



DISASTER RECOVERY POLICY NDLAMBE MUNICIPALITY

Contents

1. PREAMBLE
2. PURPOSE OF THE POLICY
3. DISASTER RECOVERY PLANNING PHILOSOPHY
4. DEFINITION OF A DISASTER EVENT
5. SCOPE OF THE POLICY
 - 5.1 Application
 - 5.2 Laws and Regulations
 - 5.3 Exclusion
6. OWNERSHIP
 - 6.1 Approval
 - 6.2 Review
 - 6.3 Implementation
 - 6.4 Sub Policies
7. RESPONSIBILITIES OF ROLE PLAYERS
 - 7.1 NDLAMBE MUNICIPAL COUNCIL
 - 7.2 IT Department
 - 7.3 IT Manager
 - 7.4 Third Party Vendors
8. POLICY
 - 8.1 Policy Statement
 - 8.2 Prevention and Mitigation
 - 8.3 Preparedness
 - 8.4 Disaster Recovery Planning
 - 8.5 Testing
 - 8.6 Disaster Declaration
 - 8.7 Normalization
9. POLICY BREACH
10. DISASTER RECOVERY OBJECTIVES
 - 10.1 Overall Disaster Recovery Budgetary Objectives
 - 10.2 Client / Server Objectives
 - 10.3 Network Objectives
 - 10.4 LAN Objectives
11. DEFINITIONS
12. DETAILED DISASTER RECOVERY RESPONSIBILITIES
 - 12.1 Municipality Information Technology Manager – On Behalf of Department
 - 12.2 IT Steering Committee /IT Department
 - 12.3 IT Department
 - 12.4 IT Steering Committee



PREAMBLE

Disaster Recovery Planning for which the Disaster recovery Committee / Department and IT are responsible, is the section that deals with the restore and recovery processes of the computer systems (technology that is; hardware and software) within the total concept of business continuity. The Operational Business Continuity Plan, for which the Disaster Recovery Department is responsible, is the section that deals with IT operational problems and office / workplace disaster recovery. These plans will form part of a comprehensive Business Continuity Plan.

PURPOSE OF THE POLICY

The purpose of the NDLAMBE MUNICIPALITY Disaster Recovery Policy is to set guidelines to be adhered to by all affected environments within the NDLAMBE MUNICIPALITY. It also wishes to ensure a coordinated synergy towards the designing and implementing of the Disaster Recovery Plans and solutions throughout the NDLAMBE MUNICIPALITY. Furthermore, it also serves to distinguish the difference between Operational Business Continuity and Disaster recovery Plans. In addition, the Disaster Recovery Plan (DRP) provides guidelines for the situations where the loss of one particular computer environment has a disastrous effect on another computer environment(s).

DISASTER RECOVERY PLANNING PHILOSOPHY

In terms of risk management, NDLAMBE MUNICIPALITY's disaster recovery planning philosophy is one of "prevention is better than cure". All reasonable, justifiable and cost-effective precautionary measures should be taken to prevent a disaster from occurring. Practical and effective disaster recovery plans and measures that provide for disaster scenarios with minimal losses under all circumstances, should act as insurance policies to ensure the continuation of "business as usual".

Therefore, in the event of a disaster situation, any Organizational Unit must be able to recover within the specified critical time frame, to avoid "service interruptions to consumers and municipal departments".

DEFINITION OF A DISASTER EVENT

A disaster event that adversely impacts on MDLAMBE MUNICIPALITY's or a department's ability to process, provide or utilize information essential to its day-to-day operations, or which causes an inability within NDLAMBE MUNICIPALITY or a department to provide customers with basic services. The term disaster includes a failure or loss (whole or partial) of equipment and/or software and/or systems (including human resources) from whatever cause including but not limited to equipment failure, industrial actions, illness, configuration, explosion, earthquake, tornado, flood, subsidence, collapse, riot, contamination by smoke, water, chemicals or otherwise.



