DISASTER RECOVERY PLAN
FOR MKHAMBATHINI
MUNICIPALITY
Document Approval

This document has been endorsed and approved by Council.

____________________________________________________
Chairperson of the Council

________________________
Date

Document Version Control

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Authorized by</th>
<th>Distribution</th>
</tr>
</thead>
</table>

Document Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date changed</th>
<th>Author</th>
<th>Reason for Change</th>
</tr>
</thead>
</table>
Contents

1. Introduction..................................................................................................................3
2. Objective of the Plan...................................................................................................4
3. Scope of the Plan.........................................................................................................5
4. Responsibility for Plan Management and Administration.........................................6
5. Plan for IT disaster recovery.......................................................................................6
  a. Plan for business continuity......................................................................................6
  b. Disaster recovery Plan..............................................................................................7
  c. Disaster notification..................................................................................................7
6. Disaster Notification and Plan Activation....................................................................7
  a. Initiation procedure indicating who should declare a disaster.................................7
  b. Damage Assessment................................................................................................8
  c. Determination of strategy to be followed .................................................................9
  d. Activation of recovery site ......................................................................................9
  e. Movement of backup materials .............................................................................10
  f. Notification of staff involved...................................................................................10
  g. Ordering of new equipment....................................................................................11
  h. Contact details........................................................................................................11
  i. Responsibilities of each party with regard to disaster recovery............................11
7. System and business recovery procedure....................................................................12
  7.1 Business Unit Recover...........................................................................................12
  7.2 System Recovery...................................................................................................13
    7.1.2 Install and test equipment................................................................................13
    7.2.2 Recover and test operating system and applications.......................................13
    7.2.3 Update to point of disaster.............................................................................13
    7.2.4 Process backlog transactions..........................................................................14
    7.2.5 Configure and test network connections (local area network and remote access) .........................................................................................................................14
    7.2.6 Establishment communication links...............................................................14
    7.2.7 Establish controls to ensure that security is maintained..................................14
8. Primary site procedure................................................................................................14
  a. establishment site security......................................................................................14
  b. perform a detailed damage assessment...................................................................15
  c. obtain contractor and vendor estimates for repairs or replacements ...................15
d. compile a salvage/refurbish plan

9. Monitor progress

10. Re-establishment of normal operations
    a. order replacement furniture and equipment
    b. install and test equipment
    c. back up prior to move
    d. recover and test operating system and applications
    e. control and monitor completeness and accuracy of migration
    f. Process backlog
    g. Configure and test network
    h. Return to normal processing

11. Post recovery review

12. Plan maintenance and testing

13. Disaster Preparedness
Introduction:

A disaster is an incident or natural event that causes great damage and loss to life. An ICT Disaster can be defined as any natural or unnatural act or incident which results in ICT system or server downtime.

The following events may be classified as IT disasters for Mkhambathini Municipality.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power failure</td>
<td>Loss of power to the municipality due to load shedding, power supply shortage, cable theft, generator failure etc.</td>
</tr>
<tr>
<td>Theft</td>
<td>Theft of critical computer equipment which results in total services shut down and or non availability &gt; this will include theft of a files server, router, Telkom line, core switches etc.</td>
</tr>
<tr>
<td>Vandalism</td>
<td>Vandalism of IT infrastructure by aggrieved Staff, Public and or any other person wishing to disrupt Municipal processes, these will include cutting of fibre cables, destroying servers or any other equipment on the network which is required to access various services offered by IT</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Deliberate sabotage of computer or network equipment for the purpose of rippling Municipal operations, This includes deletion data and of data bases or making changes thereof.</td>
</tr>
<tr>
<td>Fire</td>
<td>Loss of computer or network equipment through fire damage</td>
</tr>
<tr>
<td>Water damage</td>
<td>Loss of computer or network equipment through water damage which can be caused by rain, floods water overflows from broken pipes or wind etc.</td>
</tr>
<tr>
<td>Wind</td>
<td>Damage to IT equipment or services due to wind etc.</td>
</tr>
<tr>
<td>Hardware failure</td>
<td>System or services failure hardware faults on server and core network equipment.</td>
</tr>
<tr>
<td>Accident</td>
<td>Loss of damage to IT equipment and services due to accidents.</td>
</tr>
<tr>
<td>Negligent</td>
<td>System and service down time due to negligent actions by users, technicians or Managements failure to take decisions on critical IT requests.</td>
</tr>
</tbody>
</table>

2. Objectives of the Plan

ICT has become an integral part of the day operations of the Municipality which has made it to be one of the key resources which are required to assist the Municipality in achieving its service delivery mandates.

