

**DISASTER RECOVERY & BUSINESS  
CONTINUITY PLAN FOR ICT SERVICES**



**INGQUZA HILL  
LOCAL MUNICIPALITY**

## Table of Contents

### Contents

<b>1.</b>	<b>Introduction .....</b>	<b>4</b>
<b>2.</b>	<b>Definition of Disaster .....</b>	<b>4</b>
<b>3.</b>	<b>Statement .....</b>	<b>5</b>
<b>4.</b>	<b>How the plan is activated and implemented .....</b>	<b>6</b>
<b>5.</b>	<b>DR\BC for ICT Services Document Storage .....</b>	<b>7</b>
<b>6.</b>	<b>Overview of ICT Infrastructure .....</b>	<b>7</b>
<b>7.</b>	<b>Risk Assessment and Business Impact Review .....</b>	<b>8</b>
<b>8.</b>	<b>Physical equipment .....</b>	<b>9</b>
<b>9.</b>	<b>Disaster Recovery Plan .....</b>	<b>17</b>
<b>10.</b>	<b>Testing the plan .....</b>	<b>24</b>
<b>11.</b>	<b>Review – Maintenance of the plan .....</b>	<b>25</b>
<b>13.</b>	<b>Acronyms .....</b>	<b>25</b>
<b>14.</b>	<b>Definitions .....</b>	<b>26</b>

## **1. Introduction**

Most municipalities recognize that the drive towards electronic government inevitably increases reliance on ICT and hence increases the risks and impacts of failures in supporting systems. Similarly, the rate of change in the use of ICT means that a full inventory review and overhaul of contingency plans must become a regular process rather than a once-off event. Also, most municipalities will already have an overall plan and management structure in place to deal with major catastrophes.

We focus specifically on DR and BC Plan for ICT Services and aim to plan and provide cost-effective solutions to assure business continuity within that framework. This Disaster Recovery and Business Continuity Plan for ICT Services describe the approach we have successfully adopted in solving local councils' problems and describe the specific services we offer. In particular, we recognize that a major constraint is always cost and this plan ensures the lowest cost solution available.

Disasters are, fortunately, are rare but when they do occur they can have devastating consequences. Many services will quickly be brought to a standstill in the event of prolonged computer breakdown. The vulnerability of the municipality's services to the effects of a computer failure have increased remarkably in recent years as more and more reliance has been placed on computerized systems to manage services. This is likely to continue in the coming years as ICT systems are increasingly used as a means of generating efficiencies.

## **2. Definition of Disaster**

"For the purposes of this plan a Disaster is defined as loss or damage of part or all of the municipality's ICT Infrastructure, which would have a very high business impact on the institution's ability to deliver ICT Services."

Also can be defined or can include major terrorist outrages and, while a "911" type event may be exceedingly unlikely in our municipality, such attacks cannot, unfortunately, be ruled out. Fire, flood, power cuts, gas/chemical leaks, network failures and thefts form the most common set of disaster events. In addition to disrupting ICT, they often have severe consequences in terms of staff and premises. We take all these into consideration in our plans.

In terms of minor disasters, BC and DR Plans for ICT Services should merge seamlessly into our normal everyday service management procedures - viruses, machine failures, network outages etc. are so common that everyone should already have systems in place to cope with these. Our approach is to ensure that the ICT disaster plan is fully consistent with, and makes as much use as possible of our existing procedures.

Key software systems which are specifically referred to in this plan include:

- I. Financial Management System (Munsoft)
- II. Email System and Firewall (Ms exchange 2016 Active directory)
- III. Human Resource and Salaries Management System (Payday System)
- IV. Antivirus and File Server (Eset Nod 32)

Servers & Server

Room Switches and

Routers Optic fiber

routers PABX

Workstations

Laptop

### **3. Statement**

Council has to approve the following policy statement:

- The municipality's comprehensive Disaster Recovery and Business Continuity Plan for ICT Services shall be reviewed annually.
- A risk assessment shall be undertaken periodically to determine the requirements for the Disaster Recovery and Business Continuity Plan for ICT Services.
- The Disaster Recovery and business Continuity Plan for ICT Services should cover all essential and critical infrastructure elements, systems and networks, in accordance with key services delivery activities.
- The Disaster Recovery and Business Continuity Plan for ICT Services should be annually tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- Users and administrators must be made aware of the Disaster Recovery and Business Continuity Plans for ICT Services and their own respective roles.
- The Disaster Recovery and Business Continuity Plan for ICT Services are to be kept up to

date to take into account changing circumstances.

