XHARIEP DISTRICT MUNICIPALITY

IT Disaster Recovery Plan

AN AREA OF UNFOUND DIVERSITY

DOCUMENT SIGN OFF

NAME AND SURNAME:	DESIGNATION:	DATE:	SIGNATURE:
Ms. LY Moletsane	Municipal Manager		
Adv. ZQ Majenge	Director: Corporate Services		
Mr. A Tyhokolo	Manager IT		

DOCUMENT CONTROL

Author	Andile Tyhokolo
File Name	IT Disaster Recovery Plan
File Path	
Date Created	June 2014
Date Last Edited	2017
Number of Pages	

DOCUMENT VERSION

Version	Revision Date	Author/Modifier	Revision Description
1.1	04/06/2014	Andile Tyhokolo	Document Creation

TABLE OF CONTENTS

1. INTRODUCTION

This Disaster Recovery Strategy summarizes the strategies developed for Xhariep District Municipality and contains the strategic intentions and guidelines on IT Disaster Recovery Management at Xhariep District Municipality. This Strategy will ensure that effective IT Disaster Recovery Planning is implemented and maintained so that Xhariep District Municipality can recover in the event of a major disruption, crisis or disaster which threatens the ongoing operation of Xhariep District Municipality.

2. PURPOSE OF THE IT DISASTER RECOVERY PLAN

To ensure Business Continuity through contingency planning
To set out requirements to ensure continuity of IT Systems in the event of a disaster (natural or manmade)
To describe the processes to be followed by the municipality to ensure business continuity and normal operations in an event of a disaster

3. OBJECTIVES OF THE IT DISASTER RECOVERY PLAN

The Objectives of IT Disaster Recovery plan for Xhariep District Municipality are:

- To ensure compliance with regulatory, statutory and legal requirements relative to business continuity for Xhariep District Municipality
- To ensure that the Xhariep District Municipality adopts a strategy that will eventually lead to compliance with the Good Disaster Recovery Practice defined by the Business Continuity Institute (BCI), and the standards encapsulated in BS25999 (the internationally recognized standard for Business Continuity Management)
- To ensure that effective measures are in place to maintain the physical IT assets of Xhariep District Municipality in the event of a disaster
- To reduce the probability of disaster or outages occurring and the impacts thereof
- To document the critical IT business processes and supporting infrastructure
- To provide a platform for management to formally approve the relevant Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- To clearly define recovery strategies for critical IT supported processes and critical IT infrastructure;
- To ensure that recovery strategies take cognisance of risk transfer, elimination, treatment and acceptance
- To lay down a high-level framework for crisis communications management
- To clearly define business continuity roles and responsibilities within Xhariep District Municipality

4. SCOPE OF THE IT DISASTER RECOVERY PLAN

This strategy applies to all computer systems and infrastructure within the ownership and/or control of Xhariep Municipality. This strategy forms the basis IT Business Continuity Plan and will link to the Xhariep District Municipality Major incident Plan.

5. DEFINITION OF A DISASTER

It is a sudden, unplanned catastrophic event that renders the organizations ability to perform mission-critical and critical processes, including the ability to perform normal production processing of systems that support critical business processes

A disaster can be the result of a significant damage to a portion of operations, a total loss of facility, or the inability of the employees to access that facility

A disaster can be natural or manmade

6. DISASTER RECOVERY

It is a process an organization utilizes to recover access to their software, data and or hardware that are needed to resume the performance of normal, critical business functions after an event of either natural or manmade disaster

7. OWNERSHIP OF THE IT DISASTER RECOVERY PLAN

The ownership of the IT Disaster Recovery Plan resides with the (Check the ACT or PMS) Manager, whose responsibility will be to:

- Maintain the IT Disaster Recovery Plan
- Testing of the plan as per this strategy
- Development and maintain up to date recovery procedures

8. BUSINESS CONTINUITY COMMITTEE

This committee operates at a tactical level and is comprised of Senior Management. In the event of a disaster, the team shall operate from a predefined Command Centre. The Director: Corporate Service will be responsible to establish the following for the committee in the event of a disaster:

- IT Infrastructure
- IT enabling systems
- IT Communication links
- And Access to transversal systems

9. IT RECOVERY TEAMS

- Emergency Management Team (EMT)
- Disaster Recovery Team (subset of Business Continuity Committee)
- IT Technical Support Team

10. ROLES AND RESPONSIBILITIES OF IT DISASTER RECOVERY TEAMS

10.1. Emergency Management Team

Responsible for overall coordination of the disaster recovery effort, evaluation and determining disaster declaration and communication to senior management

Support Activities

- Evaluate which recovery actions should be invoked and coordinated with the corresponding disaster recovery teams
- Analyzes damage assessment findings
- Sets restoration priority based on the damage assessment reports in collaboration with IT Technical Support
- Provides senior management with ongoing status information
- Acts as a communication channel to corporate teams and major customers
- Work with vendors, carriers and IT Technical Support to develop a rebuilt/repair schedule

10.2. Disaster Recovery Team

Responsible for overall coordination of the disaster recovery effort, establishment of the emergency command area (if needed) and communications with senior management, the Emergency Management Team and the IT Technical Support Team

Support Activities

- Coordinate with Emergency Management Team, senior management and IT Technical Support Team
- Assist with determination of disaster recovery needs with the IT Technical Support Team
- Establish command center and assembly areas
- Notify all institution department heads and advise them to activate their plan(s) if applicable, based on the situation of the disaster
- If there is not disaster declared, take appropriate action to return to normal operations using regular operations staff
- Determine if carriers, vendors and other teams are needed to assist with detailed damage assessment
- To prepare post disaster briefing report
- Coordinate the development of the revised disaster recovery plan and ensure they are updated annually

10.3. Technical Support Team

The IT Technical Support Team will facilitate the recovery of the technical aspects in a disaster and restoration activities

Support Activities

Upon notification of disaster declaration, the team will review and provide support as follows:

- Facilitate disaster recovery and restoration activities; provide guidance on replacement equipment and systems, as required
- Testing of IT operations to ensure IT is functioning normally

11. TEAM MEMBERS RESPONSIBILITY

- Each team member will designate an alternate/backup
- All team members must keep an updated contact list of team members' home, work and cellphone numbers both at work and at home
- All team members must keep this plan for reference incase the disaster happens after normal working hours
- All team members must familiarize themselves with the contents of this plan

12. INSTRUCTIONS FOR USING THE DISASTER RECOVERY PLAN

12.1. Invoking the Plan

If the initial assessment of an IT disruption indicates a potentially prolonged outage (e.g. longer than 8hrs), this plan (DRP) becomes effective when the disaster is declared by senior management. The plan will be effective until the operations are resumed in all affected areas

12.2. Notification

Regardless the circumstances under which an IT disaster occurs, but the Emergency Management Team and the Disaster Recovery Team must be activated immediately. These teams must be notified even when there is a suspicion or an indication that a disaster might or is about to occur.

If incident is within working hours:

Upon observation and notification of a serious IT disruption at the municipal premises, ensure that the personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the EMT and DRT ***(see appendix B for contact list***)

If incident out of hour working hours:

IT Technical Support Team personnel must contact the EMT and the DRT and provide status of the incident.

The EMT will provide the following information:

Location of the incident

Type of the incident (e.g. natural, fire, flood etc.)

