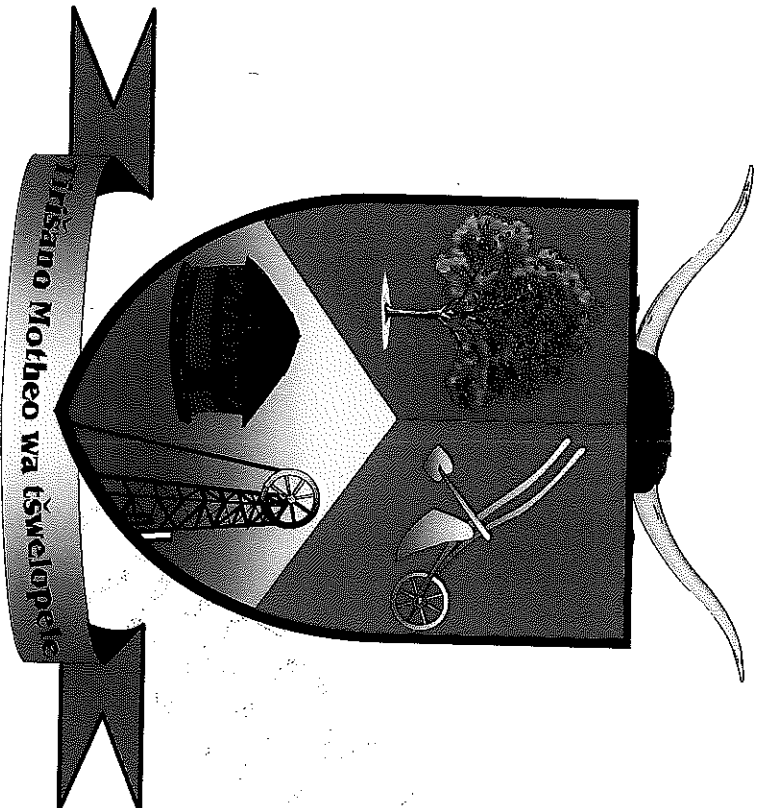



FETAKGOMO LOCAL MUNICIPALITY



Council Resolution No. C13/2014

DISASTER RECOVERY PLAN

FETAKGOMO LOCAL MUNICIPALITY
REGISTRY
PO BOX 818
APPEL
07559

Received by: 
Date: 2014-08-18

1. Overview

Fetakgomo local municipality dependent on information and communication technology to operate effectively and efficiently. Information is therefore a valuable asset to the municipality as any other physical asset or intellectual property owned and produced by the municipality. All operations are extremely time-dependent and even if the municipality loses one hour of productivity it may affect the organization.

IT systems are vulnerable to a variety of disruptions ranging from mild disruption such as short-term power outages or disk drive failures to severe disruptions such as the destruction of equipment or fires.

Vulnerabilities may be minimized or eliminated through technical, managerial or operational solution as part of the municipality's risk management effort. It is however virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing on effective and efficient recovery solutions.

It is vital for the municipality to have a proper disaster recovery plan in place.

This disaster recovery plan outlines the nature and location of municipal systems and the necessary actions required to ensure that it will be able to resume normal business function (or as close to it as possible) in the event of a disaster occurring as a result of whatever cause, whether storm, fire, natural disasters or malicious attacks, intending to destroy organizational information and systems. The IT function of the Fetakgomo local municipality is focused on ensuring that vital assets are restored to working order as quick as possible as failing to do so may hamper the goal of the municipality of providing efficient and effective services to the South African public and specifically the people of Fetakgomo.

It is therefore the intention of the municipality to comply with industry best practices, international standards and corporate governance regulatory requirements for developing and maintaining business continuity and that best meet the needs of the government.

2. Scope

This plan will guide the municipality through the many activities associated with achieving its recovery objectives. It assumes that recovery team participants have a reasonable knowledge of municipal business processes and had formal training in the various computing disciplines applicable to their respective areas.

This plan covers recovery of the following business processes and systems supporting those business processes.

2.1 Business Processes

Critical Processes	Critical scenarios	Priority
Community services	Community services is responsible for disaster management, environmental management, sports, arts and culture issues, administration of Thusing services centers, traffic management and environmental management,	Priority two

	the information derived from this unit forms the integral part of the municipality. Without the information informed decisions won't be made by the municipality.	
Mayor's office	The office of the mayor has programmes to support Women, elderly, disability and youth. They also provide political support to the councillors.	Priority one
Human Resource	Human resource has the responsibility to develop Employment Equity Plan and Job descriptions of the municipal employees. They also need to recruitment personnel on behalf of the municipality. Ensure that there is a fair and equitable system to deal with grievance performance Management. They form critical part of the municipality as they deal with human elements of the municipality.	Priority one
Administration	The administration unit is responsible for switch board operations, registry, records management, ward committee support, council support and fleet management of the municipality. If the disaster hits the municipality information around fleet and records might be lost. The municipality information around fleet and records might be lost. The municipality can be subjected to litigation due to the municipality been unable to produce required documentation and it may also to audit quires.	Priority one
Revenue and Expenditure	Currently, the municipality does not have a structured revenue base or a billing system. Potential revenue from service charges for things like water and electricity is also possible because the Municipality does not perform those functions. However the municipality collects money from renting the halls, the BnB, buying of tender documents and car licenses. If the Fetakgomo local municipality is unable to manage revenue, it might be exposed to financial loss due to leakage expenditure.	Priority one
Supply Chain Management	Supply Chain management is responsible for purchasing of stock logistics, and asset management. The unit uses BAUD for asset management, cash focus for payments and Munsoft for printing of orders. For supply chain life without their system will be difficult to accurately report on their activities	Priority one
Budget	The division monitors the different budgets for the municipality and they use the Munsoft system to manage and control the budgets. Without the application, the processes shall	Priority one

IDP	stand still.	IDP , Programmes are managed and operated of programmes is depended on how the unit can monitor the progress of the different programmes.	Priority three
LED	One of the KPAs of the municipality is to create jobs and if LED's performance is not monitored and recorded it will be difficult for the municipality to track number of jobs, SMMEs, and entrepreneurial training provided to the youth	Priority two	
Town planning	The section is responsible for the Land use, Rezoning, town planning application, land use application and consolidation. This is a critical component of the municipality, records need to be kept in the safe place for future references.	Priority three	
Legal Services	The division is responsible for drafting of contracts, litigations and providing legal advices to the municipality. To also facilitate contracts enforcement action plan	Priority two	
Internal Auditing	The internal audit is responsible to governance, risk management and insure the good control in all the system of the municipality.	Priority two	

2.2 IT Systems

This DR plan caters for the following municipality servers/applications only:

Server Room Location	Primary Server Name	Secondary Server Name	Package Name	Priority
Fetakgomo	With service provider	With service provider	Munsoft	One
Fetakgomo		With service provider	VIP	Three
Hosted at service provider	No server	No server	Cash Focus	Four
Hosted at the Department of Road and Transport	Hosted at the Department of Road and Transport	Hosted at the Department of Road and Transport	Vehicle registration	One
Fetakgomo	No server	No server	Record Retention	Three
Fetakgomo	FILESRV	Main domain	File Server	Three
Fetakgomo	MailsRV	Exchange Server	Exchange	One
Fetakgomo	AntivirusSVR	Proxy	Proxy	One

3. Benefits

Developing a disaster recovery plan will:

- a) Provide the municipality with a sense of security;
- b) Minimize the risk of delays;
- c) Guarantee reliable of standby systems;
- d) Provide a standard for testing the plan;
- e) Minimize necessary decision-making during a disaster;
- f) Establish a DR team to manage disaster;
- g) Coordinate recoveries, ensure business continuity and protect municipal systems from major disruptions or disasters;
- h) Address the recovery of resources, products and services following a disaster within the computer room or on the network affecting municipal systems;
- i) Determine the events that can adversely affect the effective functioning of municipal systems and the damage from such events, the time scale needed to restore normal operations and the controls that can be implemented to reduce the impact.