#### **4. How the plan is activated and implemented**

ICT must establish and maintain a Disaster Recovery Site with the capacity to host all essential systems.

In the event that a disaster is declared by the Ingquza Hill Local Municipality's Executive management, the Head of ICT will be responsible for activating the plan and monitoring the progress of disaster recovery procedures, reporting to IHLM Executive Management and undertaking any further action as necessary.

Responsibilities are:

- Respond immediately to a potential disaster and call emergency services.
- Assess the extent of the disaster and its impact on the municipality.
- Decide which elements of the disaster recovery plan should be activated.
- Establish and manage disaster recovery team to maintain vital services and return to normal operation.
- Ensure employees are notified and allocate responsibilities and activities as required.

##### **4.1. Plan triggering events**

Key trigger issues that would lead to activation of the ICT Disaster Recovery and Business Plan for ICT Services are:

- Total loss of all communications for a time exceeding 48 Hours.
- Total loss of electricity for a time exceeding 5 working days.
- Flooding of the premises
- total collapse of the building

##### **4.2. DR & BC Plan for ICT Services Team member's responsibility includes:**

- Establish facilities for an emergency level of service within 1 business day after the declaration of the disaster;
- Restore key services within 1 business day of the incident;
  - Return to business as usual within 3 business day after the incident (depending upon incident);
- Coordinate activities with disaster recovery team, first responders, etc.

## 5. DR\BC for ICT Services Document Storage

Copies of this Plan and hard copies will be stored in secure locations to be defined by the municipality. Each member of the Disaster Recovery and Business Continuity Plan for ICT Services Team will be issued a hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

## 6. Overview of ICT Infrastructure

The Ingquza Hill Local Municipality currently has three sites that are connected with VPN, but each site connects to the internet with SDWAN using MTN Towers.

These sites are as stated below:

1. Main Building (Flagstaff Offices)
2. Corporate Services (Lusikisiki Offices) and
3. Testing Centre (DLTC)

The IHLM Server Room (Main Offices) at Flagstaff Offices comprises:

- 4 servers
- Telkom routers
- CISCO Routers and Meraki Firewall  
Cisco Router – 48 ports
- Patch panels
- PABX Voice switches and Telkom opticon
- Optic Fiber Media converters
- UPS

Main Offices has:

- Ubiquiti Switch 24 ports x2
- ARUBU switch 48 ports x1
- Cisco switches 48 ports x 1

- Ubiquiti Switch 48 ports x2
- Cisco switches 24 ports x 2
- D-Link Switch 24 ports x1
- Neat Gear switch 16 ports x1

Testing Centre (DLTC) has:

- Ubiquiti Switch 24 ports x2
- ARUBU switch 48 ports x1
- Ubiquiti switches 48 ports x 1

**A detailed network topology diagram shown in figure 1 below:**

Server room at Flagstaff Main Office is located on the ground floor and the server room at the Lusikisiki Office is Located on ICT Office and the server room at Testing Centre (DLTC) is in the ground floor, Flagstaff server rooms has a Biometrics security, Corporate services is not secured and Testing Centre server room is secured with a Biometrics control. The Server room has permanent installations which provide air conditioning to maintain air temperatures suitable for the equipment located in them. In the event of failure of one of the permanent installations, portable air conditioners will be used temporarily until the permanent installations are fixed.

## **7. Risk Assessment and Business Impact Review**

Likelihood\severity	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Rare (1)	Low	Low	Low	Low	Medium
Unlikely (2)	Low	Low	Medium	Medium	High
Possible (3)	Low	Medium	Medium	High	High
Likely (4)	Low	Medium	High	High	Very high
Almost certain (5)	Medium	High	High	Very High	Very high

### 8. Physical equipment

Location	Network	Type of Loss/	Likelihood	Severity	Business impact	Precautions in Place
Flagstaff	Servers running ICT Services	Fire Theft Water Damage Vandalism	1	5	Loss of a single server will result in only a 48 hours Downtime.	The server room has an air conditioner, steel door with Biometrics
		Hard disc failure	3	5	The impact of the loss of disks would be as	For the financial system and Payroll system