Summarize the damage (e.g. minimal, heavy, total destruction)

Meeting location that is a safe distance from the disaster scene

An estimated time frame when the disaster/damage assessment group can enter the facility (if possible)

The EMT will contact the respective team leaders and report that a disaster involving IT infrastructure has occurred

12.3. Disaster Declaration

The Senior Management Team, with inputs from the Emergency Management Team, Disaster Recovery Team and IT Technical Support Team, is responsible for declaring a disaster and activating disaster recovery teams as outlined in the plan

In a major disaster, affecting multiple organization locations, the decision to declare a disaster will be determined by Xhariep District Municipality's senior management. The Emergency Management Team, Disaster Recovery Team and IT Technical Support Team will respond based on the directives specified by the senior management

Decide Cause of action:

Based on the information obtained, the EMT and DRT decide how to respond to the event;

- Mobilize IT Technical Support Team
- Repair/Rebuild existing IT infrastructure
- Relocate to new facility if necessary

Informing team members of decisions:

If a disaster is not declared, the IT Unit will continue to address and manage the situation through its resolution and provide periodic status updates to the EMT and DRT

If a disaster is declared, the EMT and DRT will notify the IT Technical Support Team immediately for the deployment of the IT Disaster Recovery Plan

Declare disaster, if the situation is not likely to be resolved within predefined time frames. The person that is authorized to declare an IT Disaster must have at least one backup person who is also authorized to declare a disaster in the event the primary person is not available ***(see appendix I for Contact networking and equipment vendors)***

12.4. Conduct a Detailed Damage Assessment (This should be done before declaring a disaster)

Under the direction of the local authorities, the IT TST, EMT and the DRT, assess the damage to the IT infrastructure and related assets. Include vendors/suppliers of the IT equipment and services to ensure that their expert opinion regarding the condition of the IT infrastructure determined as soon as possible

Participation in the briefing on assessment requirement;

- Assessment procedures
- Gather requirements
- Safety and security issues

NOTE: Access to the facility following a fire or potential chemical contamination will likely be denied for 24hours or longer.

Document assessment results using Assessment and Evaluation Forms (see appendix G)

<u>Build Access Permit by:</u>

- Conducting an on-site inspection of affected areas to assess damage to essential records (files, manuals, contracts, documentation, etc.) and electronic data
- Obtaining information regarding the damage to the IT infrastructure e.g. environmental conditions, physical structure integrity, IT equipment, etc.) from the DRT

Develop a restoration priority list, that identifies facilities, vital records and equipment needed for the resumption of IT operations that could be restored and retrieved quickly

Recommendations for required equipment

12.5. External Communications

Pastel and VIP Vendors

Backup Service Providers

And all other relevant stakeholders

13. EMERGENCY MANAGEMENT PROCEDURES

The following procedures are to be followed by IT operations personnel and other designated Xhariep District Municipality employees in the event of a disruption in IT operations or related outages. Where uncertainty exists, the more reactive actions should be followed to provide maximum protection and personnel safety.

These procedures must be made available to Xhariep District Municipality's management personnel to keep for reference.

In an event of any situation where access to the building housing IT infrastructure is denied, personnel should report to alternative locations. The supervisor or management must be notified via telephone. Primary and secondary alternative locations are listed below.

Alternative Locations:

Xhariep District Municipality Main Building (Primary Location)

Planning and Development Building (Secondary Building)

13.1. Natural Disaster

In an event of a major catastrophe affecting Xhariep District Municipality's IT operations this procedure must be followed

Procedure

STEP	ACTION
1	Notify Emergency Management Team, Disaster Recovery Team and the IT Technical Support Team of the impending event as time permits
2	The teams must assess the impending disaster and advise the Senior Management accordingly
3	Senior Management must declare the impending disaster
4	After declaring the disaster Senior Management must give directives to the respective teams
5	- Backup generators must be on standby - IT Technical personnel must be on standby - If necessary communication to all relevant stakeholders, both internally or externally must commence - Prepare Alternative Locations - If necessary set up and prepare to request backup data to resume operations

13.2. Fire Disaster

If there is fire or smoke in the facility where the IT Infrastructure assets are located, evaluate the situation and determine the severity, and categorize the incident as major or minor and take the appropriate action as defined below.

Personnel can attempt to extinguish minor fires using handheld fire extinguishers located throughout the facility. Any other major fire or smoke incidents will be handled by qualified building personnel until the local fire department arrives.