4. Developing a disaster recovery plan

4.1 Planning areas

Various scenarios that forms the basis of the plan was considered and a multitude of assumptions were made in the process.

The key principles that plan applies to are:

- a) Critical unrecoverable hardware failures such as servers or switches;
- b) Any computer room facilities, servers or business processes as listed in section 2.2 becoming inaccessible preventing the municipality from performing its normal operational functions;
- c) A predetermined disaster recovery site and IT resources that will be used to recover critical system functionality during an emergency that prevents access to any of the regional systems or servers.

4.2 Sections of the plan

The DRP consists of four (4) main sections that are divided into subsections. Those are:

- a) DRP ownership, change and version control;
- b) The DRP strategy;
- c) The disaster recovery process; and
 - i) the alert phase;
 - ii) the recovery phase; and
 - iii) the return to normal phase
- d) Annexures

4.3 Ownership, change and version control

4.3.1 Designated plan owner

The DRP forms part of the overall municipal business continuity plan, but each DRP still has its own designated owner. The owner of the plan is IT management in the corporate services business unit of the municipality. The DRP owner has to ensure that the correct recovery strategy is adopted.

The Fetakgomo local municipality management takes overall responsibility for the plan in terms of:

- a) Maintaining the plan e.g. regular updates that accurately reflect changes in the production environment should be done on at least a monthly basis;
- b) Scheduled recovery tests that include specific recovery objectives for each test;
- c) Correct and up-to date technical procedures;
- d) Ensuring that the plan is reviewed when there are:
 - i) additions, deletions or upgrades to hardware platforms;
 - ii) additions, deletions or upgrades to system software;
 - iii) changes to system configuration;
 - iv) changes to application software;
 - v) changes that affects the availability of the disaster recovery facility;
 - vi) changes to staff identified by name in the plan;
 - vii) changes to off-site backup procedures;
 - viii) changes to application backups; and
 - ix) changes to vendor lists maintained in the plan.

4.3.2 Access to and users of the plan

The plan contains confidential information. Uncontrolled access to the plan may lead to security breaches and business risks. A signed hard copy will be kept by the municipal manager for security reasons and the other copy will be kept by the designated disaster recovery coordinator and yet another copy will be stored in a sandbox at a pre-determined disaster recovery site. A soft copy of the plan will be kept on the municipal governance system (document management system). Note that all printed copies of the plan, except the PDF master copy, are uncontrolled.

The plan and its contents would only be accessible to municipal staff member that play an active role in the recovery process. In terms of awareness to the rest of the organization, a high-level overview of the plan will be made available for general perusal.

4.3.3 Management signoff of the plan

The office of the Municipal Manager needs to take ultimate accountability for the information contained in the plan. Lack of managerial commitment may lead to recovery failure and ultimately a business risk.

Table 1: Accountable managers

Name	Designation	Work Tel	Cell number
Matumane N.D	Municipal Manager	015 622 8001	071 462 1421
Maredi M.F	Chief Financial Officer	015 622 8006	084 411 5796
Phasha M.I	Director Corporate Services	015 622 8014	082 820 4996
Marome P.O.S	IT Manager	015 622 8094	076 268 3896

4.3.4 Version and change control of the plan

It is inevitable in the changing environment of the IT industry that this disaster recovery plan will become outdated and unusable unless someone keeps it up to date. Changes that will likely affect the plan fall into several categories. Those categories are:

- a) Hardware changes;
- b) Software changes;
- c) Facility changes;
- d) Procedural changes ; and
- e) Personnel changes

As changes occur in any of the above mentioned areas, the municipality IT business unit, through the designated disaster recovery coordinator will determine if changes to the plan are necessary. This decision will require that managers be familiar with the plan in some detail. The common changes that will require plan maintenance are listed in above.

The staff in the affected area will make changes that affect the platform recovery portions of the plan. After the changes have been made the municipal disaster recovery management will be advised that the updated documents are available. They will incorporate the changes into the body of the plan and distribute as required.

All updates or changes to the disaster recovery plan shall comply with the change control policy with regards to assessing if the change is necessary, validating the adequacy of the acceptance test, scheduling the promotion into a test environment, notifying the appropriate functions and verifying whether the change was implemented successfully.

4.3.5 Recovery information –roles and responsibilities

Role	Responsibility
Disaster Recovery Coordinator	Responsible for the implementation of the DRP, and overall compliance with, the Disaster Recovery Policy within their area of responsibility.
IT Manager	Communicate all decisions/upgrades/changes/new implementations in respect of technology that will directly impact disaster recovery capabilities and procedures to the Disaster Recovery Department.
IT manager	Compile and maintain, in accordance with standards, and with the assistance of the Disaster Recovery Department, individual Disaster Recovery procedure and supply a copy thereof to the Disaster Recovery Department.
Registry clerk	Active involvement in disaster recovery tests and the production of a detailed test log.

Disaster Recovery Coordinator	Provide a full consultation service on the compilation of individual Brief Impact and Risk analysis.
-------------------------------	--

5. Recovery scenarios

This section describes the various recovery scenarios that can be implemented, depending on the nature of a disaster and the extent of the damage. The Disaster Recovery Coordinator decides which recovery scenario to implement when the Disaster Recovery Plan is invoked.

5.1 Scenario 1: minor damage

In this scenario only a part of the computer processing environment may be affected, but the communication lines and network are still active. The goal of the recovery process in this case is to move the applications from unavailable systems to the standby facility. In this scenario the building is still available and the user can use normal office space to wait for systems to come on line.

Table 2: Action Plan

Task	Team
Evaluate the damage	Disaster Management Facilities and Operations
Declare a disaster	Municipal Manager
Identify the concerned applications	IT Manager
Request the appropriate resources at the Standby Facility	ITRT
Obtain the appropriate backups	IT Officer
Restart the appropriate applications at the Standby facility	IT Manager
Inform users of the new procedures	Communications
Order replacement equipment to replace the damaged computers	CMT and ITRT
Install replacement equipment and restart the applications	ITRT
Inform users of normal operations	Communications

5.2 Scenario 2: major damage

In this scenario a major disaster occurred. It could be that the building communication lines are unavailable. When such major damage occurs the disaster recovery process as stipulated in the next section will be executed.

