Molemole Municipality

ICT Policies and Procedures

Disaster Recovery Policy

Document Name: Disaster Recovery Policy

Document Information

Policy	Disaster Recovery Policy
File Name	Disaster Recovery Policy.doc
Date Issued	August 2016
Manual	IT Policies and Procedures Manual
Section	09 Business Continuity
Applicability	This is applicable to all IT personnel who are allocated responsibilities for disaster recovery.
Situations	This policy is used to ensure that the IT disaster recovery strategy and plans are carried out as part of the larger business continuity responsibilities of the municipality.
Changes	V001 : Initial Version
Policy Owner	Municipal Manager
Policy Enforcer	IT Manager

Contents

1. Overview

1.1. General Purpose

Information and information resources are valuable assets of Molemole Municipality and they form an important part of the operation and management of the municipality.

This and other policies have been put into place in order to protect these and to promote integrity, security, reliability and privacy of the entire information infrastructure including the information and data it contains, the network, the computers and other access devices.

1.2. Background to this Policy

All organisations have a fundamental responsibility to protect their assets. This responsibility is outlined in all statements of corporate responsibility and this extends to the protections required to ensure continuity of the organisation when confronted with a wide range of corporate risks.

This policy does not concern the risks analysis, nor the general corporate strategies and plans to deal with business continuity, but is focussed specifically on its responsibility to ensure continuity of the information assets, resources and services.

This policy provides the basic rules which govern best practice, but does not provide the details of exactly how these policies will be implemented. These are included into the Disaster Recovery Standards which will be adapted for new situations as they emerge within the information infrastructure.

The benefits of this policy are expected to be realised only when a disaster strikes and the specific elements of this policy were found to have been implemented to the full. As a result it is very important to dispel the notion that disaster recovery planning is a waste of time and that missing a backup is not that important. Every part of this is a non-negotiable requirement of an effective disaster recovery policy.

2. Scope

2.1. This policy is concerned with the actions that will ensure that the entire IT infrastructure can be reproduced as best as possible when certain types of disaster-type situations occur, or that specific elements of this infrastructure can be reproduced.

2.2. The term "disaster" is often meant to imply catastrophic disaster when considering the disaster recovery plan for the organisation. However, in this context it is used to mean the loss of any part of the information infrastructure or resources.

2.3. This is applicable to the following kinds of loss:

- Personnel loss: in which key personnel are lost to the organisation through ill health, death or moving to another organisation.
- Infrastructure loss: if some or all of the IT infrastructure is lost, including servers, networks, the server facilities and related areas. This includes the theft of critical computing facilities such as servers and critical workstations.
- Information loss: in which information assets, data, database or other types of stored information are lost through various reasons, such as inadvertent deletion of critical data.
- Application loss or breakdown: in which specific applications fail and cannot be recovered. This is often due to software bugs in applications for which only object code is available, such as with proprietary software. This is also a potential result from undetected threats such as viruses.

2.4. This policy does not include any specifics concerning the high-level disaster recovery strategy or plan, including the following:

- Analysis of specific risks, and management of these risks in terms of probability analysis, impact analysis and recommended countermeasures.
- The role of insurance in risk mitigation.
- The formulation of specific plans for disaster recovery.
- The incorporation of disaster recovery plans for IT services into the organisation's disaster recovery plans.

2.5. This policy does not include contingency plans, organisational roles and responsibilities, or detailed recovery procedures. Rather, this policy provides the framework of good practice for what the detailed plans are required to contain.

2.6. The responsibility for disaster recovery is the head of the institution, which in the case of a municipality is the municipal manager. However,

for less critical losses, which can also be covered in the scope of this policy, the IS manager must maintain responsibility.

2.7. The distinction between when the municipal manager or the IT manager will be responsible is whether the municipality as a whole is threatened by the extent of a loss, in which case the municipal manager must take the responsibility.

