - Fiscal
    - Personnel required (excluding the ICT DR Team)
    - 3rd Party resources
    - Tools
    - Hardware & Software
    - Logistics
    - Other
- Communications (for the purpose of Recovery only)
    - ICT DR Team
    - Extended team
    - 3rd parties
    - Municipal Manager
    - Municipal Management
    - Line Managers
    - Municipal Operations

This is depicted in the summary schematic below:



8.5.1 ICT Recovery Operations Centre establishment

The ICT Recovery Operations Centre (IROC) will be the physical office(s) that will be used in the event of a major Disaster. This is where the ICT DR Team and 3rd parties/vendors will first gather to establish the steps for dealing with the current Disaster. Setting up and operating this command centre is the responsibility of the ICT DR Team leader.

(a) IROC Location

<Note: this section must be edited by the Municipality, if relevant>

The IROC is provisioned at the following physical location, in the event of a Disaster declaration. The location will be confirmed at the time of Disaster declaration by the ICT DR Team Leader. (See Appendix A).

(b) IROC Centre checklist

The IROC must be adequately equipped with the required communications facilities and technology to access critical systems.

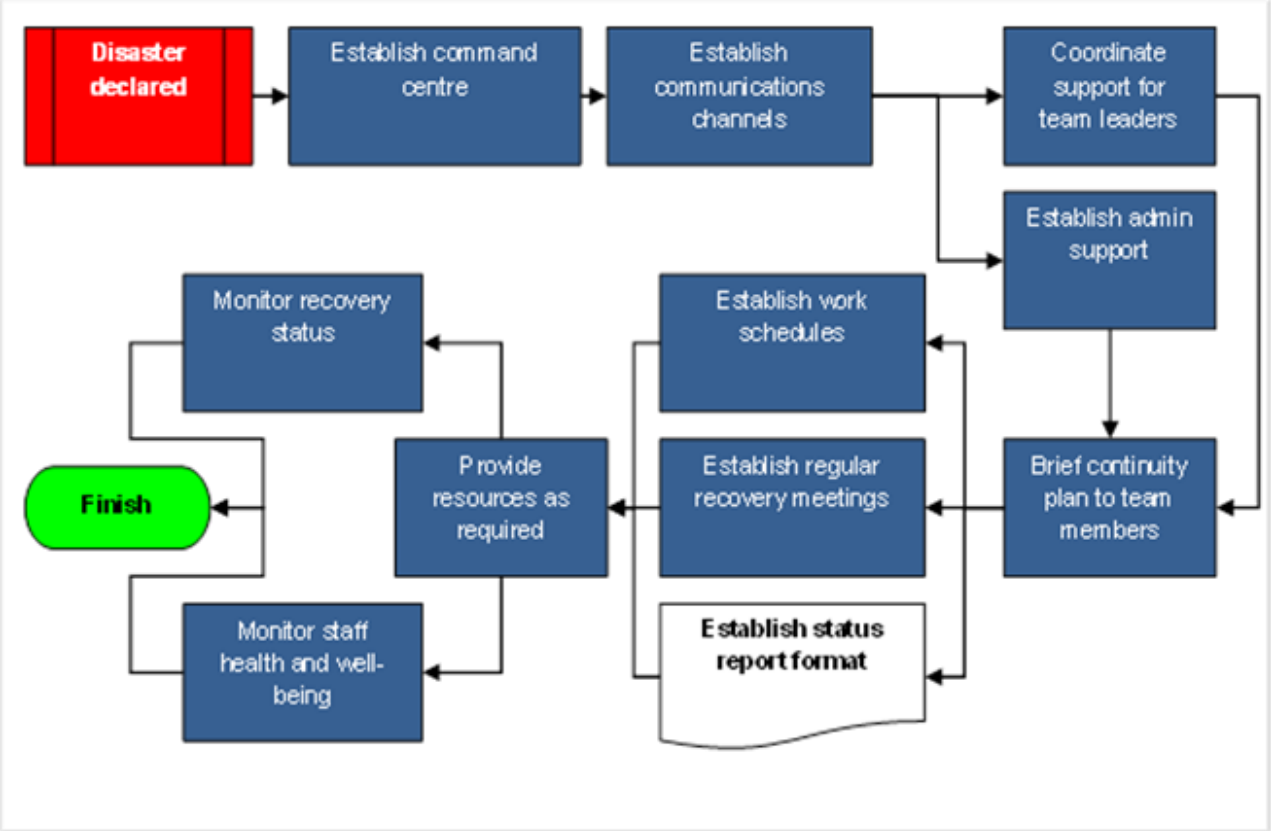
In addition to the communications facilities, the IROC should be outfitted with, or have ready access to: food; clothing; sleeping accommodations and other supplies needed to manage the recovery effort.

The table below, summarises the checklists for the IROC Centre.

Activity	Description	Acceptable?
Establish an IROC work location for key members of each activated recovery team, business area and vendor.	Ensure that adequate furniture, fixtures, computers, telephones, supplies and space are provided for the team & additional attendees. Check key items such as: overhead projector & accessories, white board & pens, facsimile facility, table and chairs, general type	

Activity	Description	Acceptable?
	stationary, lockable cupboard for plans and documentation. Paper copies of full ICT DR Plan and related appendices & forms. Prepare signs that identify the room or work area assigned to specialist activity (if required e.g. ICT technical recovery in one area).	
Establish incoming and outgoing communication channels.	Assign specific telephones to be used for *incoming* and *outgoing* calls. Continue business area notification activities until all personnel have been notified. Assign personnel to monitor the telephones designated for incoming calls. Inform the telephone operators to direct all return calls to the assigned extension(s) at the IROC. Check critical communications lines to ICT Recovery team and other key stakeholders is working.	
Coordinate business area support with team leaders during the recovery.	Meet with security representative and business representatives to assist to provide tighter than normal security for personnel and property, if required. Request that access to IROC only be authorised to personnel who have proper identification (ID badge, tag, etc.). Work with the facility team to identify equipment requirements and arrange for procurement to provide Heavy duty copy machines;	
Ensure all third party vendors are contacted and notified of the situation.	Follow-up on Disaster Declaration initial steps.	
Explain the recovery plan to core recovery team members.	Review the work to be done to clarify responsibilities and answer any questions.	
Establish status reporting processes and formats.	Follow-up on Disaster Declaration initial steps.	
Create status charts, using flip charts or other media, for display at the IROC.	Create information status display chart. Create a general message board. Create a personnel accommodation board (if applicable)	
Establish regular meetings.	Keep all IROC personnel informed of the recovery progress. Advise recovery team leaders. Arrange and organise a meeting place. Record minutes of the meetings. Have minutes typed, obtain approval, and distribute them.	
Establish work schedules for 24 hour coverage.	Align the after-hours work effort with the RTO.	
Continue to evaluate the level of people and resources and add or remove as needed.	Human resource management and procurement are the focal points for people and resources.	
Monitor personnel for signs of fatigue.	Sufficient rest is required to maintain an efficient recovery operation. For health and efficiency reasons, no recovery personnel should work excessive hours without an eight-hour rest period.	