In the event of a major fire,

Procedure:

STEP	ACTION
1	Notify the Emergency Management Team and Disaster Recovery Team, and
2	The EMT will call 10111 and/or the local fire department
	The EMT and DRT will assess the incident and notify the Senior Management Team
3	The EMT, DRT and SMT will prepare to execute the evacuation plan for present staff
4	EMT, DRT and Qualified Building personnel will establish security at the location and not allow access unless notified by the Municipal Manager or the person delegated by the Municipal Manager
5	All personnel evacuating the facility will meet at their designated outside location and follow instruction given by the designated authority. **Under no circumstances may any personnel leave without the consent of a supervisor**
6	IT Technical Support Team must be on stand by
7	Prepare alternative locations
6	If necessary set up and prepare to request for backup data to resume operations

13.3. Floods or Water Damage

In an event of floods or broken water pipe near any IT Infrastructure location the following must happen.

Procedure:

STEP	ACTION
1	Notify the EMT and the DRT

2	The EMT and the DRT will assess the incident and determine if outside assistance is needed. The teams will report to the SMT and is necessary dial 10111 or 112 immediately
3	The SMT will notify all other personnel in the facility incident and prepare the execution of the evacuating plan if necessary
4	IT Technical Support must be on standby
5	Prepare alternative locations if deemed necessary
6	set up and prepare to request for backup data to resume operations if necessary
7	If water is detected below raised floor it may be a different cause: If water is slowly dripping from an air conditioner unit and not endangering equipment, contact repair personnel immediately If the water is of a major quantity and is flooding (water main break), immediately EMT, DRT and the SMT and commence with the implementation of the evacuation plan.

14. DISASTER RECOVERY PLAN REVIEW

This Disaster Recovery Plan must be reviewed annually and must be exercised annually. The testing, be in the form of a walk-through or a mock up disaster or a component testing must take place as defined in the Municipal Disaster Recovery Plan. Additionally, considering the dynamic environment within the municipality, it is important to review the list of personnel and phone numbers contained in the DRP regularly.

The hard copy version of the DRP will be stored in a common location where it can be viewed by site personnel, EMT, DRT and SMT. Electronic version must be available the municipal network resources as provided by the IT Technical Support Team.

15. ALERTS, VERIFICATION AND DECLARATION PHASE

15.1. DRP Checklist

The DRP checklist and the Network Diagram are presented in the following two sections. The checklist and network diagram must be used by the IT Technical Support Team as a quick reference when executing the Disaster Recovery Plan or for training purposes.

DRP Checklist:

Responsible Personnel	Task to be completed	Status

16. EMERGENCY MANAGEMENT STANDARDS

16.1. Contingency Strategy

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

Specifically the contingency strategy focuses on:

- Establishing priorities for, and allocate the use of, technological resources;
- Establish a multi-layer approach for IT Disaster Recovery Planning as per the following diagram and discussion