2.8. This is related to the following policy:

- Register of IT Assets Policy

3. Purpose of this Policy

3.1. The purpose of this policy is to guide the development of Disaster Recovery Plans for IT Services in order to ensure minimum business impact in the event of an IT service disruption.

4. Applicability

4.1. This Policy is applicable to the following situations:

- Developing and maintaining IT contingency
- Training and testing the IT contingency plans

5. Definitions for this Policy

5.1. This policy document also defines the following specific items:

- IT contingency plan: this is the overall plan for the handling of all types of loss or disasters concerning the IT services.
- Disaster Recovery Plan: this is the total plan for the organisation to support disaster recovery and include both IT and non-IT functions.

6. References for this Policy

COBIT V4.0

6.1. There are a large number of control objectives and processes within COBIT that are relevant to disaster recovery and loss reduction of IT and information assets.

6.2. The IT Goals identified in COBIT are linked to specific control objects. The IT Goals of concern here are :

- IT Goal 14: Account for and Protect IT Assets.
- IT Goal 18: Establish Clarity of Business Impact of Risks to IT Objectives and Resources.
- IT Goal 21: Ensure IT Services and Infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.
- IT Goal 22: Ensure minimum business impact in the event of an IT service disruption or change.
- IT Goal 23: Make sure that IT services are available as required.

King II Report

6.3. Organisations are required to identify and mitigate corporate risks.

6.4. Everything associated with effective disaster recovery policies is a countermeasure to some risks, and due to the large number of possible situations that can threaten the IT assets it is essential that generic solutions are considered to mitigate as many risks as possible within the scope of the policies and procedures.

6.5. An effective policy for disaster recovery must respond to specific risks as identified in the risk management.

ISO 17799

6.6. Section 11 covers guidelines for business continuity management.

Municipal Systems Act (MSA)

6.7. S26 outlines the scope of an IDP, which must include a disaster recovery plan.

Molemole Municipality IDP 2007/11

6.8. Information Technology SBU makes specific reference to the lack of a disaster management strategy for IT services.

7. Policy Statements

7.1. This policy must be read in conjunction with the Municipal Disaster Management Plan as well as the specific IT contingency plan.

Purpose and Location of the IT Contingency Plan

7.2. The IT contingency plan must detail all of the countermeasures and mitigations that are to be conducted in the event of a loss of IT service.

7.3. The plan must be divided into two major sections:

- Preventative measures which enhance the resilience of the municipality's IT services, and which cater for the eventuality of loss of service.
- Recovery measures which outline the means of reconstitution of the IT services to an acceptable level when a loss occurs. This also includes the means by which people are trained for recovery and how such recovery processes are tested.

7.4. The plan must be reviewed and maintained on a regular basis in terms of changes in the operational environment, personnel, contact people, facilities, legislation, suppliers, processes and risks.

7.5. The recovery measures must identify urgent recovery to a minimal operating environment, followed by a plan to reconstitute the entire IT services.

7.6. This IT contingency plan must be the only approved source of guidance to be used at the time of loss in order to accelerate recovery and to avoid disputes that commonly arise in recovery situations.

7.7. The IT contingency plan must identify specific roles, and must allocate nominated personnel to these roles, in terms of how the plan will be carried out and in terms of responsibilities for the actions required for recovery. These roles must also include those responsible for all countermeasures such as backups and recovery site management.

7.8. The IT contingency plan must be kept in a safe location outside of the locations to be protected. The plan must be accessible at very short notice. Copies of the plan may be located at various locations as required including remote municipal offices. It is essential that all copies of the IT contingency plan are of the current version, and when any version changes are made, all remote copies must also be changed.

7.9. The location of the copies must be identified in the Municipal Disaster Management Plan and this must be managed by the Disaster Recovery Unit within the municipality.

Preventative Measures

7.10. A number of preventative measures are required to minimise the possibility of loss as well as to support rapid recovery in the event of loss.

