Molemole Municipality IT SERVICE

CONTINUITY MANAGEMENT POLICY

Revision: Version 1.0

Effective date: 25 – November - 2013

Molemole Municipality

Foreword

The purpose of the IT Service Continuity Policy document is to establish the activities that need to be carried out in the event of IT Disaster.

CONTENTS

1. INTRODUCTION

This policy document will provide an overall guideline that governs IT Continuity/Disaster Recovery within Molemole Local Municipality. IT Continuity Management is a continuous process of risk assessment and risk management with the purpose of ensuring that the municipality can continue to deliver its key services should a disruption arise. A disruption can arise when a threat to the IT environment materialises during the course of our normal service delivery.

IT Recovery starts by carefully agreeing to business units requirements and determining the cost of downtime or unavailability of the specific service in question, so that a realistic disaster recovery requirement can be established.

This process involves an element of awareness creation and consensus among all parties involved. To be successful in this regard, the municipality would need to understand how to define and present its requirements for ensuring IT Service Continuity in all municipal service points and its departments.

IT Continuity is business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

2. POLICY OBJECTIVES

The primary objective of this policy is to ensure that Molemole municipality has the capacity to resume operational effectiveness within a specified period of time after the onset of a disaster or other disruptive events to the municipal IT operations.

The secondary objectives are as follows:

2.1.1 Staff welfare and confidence during and after a disaster incident;
2.1.2 Continuous service delivery to Molemole communities;
2.1.3 Maintenance of client and stakeholder contact and confidence;
2.1.4 Fulfilment of regulatory requirements;
2.1.5 Control expenditure and lower costs caused by the disaster incident;
2.1.6 Apply the municipal Risk Management framework to priority areas

3. Application of this policy

This policy applies to all employees (including service providers, contractors and temporary staff) utilizing municipal systems and across all Molemole networks.

4. References and Related Legislation and Regulations

The following regulation and legislation govern the execution of the IT SERVICE CONTINUITY MANAGEMENT POLICY and were taken into consideration during the drafting of this policy:

4.1 SABS/ISO 25999
4.2 SABS/ISO 17799
4.3 Minimum Information Security Standards
4.4 Protection of Information act
4.5 Municipal Systems Act, 2000 (Act 32 of 2000)
4.6 Regulation of Interception of Communications Act

4.7 COBIT Audit framework
4.8 Electronic Communications and Transactions Act
4.9 International Standard for Risk Assessment
4.10 Molemole Approved IT and Information Security Management policy
4.11 Molemole approved Backup Policy

5. POLICY STATEMENTS

5.1 Policy Statement

All IT staff responsible for performing IT Service Continuity activities and procedures will follow the IT Recovery process as documented: An initial Risk Assessment must be undertaken in order to determine the requirements for the IT Service Continuity Plan.

5.1.1 The municipality must have in place an approved comprehensive Disaster Recovery Plan to ensure that it can recover all critical IT and information systems in the event of a disaster;

5.1.2 It is the municipality's responsibility to ensure that all critical processes can be continued in the event that a serious unplanned event occurs, which may disrupt the normal execution of IT processes;

5.1.3 It is the responsibility of all departmental managers to assist in the development and support of this plan to ensure that this IT Service Continuity policy conform to the overall acceptable standard as prescribed in the national regulations and applicable legislation;

5.1.4 The IT Service Continuity Plan must cover all essential and critical business activities which relate to its daily operations. In the event of a disaster, it must be possible for the municipality to continue operating;

5.1.5 The IT Service Continuity Plan must be periodically tested on a monthly basis to ensure that it can be reliably implemented in an emergency situation, and that management and staff understands what is required for execution;

5.1.6 The IT Service Continuity Plan must be kept up to date to take into account any relevant change within the municipality's IT and information systems environment;

5.1.7 Staff must be made aware of the IT Service Continuity Plan and their specific roles (if applicable) defined within the plan.

5.2 Policy Ownership

a. The Municipal Manager is and remains responsible for the overall implementation of this IT Service Continuity Policy.
b. This responsibility is delegated to Senior Manager: Corporate Services department who should report periodically to the Municipal Manager;
c. It is the responsibility of all municipal service points and municipal departments to ensure that they have enough information in their specific section of the IT Service Continuity Plan, to enable them to recover from an incident and continue to provide a service to clients within acceptable timeframes.

5.3 IT Service Continuity Scope

a. The IT Service Continuity Management (Disaster Recovery) policy covers all the functions contained within Molemole municipality.
b. It forms the basis for all IT Service Continuity Planning activities and is expected that the implementation of IT Continuity Management Plan within Molemole municipality will follow the guidelines and processes outlined in PAS77 (IT Continuity) AND BS25999 (Business Continuity) standards.