The process activity for establishing the IROC is summarised as follows:



8.6 Initialise Recovery Data Centre

If applicable, follow the procedures and information as provided In Appendix D, if a contracted offsite Recovery Data Centre is to be utilised.

8.7 The recovery process

This section describes the activity flows and detailed actions to be performed to restore normal business operations that the ICT DR Team must manage.

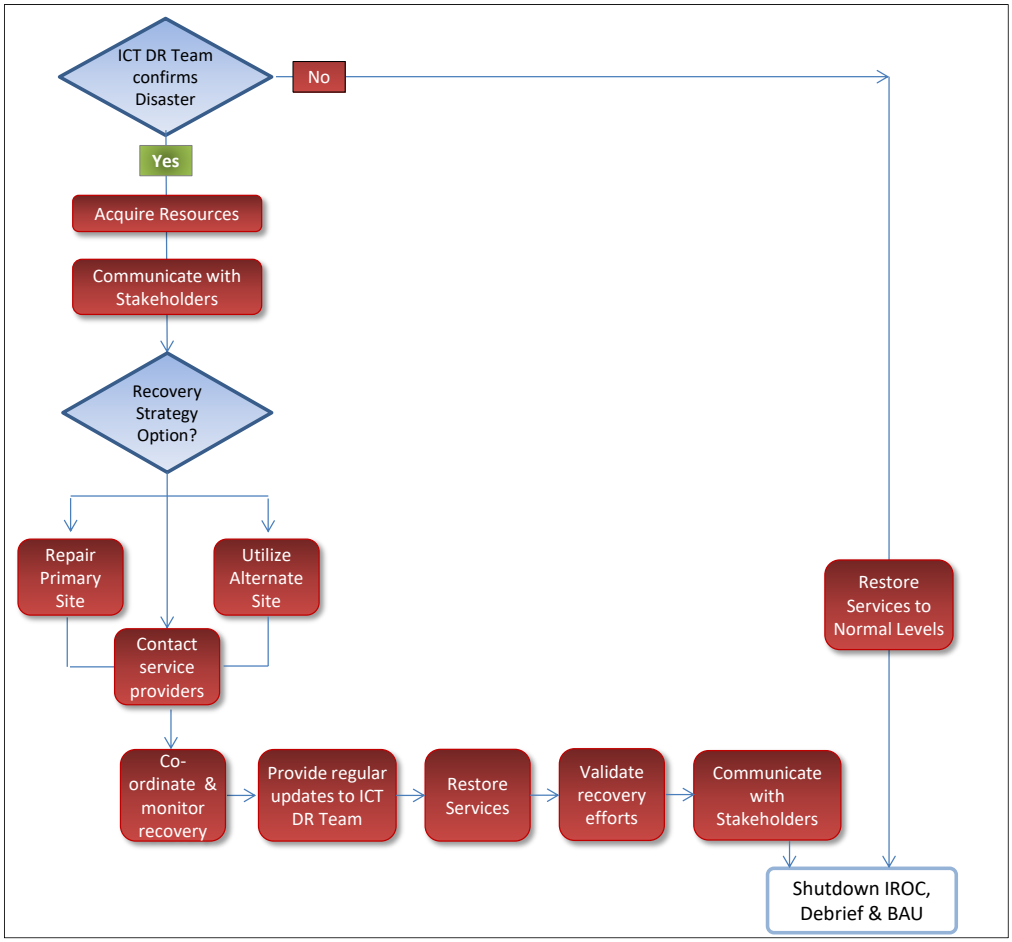
The ICT DR Team is responsible for the entire ICT Recovery process from the perspective of restoration of ICT services. This responsibility is valid from the time the team is established until all services have been returned to the primary site or new location.

The table below summarises the detailed actions for the ICT DR Team. The times shown for each step have been estimated, and accurate times will need to be established in the event of a Disaster occurring. Resources, process time and comments need to be captured in the event of a Disaster occurring.

No	Action step	Who	Time	Resources	Process time	Comments
	What do I have to do?	Who is responsible for the step to be completed?	How long will it take?	What additional resources are required?	When did I start and finish the action step?	What happened when I completed the action step?
1	Has Disaster been declared? If yes, go to step 5.	ICT DR Team leader with input from the ICT DR Team	E.g. 2 hour			
2	Restore functions & services at site.	ICT DR Team	16 hours			
3	Debriefing of the recovery.	ICT DR Team leader	4 hours			
4	**Finish.**	**If Disaster alert is withdrawn**	**1 hour**			
5	Declare a Disaster - **initiate** recovery. Agree ICT DR Strategy.	Authorised individuals within the ICT DR Team	2 hours			
6	Acquire Resources	ICT DR Team leader	4 hours			
7	Communicate with stakeholders and coordinate recovery.	ICT DR Team leader	On-going			
8	Rebuild primary site or failover to alternate.	ICT DR Team leader	16 hours			
9	Establish IROC.	ICT DR Team leader	On-going			
10	Coordinate and monitor recovery.	ICT DR Team leader	On-going			
11	Restore functions & services at site.	Each team leader.	16 hours			
12	Validate recovery.	ICT DR Team leader	48 hours			
13	Debrief of plan.	ICT DR Team leader	4 hours			
14	Finish					

8.7.1 ICT recovery function

The ICT Manager co-ordinates the ICT recovery team which consists of: all hardware, operating system software, security, applications and communications specialists. The ICT recovery team, comprising the ICT Manager and all delegated technical staff, restores affected systems using the procedures detailed in Appendices C and D. The Application Owners test and confirm the suitable recovery of Application operations by making use of Appendix E, under guidance of the ICT Manager. The figure below details the ICT recovery team activity flow.



The procedure in Appendix A015 lists the detailed **specific ICT recovery actions**.

The times shown for each step have been provided as a sample only, and accurate times will need to be established by the Municipality , both as target times *and* in the event of a Disaster occurring. The times given are indicative for each step and not cumulative.

Resources, process time and comments need to be captured in the event of a Disaster occurring.

8.8 Third Party Escalation process

This section explains the escalation process to follow in the event of a technology issue

Action	Instruction & Responsibility
Log Call with 3rd Party Service Desk.	In the event of a Disaster, this will be the responsibility of the ICT Manager.

Notify the 3rd Party Account Executive & Account Manager	The 3rd Party Account Executive & Account Manager must be notified of the issue and potential impact that it has on operations. This task is responsibility of the ICT Manager.
Monitor the resolution progress.	The progress of resolving the Incident, has to be monitored at regular intervals to ensure the DR process I sable to make informed decisions timeously. This is the responsibility of the ICT Manager.
Communicate progress of issue resolution.	The progress of the resolution of the Incident must be communicated to the Municipal Manager, to ensure communication is filtered through to the Municipal Management stakeholders.