7.11. These measures include:

- Defining and maintaining the Configuration of IT services.
- Ensuring that all threats and risks to the continuity of the IT services are identified and managed appropriately.
- The identification of critical IT services that would need to be reconstituted.
- Backups of all software, applications and data that will be required in the event of a disaster, with sufficient proof that these can be used effectively when needed.

Maintaining the Configuration

7.12. The full set of IT services must be documented in a Configuration, which identifies the key information required to reconstitute part or all of these services in the event of loss or disaster.

7.13. The Configuration is required to contain at least the following information:

- All components of the IT Services: facilities, servers, workstations, operating systems and server applications, business applications, data, peripherals.
- How these are interconnected in terms of physical cabling and configuration, application interfaces and any other interfaces.
- The detailed specification of all equipment sufficient to be able to reconstitute the equipment with replacement hardware. For computers this must include the memory and disk.
- Sources in which replacement equipment can be obtained, and the systems software required to implement the specific conditions. This may include specific versions of operating systems and patches, as well as other components that may be required.

Prioritisation of IT Services

7.14. All IT services must be identified in terms of the priority of their importance for the continued operation of the municipality. This priority list will constitute the sequence of recovery in the event of disaster.

7.15. The IT Contingency Plan must identify this priority list and classify the IT services appropriately into the following categories:

- Critical: core municipal functions which cannot operate without these IT services – the lack of these prevents the municipality from operating. These must be recovered first in any recovery situation.
- Important: these impact one or more areas that are critical in their own right, but which are not critical to the entire municipality.
- Non-critical: these impact single functional areas and can be ignored in a first-round recovery process.

7.16. As an example, it may be deemed that the Financial Systems are critical, since they are essential to the continued operation of the municipality, and no workaround is possible in the event of a disaster. However, the GIS system may be deemed to be non-critical, since a delay in recovery will not adversely impact on the entire operation of the municipality.

IT contingency plan: Procedures, Training and Testing

7.17. The IT contingency plan must identify the full extent of the recovery procedures required to reconstitute each IT Service, down to the finest level of detail.

7.18. It is expected that this plan can be run with military-style precision with clearly identified responsibilities for communications, command and control.

7.19. The recovery procedures must be able to be carried out by personnel other that those who wrote them or who manage the IT Servers.

7.20. The roles may include external service providers who may be required to assist in reconstitution of the infrastructure, applications or services, or who may be needed as experts in the event that problems are experienced in recovery.

7.21. The recovery procedures must identify the source of all of the components required to be used for reconstitution, as outlined in the Configuration.

7.22. The recovery procedures for critical systems must be tested on at least a quarterly basis or whenever there are major changes to the IT infrastructure (such as operating system or server upgrades, or new versions of the application software).

7.23. The recovery procedures for other IT services must be tested at least annually.

7.24. All personnel involved, including municipal officials and external suppliers must be adequately trained and must know their roles and responsibilities sufficiently to carry these out. These apply to both the continuous preventative measures, such as backups and configuration updating, as well as for recovery processes.

7.25. All recovery tests must be analysed in detail to identify weaknesses, and to improve the capability for recovery. These must be documented into the Disaster Recovery Testing Log.

7.26. In all cases, the recovery procedure tests must cater for the worst-case scenarios for reconstitution, on the assumption that any smaller loss situation will be covered within the test.

7.27. Various tests must be undertaken including complete rehearsals to support complete reconstitution of the entire IT infrastructure and the usage environment at an alternate location and must include the following:

- Availability and suitability of the alternate location: including agreements to use the other locations (this must be municipal owned sites where possible).
- Housing staff in the alternate location. Actually moving a number of staff to the location in order to test out the plan is recommended. This will identify constraints in terms of office facilities, transportation, catering, toilets and other facilities which may be overlooked in a plan.
- Adequate communications facilities within a stipulated period (telephones, Internet, cabling, PABX, routers).
- Establishment of the server infrastructures on a temporary basis, with the loading of all necessary systems software. This may involve simulated purchasing of alternative servers as well as their configuration.
- Recovery of application systems and data from backups with identification of the losses between the time of backup and the time of recovery.