The Municipality depends 100% on ICT for the following:

- Communicating with the outside world for funding, compliance, information exchange, linking to other Government sectors etc.
- Payment of Councilors, Employees, Suppliers, and other creditors for services rendered.
- Research and access to online information for decision making and service delivery improvements.
- Formulating Council documents namely resolutions, letters, contracts etc.
- Emailing documents
- Financial Management and Control
- Payroll Management
- Biling for Municipal Services
- Reporting to Provincial and National Treasury

The Objective of this plan is to ensure that the Municipality an recovery the above services in the event of the disasters listed in 1 above. The plan also identifies the risks and precautions to be taken to minimize loss in case of a Disaster.

3. Scope of the plan

The scope of this plan is limited to defining the rules and procedures to be followed in restoring the critical ICT services from a disaster. The plan also identifies the precautions that may be taken by the Municipality to ensure that they recover from any disaster with minimum loss.

This plan will cover the following domains:

- Disaster notifications plan and activation
- Systems and business recovery procedure
- Primary site procedures
- Re establishing processes
- Recover and test system
- Post recovery steps
- Plan maintenance

4. Responsibility for Plan Management and Administration

It is necessary that this plan is regularly reviewed and updated. The Disaster Recovery Task Team should meet annually to review the plan, to organize and review the outcomes of testing and modify the plan where appropriate. The task team should report to the Director Corporate Services. Other specialist should be co-opted on to the task team as necessary.

The plan should be stored in a fireproof safe located at the Office of the Municipal manager a copy of the plan must be stored on the designated disaster recovery Site, there should also be a copy in the server room.

Mkhambathini has established an ICT steering committee therefore all requests to review the plan must be submitted to via the committee for approval.

The document shall be controlled by updating the history on the first page and the document version.

5. Plan for IT disaster recovery

a. Plan for business continuity
IT systems are constantly threatened by downtime and loss of data. The threats are real and come from many directions. Not all of them can be avoided, the most important questions is the Municipality ready to deal with any application downtime and how fast can t go back online in as of serious system failures.

The Municipality needs to develop a practiced and logistic plan on how it will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption.

There are various methods that can be applied to ensure business continuity can be implemented with minimum cost to the Municipality.

With the above in mind the Municipality needs to have a business continuity strategy which can address minor incidents which can manifest themselves into disasters. Some examples which can be used to explain this are:

- What plan is there to back up the switchboard if he/she is off sick?
- Who will run payroll if the pay roll officer is off sick on the day payroll run is due?
- What plan is there to pay salaries and services providers if internet is down?
- Who will take over from the project managers should they decide to resign or leave the Municipality in the middle of the project.
- Are there manual systems in place to ensure business continues despite minor down times?

b. Disaster recovery plan

This disaster recovery plan will outline the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure to the Municipality after natural or human induced disaster.

The disaster recovery plan will not work if the Municipality is not prepared for a disaster, to do so the Municipality needs to have the following in place.

- Backups must be done daily.
- There must be a remote backup storage.
- The disaster recovery site must be established and setup with basic services.
- The municipality must have insurance policies, SLA’s and warranties in place with credible service providers and vendors.

- This plan must be updated monthly and tested quarterly.
- Everyone who will take part in the recovery process must be trained on this plan their roles must be clearly outlined.

c. Disaster notification

The purpose of this section of the DRP is to enable the ICT division and the relevant stakeholders to notify all users quickly, efficiently and effectively in the event of a disaster. The goal is to improve response time and to quickly mobilize all resources and bring back the ICT service online in the quickest time possible.

(Notification Procedure)
1. The following notification tree is to be followed in notifying users of an IT disaster once it's been declared as such in terms of this Plan.

I. Each member of the disaster recovery team (DRT) must keep a recovery of this plan and the latest contact details of all Municipal Staff at work and at home, if you have a vehicle a copy must be kept in the car as well. The head of the DRT must ensure that there are 10 copies or more of the DRP plan stored in a fireproof safe on the disaster recovery site.

II. This plan and its content are highly confidential and should not be released to anyone without the written consent of the Municipal Manager.

III. Each of the above contact points shall have their own contact list which shall be kept in the server room and updated as and when there are changes in personnel.
6. Disaster Notification and Plan Activation

a. Initiation procedure indicating who should declare a disaster

In an unlikely instant where a disaster has occurred which is likely to affect Mkambathini ICT services and or the normal operation of the Municipality, the first priority will be to ensure the personnel on site and take measures to contain the situation including summoning emergency services.