SCOPE OF THE POLICY

5.1 Application

This Policy will apply to all departments and Business Units under the control of the NDLAMBE MUNICIPALITY.

5.2 Laws and regulations

Any relevant laws and regulations applicable must be taken into consideration during the development and implementation of Disaster Recovery Plans and infrastructure.

5.3 Exclusions

The following processes are excluded from this policy as they are provided for in other areas/practices:

- The responsibility of the Head of a Business Unit/Department for the planning and provision of alternate premises for staff and/or equipment. This requirement is normally covered in the Operational Business Continuity Plan but where applicable could form part of the Disaster Recovery Plan in which case the requirements must be included in the relevant sections.

OWNERSHIP

6.1 Approval

As this policy is applicable to NDLAMBE MUNICIPALITY and its departments, approval will be recommended by the IT Department and approved by the NDLAMBE Municipality's council.

6.2 Review

The policy will be reviewed annually by the IT Steering Committee and any changes will be submitted to NDLAMBE Municipal Council approval, via the IT Department.

6.3 Implementation

It will be the responsibility of the IT Steering Committee to budget for disaster recovery and to ensure that the policy is implemented. IT Steering Committee retains primary ownership for disaster recovery plans, facilities and actions. The IT Department may facilitate the drafting of a disaster recovery plan.

In respect of the corporate systems, WAN's and LAN's responsibility lies with IT Department.

6.4 Sub Policies

The following sub-policies should be included:

Data and system backup policy and storage of backup media.
Disaster recovery plan.



RESPONSIBILITIES OF ROLE PLAYERS

7.1 Ndlambe Municipality council

The role of NDLAMBE MUNICIPALITY Council is to review and approve the NDLAMBE MUNICIPALITY Disaster recovery policy and changes to it, as recommended by the IT Steering Committee in respect of the total IT infrastructure.

7.2 IT Department

The IT department will ensure that the NDLAMBE MUNICIPALITY Disaster Recovery Policy is reviewed on an annual basis.

7.3 IT Manager

The IT Manager is responsible for ensuring that the NDLAMBE MUNICIPALITY IT Disaster Recovery Policy is implemented and that its stipulations are adhered to. Secondly, to review the Disaster Recovery Policy annually. The IT Steering Committee reports to the NDLAMBE Municipal Council. IT Department is responsible for the development and maintaining of and where applicable the obtaining of approvals for the NDLAMBE MUNICIPALITY Disaster Recovery Policy, Strategies, Standards and Procedures. The IT Department is also responsible for the distribution of this policy within the NDLAMBE MUNICIPALITY and as such ensures that policy updates are effectively communicated. Where applicable, the IT Department should also monitor the implementation of this policy, standards and procedures to ensure the effective implementation hereof.

7.4 Third Party Vendors

With reference to areas where distributed processing takes place, each such third party and contractor within the NDLAMBE MUNICIPALITY will be responsible for the implementation of, and overall compliance with Disaster Recovery Policy. These responsibilities will include identifying business needs, developing and testing of the plans to meet all requirements. This responsibility should be exercised with the assistance of the responsible IT Manager and IT Steering Committee.

It is vitally important that all externally provided systems and services (such as bureaus and other IT service providers) be included in the disaster recovery plans, as these systems may fulfil a key function in the municipality. The external service provider should be included in the policy/ plans formulation and must adhere to the principals, strategies and procedures contained therein. An audit for compliance may have to be conducted to ensure that the plans and policies have been implemented.

POLICY

8.1 Policy Statement

The level of service to be provided after a disaster must be justifiable, based on the cost of resuming that level of service versus potential losses i.e. risk/reward. Should IT Steering Committee elect not to implement the disaster recovery plan/measures, such decisions should be formally documented, in acceptance of the risk, and signed-off by the IT Manager. This risk acceptance will then be referred to the Municipality Council for ratification.



The above statement must be applied to all existing technology. The policy must also be applied to any enhancements or changes to existing technology. Further to this, the policy must be applied to any new projects, developments and or the implementation of new technology applications and hardware that have a technology impact. Disaster Recovery must be fully addressed in all relevant processes within the IT function or environment.