- Recovery of user credentials and security information.
- Resumption of operational activity on the IT services, identifying any potential problems with usage.
- Compatibility with other disaster recovery plans in force including those of the municipality as a whole.

7.28. Other tests can include: table-top tests, simulations, technical recovery testing at current and alternate sites, testing of supplier services and capabilities. The Disaster Recovery Plan must indicate what tests are most appropriate for each IT service.

IT contingency plan: recovery procedures

7.29. The recovery procedures must identify clearly the key personnel responsibility for recovery, and it is their responsibility to create the organisational team to perform the detailed recovery.

7.30. The team must consist of at least the following roles:

- Direction: key decisions on priorities, facilities, roles and responsibilities, and approving all communications.
- Communications: informing all stakeholders of the progress and status, and what they are required to do as part of the recovery. This particularly applies to users of IT services, and municipal officials. Communications to the public will take place through the Communications SBU and not directly.
- Resources: identifying all of the resources required to reconstruct the Configuration and ensuring that these are procured and configured properly.
- Infrastructure: building temporary infrastructure necessary to house the IT services including communications systems, servers, software, and reconstituting the data and applications from backups to the point of handover.
- Logistics: ensuring that all elements of movement of resources and personnel are achieved efficiently.

7.31. The IT contingency plan must be communicated to all relevant personnel as soon as possible, preferably through a team briefing and regular briefings in the course of the recovery process.

- Each backup is required to be performed on a schedule as required, and the schedule must support the recovery requirements for each IT service. For example, critical IT services may require dynamic "log-shipping" backups.

- Every day a backup schedule must be produced for the backups to be performed, and once these are done, the schedule is signed and handed to the Assistant Network Engineer for approval. The Assistant Network Engineer may request proof of completion through suitable means (such as tests of recoverability).

- Every week the backup schedule must be signed by the Network Engineer.

- The backup schedules must identify where the backups are stored, and where recovery must be performed from.

- It is essential that backups are stored off-site and that the procedures include movement of the total backup to external sites on a daily basis.

7.41. The backup media are required to be aged as follows:

- At least the latest three backups available for each application system, database, folder and files. These to be aged on a grandfather, father, son approach.

- When incremental backups are used, then a longer history is required to be maintained in the backups.

- The aging policy must support recovery from at least two failed media within the backup history.

- Full backups are maintained once per month on a permanent basis and are never destroyed.

Hot and Cold Backup Facilities

7.42. The provision of suitable infrastructure for business continuity in the event of major disasters presents significant challenges, since it is never possible to completely reproduce the IT infrastructure within the bounds of municipal budget constraints. There are few organisations that can afford to duplicate their entire infrastructure and services and these are limited to the largest commercial organisations such as the major banks.

7.43. Hot backup facilities are those that are ready and available to support movement to a new site and to be operational within hours. It is not

considered feasible to accommodate hot backups in the municipal environment due to the high cost of implementation and management.

7.44. Cold backup facilities are those in which provision is made for recovery, but that much of the infrastructure needs to be established at the sites as and when a problem arises. These will provide basic facilities such as office environments, server rooms, communications structures, but not contain any equipment, which is then required to be installed as and when an incident arises.

7.45. It is recommended that the municipality have a Cold backup facility available and that this be regularly checked.

7.46. As required, the Cold Backup facilities could operate at other municipal offices that can be transformed into an alternative site for IT services at short notice by displacing the occupants in preference to the critical IT services. This will require that the occupants of the offices are part of the disaster recovery planning so that they can clear out their offices as quickly as possible in the event of a disaster.