6 Disaster recovery processes

The municipal disaster recovery plan establishes procedures to recover municipal systems following a disruption. The plan will maximise the effectiveness of the contingency operations by means of an established plan consisting of the below phases.

Notification/ activation/ alert phase: to detect and assess damage and to activate the plan

Recovery phase: to restore temporary business operations and recover damage done to the original systems

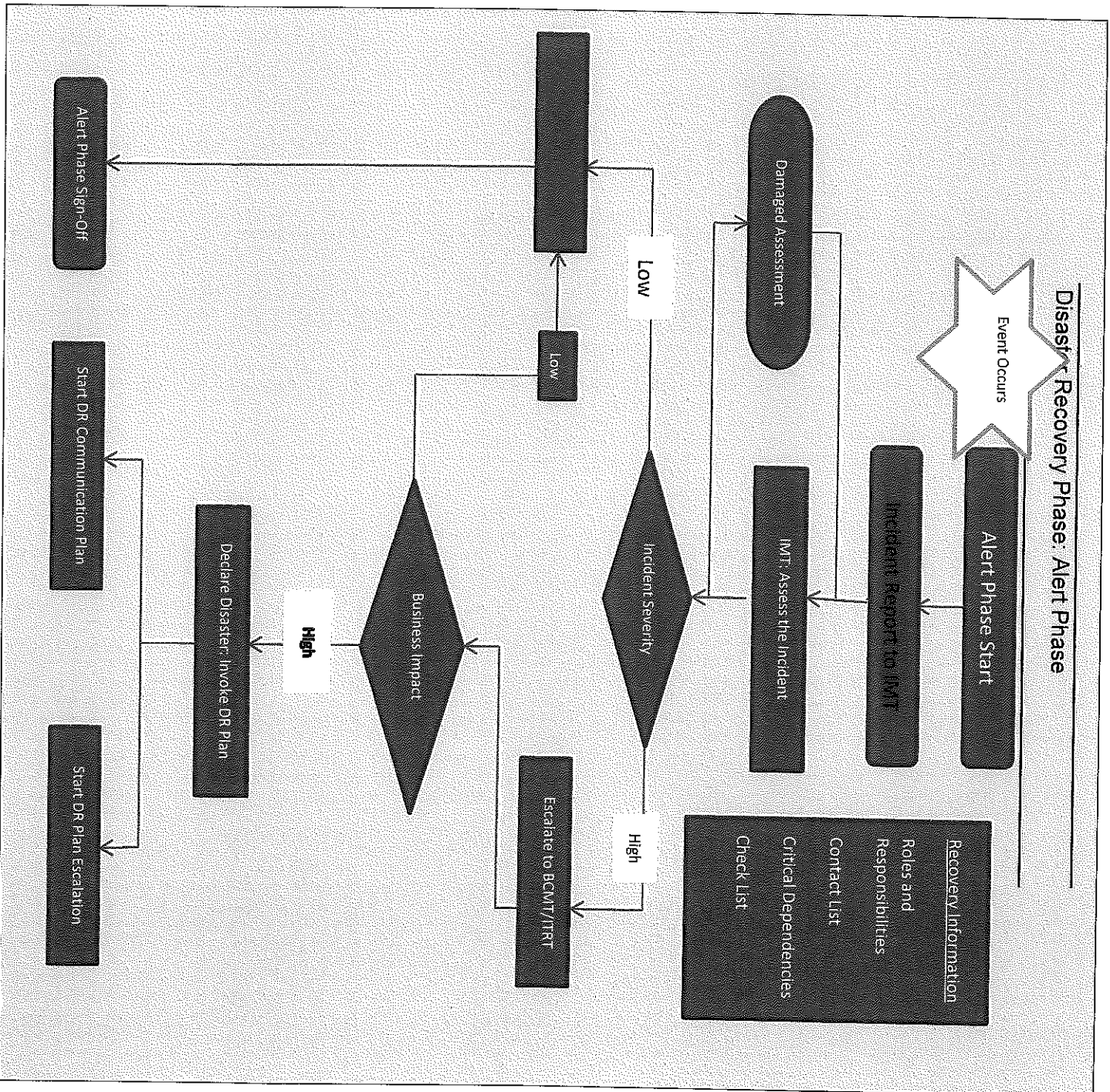
Reconstitution/ normalization phase: to restore the municipality's system processing capabilities to normal

In this section the three main recovery processes, Alert, Recovery and Return to Normal, are described in detail for the Fetakgomo local municipality.

Alert Phase: Recovery of information

This phase deals with, and provides information that must be available prior to, and immediately after a disaster happened. It includes;

- a) Reporting the incident;
- b) Damage assessment procedures;
- c) escalation and declaration criteria;
- d) declaration forms to be used when declaring a disaster;
- e) internal and external communication;
- f) recovery information, including roles and responsibilities, contact detail and critical dependencies



6.1 Reporting the incident

The person who discovers the incident must report the incident to the municipality's Help Desk at the following contact number(s):

Table 3: Incident reporting

Support Centre	Telephone number	Alternative number
Helpdesk/IT Office	015 622 8045	015 622 8094

The person who reports the incident must provide as much information as possible and provide the helpdesk official with as many observations as possible. The questions that should be answered are:

- a) which applications or systems are affected?
- b) What time did the incident occur?
- c) What is the expected outage duration (if possible)?
- d) What is the damage to equipment?
- e) What is the damage to computer room environment? And
- f) Any other relevant information.

After the incident has been reported to the helpdesk it should notify the incident management team of the problem. The IMT is responsible for covering the initial actions required to ensure the safety and welfare of the people affected by the incident, to activate the relevant recovery management teams and determine the level of response which is appropriate to the incident.

The IMT should determine whether the nature and extent of the disruption warrant the deployment of the relevant DRP, and if so should:

- a) Determine the nature of the disruption;
- b) Implement the selected procedures, securing the required resources through the BCMT/ITRT where appropriate;
- c) Identify, and where appropriate, adapt the relevant continuity procedures to ensure that the business continues to operate as near to normal a manner as possible for the duration of the disruption. All such activities should be coordinated through the BCMT/ITRT;
- d) Identify, and where appropriate adapt the relevant recovery procedures to ensure that the business recovers from disruption in a timely and controlled manner once the root cause of the disruption has been eliminated. All such activities should be coordinated through the BCMT/ITRT;
- e) Activate the BCMT/ITRT who investigates the requirement for further teams to be activated. Whilst the IMT is active, all activities should be coordinated through the BCMT/ITRT to ensure that no action taken by one IMT conflicts with actions taken by others;
- f) Communicate with all parts of the department affected by the disruption on a regular basis regarding progress and the actions initiated by the IMT;
- g) Organize once recovery actions have been completed, a thorough review of its management of the disruption so all relevant lessons from the experience can be learned and incorporated into procedures and training programmes.

6.1.1 Assessing the incident

The Fetakgomo Disaster Recovery Coordinator, through the services of the Damage Assessment Team, will assess the damage and will evaluate the situation.