In addition, the level of detail of the documentation must be consistent with the type of business, the complexity of the operating environment and service requirements. Plans must address the full range of resources for technology, including data processing, hardware (mainframes, midrange machines, servers, etc.) data communication links, personal computers, terminals, printers and where applicable workspace.

8.2 Prevention and Mitigation

Cost effective prevention and mitigation measures must be investigated and applied.

Critical technology and information systems should be protected against potential hazards and threats by means of appropriate, practical and cost-effective measures of detection. This will reduce losses and lessen the impact of uncontrollable events.

The primary objective of detective and preventative control measures is to identify and implement feasible control measures to detect and prevent the occurrence of manmade and natural hazards, as well as to mitigate the effects of actual occurrences. Contingent controls are required to reduce the seriousness of risks, should they materialize.

8.3 Preparedness

An Operational Business Continuity Plan that addresses office/workplace recovery/critical business functionalities should be compiled prior to a Disaster Recovery Plan. Disaster Recovery Plans form part of a comprehensive Business Continuity Plan.

Preparedness planning assures the identification of actions that need to be taken prior to and during disaster/emergency conditions. It will detail a plan of action, (who does what, when and where) and what resources are needed to respond to a given situation.

Planning must be based on a worst-case scenario and be flexible in order to cater for lesser events.

Depending on the recovery time frame required and the Disaster Recovery Strategy, extra computer, network and environmental equipment may need to be purchased, leased or hired, to enable a timely recovery.

All parties that must adhere to this policy are to ensure that accurate and thorough preparedness is planned.

8.4 Disaster Recovery Planning

All critical systems and technology platforms must have a disaster recovery plan developed and



maintained. All defined disaster recovery plans must be reviewed and updated on an annually basis.

Disaster Recovery planning will result in documented plans for each computer system. These plans, in conjunction with tests, will ensure that no recovery actions are overlooked during the recovery and normalization processes. Secondly, should the regular staff who performs the recovery not be available, backup personnel (or vendor staff), identified in the DR Plan, must be able to perform the recovery and normalization. It is the responsibility of all identified personnel to ensure that they are fully aware of all details contained in their disaster recovery plan/s.

Disaster Recovery planning addresses the period immediately following the declaration of a disaster to the point where an acceptable level of computer system functionality is obtained with priority on critical business processes.

All Disaster Recovery plans are to be reviewed and updated at least once a year.

8.5 Testing

All disaster recovery plans must be tested on a regular basis to ensure currency, practicality and accuracy. At least one successful test must be conducted annually.

Test results must be reported to management and remedial actions planned and taken on any test anomaly.

8.6 Disaster Declaration

A disaster shall be declared when any event as listed in paragraph 4 (Definition of a disaster) occurs. Or if an operational event occurs where the anticipated time required, substantially exceed/s the critical time frame as specified in the relevant disaster recovery plan, to rectify/restore unavailability of computer system/s. Responsibility for the declaration of a disaster rests with:

- Physical Disaster Conditions with major business impacts
The NDLAMBE Municipal Council is responsible for declaring a disaster that has a major business impact.
- Logical and isolated incidents within the centralized environment (Servers)
IT Manager is responsible for declaring disasters for isolated incidents within the centralized environment.
- Logical and isolated incidents within decentralized environments (LANs and Desktops)
IT Manager is responsible for declaring disasters for isolated incidents within the decentralized environments.

8.7 Normalization

Once recovery at the alternate site has been completed in accordance with the Disaster Recovery plan, a project should be initiated to plan and execute the return of technology systems to the original site or



new site. It is the responsibility of the IT Manager delegates to initiate the project as well as to ensure that the return to normal phase is included in the Business Continuity Plan.

POLICY BREACH

Any breach to the defined policy will be reported to the IT Steering Committee.