8.9 Debriefing

Prior to the closure of a disastrous situation and standing down of the ICT DR Team, a debriefing of all participants should be conducted.

A debriefing will ensure:

- All required recovery and normal business resumption tasks have been performed.
- On-going system, business and client impacts are being addressed.
- The Municipality can determine and understand the cause, nature and impact of the Disaster.
- Financial impacts are clearly identified and documented for insurance claims.
- Lessons learned are clearly identified and incorporated into a knowledge database for future BCP, ICT DR and Disaster management.
- Deficiencies in the current process are clearly identified in a way that projects can be established to rectify them or mitigate them.

A concise report should be produced by the ICT Team Leader, covering the above mentioned aspects. This should be contained in a central knowledge register with lessons learned incorporated into new Disaster recovery plans.

8.10 Resume Business as Usual (BAU)

The following individuals are responsible for this section:

No.	Title	Name	Contact Details
1	<title> Councillor/Manager		
2	ICT DR Team Leader		
3	ICT Manager		
4	<title> Applications Owner(s)		
5	Municipal Manager/other		

This section provides key steps to return to BAU, following the closing of the ICT Recovery processes. Key individuals responsible for this section, should be the ICT Recovery manager and the Applications Owner(s). The Application Owner(s) ensure all systems and related modules and

key integration points, are functional. The ICT Manager must co-ordinate and check that all ICT technical components (O/S, hardware, Security, applications, networks) are functional.

Step	Action	Responsible
1	Perform regular checks to confirm whether the normal site operation (location, data centre, offices etc.) is safe and functional to relocate resources back from any offsite locations.	ICT DR Team Leader
2	Decide if all applications and data will be recovered in BAU in a phased approach or at a single milestone.	ICT Recovery Manager
3	Check that all Applications Owner(s) have effective shortlist plan to return their respective applications and systems to BAU, to ensure effective planning of resources and check any key dependencies.	Applications Owners
4	Decide on the planned date, for when ICT staff and Municipal operations staff will be relocated back to main site (if and where relevant). Inform key Councillors and Managers. Decide target date for full ICT recovery.	ICT DR Team Leader
5	Communicate through key channels (see Appendix xx) to all affected staff.	<title> Councillor/Manager
6	Notify all 3rd parties of planned move date, and anticipated target date for full ICT Recovery.	ICT DR Team Leader
7	Check with Backup teams that time allocation for availability of restored data is known and communicated. Check backup is restored based on backup schedules.	ICT DR Manager
8	Prepare a communications message and/or media statement to indicate that ICT operations have resumed at Main Site.	ICT DR Team Leader
9	Follow up on Insurance claims submitted during recovery process.	ICT DR Team Leader
10	Close the recovery Offsite to Access Centre operations in a structured manner (return of Head Office equipment; save all data either utilised or created; address any site processes or issues, fees etc.).	ICT DR Team
11	Collect all key forms and documents that were actioned during ICT recovery process. Check for all signatures and key comments and inputs are captured succinctly without further delays.	ICT DR Team Leader
12	Conduct internal surveys, by email and face to face with all levels of employees affected by the ICT recovery process.	ICT DR Team
13	Convene a Review Meeting with ICT DR Team, representatives from Municipal Council or management to review key lessons, issues and gaps. Decide on actions to improve the process, assign actions, record meeting minutes.	ICT DR Team Leader

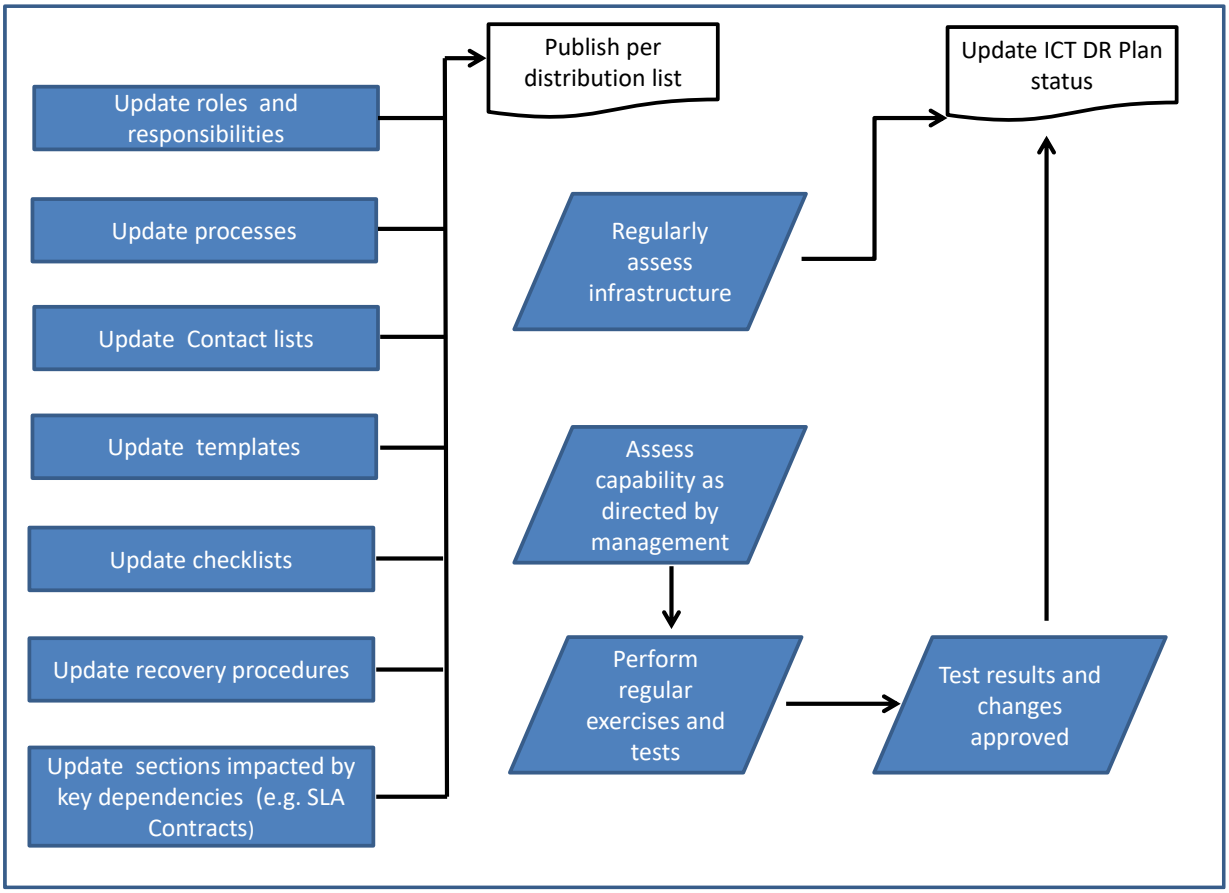
9. MAINTENANCE OF THE PLAN

Any change in the ICT environment may affect the relevance of the plan. It is therefore critical that the DRP be incorporated in the change control process as an item that needs to be considered and altered accordingly.