Table 4: Incident management team

Members	Responsibility	Telephone number
Marome P.O.S. IT Manager	Analyse the damage at the primary site after a Disaster working together with the other member. Ensure the Integrity, Availability and Confidentiality of the damaged systems are still intact and comply to the departments policies. This personnel will also act as the Disaster Recovery Coordinator for IT	015 622 8094
Phasha M.D Manager: PMU	Assist the IT Office in assessing the damage on the facility and any related peripherals	015 622 8076
Maloma M.E Manager: Administration	Ensure the security of the damaged environment and also security of the alternate site if relocation is required	015 622 8009
Rachidi L.A	Responsible for all communication forwarded to the users and to the Incident Management Team	015 622 8089

6.1.2 Damage assessment procedures

Assets may have been damaged as a result of the disaster. The checklist below could be used to speed up the damage assessment process visit every instance, verify, and assess the following:

- a) IT infrastructure and services
 - i) Main computer centre
 - ii) Server room
 - iii) Power
 - iv) Air conditioning
- b) Servers
 - i) Database
 - ii) Application
 - iii) Storage
- c) Network components
 - i) Switches
 - ii) Routers
- d) Telephones systems

- e) Test main infrastructure and equipment for connectivity
- f) Record damaged equipment and infrastructure
- g) Report back to disaster recovery coordinator.

Table 5: damage Assessment Checklist

Purpose	This form is used to assess the damage of the systems and data within four (4) hours. It documents the assessment of the damage to the building, data center, environmental controls, and computer room contents. It provides the estimated recovery time and the equipment that may be salvaged and repaired. This form may be used to notify the IT Recovery Team of the assessment, and coordinate equipment salvage where possible. It will also be used to as input to the CMT to declare the event as a disaster.		
Assess the requirement for hiring physical security to minimize possible injury, to discourage unauthorized persons from entering the facility, and to eliminate the potential for vandalism to the assets.			
Initials:	Date:	Time:	

The purpose of the checklist below is to guide a damage review and assessment of the production facilities, the network, and/or the data centre facilities following a disaster. It is also documents the assessed damage for notification to the Crisis Management Team. In using the checklist, the Team must consider:

- a) The safety of the area for employees or vendors to work.
- b) The percent of normal capacity the equipment is able to function.
- c) Action to be taken to recover or repair damage equipment to enable functioning.
- d) Timeframes for repair or replacement of the damaged equipment to enable functioning.

Infrastructure	Damage		Salvageable		Description of damage
	YES	NO	YES	NO	
Building					
Exterior					
Interior					
Data Centre					
Walls					
Ceilings					
Floor					
Environmental controls					
Electrical					
Air-con					
Water supply					
Fire suppression					
Computer Room					
Servers					
External Disk Drives					
Tape Backups					
Network Cabling					

The Crisis Management team should engage other Business Units Managers to assess the impact of the incident and the downtime. A list of these managers is attached, see Annexure B.

Should business units managers decide that the incident has no immediate impacts on the business, the Help Desk will be notified and the incident will be closed, or depending on the situation, be resolved as a fault.

Should Business Unit Managers however decide that the incident impacts negatively on the maximum allowable downtime window, a disaster is declared. The CMT informs the JMT which informs the BCM/ITR Team and the BCM/ITR Team invokes the DR plan.

6.1.3.1 Disaster Declaration Authority

Making a wrong decision to declare a disaster could be a costly exercise. The correct level of authority should therefore be defined. In the event of a disaster, only the people listed below is empowered to declare and invoke a disaster:

Table 7: designated authorities who may declare a disaster

Designation	Name	Contact no	Alternative no
CFO	Maredi M.F	015 622 8006	084 411 5796
IT Manager	Marome P.O.S	015.622.8094	076 236 3896

6.1.3.2 DISASTER DECLARATION FORM

TO: _____

FAX NO: _____

Tel no: _____

Alt no: _____

From: _____ of _____ (Business)

Company: _____
(Customer representative)

Tel no: _____

Fax no: _____

Date of declaration: _____

Time of verbal declaration: _____

Incident Number: _____

The following server(s) was/were impacted by the disaster: _____

We the undersigned, hereby confirm the telephonic and verbal declaration of a disaster. The disaster was declared on _____ this _____ day of _____, 20____ at _____ by _____, who is duly authorized to make such a declaration and his designation is that of _____.

Yours faithfully

Fetakgomo DR Plan

Signature _____

Designation _____

Once the IMT has been informed of the declaration of the disaster, it then informs the BCM/ITR Team. The following are the team members of the BCM/ITR Team:

Table 8: BCM/ITRT team

Member	Responsibility	Telephone number	Alternative number
IT Manager	Project Management and overseeing that the recovery process is properly resourced. Organize all required recovery Teams.	015 622 8094	076 236 3896
DR Coordinator	Coordinate the implementation of DRP if the disaster strikes.	015 622 8000	n/a
Network Technician	Recovery of the communication networks.	015 622 8045	083 517 0899
IT Officer	Fetch required tapes and restore of all backups and backups of both the primary and alternative site data.	015 622 8045	079 372 2357
Communication	Responsible for all communication that is set to the Incident Management team.	015 622 8089	082 563 0091

The BCM/ITRT is responsible for:

- a) Ensuring that all the facilities, people and other resources that they require to mount effective response, continuity and recovery operations;
- b) Coordinate the allocation of resources
- c) Manage communication with IMT;
- d) DR Briefing

6.2 Recovery phase

This phase deals with, and provides information that will be required to restore the system to a state of normality after a disaster has struck. It includes:

- a) DR briefing and analysis of damage from the assessment
- b) Backup procedures
- c) Recovery procedures

- b) The damage assessment report is analysed;
- c) The recovery team members review the status of their respective areas of responsibility;
- d) *The DR Coordinator reviews the overall plan with the team members;*
- e) Any adjustment to the Disaster Recovery Plan to accommodate special circumstances are decided upon; and
- f) Ongoing meetings for the duration of the recovery phase are scheduled.

6.2.2 Invoke recovery procedures

6.2.2.1 Backup procedures

The following roles and responsibilities will apply for this policy and procedures.

Table 9: Backup personnel contact details

Name	Designation	Work Tel	Cell number
Malesa MM	IT Officer (Administrator)	015 622 8045	079 372 2357
Sakala K.S	Offsite Backup Personnel	086 123 4862	082 962 4284

6.2.2 Request and delivery of required backup tapes

Backup Administrator needs to collect the required backup tapes. The off-site personnel on the off-site storage side will identify the correct full backup tape as well as the incremental backup tape. The backup Administrator is requested as a matter of urgency to transport the tape from off-site storage centre to DR Site data centre. The delivery time of the backup tape under normal circumstances is approximately 90 minutes due to the distance between the two data centres being 3 km.

6.2.2.3 Technical recovery procedures

The RACI below needs to populate with allowed and actual time to recover each of the steps listed.