					done to an offside server and can be
		Power failure (Short term)	3	3	Environmental Power Failure would affect all servers that host all ICT services within IHLM, therefore once the backup power is
IHLM Backup Server	Redhat Replication	Fire Theft Water Damage Vandalism Wind Accidental	2	3	Unable to backup data from the network using standard procedure, but no interruptions to service users.  Unable to replicate to the remote sites for Redhat
		Hard disc failure	2	2	No impact from loss of a single hard disk.  The impact of the loss of both disks would be as described
		Power failure	3	3	Once backup power is
					UPS installed – approximately 30 minutes backup.
					The system is imaged weekly using Red Hat backup and recovery . In the event of the loss of the machine this image could be restored to a
					Data replication is done daily to introduce redundancy.  Equipment protected by
					UPS installed –

				exhausted the server would	30 minutes
Linux Firewall & eMail server	Fire Theft Water	1	5	Unable to back up emails, establish connection to	Mails are backup on a PC in the main
	Hard disc failure	1	5	The impact of the loss of disks would be as described under	Backup is always available in case of any failure to our
	Power failure (Short term)	1	5	Once backup power is exhausted, the	UPS installed – approximately 20
Switch's (24 Ports)  D-Link (DGS-3120-24TC) Switch	Fire Theft Water Damage Vandalism Wind Accidental	3	4	Unable to establish connection to the main data center, meaning ICT services will be down.	Equipment protected by the manufacturer warranty – same day onsite replacement
	Hard disc			<b>Not applicable</b>	<b>Not applicable</b>
	Power failure (Short term)	2	4	Once backup power is exhausted the switches	UPS installed – approximately 20

Optic Fiber Media Converter s  Patch Panels	Fire Theft Water Damage Vandalism Wind Accidental	2	3	Connection to the technical site in Standerton from the main office will not be established, also connection form	Splicing machine procured in case the cable breaks or damaged.
---	---	---	---	---	--

	Hard disc			<b>Not applicable</b>	<b>Not applicable</b>
	Power failure (Short term)	1	2	Once backup power is exhausted the converters and	UPS installed – approximately 30
Computers (Desktops & Laptops)	Fire Theft Water Damage Vandalism Wind Accidental	2	3	Loss of a one workstation (Desktop or Laptop) will result in delayed service delivery for internal and external clients more critical to service desks –	Reserved Desktops and Laptops available as loan workstations for senior personnel.  Service provider to
	Hard disc failure	2	3	The impact of the loss of disks would be as described under fire/theft/etc. and above	Service provider to install the desired software for service delivery to
	Power failure (Short term)	1	3	Once backup power is exhausted all workstations	UPS installed – approximately 30

	PABX System PABX OfficeServe74 0 0 X 3 2 * Communication Lines – Telkom PRI 34 Channel. VOIP - SIP Trunk 64 Channel 1* Router 1* 48 Port 3 COMM Switch	Fire Theft Water Damage Vandalism Wind Accidental	2	5	Loss of a single system that runs the telephony system or any other server that will result in only a 24 hours downtime.	The server room has an air conditioner, smoke detectors, steel door with Biometrics Control, and
		Hard disc failure	2	5	The impact of the loss of disks would be as described under fire/theft/etc. and above	Service provider to install the desired software for service delivery to
		Power failure (Short term)	3	3	Once backup power is exhausted all cisco routers	UPS installed – approximately 30 minutes power
<b>Standard n (Real Time Data</b>	Servers running ICT Services	Fire Theft	1	5	Loss of a single server or	The server room has an air



Centre)		Wind Accidental			any other server that will result in only a 48 hours	steel door with a Biometrics Control and
		Hard disc failure	3	5	The impact of the loss of disks would be as described under fire/theft/etc. and above	For the financial system and the prepaid electricity system, daily replications
		Power failure (Short term)	3	3	Environmental Power Failure would affect all servers that host all ICT services within LLM, therefore once the backup power is	UPS installed – approximately 30 minutes backup.
	Ms Exchange Firewall & eMail server	Fire Theft Water	2	3	Unable to backup emails, establish connection to	Emails are backup out of site using Mimecast
		Hard disc failure	2	2	The impact of the loss of disks would be as	Out of site backup will be provided within 12 hours
		Power failure (Short term)	3	3	Once backup power is exhausted the	UPS installed – approximately 30
	Optic Fiber Media Converter	Fire Theft Water	1	5	Connect out of site using VPN. All site are stand alone in terms of	VPN is out ofsite the users will use remote