DISASTER RECOVERY OBJECTIVES

10.1 Overall Disaster recovery Budgetary Objectives

As a guideline the total of capital and operating Disaster Recovery budgets, in respect of servers, clients and LAN facilities and applications should be restricted to less than 20% of the organizational IT Operational Budget. This includes operational backup as well as disaster Recovery measures.

Although no limit is prescribed, the capital and operating budgets in respect of decentralized environments should be reasonable, justifiable and cost effective in comparison with the prevention and mitigation of potential business risks that could be attributed to a dependency on technology.

10.2 Client / Server Objectives

To reduce complexity and administration workload of Disaster Recovery Procedures to the maximum allowed by means of automation

To reduce recovery time of primary server's backup facilities in NDLAMBE MUNICIPALITY and all server related applications to 24 hours by 2013.

To limit the recovery time of centralized server backup facilities, to the actual critical time frame of the Municipality by 2013.

Where applicable, to reduces recovery time of secondary backup facilities to 18 hours by 2013.

Disaster recovery and operational recovery to become integrated to reduce cost and workload.

Disaster Recovery testing to be simplified to the point where regular testing (by means of disaster recovery systems and infrastructure) results in minimum impact to service, i.e. becomes transparent to daily service.

Perform an analysis on the impact that the loss of the server would have on LAN environments.

10.3 Network Objectives



Disaster Recovery resilience to be fully implemented within the NDLAMBE MUNICIPALITY network.

10.4 LAN Objectives

- To implement a backup strategy for all critical data hosted on production LAN's, as well as the off-site cycling thereof by 2013.
- To have effective Disaster Recovery Plans and backup facilities that have been tested, for all high priority Business Units by 2013.
- To limit the recovery time at backup facilities, to the actual critical time frames for all high priority Business Units by 2013.
- To establish a common Disaster Recovery facility for high priority Business Units and a common testing site for low, medium and high priority business units.

DEFINITIONS

11.1 Business Continuity

A plan that will enable the Business Unit to resume an acceptable level of service in an acceptable time frame, after a disaster has occurred.

11.2 Disaster Recovery

The process of reconstructing the current information technology used by a Business Unit in the event that the original system(s) is/are rendered inoperable, non-recoverable and/or inaccessible.

11.3 Operational Recovery

The process whereby problems affecting production computer systems are resolved and the computer systems reinstated at the production site. Should the estimated operational recovery time exceed the critical time frame, as stipulated in the disaster recovery plan, a disaster can be declared

11.4 Worst Case Scenario

For implementation of the organizational Disaster Recovery Policy, a worst-case scenario is regarded as the total destruction/loss of computer systems (hardware and software) for any cause what so ever.

11.5 Critical Time Frame

The critical time frame for a Business Unit is the elapsed time from the point where a disruption in computer services occurred, up to the time where critical losses will start occurring as a result of the unavailability of computer driven business processes.

11.7 Secondary Backup Facility

A secondary backup facility is an additional facility that could stand in for failure of the normal first line (primary) backup facilities.

11.8 Disaster

A disaster event that adversely impacts on NDLAMBE MUNICIPALITY's or a departments ability to process, provide or utilize information essential to its strategic day-to-day operations or which causes an inability within NDLAMBEMUNICIPALITY or a department to provide customers with basic services. The



term disaster includes a failure or loss (whole or partial) of equipment and/or software and/or systems (including human resources) from whatever cause including but not limited to equipment failure, industrial action, illness, conflagration, explosion, earthquake, tornado, flood, subsidence, collapse, riot, contamination by smoke, water, chemicals or otherwise.