Table 10: recovery procedure under annex C

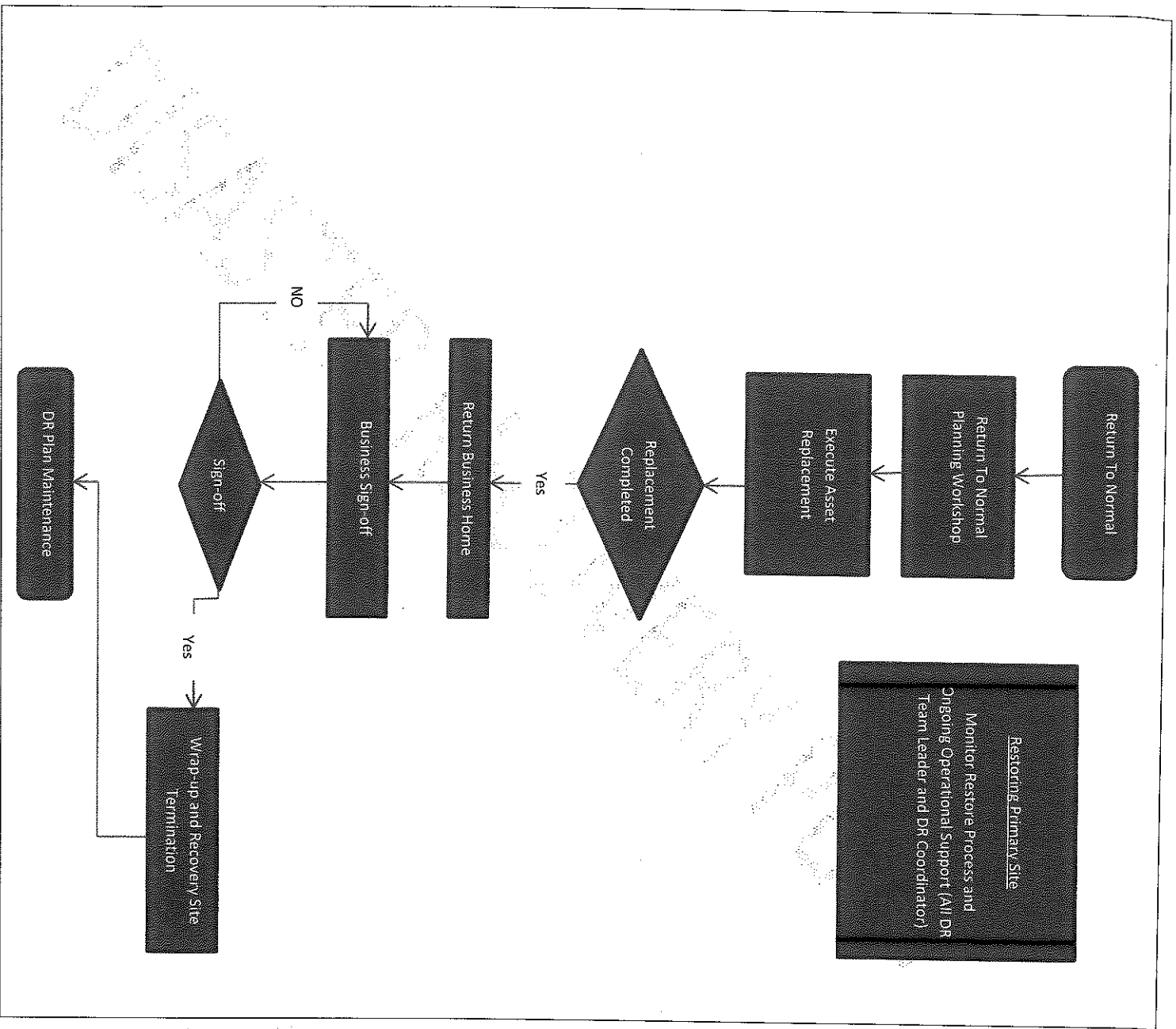
System/ Function recovery	Action Area	Accountable	Allowed Time	Actual time	Page No	Section no
Active Directory	Install the active Directory					
	Configure Active Directory					
	Restore Active Directory					
	Test active Directory					

VIP	Install the VIP Server	Configure the VIP Server							
	Restored VIP Data from Backup tapes								
Cash Focus	Install the Cash Focus server								
	Configure the Cash focus server								
Vehicle registration									

6.3 Return to normal phase

This phase deals with, and provides,

- a) Information that will be required for the replacement of daaged assets which may have resulted from the disaster;
- b) The transfer of recovered systems from the standby recovery facility to the home site computer centre; and
- c) Maintenance and testing of the plan



6.3.1 Information requirements

6.3.1.1 Return to normal checklist

Once the building abd associated infrastructure are restored at the primary datacenter (on original or new site) and staff are ready, then a planned transfer of the workload from backup *site to primary site can begin. This is essentially a reversal of the procedures by which transfer to the DR site was attained.*

These steps will take the form:

Steps	Yes	Remarks
Confirm primary site operational		
Confirm the integrity of Primary site systems		
Backup site will be informed and begin local preparations for transfer of data		
Transfer of staff from Backup site		
Make any local configuration changes required to accommodate third party connectivity		
Ensure connectivity to primary system		
Individual site managers will be informed		
Help desk will be formally informed that the primary site is operational again		
Other third parties will be informed (e.g. IT Master)		
The Disaster Recovery Plan will be reviewed in conjunction with the Disaster Recovery Coordinator and updated with any lessons learned from the live Disaster Recovery		
Communicate changes to all interested parties, including third parties		
The disaster recovery team will be de-briefed and disbanded		

6.4 Damage assessment and salvage team

The ITR Team is responsible for the assessing the damage to the LAN and LAN facilities and reporting the level of damage to the Incident Management Team. They must perform the assessment as quickly as possible following the disaster. The team is also responsible for overseeing the salvage operations required to clean up and repair the data center and for reestablishing the data center in the reconstituted or new site.

Table 11: Damage assessment and salvage team responsibilities

Post-disaster responsibilities	
Determine damage and accessibility to:	
<ul style="list-style-type: none"> The building, The data centre, The municipality's offices, Environmental controls, Computer room contents, and Office contents. (From the Damage Assessment Checklist) 	
Assess the extent of damage to the municipality's LAN and data center.	
Assess the need for physical security. (e.g. security guards)	

Estimate recovery time based upon the damage assessment. (From the Damage Assessment Checklist)
Identify salvageable hardware and communication equipment.
Apprise the Management Team on the extent of damages, estimated recovery time, required physical security, and salvageable or repairable equipment.
Maintain salvageable hardware and equipment log.
Coordinate with vendors and supplier in restoring, repairing, or replacing salvageable hardware and equipment
Coordinate transportation of salvaged equipment to recover site, if necessary.
Provide support in cleaning up the data center following the disaster.

6.5 Physical security team

The Physical Security Team provides personnel identification and access limitations to the building and floors and acts as a liaison to emergency personnel. This is crucial during the time of a disaster because of the uncommonly large number of vendors, contractors, and other visitors requiring access to the building and floors.