The ICT DR Team Leader is responsible for maintaining, updating and communicating the enhancements to the plan. All changes or enhancements should be recorded according to the ICT DR Policy and approved by the Municipality designated authority and/or Committee. Communication of changes to all relevant personnel is essential.

It is necessary for the ICT DR Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate changes should be made to the training materials. This will involve the use of formalized change control procedures under the control of the ICT Manager.

The table below outlines the DRP update process:



10. IMPLEMENTATION ROADMAP

This plan presents the recommended high level activity, starting in July 2015.

Actions - Year One	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Assemble ICT DR Team. Assign owners to customise documents.Obtain signoff. Print & handout new Versions.												
Communicate Status, IC DRP to Line Managers & Muncipal Mgt .												
Facilitate Bus Impact & Risk Analysis with Line Managers .												
Convene 2 x Reqmts meeting to handover new requirements to ICT Manager.												
Strategy: Review Recovery Approach & Technology Architecture.												
Define initiatives for Technology Upgrades, business case & costs to address gaps. Request proposals.												
Implement Technology initiatives.												
Address gaps in ICT DR Plan and Definition fo Architecture documents and update.												
Testing - Refer to ICT DR TestPlan document.												
Identify gaps & assign tasks to improve ICT DR Plan.												
Review, audit preparation.												

Actions - Years Two and Three	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Assemble ICT DR Team. Review status of ICT DRP maintenance changes. Check if ICT DR Team needs re-structure. Check if new owners of Sections are reqd. Align with Bus Impact & Risk Analysis changes.Obtain signoff. Print & handout new Versions.												
Communicate Status, IC DRP to Line Managers & Muncipal Mgt .												
Facilitate new/confirm Bus Impact & Risk Analysis with Line Managers . Check for document version changes												
Convene 1 x Reqmts meeting(minimum): handover new reqmts to ICT Manager.												
Strategy: Review Recovery Approach & Technology Architecture.												
Define initiatives for Technology Upgrades, business case & costs to address gaps. Request proposals.												
Implement Technology initiatives.												
Address gaps in ICT DR Plan and Definition fo Architecture documents and update.												
Testing - Refer to ICT DR TestPlan document.												
Identify gaps & assign tasks to improve ICT DR Plan.												
Review, audit preparation.												

Appendix A General Appendices

Appendix A.1 Municipality Change Management Policy

<Provide link or reference to Change Management Policy and/or Process document if existing. Applicable if Municipality insists to use Change Management process during a Disaster>

Appendix A.2 Contact Lists

IROC (Planning)

Building name	Address	Telephone	Contact person

The Municipality ICT DR TEAM

Role	Name	Home number	Mobile number	Home address
Team Lead				
Alternate Lead				
Finance Lead				
HR Lead				
Application Owner				
ICT Manager				
Operating Systems				
Hardware				
Networks				
Security				

Critical Service Provider contacts

No	Main System(s)	Technologies	Service Contracted (Summary)	Contact person	Phone no.
1					
2					
3					
4					
5					

Appendix A.3 Incident Evaluation Form

Incident Evaluation Report	
Part 1: (to be completed by ICT Manager)	
Date & Time	
Nature of Incident	
Cause of Incident	
Possible expansion of the Incident to a Disaster	☐ Yes ☐No (if yes, please justify)
Magnitude of the impact?	☐ Low ☐Medium ☐ High
Status of physical infrastructure including ICT equipment (damage caused)	☐ Low ☐Medium ☐ High
Estimated time to restore(service, specific system)?	
Notes	
Part 2: (to be completed by ICT DR Team Leader)	
Date	
Nature of Disaster	

Cause(s) of Disaster	
Possible expansion of the Disaster	☐ Yes ☐No (if yes, please give details)
Magnitude of the Disaster	☐ Low ☐Medium ☐ High
Status Check of key Municipal Departments, operations? (damage caused)	☐ Low ☐Medium ☐ High
Estimated time to restore	
Notes	

Appendix A.4 IROC (ICT Recovery Operations Centre) Location

<Note: this section must be edited by the Municipality, if relevant>

The IROC is provisioned at the following physical location, in the event of a Disaster declaration. The location will be confirmed at the time of Disaster declaration by the ICT DR Team Leader.

Building	Room	Contact Persons & Title	Contact details	
			Mobile	Office
(name of building)	Room names/ numbers	<name> <title>		

Appendix A.5 Main Data Centre Hardware Configurations

Note: This applies existing facility

Municipality to populate summaries & schematics of Hardware Configurations.

Appendix A.6 Main Data Centre Floor Plan

Municipality to populate Main Data Centre Floor Plan..

Appendix A.7 Offsite Backup Storage Facility Information (Processes, Access etc.)

Municipality to populate information on the process to activate, access and utilise such Storage facility

Appendix A.8 Municipality DR Communications Plan

Municipality to populate & develop through continuous improvement, sample message for internal and external comms for the types of messages as identified in the processes.

Phase	Groups	Comms Type/Msgs	Other	Other
Evaluation of Incident	Municipal Mgt ICT Dept ICT DR Team 3rd parties	Incident Report Notice for probable Disaster		
Declare a Disaster	As above + External (e.g. National Treasury) External (e.g. National Treasury, Provincial Treasury and the Provincial Department of Local Government	Convene ICT DR Team Contact 3rd Parties-Inform Contact 3rd Parties for Resources Contact Municipal Mgr. Status Report Procurement HR request/notification		
ICT Systems Recovery	As above	Activity Reporting Recovery Strategy		

		Services Restored Debriefs		
BAU	As above + Municipal operation s(users)	Relocation Notice BAU Update (All staff) BAU Update (Mgt) Optional Media Message Close Recovery Function (Site, services etc.) BAU Closure BAU survey ICT DR BAU Review		

Communications at critical points in the ICT Disaster Recovery process, should originate from or be approved by the ICT DR Team Leader. In a critical situation, ensure that information is only communicated from a single source to avoid confusion, error, frustration, or worse.

All communications must be cleared by the ICT DR Team Leader.

The following needs to be considered:

- Never speak to the media without prior preparation.
- Agree appropriate time slots for press to receive statements/interviews.
- If an unplanned interview is requested, seek advice from the Municipal Manager prior to the interview.
- In an unplanned interview, prepare the key points you want to say and if the first question does not give you the opportunity to give that message, start with "*before I answer that question, may I say …*"
- Remember facts are key – assume nothing.
- Avoid "no comment" responses – it suggests the worst.
- Be clear. Doubts destroy confidence and fuel speculation about dishonesty. Where appropriate a firm denial should be made.
- Be aware that someone else may be telling the story without correct information and their version sets the mood.
- People will feel privileged if told early and are trusted with the facts, they will feel disappointed if they 'discover' the truth and will become disgruntled if their story differs from the official version.