As soon as safely possible the IT or the Incident Director should be called to appraise the Situation. The ICT Officer must confirm with the Fire Officer that is safe to enter the safe before entering. If the assessment confirms that significant damage, destruction or loss has occurred then a Disaster must be declared.

Once the ICT Officer has classified this as a Disaster Director must then be notified and informed of the extent of the damage so as to determine the required intervention and notification.

b. Damage Assessment

Conducting a damage assessment after disaster is critical as it will allow the recovery team to:

- Determine the severity and magnitude of the damage
- Quantify the equipment impacted by the disaster
- Determining whether existing resources will be sufficient to the disaster

The damage assessment must be rapid, detailed, and accurate and adhere to the following:

- It should be completed and submitted to the Incident Director within 24 hours of the event.
- The data collected will be analyzed to determine the measures to be taken in response to the disaster.
- It must determine whether the need to activate the recovery site is necessary
- Delayed in completing the assessment may result in institutional damage.

There are 4 degrees of damage

<table>
<thead>
<tr>
<th>Damage</th>
<th>Description</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destroyed</td>
<td>Damage of data or equipment beyond repairs</td>
<td>Replace all Destroyed Equipment</td>
</tr>
<tr>
<td>Major</td>
<td>Partly damage to data and or equipment</td>
<td>Replace damaged parts</td>
</tr>
<tr>
<td>Minor</td>
<td>Mild damage to data and or equipment</td>
<td>Fix faulty parts</td>
</tr>
<tr>
<td>Affected</td>
<td>Disturbance to some CT services</td>
<td>Effect backup plan</td>
</tr>
</tbody>
</table>

The assessment may be unique for each system however the following areas must be addressed in the assessment:

- Cause of the outage or interruption
- Damage to the information system or data
- Potential for additional disruption of damage
- Physical infrastructure status
- Information system inventory and functional status
- Requirement for repair or replacement
• Estimated time recover or restore.

Criteria to be the activation of the disaster recovery plan

<table>
<thead>
<tr>
<th>Information system Damage</th>
<th>Facility condition</th>
<th>System criticality</th>
<th>Anticipated disruption length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Destroyed</td>
<td>High</td>
<td>30 days or more</td>
</tr>
<tr>
<td>Partial</td>
<td>Major Damage</td>
<td>High</td>
<td>15 days</td>
</tr>
<tr>
<td>None</td>
<td>Major</td>
<td>High</td>
<td>15 days</td>
</tr>
<tr>
<td>none</td>
<td>Affected</td>
<td>High</td>
<td>10 days</td>
</tr>
</tbody>
</table>

**d. Determination of Strategy to be followed**

The determined decision statement must be determined the strategy to be followed when responding to a disaster:

<table>
<thead>
<tr>
<th>Service affected</th>
<th>State</th>
<th>Duration</th>
<th>strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet and or Email</td>
<td>Not accessible</td>
<td>3 days</td>
<td>Use backup 3G or other service</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>Hardware/damage</td>
<td>2 days</td>
<td>Log call with IBM</td>
</tr>
<tr>
<td>Any and or All</td>
<td>Loss through disaster event</td>
<td>Permanent</td>
<td>Replace and restore from backup</td>
</tr>
<tr>
<td>Pastel</td>
<td>System crash</td>
<td>1 day</td>
<td>Call Pastel to restore system and replace hardware</td>
</tr>
<tr>
<td>Fortinet firewall</td>
<td>System crash corruption</td>
<td>1 day</td>
<td>Re-installed system or replace if destroyed</td>
</tr>
<tr>
<td>Network device or cables</td>
<td>Damage</td>
<td>2 days</td>
<td>Replace</td>
</tr>
<tr>
<td>Front Peripherals</td>
<td>Hardware / software failure</td>
<td>3 day</td>
<td>Repair or replace</td>
</tr>
<tr>
<td>Data</td>
<td>Data loss and or corruption</td>
<td>1 day</td>
<td>Restore form back up</td>
</tr>
<tr>
<td>All IT Services</td>
<td>Facilities destroyed and not accessible</td>
<td>5 days</td>
<td>Activate recovery site</td>
</tr>
</tbody>
</table>

**e. Activation of Recovery Site**

Mkhambathi will designate a disaster recovery site which will be used to recover from a disaster. The following sites will be established to recovery system operations until restoration of the original site.
It must be noted that these sites will be activated in terms of this plan and each site must keep a copy of this recovery plan and contact details of every critical stakeholder.