Table 12: Physical security team responsibilities

Post-disaster responsibilities
Assess damage to entries to the disaster site.
Act as a liaison to emergency personnel, such as fire and police departments.
Cordon off the data center to restrict unauthorized access.
Coordinate with Facility or Building Management for authorized personnel access.
Provide security guards, as required.
Schedule security for transportation of files, reports, and equipment.
Provide assistance in any official or insurance investigation of the damage site.

Table 13: Communication team responsibilities

Post-disaster responsibilities
Coordinate with the ITR Team on assessing communications equipment needs.
Coordinate with the IT Technical to determine communication and network equipment needs.
Coordinate with municipalities Management Team to procure needed communication equipment.
Coordinate with municipalities Management Team to procure needed cabling.
Retrieve the communications configuration from the off-site storage unit.
Plan, coordinate, and install communication equipment at the alternative site.
Plan, coordinate, and install network cabling at the alternative site.

Table 14: Hardware installation team responsibilities

Post-disaster responsibilities
Verify the pending occupancy requirements with the alternative site.
Inspect the alternative site for physical space requirements.

	Notify the recovery site of impending occupancy.
	Interface with the IT Technical about the space configuration of the alternative site.
	Coordinate the transportation of salvageable equipment to the alternative site.
	Plan the hardware installation at the alternate site.
	Install hardware at the alternative site.
	Plan, transport, and install hardware at the permanent site, when available.
	Set up and operate a sign-in, sign-out procedure for all equipment sent to and from the alternative site.

Table 15: IT recovery team responsibilities

Post-disaster responsibilities	
	Assist the IT Technical Team as required.
	Schedule a new pickup location with the off-site storage unit.
	Arrange for the delivery of off-site storage containers.
	Receive the delivery of off-site storage containers.
	Ensure backup tapes are sent to the off-site facility for storage.
	Return backup medium in storage containers to the off-site storage unit.
	Set up and operate a sign-in, sign-out procedure for all IT materials sent to and from the alternative site.
	Check the alternative site's floor configuration to assist the Hardware, Software, and Communication Teams with installation plans.
	Monitor the security of the alternative site and the LAN network.
	Coordinate the transfer of equipment, furniture, and personnel to the alternative site.

Table 16: IT technical team responsibilities

Post-disaster responsibilities	
	Restore operating systems, applications, and network software from backup medium.
	Initialize new tapes as needed in the recovery process.
	Conduct backups at the off-site location.
	Test and verify operating systems, applications, and network software.
	Modify the LAN configuration to meet the alternative site configuration.

6.5.1 Asset replacement procedures

The following checklist should be used to speed up the asset replacement process:

- a) Get detailed information on impact of disaster;
- b) Determine specifications of hardware required based on the relevant asset register (Annex A – asset register);
- c) Determine versions and specifications of software required based on the information provided by relevant role player;
- d) Determine supplier that will be respond fastest;
- e) Get delivery date from supplier;
- f) Get estimated costs for replacement;

- g) Complete the asset purchase documentation, and get management approval of the order

In the case where an asset is damaged the following RACI needs to be populated. This will identify time delays when replacing hardware and/or software and identify time impact on RTO.

Table 17: Damage assessment checklist

Impacted Asset	Impact description	Hardware/Software Specifications	Time of Impact	Approving manager	Delivery date	Time after asset fixed	Time elapsed

6.5.1.1 Preferred suppliers

This is done according to municipal procurement policy and preferred supplier.

Supplier	Commodity/Products	Telephone number	Alternative number

The contract order number should be quoted when placing an order to speed up the ordering process.

- 6.5.2 Disaster recovery plan maintenance
- 6.5.2.1 Plan maintenance checklist

The following list should be used as a guideline/reminder to maintain important elements of the plan. As a minimum requirement, the plan should be validated every 12 months.

Plan Element	Responsible person/Team	Plan validation completed (y/n)
Maintaining the strategy, plans and procedures	DR coordinator	ITR Team
Ensuring education and awareness of disaster recovery is given sufficient prominence.	DR coordinator	ITR Team
Review of the plan and risk (with their associated reduction measures), testing of the plans, controlling changes to the strategy and the plans so these are maintained to be consistent with	DR coordinator	ITR Team

each other.		
Training people to produce the strategy and plans as well as to undertake the actions embodied within the plans.	DR coordinator	ITR Team
Assurance of the quality and applicability of the plans. In this context quality refers to adaptability, completeness, data quality, efficiency, friendliness/usability, maintainability, portability, reliability, resilience, security, testability and timeliness.	DR coordinator	ITR Team

6.5.2.2 Plan maintenance schedule

The DRP must be kept up to date to reflect changes in the business. The following schedule should be adhered to:

Type of change that will influence the contents of the plan	Responsible person/team	Plan update complete (y/n)
Additions, deletions, or upgrades to hardware platforms.	DR Coordinator and Technical Administrator	
Additions, deletions, or upgrades to system software.	DR Coordinator and Technical Administrator	
Changes to system configuration	DR Coordinator and Technical Administrator	
Changes to applications software affected by the plan	DR Coordinator and Technical Administrator	
Changes that affects the availability of the Alternative DR	DR Coordinator and Technical Administrator	
Changes to contact list (including vendors/suppliers)	All parties involved	

6.5.3 Disaster recovery plan testing

Individual elements of each DRP need to be tested (or practiced or rehearsed). Final sign-off of a particular plan or element of a plan depends on when testing can be carried out. Guidelines on testing of the plan include:

- a) Testing of the plan could be in the form of a 'desk check' or detailed technical testing.
- b) An initial technical test can usually be done without the need to involve the business, such as acceptance of a new IT system. However, for subsequent tests it is prudent to get the business to be involved to 'prove' the capability and to aid mutual understanding of the activities and resources needed to achieve the common goal of business recovery.

- c) Tests may be announced or unannounced; however, in the latter case it is necessary to ensure that senior Management approval is obtained in advance otherwise it may be *difficult to achieve commitment.*

6.5.3.1 Issues to consider when planning for a test

Tests are likely to disrupt the business. When testing DRPs, it is prudent to consider:

Issues	Comments
Is it possible to time this testing to cause least disruption to your business functions or less upset to your customer?	
How much will the test cost? – is this appropriate for the additional confidence gained over other forms of testing, including a desk check?	
How can staff be trained to cope with the situation if they do not experience it in rehearsal – mode?	
Once the DRP is in operation – how will you return to normal business operations? – are there specific issues here that warrant testing in their own right.	

6.5.3.2 Fetakgomo municipality's testing procedures

Customer logs a call at helpdesk and requests to "initiate the disaster recovery plan".

(Note: Please confirm that the call is routed to ITR Team)

Helpdesk logs call and immediately notifies the operations team and supply the request reference number.

ITR team assesses the situation and determines whether they are able to recover system within one hour of the call being logged or a problem being detected. (In a test situation the answer is NO).

ITR team will invoke disaster recovery plan on their system and follow the instructions.

The test coordinator should;

- a) Note whether the operations officer uses the "quick guideline" option to get acquainted to the system (please explain this!)
- b) Refer to the strategy option to get an idea of the process;
- c) Start recovery by beginning at the top of the flowchart;
- d) Notify the relevant staff as specified;
- e) Note any changes necessary to recover effectively; and
- f) Record time it takes to recover system from the movement the call was logged

Once the system is working in backup mode users must ensure integrity and availability of data.