- Manage the control and flow of information.
- Show concern and the fact that the Municipality cares about what has happened.
- Show commitment to find out what happened and put it right.
- Be positive and truthful.
- If the facts are known, tell them.
- If the facts are not known, admit as much.
- Do not speculate; instead refer to the inquiry or investigation that will follow.
- Do not admit responsibility; rather refer to the need for the matter to be fully investigated.

Sample internal communication

Below is a sample text for internal communication to staff.

"<FullName> Municipality suffered a major disruption today caused by a fire that started in a storeroom on the first floor. All operations have ceased at the <Location> Building. Critical operations have been relocated to the <Recovery site>. Recovery teams are currently restoring critical functions within the Municipality. If you are not part of one of the recovery teams, then please go to your home and remain there until you are contacted by a Municipality representative. The Municipality has planned for this possibility and we are confident that your section will be operational in a short period of time. If you have any queries please direct them to <nominated person>. In the meantime, if you are approached for comment on this Incident by an outside party then please refer the query to <nominated person> on <telephone number> or <email address>. Do not make comment to anyone, without prior authorisation from the ICT DR Team".

Sample external communication

Below is a sample text for external communication.

"Today the <FullName> Municipality suffered a major disruption at their <Location> Building premises due to a <Disaster> and has ceased operations at that location. Emergency services are in attendance and the situation is under control [one could comment if there were injuries or deaths]. The Municipality has activated their ICT DR Plan and has commenced critical functions from their recovery site. The Municipality has planned for such an event and the contingency plans developed will enable full business operations to resume within <estimated number> days. If you have any queries please direct them to <nominated person> on <cell number> or <email address>. In the meantime, the entity would like to thank all stakeholders for their patience and understanding during this difficult period".

Appendix A.9 Main Data Centre Emergency Procedure(s)

Municipality to provide emergency and evacuation procedures for Main Data Centre.

Appendix A.10 Disaster Recovery Event Recording

Seq.	Event/Incident	Date & Time	Notified Date & Time	Message Content/type	Received/ origin	By
1	.					
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

Appendix A.11 Disaster Recovery Activity Report

Name		Role	
Time Period	<Day/24hrs/12 hrs>		

No	Activity	(logistics, ICT, other)	Complete	Any Issues
1				
2				
3				
4				
5				
6				
7				
8				

Appendix A.12 Handover Recovered Business Operations to Business Unit Leadership

Municipality to create a suitable procedure form.

Appendix A.13 Business Process/Function Recovery Completion Form

Municipality to create a suitable procedure form.

Appendix A.14 Authority to activate the ICT DR Plan

The Municipal Manager (MM) or his delegated official, has the exclusive authority to activate this plan by the process of declaring an ICT Disaster. The Municipal Manager or his delegated official will assume the role of ICT DR Team Leader, and perform the associated responsibilities.

Name	Designation	Contact Numbers	
		Mobile	Office
<name> & title	ICT DR Team Leader		(xxx) yyy yyyy
<name> & title	ICT DR Alternate Team Leader		(xxx) yyy yyyy

Appendix A.15 ICT Recovery Procedure (across all ICT members)

No	Action step	Who	Time	Resources	Process time	Comments
	What do I have to do?	Who is responsible for the step to be completed?	How long will it take?	What additional resources are required?	When did I start and finish the action step?	What happened when I completed the action step?
1	Activate ICT recovery team.	ICT DR Team leader	2 hours			
2	Assess impact.	ICT Manager	4 hours			
3	Disaster declared? If yes, go to step 5.	ICT DR Team leader	2 hour			
4	Restore services to normal levels and go to step 14.	ICT Manager	16 hours			
5	Repair primary site or go to step 9.	Facilities/ ICT Manager	16 hours			
6	Restore operating systems/applications as needed.	ICT Manager	16 hours			

No	Action step	Who	Time	Resources	Process time	Comments
	What do I have to do?	Who is responsible for the step to be completed?	How long will it take?	What additional resources are required?	When did I start and finish the action step?	What happened when I completed the action step?
7	Restore data. Communications.	ICT Manager	16 hours			
8	Critique plan – finish.	ICT Manager	1 hour			
9	Utilise alternate site recover systems.	ICT Manager				
10	Restore operating systems/applications.	ICT Manager	16 hours			
11	Restore data communications.	ICT Manager	16 hours			
12	Validate restored services and provide feedback.	ICT Manager	1 hour			
13	Communicate with stakeholders.	ICT DR Team leader				
14	Deliver critique of DRP.	ICT Manager	2 hours			
15	**Finish**					

Appendix B Critical Business Functions

This appendix contains the list of Municipal critical business functions that are dependent on ICT services. A sample table is provided but must be edited once the ICT DR Business Impact & Risk Analysis document has been updated/completed within the annual cycle.

The MTO is the amount of time the identified critical business function may be unavailable before the Municipality is severely impacted. The RPO is 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. The MTO and RPO are based on a 24 hour day/ 7 day week allowed for recovery.

Appendix B.1 Critical Business Function requirements (dependant on ICT services)