Multi-Layer Approach to Disaster Recovery

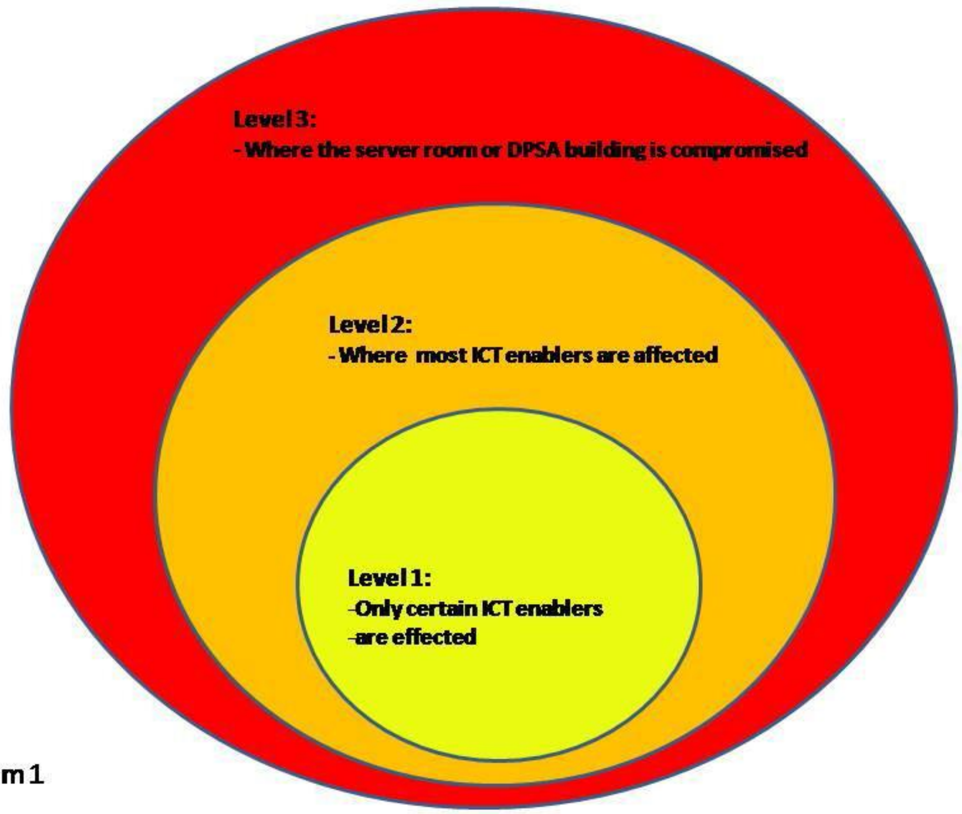
Level 3:
- Where the server room or DPSA building is compromised
Level 2:
- Where most ICT enablers are affected
Level 1:
-Only certain ICT enablers
-are effected

Diagram 1

Level 1:

In order to build the capacity to mitigate a Level 1 disaster, the municipality must maintain a single backup server. This server must be configured to take over the role and function of any of the current servers in operation. It must thus be of the same technical specification. Back-ups will be stored in a fire-proof safe in the main building of the Xhariep District Municipality. In an event of a Level 1 disaster that may causes the primary servers to not function, this backup server must be utilized as a temporary server while the main servers are being repaired. Xhariep District Municipality will endeavor to source funds to implement the following technologies in order to mitigate the risk of technological failure causing a technological disaster. Duplicate storage that can replicate the live data on the storage devices. Currently Xhariep District Municipality has appointed a service provider to store daily backup's offsite.

Level 2:

In order to build the capacity to mitigate Level 2 disasters a dual-core backbone must be installed in the Xhariep District Municipality main building (Trompsburg) to cater for LAN disasters. A backup LAN switch will be held in the store room for recovery purposes. In the server room technology will be implemented where redundant servers can take over the functionality of primary servers and storage devices when a disaster occurs. Xhariep District Municipality will endeavor to source funds to implement the technologies. The daily backups are currently stored off site.

The following will be implemented:

Data ageing and archiving solution for data and e-mail

Virtual servers to take over the roles of the following servers:

File Server
Active Directory
And any other server that may be procured in the future
The e-mail server

Level 3:

This constitutes a total disaster where all ICT infrastructure to render services are incapable of delivering ICT services from inside the Xhariep District Municipality building. This implies that off-site recovery has to be made available. There are three types of solutions available in this realm. Each one of these is linked to a different cost structure. This level of Disaster Recovery, which is an ideal solution for the institution, will be developed over a period of time. The municipality must source funds for this development to be realized. The output of this phase will be a 'cold-recovery site'.

The following table shows the Phases of development.

Phase	Description	Elements
Phase 1	A single redundant server is maintained in the Server Room	When a disaster occurs, the Xhariep District Municipality will negotiate with a Service Provider for a recovery site and infrastructure. The Battle-Box and backups will be obtained from the service provider. Recovery will take place. Note: This is a lengthy process that can take a week or more to negotiate.
Phase 2	In this phase the Battle-Box will be stored off-site together with the daily backups. This is stored at the Disaster Recovery Site. A Cold Disaster Recovery Site will be negotiated with a service provider. The necessary infrastructure will be available for both recovery of IT enabling systems and access and seating for BCC members and transversal system access.	When a disaster occurs, the BCC, Management and transversal system users relocate to the recovery site where the Information Technology Officer will setup and configure all access. This type of disaster recovery can be obtained in 24 hours.