Once they are satisfied, they should contact the IRT team staff to notify that they are satisfied with the test.

ITR Team staff must then initiate the normalization process and verify that all system is available.

DR Coordinator to setup post test meeting to discuss any issue that need attention. All parties who were involved in the pre-test meeting need to identify all the issues, which came up during the test, and such issues need to be resolved as a matter of urgency.

7 Server environments for Fetakgomo municipality.

Server name: beta
IP address: 10.55.48.119
Make: HP
Operating system: Windows server 2008 R2 Standard
Applications and windows server components installed on this server
Attix5Pro
Pastel Evolution
Microsoft SQL server 2008
System Endpoint Protection

Server name: Feta-mail
IP address: 10.55.48.120
Make: HP
Operating System: Windows server 2008 R2 Standard
Applications and windows server components installed on this server
Domain controller
Internet Information Server
Microsoft Exchange 20010
Attix5Pro SE
Symantec Endpoint Protection

Server name: Proxy
IP address: 10.55.48.126
Make: Fujitsu Siemens
Operating System: Linux
Applications and windows server components installed on this server
Squid Proxy server for internet access to users

Annex A.

Acronyms

BCMT	Business Continuity Management Team
BA	Bar Coded Asset Audit
BCM	Business Continuity Management
BU	Business Unit
CMT	Crisis Management Team
CFO	Chief Financial Officer
DRP	Disaster Recovery Plan
DNS	Domain Name Service
DR	Disaster recovery
HR	Human Resource
ICT	Information and Communication Technology
ITR	Information technology Recovery
IMT	Incident Management Team
IP	Internet Protocol
IDP	Integrated Development Programme
IT	Information Technology
ITRT	Information Technology Recovery Team
ISP	Internet Service Provider
KM	Kilometer
LED	Local Economic Development
LOB	Line of Business
LAN	Local Area Network
NIC	Network Interface Card
PO	Post Office or Purchase Order
PDF	Portable Document Format
RAID5	Redundant Array of Independent Disk
RACI	Responsibility Accountability, Consult and Inform
RTO	Recovery Time Objectives
SOL	Structure Query Level
SLA	Service Level Agreement
SITA	State Information Technology Agency
SP2	Service Pack 2
WAN	Wide Area Network

Annex B. Insurance

Table 18: Insurance cover held by organization

Name of policy	Type of cover	Period of Cover	Amount of cover	Person responsible for maintaining cover	Next renewal date
Municipal Building, furniture and any other property owned by the municipality	Comprehensive cover with Alexander Forbes	Financial year	R87 0500 000.00	Chief Financial Officer and Municipal Manager	30 June 2015

Annex C. Fetakgomo Municipality – asset

Table 19: Hardware list and configuration in the production environment

Server name:	
Operational description :	Exchange server
Type	HP ProLiant ML350
Processors	Intel (R) Xeon (R) CPU
Memory	4 GB
Drive Capacity	545 GB
IP - Configuration	
IP Address	10.55.48.120
Default Gateway	10.55.48.1
Subnet Mask	255.255.255.0
Primary DNS	10.55.48.102
Secondary DNS	10.55.48.102
Other	
Operating System	Microsoft Windows Server 2008
Service Pack	2
Product keys	
Applications	Exchange Server 2010
Version or updates	
System settings	
Supplier	
Contact details	
Warranty	
Additional warranties	
Server name:	
Operational description:	Domain Control
Type	HP ProLiant DL 380 G7
Processors	Intel (R) Xeon (R) CPU
Memory	12.0 GB
Drive capacity	546 GB
IP-Configuration	

IP Address	10.55.48.102
Default Gateway	10.55.48.1
Subnet Mask	255.255.255.0
Primary DNS	10.55.48.102
Secondary DNS	10.55.48.102
Other	
Operating system	Microsoft Windows Server 2008
Service packs	1
Product keys	
Applications	
Version or updates	
System settings	
Supplier	
Contact details	
Warranty	
Additional Warranties	

Server name:	
Operational description: Application server	
Type	IBM
Processors	2.3 GH
Memory	8 GB
Drive capacity	300 GB
IP-Configuration	
IP Address	10.55.48.122
Default Gateway	10.55.48.1
Subnet Mask	255.255.255.0
Primary DNS	10.55.48.102
Secondary DNS	10.55.48.102
Other	
Operating system	Munsoft
Service Packs	
Product keys	
Applications	
Version or Updates	
System Settings	

	completion time/date
1. Assess damage (see form attached)	
On-site survey of main structures including supports, walls and roof	
Safety issues	
Access problems	
Evaluate re-usability	
Identify further inspections required	
Advise insurance company	
Advise ITRT leader	
2. Assess non-structural damage	
On-site survey of all non-structural facilities	
Determine damage to power, lighting, heating, cooling and ventilation.	
Determine damage to internal partitioning	
Determine damage to doors, windows and floors	
Determine damage to decoration	
Determine damage to fixtures and fittings	
Determine damage to furniture	
Evaluate recovery period prior to re-occupation	
Advise ITRT leader	
3. Power, lighting, heating, cooling and ventilation	
Prepare detailed list of damage	
Assess recoverability of each damage component	
Prepare preliminary specification of repair work or replacement	
Identify availability of suitable vendors	
Determine estimated costs	
Instruct vendors	
Monitor progress	
Advise ITRT leader	
4. Internal partitioning	
Prepare detailed list of damage	
Assess recoverability of each damage component	
Prepare preliminary specification of repair work or replacement	
Identify availability of suitable vendors	
Determine estimated costs	
Instruct vendors	
Monitor progress	

Advise ITRT leader		
5. Doors, Windows and floors		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
6. Decoration		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
7. Fixtures and fittings		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
8. Furniture		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		

Ensure suitable safety levels		
Advise ITRT leader		
2. Arrange repair		
Check to see if vendor maintenance support is available		
Have damage assessed by telecommunications maintenance/repair engineer		
Obtain estimates for repairs, for cost and period of repair		
Notify insurance company		
Instruct telecommunications vendors/maintenance firm to effect repairs		
Maintain inventory of equipment sent for repairs		
Monitors that equipment is repaired on time and test on return		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure equipment specification is still suitable for organization's purposes		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise ITRT leader		

Complete the roles and responsibilities of individual employees on the restoring communications systems form.