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
Ensure compliance with legislation.	Corporate Services - Legal	*Daily*	*Lexis Nexis*	*2 months*	*None*	*8*
Provide legal opinions and advice.	Corporate Services - Legal	*Ad-hoc*	*Lexis Nexis*	*1 year*	*None*	*8*
Support to council and staff.	Corporate Services - Legal	*Daily*	*Email*	*1 week*	*None*	*8*
Attend to litigation.	Corporate Services - Legal	*Ad-hoc*	*Lexis Nexis*	*2 months*	*None*	*8*
By law enforcement.	Corporate Services - Legal	*Ad-hoc*	*Lexis Nexis*	*1 month*	*None*	*8*
Monitoring and commenting on changes in legislation.	Corporate Services - Legal	*Daily*	*Lexis Nexis*	*1 month*	*None*	*8*
Contract management.	Corporate Services - Legal	*Daily*	*MS Office*	*1 week*	*None*	*1*
Compilation and management of agendas, minutes, items and correspondence.	Corporate Services - Administration	*Daily*	*MS Office* *Email*	*1 day*	*None*	*4*
Compile and maintain resolution register.	Corporate Services - Administration	*Daily*	*MS Office*	*1 week*	*None*	*1*
Funeral assistance.	Corporate Services - Administration	*Ad-hoc*	*SAMRAS*	*1 month*	*None*	*1*
Manage switchboard.	Corporate Services - Administration	*Daily*	*Manual process/PABX system*	*1 day*	*None*	*2*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
Manage filing.	Corporate Services – Records Management	*Daily*	*Metrofile datastore*	*1 day*	*None*	*2*
Manage and maintain general valuation roll.	Corporate Services – Valuations	*Every 4 years*	*Metval pro*	*1 week*	*None*	*3*
Manage and maintain supplementary valuation rolls.	Corporate Services – Valuations	*Bi-annually*	*Metval pro*	*2 weeks*	*None*	*3*
Manage and maintain immovable asset register.	Corporate Services – Valuations	*Annually*	*Metval pro* *SAMRAS*	*1 week*	*None*	*2*
HR administration.	Corporate Services – Human Resources	*Daily*	*SAMRAS*	*1 week*	*None*	*2*
Records management.	Corporate Services – Human Resources	*Daily*	*Metrofile datastore*	*1 week*	*None*	*1*
Manage training.	Corporate Services – Human Resources	*Weekly*	*Personnel director*	*1 week*	*None*	*2*
Ensure all servers are operational.	Corporate Services – Information Technology	*Daily*	*Manual process/ Network Management System*	*1 day*	*None*	*5*
Ensure all Municipal systems are functioning correctly.	Corporate Services – Information Technology	*Daily*	*Manual process/ Network Management System*	*1 day*	*N/A*	*4*
Ensure connectivity is functioning optimally.	Corporate Services – Information Technology	*Daily*	*Manual process/ Network Management System*	*1 day*	*N/A*	*4*
Support of all the Municipality users and councillors.	Corporate Services – Information Technology	*Daily*	*Helpdesk system*	*1 day*	*24*	*1*
Ensure security of the Municipality systems and information.	Corporate Services – Information Technology	*Daily*	*AVG* *Shorewall Firewall* *Spam Assassin*	*1 day*	*24*	*2*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
Ensure effective backups of data and critical systems.	Corporate Services – Information Technology	*Daily*	*Linux scripts* *R sync* *F backup*	*1 day*	*24*	*3*
Investigate new technologies and best practices.	Corporate Services – Information Technology	*Daily*	*Internet*	*1 week*	*N/A*	*2*
Manage and develop ICT policies.	Corporate Services – Information Technology	*Annually*	*Internet*	*1 year*	*N/A*	*2*
Management of ICT assets and infrastructure.	Corporate Services – Information Technology	*Daily*	*Manual process/Asset Mgt system*	*1 month*	*744*	*1*
Attend management meetings.	Office of the Municipal Manager – Performance Management	*Weekly*	*MS Office*	*1 week*	*None*	*1*
Manage performance.	Office of the Municipal Manager – Performance Management	*Daily*	*MS Office*	*None*	*None*	*2*
Monitoring and evaluation.	Office of the Municipal Manager – Performance Management	*Daily*	*MS Office*	*None*	*None*	*4*
Serve on committees for Municipal Manager.	Office of the Municipal Manager – Performance Management	*Ad-hoc*	*Email*	*None*	*None*	*4*
Deal with ward committees.	Office of the Municipal Manager – Public Participation	*Every 2 months*	*MS Office*	*1 week*	*None*	*16*
Deal with communities.	Office of the Municipal Manager – Public Participation	*Every 2 months*	*MS Office*	*1 week*	*None*	*16*
Manage mobilisation for events.	Office of the Municipal Manager – Public Participation	*Ad-hoc*	*Manual process*	*1 week*	*None*	*16*
Communicate with communities.	Office of the Municipal	*Every 2 months*	*MS Office*	*1 week*	*None*	*16*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
	Manager – Public Participation					
Liaise with media.	Office of the Municipal Manager – Communications	*Daily*	*MS Office*	*1 day*	*None*	*4*
Communicate with communities.	Office of the Municipal Manager – Communications	*Daily*	*MS Office*	*1 day*	*None*	*4*
Administration of Municipal website.	Office of the Municipal Manager – Communications	*Daily*	*Website interface*	*1 day*	*None*	*2*
Manage publications for the Municipality.	Office of the Municipal Manager – Communications	*Weekly*	*Website interface*	*1 month*	*None*	*1*
Community profiling.	Office of the Municipal Manager – Programme	*Daily*	*MS Office*	*1 day*	*None*	*3*
Manage HIV/Aids programs.	Office of the Municipal Manager – Programme	*Daily*	*MS Office*	*1 day*	*None*	*1*
Manage gender, disability and senior citizen program.	Office of the Municipal Manager – Programme	*Daily*	*MS Office*	*1 day*	*None*	*2*
Promote youth development.	Office of the Municipal Manager – Youth Development	*Daily*	*Youth database* *MS Office*	*1 day*	*None*	*3*
Create job opportunities.	Office of the Municipal Manager – Youth Development	*Daily*	*Internet*	*1 day*	*None*	*1*
Improve living conditions.	Office of the Municipal Manager – Youth Development	*Daily*	*MS Office* *Internet*	*1 day*	*None*	*3*
Manage cashiering.	Finance - Revenue	*Daily*	*SAMRAS* *Contour Prepaid*	*None*	*None*	*8*
Manage monthly billing.	Finance - Revenue	*Daily*	*SAMRAS* *MS Office* *Email*	*5 day*	*None*	*8*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
			Internet			
Manage customer care.	Finance - Revenue	*Daily*	*SAMRAS*	*2 days*	*None*	*1*
Manage disconnections.	Finance - Revenue	*Daily*	*SAMRAS* *geoReality* *Grapevine*	*5 days*	*None*	*5*
Manage indigent consumers.	Finance - Revenue	*Daily*	*SAMRAS* *geoReality*	*10 days*	*None*	*1*
Manage legal process.	Finance - Revenue	*Daily*	*SAMRAS* *geoReality* *ITC*	*15 days*	*None*	*10*
Manage payments.	Finance - Expenditure	*Daily*	*SAMRAS*	*5 days*	*None*	*6*
Manage the pay office.	Finance – Pay Office	*Daily*	*SAMRAS*	*1 day*	*None*	*6*
Procure goods and services.	Finance – Supply Chain	*Daily*	*SAMRAS*	*3 days*	*None*	*10*
Manage the bid office.	Finance – Supply Chain	*Daily*	*Manual process*	*3 days*	*None*	*4*
Manage internal control.	Finance – Internal Control	*Daily*	*SAMRAS*	*5 days*	*None*	*3*
Prepare annual financial statements.	Finance – AFS	*Daily*	*SAMRAS*	*5 days*	*None*	*5*
Manage and oversee budget office.	Finance – Budget Office	*Daily*	*SAMRAS*	*3 days*	*None*	*3*
Meetings with Executive Management.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*1 month*	*None*	*5*
Implement action plans.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*9*
Communicate with stakeholders.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*5*
Submit applications.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*5*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
Compile business plans.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*5*
Manage housing section.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*4*
Disposal of land.	Development, Planning and Housing - Housing	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*2*
Compile IDP and SDF.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails* *GIS*	*1 week*	*None*	*4*
Public participation.	Development, Planning and Housing - Town Planning	*Bi-annually*	*MS Office* *Emails*	*6 months*	*None*	*3*
Development of plans.	Development, Planning and Housing - Town Planning	*Bi-annually*	*MS Office* *Emails* *GIS*	*6 months*	*None*	*3*
Mapping and planning.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails* *GIS*	*1 day*	*None*	*3*
Maintenance of GIS.	Development, Planning and Housing - Town Planning	*Annually*	*MS Office* *Emails* *GIS*	*1 day*	*None*	*1*
Statutory applications.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails* *GIS*	*1 day*	*None*	*5*
Provide support to other Departments.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails* *GIS*	*1 day*	*None*	*5*
Deal with general public.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails* *GIS*	*1 day*	*None*	*4*
Compile SDBIP.	Development, Planning and	*Quarterly*	*MS Office*	*1 week*	*None*	*2*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
	Housing - Town Planning		*Emails*			
Meetings with Executive Management.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails*	*1 month*	*None*	*5*
Implement action plans.	Development, Planning and Housing - Town Planning	*Daily*	*MS Office* *Emails*	*5 days*	*None*	*9*
Marketing and branding of Municipality to prospective investors and .tourists	Development, Planning and Housing - Local Economic Development	*Daily*	*MS Office* *MS Publisher*	*1 week*	*48*	*4*
Visit businesses to keep them in Ladysmith and to expand services.	Development, Planning and Housing - Local Economic Development	*Quarterly*	*MS Office*	*2 weeks*	*None*	*5*
Development of cooperatives and SMME's.	Development, Planning and Housing - Local Economic Development	*Daily*	*Internet*	*1 day*	*None*	*1*
Enterprise development.	Development, Planning and Housing - Local Economic Development	*Daily*	*MS Office*	*2 days*	*None*	*2*
Agricultural development.	Development, Planning and Housing - Local Economic Development	*Daily*	*MS Office*	*2 days*	*None*	*12*
Maintain and preserve historical items.	Development, Planning and Housing - Tourism and Museum	*Daily*	*MS Office* *MS Publisher*	*1 day*	*None*	*6*
Maintain and preserve historical archives.	Development, Planning and Housing - Tourism and Museum	*Daily*	*MS Office* *MS Publisher*	*1 day*	*None*	*6*
Host events to promote historical culture of Ladysmith.	Development, Planning and Housing - Tourism and Museum	*Ad-hoc*	*MS Office* *MS Publisher*	*2 weeks*	*24*	*6*