8. Procedure: Verify Previous Day Backups

Trigger

8.1. This procedure is carried out at the start of every day.

Requestor

8.2. This procedure is performed on a regular basis and the original requestor will be deemed to be the IT Manager.

Responsibility

8.3. The Technician carries out this procedure.

8.4. The Desktop Tehnician is responsible for the daily checking and sign-off and check of off-site storage of tapes.

8.5. The IT Manager is responsible for the weekly checking of backups and off-site storage and sign-off.

Steps

Seq	Activity	Who	Timing

Seq	Activity	Who	Timing
1	Logon to the Network Backup Administration Console. APPLICATION ADDRESS? WHICH COMPUTER TO USE? (e.g. Computer Room?) Print out the Daily Backup Report.	Desktop Technician	At 0800 every morning
2	Check previous day's backup report to ensure that there are no problems arising from the Backup Report. Sign the Backup Report.	Desktop Technician	08:00
3	If any system backups were unsuccessful then these are performed manually and the errors are noted for future consideration. A new Backup Report must be produced for this manual backup which must also be signed by the Assistant Network Engineer. The source of the errors must be identified and fixed as soon as possible, preferably before the next backup.	Technician	Immediatel y
4	Every Monday a duplicate tape is created from the latest full Backup Tape, which is then used to simulate recovery procedures.	Desktop Technician	
5	A final Backup Report is produced indicating the following: • Which systems were backed up and which data files and folders were included. • The tape numbers onto which the backups were performed. • The date and time of completion. • A record of any problems that occurred in the backup procedure.	Desktop Technician	
6	Backup reported checked and signed off.	IT Manager	Daily/ Weekly
7	The tape is prepared for submission to the Protection Services. This must be performed on a daily basis even if the tape is not full.	Technician	
8	The Protection Services will collect the backup tape and produce a proof of collection. This must be scheduled for latest 0900 every morning.	Protection Services	09:00
9	The Backup Report and the Proof of Collection are submitted to the IT Manager.	Desktop Technician	By 09:30 every morning
9	The Desktop Technician submits the Backup Report and the Proof of Collection to the IT Manager (weekly) for review.	Desktop Technician	By 10;00 every morning

Seq	Activity	Who	Timing
10	The IT Manager may request additional checks to be performed to verify the backup. They may also wish to check the backup tape.	IT Manager	Any time
11	The IT Manager (weekly) signs the Backup Report as proof of acceptance that the backups were carried out properly.	IT Manager	By 11:00
12	The IT Manager files the Backup Report and the Proof of Collection within the Document Management System.	IT Manager	By 12:00

Forms and Registers

8.6. Form 09-50 Daily Backup Report. This is an output from the Backup Software.

Practice Notes

8.7. The Protection Service is any service which has been contracted to collect and stores the backups off-site.

Enforcement

8.8. This procedure is enforced by the IT Manager.

9. Procedure: System Backups

Trigger

9.1. This procedure is required to be run daily. This will be performed outside of normal working hours in order to minimise disruption of the facilities.

Requestor

9.2. This procedure is performed on a regular basis and the original requestor will be deemed to be the IT Manager.

Responsibility

9.3. The IT Manager will be responsible for carrying out this task.

Steps

Seq	Activity	Who	Timing

Seq	Activity	Who	Timing
1	Logon to the Network Backup Administration Console. APPLICATION ADDRESS? WHICH COMPUTER TO USE? (e.g. Computer Room?)	Desktop Technician	1600 every Day
2	The Technician produces a Scheduled Backup Report indicating the systems, databases, data files and folders that are to be backed up. This must be produced monthly or any time that the contents of the backup schedule changes. This must include the data backups as well as system backups as required.	Desktop Technician	
3	The Network Engineer or their delegated authority signs the Scheduled Backup Report to indicate their acceptance of the files and folders to be backed up. This must correspond to the relevant parts of the Information Assets Register.	IT Manager	
4	The Assistant Network Engineer checks that all of the files and folders as indicated in the Scheduled Backup Report are present on the scheduled backup to be performed. Spot checks to be performed by the Network Engineer on a weekly basis.	IT Manager	
5	The Technician executes the scheduled backup process and checks that it is executing properly.	Desktop Technician	

Forms and Registers

9.4. Scheduled Backup Report IT-09-52.

Practice Notes

9.5. Special consideration must be given to database backups, since these are often running continuously. The backup facilities must integrate with the database backup processes to ensure that the backups taken are able to be recovered.