	This site is linked to the municipality network as necessary.	
Phase 3	In this phase the Battle-Box will be stored off-site together with the daily backups. This is stored at the Disaster Recovery Site. A Hot Disaster Recovery Site will be negotiated with a service provider. The necessary infrastructure will be available for both recovery of ICT enabling systems and access and seating for management and transversal system access. This site is linked to the municipality network as necessary. The Disaster Recovery site will run a complete duplicate of what is operational at the main Xhariep building in Trompsburg.	When a disaster occurs, the BCC, Management and transversal system users relocate to the recovery site where Information Technology Officer will setup and configure all workstation and notebook access. All servers will be operational at all times in this phase and thus have the best recovery time.
Decision: Between the current and 2014/15 financial years the Xhariep District Municipality Information Technology Manager must negotiate and establish a service level agreement for the implementation of a Phase1 and 2 solution. A phase 3 solution must be negotiated in the following financial year 2015/16. It must be kept in mind that the availability of the solutions in the phases are guided by available budget. It must furthermore be kept in mind that the implementation of Phase 3 may be regulated in the next year in which case the priority on this implementation will be changed.		

16.2. Backup Strategy

These strategies are based on the common backup strategies for data protection

Phases	Description
Phase 1	1. Backups of VIP must be made to the File Server on a daily basis 2. The VIP data from the file server will be backed up every night to a redundant server in a separate room here at the municipal premises (onsite) 3. Backups of the Pastel System must be made on a daily basis on the file server 4. Pastel data on the file server will be backed up every night to a redundant server in a separate room here at the municipal premises (onsite) 5. Users of the system must work from a secured and controlled network server where their data will be store safe and secured. Even when one's machine should crash or be stolen, the data will still be available on the network server 6. The data on the network server must also be stored in the redundant server in a separate room here at the municipal premises (onsite) 7. Backup of the Active Directory be made in the redundant server in a separate room here at the municipal premises (onsite) and this data must be updated on the weekly basis on the redundant server 8. Backup of CCTV footage to be stored for 1 month in the live environment 9. And a footage of 2 months running excluding the current month, must be kept on tapes and the tapes must be stored in the secured storage place.
Phase 2	Backups of data referred to in Phase 1 (except for the CCTV Footages)must be stored at an offsite storage facility that meets the standards for data storage by a reputable service provider
Phase 3	Backups made in Phase 2 must be backed up in the Cloud
Decision: The different handling of backups and archiving must be implemented to match each one of the phases mentioned in this table	

16.3. Recovery Time and Point Objectives

The Recovery Time Objectives and Recovery Point Objectives (RPO) metrics have been mapped to the applications and the underpinning IT infrastructure for XHARIEP DISTRICT MUNICIPALIY, and the following table shows the priorities and backup cycles:

Priority 1 systems/applications

			Backups		
Priority	System/Application	Server Name	Daily	Weekly	Monthly
1	VIP	File Server	✓		✓
1	PASTEL	File Server	✓		
2	Active Directory	Domain Server		✓	

2	User Documents	Documents file	✓		

16.4. Disaster Recovery Battle Box

Information Security Officer is required to create a Disaster Recovery Battle Box. The content of the battle box will contain information and items that will be utilized to manage the recovery from a disaster. The following must be contained in the box:

Item	Comments
Copy of the IT Disaster Recovery Plan (fully populated)	This must be the latest relevant copy
Copy of all operating systems used in Xhariep District Municipality	Must include all setup instructions and configurations
Copy of all software, systems and Applications used in Xhariep District Municipality	Must Include all setup instructions and configurations
Copy of all passwords	Sealed in an envelope by the system owner and updated on a monthly basis
Relevant backup disks	All data backed up
Decision: The content of the Battle-Box will be updated on a monthly basis and signed off as such. The Battle-Box will be stored on site in the IT Storeroom and with the service provider. And in Phase 3 it will be moved to the DR Site.	