3120-24TC) Switch  Patch Panels	Accidental			With VPN that is Onsite.	Will assist VPN out offsite and the VPN Onsite
	Hard disc	1	5	<b>Not applicable</b>	<b>Not applicable</b>
	Power failure (Short term)	1	5	Once backup power is exhausted the converters and	UPS installed – approximately 30
Computers (PC's\laptops )	Fire Theft Water Damage Vandalism Wind Accidental	3	4	Loss of a one workstation (Desktop or Laptop) will result in delayed service delivery for internal and external clients more critical to service desks –	Reserved Desktops and Laptops available.  We need to have a spare workstation in order to borrow users.
	Hard disc failure	3	3	The impact of the loss of disks would be as described under fire/theft/etc. and above	Service provider to install the desired software for service delivery to
	Power failure (Short term)	2	4	Once backup power is exhausted all workstations	UPS installed – approximately 20
Cisco Router  RD 800 - 3	Fire Theft	2	3	No connection to the regions meaning	A spare for each cisco router type is

	RD 600 – 2 Cards slots	Wind Accidental			on regional pay points.	immediate replacement by ICT network technician
	SXT - 1 Card Slot	Power failure (Short term)	3	3	Once backup power is exhausted all	UPS installed – approximately 20
	PABX System  PABX OfficeServe74 0 0 X 3  2 * Communication Lines – Telkom PRI 34 Channel. VOIP - SIP Trunk 64 Channel  1* Router 1* 48 Port 3 COMM Switch  Telephon	Fire Theft Water Damage Vandalism Wind Accidental	1	2	Damage of a system that runs the telephony system or any other server that will result in only a 24 hours	The server room has an air conditioner, steel door with a Biometrics control, and raised floor.
		Hard disc failure	2	3	The impact of the loss of disks would be as described under fire/theft/etc. and above	Service provider to install the desired software for service delivery to continue after
		Power failure (Short term)	2	3	Once backup power is exhausted all Cisco routers would shut	UPS installed – approximately 30 minutes power supply.

## 9. Disaster Recovery Plan

There are two distinct elements to this Plan. Disaster could consist of failure of a particular element of the ICT infrastructure, for example, a server or voice switch. Additionally a major disaster such as Fire or Flood could knock out an entire site, large part of a site which contains key systems.

The first table below details steps to be taken in the event of loss of any individual key system. The second table then outlines procedures to be followed in the event of loss of an entire site or a large part of a site which contains key systems.

**9.1 Table showing procedures for recovery of individual network elements**

Location	Network	Type of Loss / Damage	Recovery Procedures
Flagstaff	Servers Running ICT Services for IHLM.	Total Loss of a single Server	<ol style="list-style-type: none"> <li>1. Engage SCM to procure a replacement server.</li> <li>2. IHLM ICT to configure IHLM ICT baseline configurations on the new server and apply relevant policies and procedures.</li> <li>3. Relevant service provider to setup application</li> </ol>
		Hard Disk failure	as described under total loss of a single
		Other hardware failure	as described under total loss of a single

		Software failure	as described under total loss of a single
		Power failure	UPS installed – approximately

Meraki Firewall & eMail Server	Total Loss of a single Server	<p>6. Engage SCM to r e n e w a contract with BCX.</p> <p>7. IHLM ICT to configure IHLM ICT baseline configurations on the new server and apply relevant policies and procedures.</p> <p>8. IHLM ICT and r e l e v a n t S e r v i c e</p>
	Hard Disk failure	as described under total loss of a single
	Other hardware failure	as described under total loss of a single
	Software failure	as described under total loss of a single
	Power failure	UPS installed – approximately
Cisco Switch	Total Loss of a single switch	1. Get a spare switch from the media library
Optic Fiber Media		

			connect it to the network
		Power failure	UPS installed – approximately
Computers\Laptops	Total Loss of a single workstation		<ol style="list-style-type: none"> <li>1. Get a loan workstation from ICT Operations team.</li> <li>2. Configure the workstation to</li> </ol>
	Hard Disk failure		<ol style="list-style-type: none"> <li>1. Always save your information on My Document for backup.</li> </ol>
	Other hardware failure		<ol style="list-style-type: none"> <li>1. Get a spare part from ICT Media Library.</li> </ol>
	Software failure		Restore licensed software with
	Power failure		UPS installed – approximately
Cisco Routers	Total Loss of a single Router		<ol style="list-style-type: none"> <li>1. Get a spare from the media library</li> <li>2. ICT Technician installs it.</li> </ol>
	Network Card failure		As stated above
	Other hardware failure		As stated above
	Software failure		As stated above