DETAILED DISASTER RECOVERY RESPONSIBILITIES

Ndlambe Municipality's Information Technology Manager – On Behalf of Department

12.1 General Responsibilities

Responsible on behalf of the municipality, for the implementation of, and overall compliance with, the Disaster Recovery Policy within their area of responsibility

Ensure that disaster recovery is addressed and included in respect of all existing systems, major enhancements and new developments. To identify disaster recovery municipality's requirements, impact and risks, in accordance with the standards and support of the IT Steering Committee and the IT department. Ensure that deficiencies in terms of disaster recovery are identified and that projects to address them as initiated. Responsible for budgeting of all applicable costs, related to disaster recovery. Member of the IT Steering Committee

12.2 Specific responsibilities in respect of Distributed Environments (LAN's and Desktops)

- To take ownership and ensure that a disaster Recovery Plan exists, is maintained and provides for all the technology systems under his/her control.
- To develop a disaster recovery plan in accordance with the approved disaster Recovery policy and Standards, with the support of the IT steering Committee, IT department.
- To ensure that all critical data is backed-up on a daily basis and stored off-site.
- Scheduling, planning and reporting on testing of disaster Recovery Plans in accordance with the approved standards supplied by the IT Steering Committee.
- Ensure that all objects (systems and hardware) are tested annually.
- Ensure that all problems identified during tests are resolved and that the relevant disaster recovery plans are updated.
- Ensure that the Disaster Recovery Plan is reviewed and updated on an annual basis and if changed, supply the IT steering Committee electronically updated copy.
- Take responsibility for ensuring that the DR process is followed in the event of a disaster.
- To form, under normal circumstances and a disaster situation, a communication line between service providers and IT Department. This is to ensure that clarity exists on the understanding and interpretation of disaster recovery requirements/measures in terms of the implementation of, and overall compliance with, the disaster recovery Policy within their area of responsibility.



- To assist service providers to ensure that disaster recovery is addressed and included in respect of all existing systems.
- To assist in the identification of disaster recovery business requirements, impact and risks, in accordance with the standards and support of the IT steering committee and IT department.
- To assist and monitor that deficiencies in terms of disaster recovery are identified and projects to address them initiated.

12.3 IT Steering Committee / IT Department

General Responsibilities:

- Compilation, submission for approval, maintenance, reviewing and publicizing for implementation of all Disaster Recovery Policies, Strategies and Standards.
- To monitor that strategic disaster recovery directions (decisions) are implemented within NDLAMBE MUNICIPALITY.
- To provide a comprehensive consultation service through guidance and assistance on Disaster Recovery.
- To report on Disaster Recovery preparedness of all NDLAMBE MUNICIPALITY Business Units to immediate Management.
- To schedule, arrange and report on preparedness and project progress in the IT Steering Committee meeting.
- To compile annually Disaster Recovery status report for the Ndlambe Municipal Council.
- To take action on requests / priorities from Ndlambe Municipal Council.

12.4 IT Manager / Third Manager

- To provide a comprehensive consultation service through guidance and assistance on the compilation of individual Disaster Recovery Procedures.
- To combine individual procedures into separate complete Disaster Recovery Plans for individual Mainframe Midrange and Server platforms.
- To distribute complete Disaster Recovery Manuals, including off-site copies.
- To compile and publicize annual test schedules to include at least on test per platform.
- To compile comprehensive test plans.
- To schedule and co-ordinate tests as per test schedule.
- To schedule and chair the post-mortem meetings.
- To report on all Disaster Recovery test results.
- To ensure that all problems that are identified during Disaster Recovery tests are allocated and resolved.
- Ensure that the Disaster Recovery Plan is reviewed and updated on an annually basis
- To initiate, monitor and report on new disaster recovery projects, where required.



- To perform brief impact analyses in respect of required availability of critical applications to serve as input to SLAs (Service Level Agreements – if I use) and long terms disaster recovery strategy / objectives.
- Take responsibility for ensuring that the DR process is followed in the event of a disaster.

12.5 Distributed Environment (LAN's and Desktop)

To provide a full consultation service on the compilation of individual Disaster Recovery Plans which includes:

- A brief impact and Risk analysis.
- A User requirement in terms of applications and workstations.
- A technical Requirement to satisfy the User Requirement.
- An Executive summary and specific recommendation on disaster recovery issues.
- Compiling of a single overall document to include all requirements and recovery procedures.
- To monitor resolution of major problems / issues resulting from tests.