The following table describes the sites that will be used for disaster recovery.

<table>
<thead>
<tr>
<th>Site</th>
<th>Type</th>
<th>Description</th>
<th>Setup time</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMgungundlovu District Municipality</td>
<td>Cold Site</td>
<td>Remote site with adequate space for servers etc. with telephone and Data line including electricity and Environmental controls.</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Mkhambathini Boardroom</td>
<td>Warm site</td>
<td>Partially equipped offices spaced That contain some or the entire System hardware, software and Network infrastructure. The warm Site is maintained in an operational Status ready to receive the relocated System.</td>
<td>12 Hours</td>
</tr>
<tr>
<td>Library</td>
<td>Hot site</td>
<td>Alternate server room adequately sized To support the network and system Infrastructure.</td>
<td>8 Hours</td>
</tr>
</tbody>
</table>

The above listed disaster recovery sited will be activated based on the following criteria.

- The primary must be totally un-usable
- Network services must be anticipated to be down for more than 15 days
- The primary site must be non-functional
- Use of current infrastructure must be impossible

Movement of backup materials

Mkhambathini currently uses a NAS box to backup its information, in case of a disaster the NAS box will be moved to the recovery site by the ICT Officer. The ICT Officer must ensure that the drives are securely attached and must also ensure that there is no items in the vehicle that can damage the NAS during transportation.

The municipality will enter into a service level agreement with service providers to provide offsite storage as the municipality does not have this capacity.

A register will be kept to monitor movement of the backup devices and material. Data must be backed up with password protection and or encryption to protect it from being stolen.
The backup device must be accompanied by the backup software used to back up the original data. The finance server is backed up on tape therefore the tapes must not be stored near magnetic items, direct sunlight or any other objects which could destroy them.

f. Notification of staff involved

The staff involved in the disaster recovery will be notified in terms of this plan. Each staff member must be issued a letter of indemnity in which they must agree to be part of the disaster recovery team. These staff members must be present at all times when testing this plan.

g. Ordering of new equipment

The municipalities supply chain processes can be cumbersome and may delay the recovery time when ordering replacement or new equipment for the disaster recovery. To avoid this Municipality must:

i. Ensure that all equipment and data are covered by a reputable Insurance company

ii. Enter into Service Level Agreement with an ICT service provider for the provision of ICT infrastructure services in case of disaster this must cover the following critical devices and or software:

a. Servers
b. Firewalls
c. Switches
d. Network cables
e. Printer
f. Desktops
g. Laptops
h. Data points and patch panels
i. Server cabinet
j. Routers

h. Contact Details

A database of the critical contact persons and vendors must be kept in the server room and the disaster recovery sites. The ICT Officer must update these contact details monthly to ensure that the database is up to date and current.

The contact list must be attached to this plan and copies must be kept as follows:
• Server room
• Recovery Site
• Copies issued to the members of the Recovery Team
• Stored in the safe with backup tapes

i. Responsibilities of each party with regard to disaster recovery

In order to have a full proof disaster plan Mkambathini needs to assemble the right team who will be key role players in formulating, implementing, maintaining and reviewing the computer systems disaster recovery plan.

As a minimum the team will consist of:

• The Head of Corporate Services (Incident Director)
• Chief Financial Officer
• Head of Information and Communication technology (ICT)
• ICT Service providers for each system
• Payroll administrator
• Financial system user responsible for backup
• Dually designated user for each application Technical services representative
• ICT Steering Committee

The team is headed by the Head Corporate Services who is a member of the organizations senior management team. She/he will bring a broad strategic perspective to the team, and provide a link to the major decision making forums of the organization.

The Head of ICT has a detailed knowledge of network topology hardware development, security precautions, backup systems and technical specifications.

Finance and payroll are among the most mission critical systems for Mkambathini. The system users have a detailed knowledge of these systems, their backup and recovery precautions.

Lastly the team must involve a senior representative from the Technical services. Many potential disasters could involve fires, floods etc and the first priority in these cases will be to evacuate the building safely. Additionally the disaster will most often be discovered by a member of the building or care taking staff, and the plan will have to clearly identify lines of communication so that key personnel can be informed, and the plan activated if appropriate.

The technical services representative will bring a detailed knowledge of the procedures for raising the alarm evacuation procedures, containing emergency services, building and electricity repair services.