		Power failure	UPS installed – approximately
			30 minutes power
	PABX System	Total Loss of a single Server	<ol style="list-style-type: none"> <li>1. Engage SCM to procure a new server.</li> <li>2. IHLM ICT to configure LLM ICT baseline configurations on the new server and apply relevant policies and procedures.</li> <li>3. Relevant service provider to s e t u p</li> </ol>
		Hard Disk failure	as described under total loss of a single
		Other hardware failure	as described under total loss of a single
		Software failure	as described under total loss of a single
		Power failure	UPS installed – approximately

**9.1. Table showing procedures for recovery in case of loss of entire site or large part of a site which contains key systems.**

Location	Type and	Recovery procedure	Persons responsible
Flagstaff	Flood / Fire (Entire site)	Connecting out site with VPN. Testing Centre has Munsoft and Payday Servers, will route all user to those servers.	ICT Manager

		Access to all Revenue Generating Systems (munsoft and Payday) to be provided at DLTC Office.	ICT Manager
		Telkom to re-route main switchboard telephone number voice switch at Standerton Regional Office.	. ICT Manager
		Replacement equipment, as per official inventory, to be ordered at the first opportunity for installation as soon as suitable alternative accommodation becomes available.	ICT Manager
		IHLM ICT Team to be responsible for setting up replacement PCs.	ICT Manager

		Replacement voice switches to be ordered at the first opportunity for installation as soon as suitable alternative accommodation becomes available. Once installed, Telkom to re-route main switchboard telephone number	ICT Manager
	Flood / Fire (Localised	Replace equipment, as per official inventory, to be ordered	ICT Manager

	part of building containin	opportunity for installation at alternative cabling position.	ICT Manager
		IHLM ICT technicians and Engineers to assist	ICT Manager
		Cabling contractors and IHLM ICT Services team to install replacement network cabling for voice and data to affected areas of the building following repair.	ICT Manager
		Re-connect PCs to new cabling in affected areas.	ICT Manager

## 10. Testing the plan

Each of these tests will have to be planned in advance in order of priority. Some of these tests will require significant amounts of staff time and in some cases expenditure with external contractors which will need to be scheduled in work programs and budget requested through the usual IHLM supply chain process.

Wherever possible these tests should be carried out during normal office hours, and not involve any downtime of live servers during core working hours. In addition to these tests, the following should be carried out regularly:

- Test restores from disk and tape to ensure that backups are reliable.
- Tests of UPS systems to ensure they are functioning correctly.

It is imperative that backups are checked daily to ensure they are operating correctly. Automated emails will be generated daily detailing success or failure of individual backup jobs.

## **11. Review – Maintenance of the plan**

This plan is to be reviewed annually or shortly after the installation of any new key ICT infrastructure by the Head of ICT Service. When installing any new infrastructure due regard must be given beforehand to any impact that the installation will have on this plan. Copies of this plan are to be stored in fire-proof safes at all offices which is Flagstaff Main Office, Corporate Service (Lusikisiki offices) and Testing Centre sites. The backup is store out offsite. Therefore the IHLM Backup is secured, safe and available when is needed.

## **13. Acronyms**

ICT : Information and Communications  
Technology

DR : Disaster Recovery

BC : Business Continuity

FMS : Financial Management System

PABX : Private Automatic Branch

Exchange IHLM : Inggquza Hill Local

Municipality

GIS : Geographic Information

Systems WSUS: Windows Systems

Update Server

VOIP : Voice over Internet Protocol.

IP : Internet Protocol

## 14. Definitions

Disaster Recovery Plan : is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

Business Continuity Plan : is best described as the processes and procedures that are carried out by an organization to ensure that essential business functions continue to operate during and after a disaster.

ICT Infrastructure and Services: offers a range of technologies to assist organization in running efficiently.

These services are essential to the everyday mechanics of an organization and integral to effective service delivery. These include hardware, software, networking and implementation.

Server : is a running instance of an application (software) capable of accepting requests from the client and giving responses accordingly, **Servers** can run on any computer including dedicated computers, which individually are also often referred to as "the **server**".

Switch : is a computer networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device

Router : is a networking device that forwards data packets between

computer networks

**Workstation** : is a special computer designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a local area network and run multi-user operating systems.

**Virtual Server** : a method of server hosting using virtual machines.

**Hard Disk Drive information** : is a data storage device used for storing and retrieving digital information using rapidly rotating disks (platters) coated with magnetic material.

<b>Council Resolution:</b> 11-15 June 2023	<b>Approval Date:</b> 29 June 2023
<b>Effective Date:</b> 29 June 2023	<b>Next Review Date:</b> 2024
<b>Signature:</b> Cllr. S.B. Vatsha <b>Honourable Speaker</b>	