12.6 IT Department

- To communicate all decisions/upgrades/changes/new implementations in respect of technology that will directly impact disaster recovery capabilities and procedures to the IT Steering Committee and to update the relevant DR plans.
- Ownership of disaster recovery plans within the centralized environment lies with the IT departments responsible for the support of the system / equipment.
- To compile and maintain, in accordance with standards, and with the assistance of the IT Steering Committee, individual Disaster Recovery Procedures and supply a copy thereof to the IT steering Committee.
- To review individual Disaster Recovery Procedure directly after tests and if changed, supply the IT Steering Committee with an electronically updated copy.
- Active involvement in disaster recovery tests and the production of a detailed test log.

Actions and involvement to resolve as HIGH PRIORITY:

- Own identified issues / problems
- Issues / problems resulting from test
- Specific DR projects or actions requested by NDLAMBE Municipal Council.
- Attendance of and active involvement in tests and pre-test, post-mortem, problem solving and other general Disaster recovery meetings.

12.7 IT Steering Committee

- Review and approve changes to the Disaster Recovery Policy.
- Review and approve changes to long term disaster recovery objectives.
- Monitor and evaluate compliance to and the implementation of the Disaster Recovery Policy
- Monitor and ensure adherence to Disaster Recovery Service Level Agreements.
- Make recommendations in support of budget expenditure for the implementation of strategic decisions.
- Prioritize and make recommendations in support of disaster Recovery projects.



- Receive and discuss project progress feedback/status reporting and recommend any additional actions.
- Receive and discuss disaster recovery test reports and recommend any additional actions/strategies.
- Receive and discuss feedback from Municipality Council.
- Review new risks and actions to mitigate.
- Receive and action audit reports and informed opinions from the Auditors.

Attendees: IT Manager (Chairman)
All business Information Officers (if in existence) and I.T support service providers.
Departmental Heads
Manager Internal Audit (if in existence)

NDLAMBE MUNICIPALITY DISASTER RECOVERY PLAN

1.1 Plan introduction

NDLAMBE Municipality recognizing their operational dependency on computer system, including the Local Area Network (LAN), Database Servers, Internet, Intranet and e-Mail, and the potential loss of revenue and operational control that may occur in the event of a disaster; authorized the preparation, implementation and maintenance of a comprehensive disaster recovery plan.

The intent of a Disaster Recovery Plan is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster.

1.2 Mission and Objectives

1.2.1 The Mission

To establish defined responsibilities, actions and procedures to recover the municipalities computer, communication, and network environment in the event of an unexpected and unscheduled interruption. The plan structure to attain the following objectives:

- Recover the physical network within the Critical Time Frames, established and accepted by the user Community.
- Recover the applications within the Critical Time Frames established and accepted by the IT Steering Committee.
- Minimize the impact on the business with respect to rand losses and operational interference.

1.2.2 Objectives

As a guideline the total of capital and operating Disaster Recovery budgets, in respect of servers, clients and LAN facilities and applications should be restricted to less than 20% of the organizational IT Operational Budget. This includes operational backup as well as Disaster Recovery measures. Although no limit is prescribed, the capital and operating budget in respect of decentralized environments should be reasonable, justifiable and cost effective in comparison with the prevention and mitigation of potential business risks that could be attributed to a dependency on technology.



1.2.3 Client / Server Objectives

- To reduce complexity and administration workload of Disaster Recovery Procedure to the maximum allowed by means of automation.
- To reduce recovery time of primary server backup facilities in NDLAMBE MUNICIPALITY and all server related application to 24 hours by 2013.
- To limit the recovery time of centralized server backup facilities, to the actual critical time framed of the Municipality by 2013.
- Where applicable, to reduce recovery time of secondary backup facilities to 18 hours by 2013
- Disaster recovery and operational recovery to become integrated to reduce cost and workload
- Disaster Recovery testing to be simplified to the point where regular testing (by means of disaster recovery systems and infrastructure) results in minimum impact to service. i.e. becomes transparent to daily service.
- Perform analysis on impact that the loss of the server would have on LAN environments.