D.4. Systems (hardware and software)

Table 24: Procedure for recovering hardware

Activities	Resources required	Estimated completion time/date
1. Access physical damage (see form attached)		
On-site inspection to identify hardware affected by emergency		
Arrange temporary power if necessary		
Ensure area around electrical equipment is dry and clear		
Test each item of hardware		
Prepare a record of all hardware damaged or not working		
Ensure suitable safety levels		
Advise ITRT leader		

2. Arrange repair to equipment		
<i>Check to see if vendor maintenance support is available</i>		
Have damage assessed by IT hardware maintenance/repair engineer		
Obtain estimates for repairs, for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to effect repairs		
Maintain inventory of hardware sent for repair		
Monitor that hardware is repaired on time and test on return		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure hardware specification is still suitable for organisation's purpose		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise ITRT leader		

Completed by	Name	Date
Approved by	Name	Date

Table 25: Procedure for recovering networks

Activities	Resources required	Estimated completion time/date
1. Assess damage (see form attached)		
On-site inspection to identify LAN and WAN network servers affected by emergency		
Arrange temporary power if necessary		
Ensure that the area around electrical equipment is dry and clear		
Test each LAN and WAN network server		
Prepare a record of all network components damaged or not working		
Ensure suitable safety levels		
Assess damage to network software through stringent test		
Assess damage to hubs, modems and routers		
Assess damage to ISP links and website		
Advise ITRT leader		

2. Arrange repair		
<i>Check to see if vendor maintenance support is available</i>		
Have damage assessed by IT networks maintenance/repair engineer		
Identify backup and recovery network tapes		
Obtain estimates for repairs for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to effect repairs		
Maintain inventory of network items to be repaired		
Monitor that network items are repaired on time and tested		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure network specification is still suitable for organisation's purpose		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders for replacing equipment and software		
Advise ITRT leader		

Complete roles and responsibilities of individual employees on the recovery of IT networks form.

Table 26: Procedure for recovering operating systems

Activities	Resources required	Estimated completion time/date
1. Assess damage (see attached form)		
On-site inspection to identify operating systems affected by emergency		
Arrange temporary power if necessary		
Ensure area around electrical equipment is dry and clear		
Test each operating systems		
Prepare a record of all operating systems damaged or not working		
Ensure suitable safety levels		
Advise ITRT leader		
2. Arrange repair		

Check to see if vendor maintenance support is available		
Have damage assessed by IT operating system maintenance/repair engineer		
Obtain estimates for repairs, for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to affect repairs		
Maintain inventory of operating systems to be repaired		
Monitor that operating systems are repaired on time and tested		
Advise IT/RT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure operating system specification is still suitable for organisation's purposes		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise IT/RT leader		

Complete roles and responsibilities of individual employees on the recovery of IT operating systems form.

Table 27: Procedure for recovering application systems

Activities	Resources required	Estimated completion time/date
1. Assess damage (see attached form)		
On-site inspection to identify application systems affected by emergency		
Arrange temporary power if necessary		
Ensure area around electrical equipment is dry and clear		
Test each application systems		
Prepare a record of all application systems obviously damaged or not working		
Ensure suitable safety levels		
Advise IT/RT leader		
2. Arrange repair		
Check to see if vendor maintenance support is available		
Have damage assessed by IT application systems maintenance/repair engineer		

Obtain estimates for repairs for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to affect repairs		
Maintain inventory of application systems to be repaired		
Monitor that application systems are repaired on time and tested		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure application system specification is still suitable for organisation's purposes		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise ITRT leader		

Complete roles and responsibilities of individual employees on the recovery of IT application systems form.

Completed by	Name	Date
Approved by	Name	Date

D.5. Production equipment

Table 28: Procedure for recovering production equipment

Activities	Resources required	Estimated completion time/date
1. Assess damage (see attached form)		
On-site inspection to identify areas affected by emergency		
Arrange temporary power if necessary		
Ensure area around electrical equipment is dry and clear		
Test each item of production equipment		
Prepare a record of all production equipment obviously damaged or not working		
Ensure suitable safety levels		
Advise ITRT leader		
2. Arrange repair		
Check to see if vendor maintenance support is available		

Have damage assessed by maintenance/repair engineer		
Obtain estimates for repairs, for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to affect repairs		
Maintain inventory of production equipment sent for repairs		
Monitor that production equipment is repaired on time and test on return		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure production equipment specification is still suitable for organisation's purposes		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise ITRT leader		

Completed by	Name	Date
Approved by	Name	Date

Other equipment

Table 29: Procedure for restoring other equipment

Activities	Resources required	Estimated completion time/date
1. Assess damage (see attached form)		
On-site inspection to review areas affected by emergency		
Arrange temporary power if necessary		
Ensure area around electrical equipment is dry and clear		
Test each item of equipment		
Prepare a record of all equipment obviously damaged or not working		
Ensure suitable safety levels		
Advise ITRT leader		
2. Arrange repair		
Check to see if vendor maintenance support is available		
Have damage assessed by maintenance/repair		

engineer		
Obtain estimates for repairs for cost and period of repair		
Notify insurance company		
Instruct vendors/maintenance firm to affect repairs		
Maintain inventory of equipment sent for repairs		
Monitor that equipment is repaired on time and test on return		
Advise ITRT leader		
3. Arrange replacements		
Prepare list of non-repairable equipment		
Ensure equipment specification is still suitable for organisation's purposes		
Obtain vendor quotes or replacements		
Notify insurance company		
Issue purchase orders		
Advise ITRT leader		

Complete the roles and responsibilities of individual employees on the restoring other equipment form.

Completed by	Name	Date
Approved by	Name	Date

Table 30: Procedure for recovering server room facilities

Activities	Resources required	Estimated completion time/date
1. Assess damage (see attached form)		
On-site survey of main structures including supports, walls and roof		
Safety issues		
Access problems		
Evaluate re-usability		
Identify further inspections required		
Advise insurance company		
Advise ITRT leader		
2. Assess non-structural damage		
On-site survey of all non-structural facilities		
Determine damage to power, lighting, heating, cooling and ventilation.		
Determine damage to internal partitioning		
Determine damage to doors, windows and floors		

Determine damage to decoration		
Determine damage to fixtures and fittings		
Determine damage to furniture		
Evaluate recovery period prior to re-occupation		
Advise ITRT leader		
3. Power, lighting, heating, cooling and ventilation		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
4. Internal partitioning		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
5. Doors, Windows and floors		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
6. Decoration		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair		

work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
7. Fixtures and fittings		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
8. Furniture		
Prepare detailed list of damage		
Assess recoverability of each damage component		
Prepare preliminary specification of repair work or replacement		
Identify availability of suitable vendors		
Determine estimated costs		
Instruct vendors		
Monitor progress		
Advise ITRT leader		
9. Identify need for temporary locations		
Assess space required		
Assess period for temporary relocation		
Identify any special requirements		
Contact real estate broker		
Inspect possible temporary sites		
Decide on suitable site		
Prepare site for temporary occupation		
Issue purchase orders for replacing equipment/furniture and other damage items		
10. Relocation to temporary premises		
Notify all affected management and staff of temporary location		
Advise possible period at temporary location		
Notify customers and suppliers of the		

change of address/contact details		
Arrange to transport undamaged items to temporary premises		
11. Prepare to return to original premises		
Notify all affected management and staff of relocation date		
Notify customers and suppliers of relocation		
Arrange transport of furniture and equipment to original premises		

Complete roles and responsibilities of individual employees on the recovery of server room facilities form.

Completed by	Name	Date
Approved by	Name	date

C13/2014.

30/07/2014.

Council Resolution No.

Date



30/07/2014.

Mampheko K.K

Date

The Speaker