Critical business functions	Performed by	Frequency	Systems used	MTO	RPO (hrs)	Onsite users
Reselling of electricity to consumers.	Infrastructure and Services - Electrical	*Daily*	*SAMRAS* *Contour Vending System*	*1 day*	*None*	*6*
Create new civil infrastructure.	Infrastructure and Services - Civil	*Daily*	*Internet*	*1 week*	*None*	*25*
Traffic management.	Community Services – Public Safety	*Daily*	*Traffman* *eNatis* *SAMRAS*	*1 day*	*None*	*6*
Fire management.	Community Services – Public Safety	*Daily*	*Hazdata system*	*None*	*None*	*24*
Registration and licensing of motor vehicles and drivers.	Community Services – Public Safety	*Daily*	*eNatis*	*2 hours*	*None*	*15*
Fleet management.	Community Services – Public Safety	*Daily*	*Netstar* *KAMIS* *SAMRAS*	*2 days*	*None*	*8*
Manage security.	Community Services – Public Safety	*Daily*	*CCTV system* *FBI alarm system* *Paradox* *Watchman*	*1 day*	*None*	*25*
Develop, provide and maintain recreational facilities.	Community Services – Parks and Recreation	*Daily*	*MS Office*	*1 week*	*None*	*9*
Provision and maintenance of community halls and service centres.	Community Services – Parks and Recreation	*Daily*	*MS Office*	*1 day*	*None*	*9*
Provide and maintain library facilities.	Community Services – Parks and Recreation	*Daily*	*KZN Provincial Database*	*1 day*	*None*	*9*
Manage the pounds.	Community Services – Parks and Recreation	*Daily*	*MS Office*	*1 day*	*None*	*5*

Appendix B.2 ICT service recovery requirements

<The following sample table must be re-edited to reflect the Municipality's ICT Services Recovery requirements.>

Service	Description	Used by	Recovery dependencies	Recovery time requirements		
				MTO (hrs)	RTO (hrs)	RPO (hrs)
LAN/WAN	*Network to cater for connectivity to all systems*	*All employees*	*Routers, switches, diginet link, firewall, Telkom NTU*	*24*	*16*	*N/A*
Desktops	*Desktops to provide client functionality for users*	*All employees*	*Operation systems, client software, network connectivity, servers*	*24*	*16*	*None*
Mail server	*Electronic messaging system*	*All employees*	*Mail server software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
Lexis Nexis	*Legal library software*	*Corporate Services - Legal*	*Lexis Nexis software, operating system, databases, storage, network connectivity, antivirus*	*744*	*736*	*None*
MS Office	*Office productivity suite*	• *All*	*Operating system, storage, network connectivity, antivirus*	*None*	*None*	*None*
Ristar	*Switchboard management system*	• *Corporate Services - Administration*	*Ristart software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
SAMRAS	*Municipal financial management system*	• *Corporate Services – Administration* • *Corporate Services – Valuations* • *Corporate Services – Human Resources*	*SAMRAS software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*

Service	Description	Used by	Recovery dependencies	Recovery time requirements		
				MTO (hrs)	RTO (hrs)	RPO (hrs)
		• *Finance – All* • *Infrastructure and Services – Electrical* • *Community Services – Public Safety*				
Personnel director	*Training software*	• *Corporate Services – Human Resources*	*Personnel director software, operating system, databases, storage, network connectivity, antivirus*	*168*	*160*	*None*
Metrofile datastore	*Document tracking system used to track document locations*	• *Corporate Services – Records Management* • *Corporate Services – Human Resources*	*Metrofile software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
Metval Pro	*Land and property valuation*	• *Corporate Services - Valuations*	*Metval Pro software, operating system, databases, storage, network connectivity, antivirus*	*168*	*160*	*None*
Ruckus Zone Director	*Wireless network management software*	• *Corporate Services – Information Technology*	*Ruckus Zone Director software, operating system, network devices, network connectivity*	*24*	*16*	*N/A*
Shorewall Firewall	*Linux Firewall*	• *Corporate Services – Information Technology*	*Shorewall software, operating system, databases, storage, network connectivity,*	*24*	*16*	*24*
Spamassassin	*Linux anti-spam software*	• *Corporate Services – Information Technology*	*Spamassassin software, operating system, databases, storage, network connectivity,*	*24*	*16*	*24*
Internet	*Internet access*	• *All*	*Operating system, network connectivity, antivirus*	*24*	*16*	*N/A*