13.2.4 Network Objectives

Disaster Recovery resilience to be fully implemented within the NDLAMBE MUNICIPALITY network.

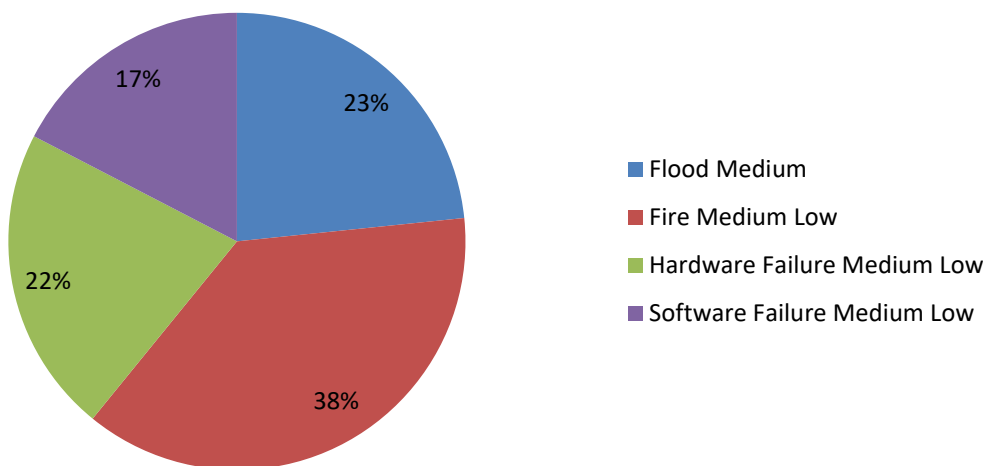
13.2.5 LAN Objectives

- To implement a backup strategy for all critical data hosted on production LAN's, as well as the off site cycling thereof by 2013
- To have effective Disaster recovery Plans and backup facilities that have been tested, for all high priority Business Units by 2013
- To limit the recovery time at backup facilities, to the actual critical time frames of all high priority Business Units by 2013
- To establish a common Disaster recovery facility for high priority Business Units and a common testing site for low, medium and high priority business units.



14 .Risk Analysis

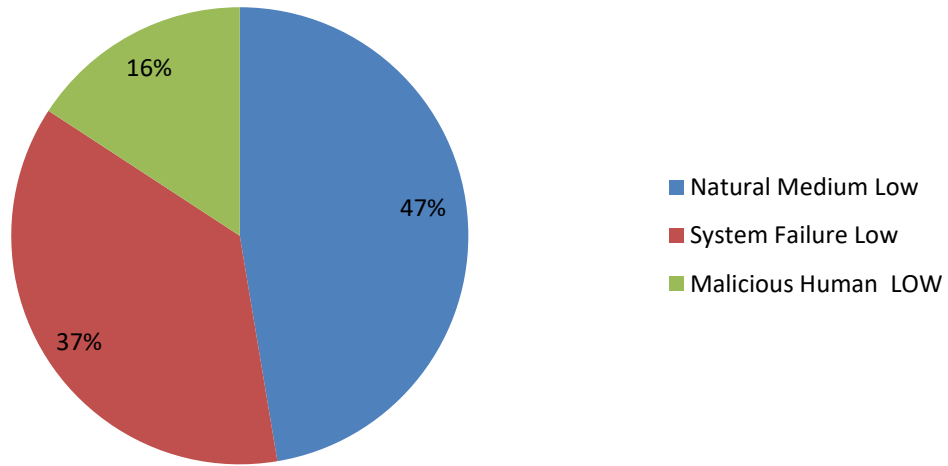
Ndlambe Risk Chart



Risk Area's		
Flood	Medium	50%
Fire	Medium Low	48%
Hardware Failure	Medium Low	40%
Software Failure	Medium Low	32%



Threats



Threats		
Natural	Medium Low	27%
System Failure	Low	21%
Malicious Human	Low	9%