6. IT Unit Responsibilities

In order to support the above objectives fully the IT Unit of the municipality through the assistance of ICT Steering committee of the municipality is expected to ensure that it:

- Identifies all critical business processes, functions and outputs;
- Identifies and assess any threats to those business processes, functions and outputs;
- Puts into place measures to eliminate those threats, or if it is not possible, develop plans to mitigate and manage them, should they occur;
- Fully comply with all the requirements of the IT Service Continuity Management Policy;
- Evaluate and recommend strategies for the reduction or transfer of risk (including appropriate insurance, where available);
- Develop the IT Service Continuity strategy consistent with the organisation's overall business and security strategy;
- Regularly test, review, and update all procedures relating to the IT Service Continuity Plan;
- Ensure IT Service Continuity Planning is integrated into departmental functions and daily operations;
- Allocate responsibility to individuals in their business units to fulfil the requirements of the IT Service Continuity plan;
- Ensure that records are managed in accordance with the approved records management policy and that all the required IT Continuity documentation and records are available and current.
- Compile period reports on the state of IT Service Continuity Plan and recommend appropriate updates for effectiveness of the policy.

7. Key Risk Areas

The key areas that can affect our delivery of service as at the time of writing this policy are as follows:

7.1 The denial of access to Municipal facilities due to:

7.1.1 Vandalism
7.1.2 Accidental fire or arson
7.1.3 Scene of crime investigation
7.1.4 Dangerous structures
7.1.5 Flooding

7.2 Staff shortages due to;

7.2.1 Loss of key staff/skills in the municipality
7.2.2 Industrial action [strikes, go-slows, protestations]
7.2.3 Fuel shortages
7.2.4 Prolonged severe weather conditions

7.3 Denial of service due:

7.3.1 Failure of a supporting service such as:-
- 7.3.1.1 Computing system failures
- 7.3.1.2 A sub-contractor's business failure
- 7.3.1.3 Telephone system failures

7.3.2 Unavailability of proprietary and critical information

7.4 IT Service Continuity Policy Violation

a. Violations of this policy will be subject to disciplinary action as described in HR Policy, Code of Conduct as per Municipal Systems Act, 200 (Act 32 of 2000) as well as in accordance with the South African Labour Relations Act (Act no.66 of 1995);
b. All municipal employees, contractors or temporary staff who have been granted the right to use the municipal Internet access are required to sign this agreement confirming their understanding and acceptance of this policy.
c. All employees, contractors or temporary staff who have been granted the right to use the department's Internet facilities are required to sign the internet user undertaking confirming their understanding and acceptance of this policy.
d. As already stated, non-compliance of this policy may lead to disciplinary actions, legal liability as well as internet privileges for the user in violation revoked.

7.5 Review of This Policy

a. The Policy document will be reviewed after every 3 years from the date of approval.
b. Where the policy is materially revised, this will be published before the end of the third quarter of the financial year to ensure that budgetary issues which may arise can be addressed during the annual budgetary cycle;
c. The revised document will be agreed and approved by role players as listed herein;
d. Review of the policy must relate to the operational circumstances within the municipality and the overall Integrated Development Plan, addressing any relevant changes in municipality, its operations or operating environment and any legislative requirements, which may have occurred since the previous revision.

DRP Standards and Guideline

1. Key Role players and their Responsibilities

In order for Disaster Recovery to be successful, the following input requirements are essential:

1.1 Internal:

1.1.1 Change Management – Changes to the IT Infrastructure need to be reviewed for impact and risk to ongoing Disaster Recovery requirements.

1.1.2 ICT Manager – The manager (ICT) through the guidance from the IT Service Continuity Steering Committee is always responsible for defining and maintaining the framework for IT Service Continuity Management which includes policy, strategy, overall implementation, plan documentation structure, provision of business and support unit templates, tests and training requirements, review and change management requirements as well as initiating tests and reviews.

1.1.3 Budget & Treasury department– The IT Unit, together with the municipal ICT Steering Committee (ISC) works closely with Budget & Treasury department to fully understand the cost implication of delivery required by Disaster Recovery at justified costs.

1.1.4 Security Management - Security requirements are taken into account in the IT Recovery design activities.

1.1.5 Municipal ICT Steering Committee -ISC helps to define the Business Requirements for IT Recovery and also help in identifying the Vital Business Functions. ISC also plays a major role in the actual reporting of Disaster Recovery achievements on a consistent basis. ISC also provides IT Recovery information on Underpinning Contracts.

1.1.6 Support Units - It is the responsibility of the support units to ensure that they have enough information in their specific section of the IT Continuity Plan, to enable IT to recover the infrastructure and services required to support business recovery activities within acceptable timeframes.