Each team member must have a copy of the plan and copies must be placed in a secure location at each of the Municipalities buildings namely, Protection services, Technical Services and at the Head Office.

The responsibilities of the above mentioned shall be the following:
<table>
<thead>
<tr>
<th>Role Player</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Director</td>
<td>Declares the incident and run the command centre</td>
</tr>
<tr>
<td>CFO</td>
<td>Lead the Financial application disaster recovery team</td>
</tr>
<tr>
<td>Head ICT</td>
<td>Conduct an assessment and recommend the strategy to be followed in response to a disaster.</td>
</tr>
<tr>
<td>ICT Service Providers</td>
<td>Provide specialized support and advice on their applications and/or hardware.</td>
</tr>
<tr>
<td>Payroll super user</td>
<td>Restore payroll to the last backed up status</td>
</tr>
<tr>
<td>Financial system Super User</td>
<td>Restore the finance application to the last backed up status</td>
</tr>
<tr>
<td>Supply Chain Manager</td>
<td>Provide logistical support to fast track the procurement of Recovery equipment.</td>
</tr>
</tbody>
</table>

7. Systems and business unit recovery procedure:

7.1 Business Unit Recovery
The recovery of each business unit may vary as they are each unit, the following priority will be considered when recovering from a disaster:
- a. ICT division (server room and network)
- b. Finance Department
  - i. Financial Management (Debtor and Creditors)
  - ii. Supply chain
  - iii. Billing
  - iv. Payment
  - v. Payroll
- c. Office of the Municipal Manager
- d. Corporate services
- e. Technical services
- f. Planning and Development

7.2 System Recovery
Each system is and as such shall be recovered differently; the following steps will be taken when recovering the systems.

7.2.1 install and test equipment
Systems are dependent on hardware, therefore the first step will be to procure or revive the hardware required to run the system in the following order of priority:

- Servers
- Network peripherals and cables
- Desktops and Laptops
- Printers
Each of the above listed equipment will be installed and tested by the system recovery team which will consist of the ICT Technicians, system vendors and super users.

7.2.2 Recovery and test operating system and applications

Once the equipment have been installed and tested the next step will be to install the operating system and the applications, these shall be installed as follows:

- Network operating system on all server
- Microsoft Exchange(email services)
- Finance application system
- Payroll application
- Antivirus
- Firewall and proxy servers
- Finance application system
- Payroll application
- Antivirus
- Firewall and proxy servers
- Desktop operating Systems
- Desktop applications and clients

Note: Screen shots of each application configuration must be captured and attached to this plan. The ICT must update these screen shots and when there is a configuration change.

7.2.3 Update to point of disaster

The data will be restored to the last successful and available backup which was made of all the systems in the network. The recovery software media and the license keys including contact details for the support must be attached to this plan and copies must be kept in a category safe in the recovery sites.

Upon total system recovery the data and databases will be restored in the following order:

- Finance system database
- Payroll database
- User files
- Mailboxes

7.2.4 Process backlog transactions

A data capturing team will be setup to capture transaction backlogs from the manual system. Each system will have a team of data capturers. Batch files will be used to capture and upload large data into the different applications.

7.2.5 Configure and test network connections(Local Area Network, Wide Area Network and remote access)

a. The Local Area Network will be setup and configured to use both wireless and cat5e technologies. Laptops will connect via wireless and desktops will use cables including printers

b. The Wide Area Network will be connected using 3G and ADSL or whichever other connection to the internet is available. The internet service providers will be contacted to route SMTP and HTTP traffic accordingly.

7.2.6 Establish Communication links

Telecommunications and data services will be totally dependent on the availability of network signal and connection. The two critical communication links required for operations are the internet connection and the voice connection.
The disaster recovery site must be equipped with an ADSL line, PRI or ISDN line, and 3G cards to be used for recovering communication links.

7.2.7 Establish controls to ensure that security is maintained

Data protection and equipment security is of vital importance during the recovery process. The security officer will be responsible for ensuring that all equipment and data are safe and secure.

PC lock cables must be used to secure computer equipment to prevent theft at the recovery site. The server must be kept in a secure location preferable away from the users.