9.6. Database backups must be performed by the database management systems. These must be scheduled to be performed BEFORE the tape backups are done.

Enforcement

9.7. This procedure is enforced by the IT Manager.

10. Procedure: Recovery Testing

Trigger

10.1. This procedure must be run at least weekly and on an ad hoc basis when requested. The scheduled procedure will occur on a weekly basis every Monday.

10.2. On a quarterly basis a full recovery must be conducted on the basis of the ICT Contingency Plan.

Requestor

10.3. The ad hoc recovery test can be performed any time as requested by the IT Manager.

Responsibility

10.4. The IT Manager will be responsible for carrying out this task.

Steps

Seq	Activity	Who	Duration
1	Obtain the most recent tape backup (or copy as appropriate).	IT Manager	
2	Check that the Backup Reports indicate this as the latest backup tape or copy by the number and date written onto the tape. Approve the Recovery Process.	IT Manager	
3	Confirm the details of the files and folders written to the tape from the Backup Report.	IT Manager	
4	Place the tape into the tape drive and use the Backup System to identify the contents of the tape. This content is checked against the Backup Report.	Desktop Technician	
5	The files and folders are copied from the backup tape onto a separate server with sufficient space. This will check that the media can be read and that the data files are readable and recoverable.	Desktop Technician	
6	The files and folder sizes and dates on the separate server must be checked against the sizes and dates to ensure that they are the same.	Desktop Technician	
7	Any errors are noted immediately on the Recovery Test Form. A plan of action to fix the errors must be instituted immediately.	Desktop Technician	

Seq	Activity	Who	Duration
8	A full recovery test is performed to ensure that each and every file and folder can be used by the corresponding applications.	Desktop Technician	
9	The Recovery Test Report is completed and handed to the IT Manager as proof that the recovery is possible. The IT Manager may request additional recovery tests at this time.	Desktop Technician	

Forms and Registers

10.5. Recovery Test Report 09-51.

Practice Notes

10.6. In practise it may be very difficult to fully test the recovery process. However, this is an integral element of a successful backup procedure. As a result, it is imperative that the facilities exist to duplicate the applications for testing purposes, and it is recommended that an alternative server be provided to support full recovery testing. This server is not required to support the full performance of the live server, but must have sufficient capacity to ensure proof of recovery.

Enforcement

10.7. This procedure is enforced by the IT manager

11. Forms / Registers

Backup Schedule

11.1. This is used to identify the specific backups to be performed each day, and the results of these.

11.2. This is required to be stored as part of the IT contingency plan, since one of the first things required in a recovery situation is the location and status of the latest backups.

11.3. It is assumed that a single backup will include a number of applications and data sets and will all be stored with a single backup code.

11.4. Contents of this backup schedule include the following:

- The date (one schedule for each day).

- The overall responsibility for the backup process (a single person allocated this responsibility).
- The specific backups to be performed: applications, databases, folders.
- The form of the backups: tape, DVD.
- The location where the backups are stored (off-site).
- The labelling of the backups.
- The date and times when the backups were completed.
- Signature of the responsible person.
- Signature of the IS manager.

11.5. This backup schedule must be stored with the IT contingency plan, and a copy retained with the physical backup media.

12. Review and Audit

12.1. This policy will be reviewed after every 3 years from the date of approval.

12.2. The enforcement of this policy will be audited as follows:

- The backups are being performed as required and the media stored in the location at which they are indicated.
- The media contain the backups as indicated on the schedule.
- The media contain backups that are recoverable.
- The backup media are aged according to the approved policy.

* * * END OF DOCUMENT * * *

Cllr. Paya ME
Mayor

31/05/2022
Date