Service	Description	Used by	Recovery dependencies	Recovery time requirements		
				MTO (hrs)	RTO (hrs)	RPO (hrs)
Youth database	*Database for youth development*	• *Office of the Municipal Manager – Youth Development*	*Youth database software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
Contour Vending System	*Prepaid vending system for electricity*	• *Finance – Revenue* • *Infrastructure and Services - Electrical*	*Contour Vending System software, operating system, network connectivity, antivirus*	*None*	*None*	*None*
geoReality	*Credit checking system*	• *Finance – Credit Control*	*geoReality software, operating system, databases, storage, network connectivity, antivirus*	*120*	*112*	*None*
Grapevine	*Bulk SMS messaging system*	• *Finance – Credit Control*	*Grapevine software, operating system, network connectivity, antivirus*	*120*	*112*	*None*
ITC	*Credit checking system*	• *Finance – Credit Control*	*Operating system, network connectivity, antivirus*	*360*	*352*	*None*
GIS	*Geographical Information System*	• *Development, Planning and Housing – Town Planning*	*GIS software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
MS Publisher	*Publications editing software*	• *Development, Planning and Housing – Local Economic Development*	*MS publisher, operating system, network connectivity, antivirus*	*168*	*160*	*48*
Traffman	*Traffic management and contravention system*	• *Community Services – Public Safety*	*Traffman software, operating system, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*
eNatis	*Vehicle licensing and management system*	• *Community Services – Public Safety*	*eNatis software, operating system, network connectivity, antivirus*	*24*	*16*	*None*

Service	Description	Used by	Recovery dependencies	Recovery time requirements		
				MTO (hrs)	RTO (hrs)	RPO (hrs)
Hazdata system	*Hazardous materials systems*	• *Community Services – Public Safety*	*Hazdata software, operating system, databases, storage, network connectivity, antivirus*	*None*	*None*	*None*
Netstar	*Vehicle tracking system*	• *Community Services – Public Safety*	*Netstar software operating system, databases, storage, network connectivity, antivirus*	*48*	*40*	*None*
KAMIS	*Vehicle costing and workshop expenditure system*	• *Community Services – Public Safety*	*KAMIS software, operating system, databases, storage, network connectivity, antivirus*	*48*	*40*	*None*
Security systems	*Security management and monitoring systems*	• *Community Services – Public Safety*	*Security software, operating system, CCTV cameras, DVR, databases, storage, network connectivity, antivirus*	*24*	*16*	*None*

Appendix C Recovery Data Centre Appendices

Note: This section applies if the Municipality has contracted an offsite Data Centre that will be utilised for recovery of key ICT systems and applications in the event of a Disaster.

Appendix C.1 Recovery Data Centre Activation Procedure

Appendix C.2 Recovery Data Centre Hardware Configurations

Appendix C.3 Recovery Data Centre Hardware Configuration Diagram

Appendix C.4 Recovery Data Centre Floor Plan

Appendix D Network Appendices

Appendix D.1 Network Configuration Diagram – Normal Operations

Appendix D.2 Network Disaster Recovery WAN Cutover Procedure

Appendix E Application(System) Recovery Appendices

Appendix E.1 <System or Application> Recovery Procedure

Sample shown [TO BE CHECKED WITH MO]

Recovery Procedure for Applications	<Application name>
THESE PROCESSES MAY NOT BE EXECUTED UNTIL THE REQUIRED PERMISSION AS PER <name> MUNICIPALITY IC DR PLAN TO PERFORM RECOVERY PROCEDURES HAS BEEN GIVEN	
INSTRUCTIONS • PERFORM EACH STEP EXACTLY AS INDICATED. • IMMEDIATELY INFORM THE ICT DR RECOVERY MANAGER OF ANY PROBLEM THAT OCCURS WHILE THE STEP IS EXECUTED. • MARK EACH STEP AS COMPLETED AND ADD ANY COMMENTS RELATED TO THE ACTION. • DETERMINE IF REMOTE ACCESS (NETWORK CONNECTIVITY) IS POSSIBLE, IF NOT, RECOVERY TO TAKE PLACE FROM THE DR SITE.	

Production Server	• Location of Production Server(s): • Server Model: • Operating System: • CPUs: • Memory:

	• Total Disk: • System Handle: • System Serial #: • DNS Entry: • IP Address: • Other: Production Server(s)
Hot Site Server	<Provide details>
Applications & modules	
Associated Servers	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

The following describes the actions that need to be followed if the File and Print Production server becomes unavailable for any reason.

Action 1: Prepare for Restore

Expected Duration: 5 minutes

Step	Responsible	Machine	DESCRIPTION OF ACTION	COMPLETE	COMMENTS
1.1			Example: All Infrastructure Support Analysts logon on with their personal passwords. If 3rd Party Supplier infrastructure support technicians to aid in recovery, individuals to be added to the Domain Admin group. Obtain Password from Administrator if required.		
1.2			Verify that hardware configuration meets requirements as per Hardware Configuration list.		
1.3			Encryption keys		

Action 2: Recover <name> Application Server

Expected Duration: <TIME LENGTH> minutes

Step	Responsible	Machine	DESCRIPTION OF ACTION STEP	COMPLETE	COMMENTS
2.1					
2.2					
2.3					
2.4					
2.5					

Step	Responsible	Machine	DESCRIPTION OF ACTION STEP	COMPLETE	COMMENTS
2.6					
2.7					
2.8					

<Insert any key screen shots with appended instruction & arrows>

Action 3: Technical Tests

Expected Duration: <TIME LENGTH> **minutes**

Step	Responsible	Machine	DESCRIPTION OF ACTION	COMPLETE	COMMENTS
3.1					

Appendix E.2 <System or Application> 2 Recovery Procedure

Appendix E.3 <System or Application> 3 Recovery Procedure

Appendix E.4 <System or Application> 4 Recovery Procedure

Appendix E.5 <System or Application> 5 Recovery Procedure

Appendix E.6 OTHER APPENDIX CHECKLISTS

Appendix E.7 Finance management

In the event of a Disaster finance must make provision for the following:

- Assess the cash availability of the Municipality, to determine the capability (or suitability) of processing employee payroll early, or to provide advances to employees.
- Assess the status of the accounts to ensure bills are paid timely and that grants are paid when due.
- Establish a process for managing, tracking, and monitoring expenditures during the Disaster.
- Review and approve estimates for repairs and other expenditures that are submitted during the recovery period.
- Communicate with Treasury to get additional funds to make provision for staff and families that might need immediate therapy and medical assistance.
- Upon resumption of business operations, assess the status of the Municipality's finances and report to the relevant authorities.

Appendix E.8 Human resource management

Human resource management must specifically address the following needs:

- Track employees who may have been injured in the event or not available for work due to leave of absence and/or vacations.
- Provide support for injured employees and their families including facilitating access to emergency or on-going medical or psychological services.
- Assist employees with financial, legal, and insurance issues related to the injury or death of an employee or family member.

- Prepare and update an employee head count to determine who is available for recovery operations and who may be available later for business continuity activities. If temporary staff or contractors are needed, they can help select, manage, oversee, and monitor temporary staff as well as manage timecards and other payments for such staff.
- Determine the status of payroll and ensure employees get paid in a timely manner.