8. Primary site procedure:

a. Establish site security
   The recovery team must first ensure that it's safe to return to the recovery site with approval from the fire officer. Site security must then be assessed in line of the following:
   - Parameter Security
   - Logical Access
   - Physical Security
   - Environmental security

b. Perform a detailed damage assessment

A damage assessment team will be informed to assess the damage and to facilitate the replacement of equipment. This team shall be made up of IT officer, Asset Controller, Supply chain Manager, and the assessor from the insurance company. The responsibility of this team will be to conduct a detailed assessment of the damage and to compile an assessment report which must stipulate the following:
   - List of damage equipment
   - The impact of the damage
   - The cost of the equipment lost
   - Recovery
   - Future recommendations

c. Obtain contractor and vendor estimates for repair or replacements

The supply chain unit must use the damage assessment report to facilitate the procurement of the damage equipment and software. Some equipment and software may require that the supply chain division be vendor specific.

d. Compile a salvage/refurbishment plan

Every disaster is unique and as such the damage will vary, therefore it is crucial equipment, services, and data which are salvageable be repaired or refurbished taking into account E-waste and cost service.

9. Monitor progress

Progress will be monitored by the incidents director from the incident command centre. The head of each disaster team will give four hourly reports to the command centre.

10. Re-establishment of normal operations:
The process of re-establishing normal operation must be done as follows:

a. Order replacement furniture and equipment

The list of equipment to be ordered will be identified by the disaster assessment team and funding shall be sourced from the insurance if applicable else from other means possible, the last resort being from a loan or why entering into a budget contract with treasury.

b. Install and test equipment

New equipment will be installed by the ICT technician who will design the installation checklist which will also be used to test the equipment. The users will also assist in testing the equipment and will also check if all their data has been recovered.

c. Backup prior to move

Before returning to the primary site, all data which was processed at the recovery site must be backed up and tested to ensure that it can be recovered. Two copies of this data must be kept to avoid a disaster of data loss and corruption. The data must be backed up on two different backup media and technologies.

d. Recovery and Test operating system and applications

The primary site systems will be restored from the recovery site, the procedure to be followed will be as follows:

- Restore the server in the server room
- Install all network equipment in the server room
- Connect the firewall routers and switches and configure them
- Install the finance application and other mission critical systems
- Restore user files and profiles
- Restore exchange
- Re-direct SMTP and http traffic to its original IP address
- Restore users’ desktops and printers.

e. Control and monitor completeness and accuracy of migration

The following control and testing mechanisms will be used to monitor the migration process.

Email : telnet port 25 of the SMTO server, router and external mail relay server

Internet : Access an external internet site

Proxy : go to www.whatismyipaddress.com to verify proxy server

Payroll : check the last month rolled over and print a list of all employees

Finance : Setup a quality assurance team that will check and test each module

Database : Run database integrity checks

User files : Each user must check their files to ensure they have been restored
Active Directory

f. Process backlog

Each business unit must setup a team to assist with the processing of any backlog that may have occurred during the recovery process. This will include responding to email etc.

g. Configure and test network

The network will be setup and tested during the installation process however the configuration and testing will involve the following:

- Password protecting all switches, printers and other peripherals
- Firewall configuration including mail and internet filtering
- Configure WSUS
- Optimization of DNS, DHCP and replication services
- Apply the security policy recommendations
- Setup backup and test it
- Re-deploy the antivirus solution and update all machines
- Conduct the network audit.

h. Return to normal processing

The success of the disaster recovery process will be realized when the users are back to normal working operations pre-disaster. Following the above process will ensure that the users are back online.

11. Post-recovery review:

Once the site has been successful restore and all the services and users are back online the ICT Steering committee will conduct the special meeting to assess and evaluate the response time of the disaster Recovery Team.

The Disaster Recovery Team will then conduct the post disaster review and update this plan accordingly where necessary.

The ICT Officer must update all network diagrams and conduct a detailed ICT audit so that the plan is updated. The list of new equipment must be submitted to the insurance company and any changes to the IP addresses must be communicated with the ISP and the various stakeholders.

12. Plan maintenance and testing:

The IT Officer is the custodian of this plan he/she will be responsible for updating the plan and ensuring all the critical stakeholders have the latest version of the plan. Quarterly test must be conducted to analyze the effectiveness of the plan and to ensure minimum down time in case of the disaster.

13. Disaster preparedness

A critical requirement for disaster recovery is ensuring all necessary information is available to assure that hardware, software and data can be returned to a state as close to “pre-disaster” as possible. Specifically, the section addresses the backup and storage policies as well as documentation related to hardware configurations, applications, operating systems, support packages and operating procedures.
Backup/Recovery tapes are required to return systems to a state where they contain the information and data that was resident on the system shortly prior to the disaster. At Mkhambathini full backups of all servers are performed weekly.