APPENDIXES

Appendix A: Xhariep District Municipality Recovery Teams Contact List

Emergency Management Team:

Name	Address	Home	Mobile
Teboho Chabe	45 Jan Str, Trompsburg		082 307 9216
Eugene Prince	Phaliso View, Trompsburg		074 643 5467

Disaster Recovery Team:

Name	Address	Home	Mobile
Teboho Chabe	45 Jan Str, Trompsburg		082 307 9216
Eugene Prince	Phaliso View, Trompsburg		074 643 5467
Sankase Mqungquthu			083 707 8231
Antonie Reachable			082 829 5660
Noli Liloch			072 119 1252
Motlatsi Lekoala			081 756 1286

IT Technical Support Team:

Name	Address	Home	Mobile
Mr. Andile Tyhokolo			083 262 9664
Ms. Sheila Senoge			073 301 8717

Senior Management Team:

Name	Address	Home	Mobile
Mr. Martin Kubeka			082 933 6056 078 123 1856
Mr. Levy Mashiane			082 857 2287
Mr. Mopedi Mohale			072 536 2483
Mr. Mbuyiselo Khapha			072 975 9562

Appendix B: Emergency Numbers

Organization Name	Contact Person	Landline	Mobile
Health Dept. (EMS)	Mr. Mmota		083 708 9346
Provincial Disaster Management	Mr. James Mndi		082 821 5078
SAPS	Col. Guma	10111	082 466 8639

Appendix C: Emergency Command Center

Xhariep District Municipality

20 Louw Street

Trompsburg

Contact: 051 713 9300

Appendix D: Emergency Response Activities

No:	Action	Responsible Person
1.	Identify and assess IT operations disruptions	IT Officer
2.	Review with IT Management	IT Officer
3.	Decision to invoke IT DRP	IT Manager
4.	Activate EMT and DRT	IT Manager
5.	Initiate DRP activities	EMT and DRT
6.	Evacuate area if Necessary	EMT, DRT and SMT
7.	Initiate remedial actions to recover IT Operations	IT Technical Support Team
8.	Contact appropriate Vendor and Suppliers	IT Technical Support Team
8.	Follow through on recovery procedures	EMT, DRT and IT TST
9.	Report to Senior Management	EMT, DRT and IT TST

Appendix E: Incident or Disaster Form

Upon notification of an IT operations disruption the EMT, DRT and IT TST will make inputs into the form. The document will be continually updated until the unit has resumed normal business operations

DISASTER FORM	
Incident Date and Time:	
Incident Type:	
Incident Location:	
Building Access Issues:	
Projected Impact to Operations:	
Running Log (On going incidents):	

Appendix F: Critical Equipment Status Form

CRITICAL EQUIPMENT STATUS ASSESSMENT AND EVALUATION FORM			
No:	**Equipment**	**Condition**	**Comments**
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Conditions:

OK – Undamaged

DBU – Damaged, but usage

DS – Damaged, required salvage before use

D – Destroy, requires reconstruction

Appendix G: Critical Network channel Status Form

CRITICAL NETWORK CARRIER CHANNEL STATUS ASSESSMENT AND EVALUATION FORM			
No:	**Carrier Services**	**Condition**	**Comments**
1.			
2.			

3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Conditions:

OK – Undamaged

DBU – Damaged, but usage

DS – Damaged, required salvage before use

D – Destroy, requires reconstruction

Appendix H: Building Evacuation Information

Refer to the Xhariep District Municipality Evacuation Plan

Appendix I: Inventory of Computer and Network Equipment

Refer to the Xhariep District Municipality Assets Register

Appendix J: Inventory of Backup Network Services and Equipment

Refer to the Xhariep District Municipality Assets Register

Appendix K: Approved Vendor List

Refer to Xhariep District Municipality Supplier Database