1.2 External:

1.2.1 All 3rd Party Vendors and Service Providers

1.2.2 Provincial and National Sector/sister departments [CDM, COGHSTA, NT, SITA]

2. IT Service Continuity Management Process

2.1 The IT Continuity Management process will consist of four stages:

Stage 1: Planning
Stage 2: Implementation and Operation of IT Service Continuity Strategy
Stage 3: Monitoring and Review
Stage 4: Maintenance and Improvement

a. The first two stages involve the establishment and implementation of IT Service Continuity task team.
b. The final two stages ensure an ongoing operational management of the process.

Stage 1: Planning

This stage covers the establishment of the IT Continuity Management process, including sponsorship, budget approval and identification of appropriate resources.

Stage 2: Implementation and Operation of IT Service Continuity Strategy

This stage provides the foundation for IT Continuity Management and is critical to determine:

2.1.1 How well the municipality is prepared and capacitated to survive an IT interruption or disaster;
2.1.2 Any costs that will be incurred as a result of a business interruption or disaster;
2.1.3 Requirements identified through the Business Impact Analysis and Risk Assessment activities;
2.1.4 The outputs from the above activities that will feed into the IT Service Continuity Management strategy, which proposes risk reduction measures and recovery options, in support of business continuity.

Once the IT Service Continuity Strategy has been agreed, the IT Continuity Management lifecycle will move into the actual implementation activities.

These activities will include:

- Establishing IT Service Continuity Management Plan with clear roles and responsibilities for any personnel who will be involved in a recovery;
- Developing Training, awareness and competency plans;
- Developing implementation and supporting plans;
- Developing and implementing an incident response structure;
- Providing resources to implement risk reduction measures that are detailed in the IT Continuity Strategy;
- Procuring recovery facilities;
- Providing continuity capability through initial testing;
- Embedding IT Continuity in the municipal culture;
- Developing and implementing change management procedures;
- Testing of the IT Continuity Plan;
- IT Continuity documentation and records management

Stage 3: Monitor and Review

3.1 The completion of the first two stages of the IT Service Continuity Management process will mean that an IT Continuity Management solution has been analysed, agreed and implemented within the organisation.

3.2 Molemole municipality must to ensure that the strategy and recovery facilities are maintained as part of day-to-day municipal activities.

1. The IT Unit and the municipal ICT Steering Committee has the responsibility for maintaining the IT Continuity Management environment through a series of operational management activities.

2. These activities will include:

   Internal and External reviews –reviewing of IT Continuity activities at agreed time intervals. The Management Committee will ensure that IT Continuity Plan is tested at planned intervals.

   Management reviews of the IT Continuity Plan – The test results from above will feed into the management review of the IT Continuity Plan. The decisions and actions recommended by management will feed into the Maintenance and Improvement stage.

Stage 4: Maintenance and Improvement

The completion of stage three will mean that the status of IT Continuity Plan in the municipality will have been established and there could be a need for improvement and making changes to suit the current requirements of the municipality

The ICT Manager, assisted by ISC will document all procedures for corrective and preventative action to ensure that the municipality's IT Continuity Plan conforms to the PAS77 AND BS25999

standard. All such procedures, minutes, records pertaining to the IT Continuity Plan will form part of the municipal IT Continuity records and documentation as required by the PAS77 AND BS25999 standard.

3. Backup and Offsite Storage

3.1.1 All users using desktop applications will be required to comply with the municipal Data Backup policy;

3.1.2 The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

3.1.3 The Municipality's Information Resources backup and recovery process for each system must be documented and periodically reviewed.

3.1.4 Offsite backup storage facilities for Molemole municipality will be handled by SITA and shipped by the municipality's authorized official as per the service level agreement with SITA. Backed up media must be shipped to SITA premises on a monthly basis and a log-book must be signed by the receiver of backup media;

3.1.5 Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest municipal sensitivity level of information stored. This shall be as determined in line with MISS.

3.1.6 A process must be implemented to verify the success of Molemole municipality's electronic information backup through quarterly restoration tests. Backups must be periodically tested to ensure that they are recoverable. Test results should be filed as per the municipal records management policy;

3.1.7 Signature cards held by the offsite backup storage vendor(s) for access to Molemole municipality's backup media must be reviewed annually or when an authorized individual leaves the Municipality or SITA;

3.1.8 Backup media in transit shall comply with all the requirements of MISS and in addition to meeting these requirements the backup media shall be encrypted to ensure that it is protected against unauthorized access;

3.1.9 Backup tapes must be clearly marked for as per the agreed backup frequencies for ease of identification in times of need

Annex A : Abbreviations and Definitions

A.1 Abbreviations

SITA	State Information Technology Agency
ISC	ICT Steering Committee
MISS	Minimum Information Security Standard
DRP	Disaster Recovery Plan

17. Approval of Policy

This policy shall be effective from the date of approval and shall be reviewed after three years from the date of approval or should the need arise.

Approved/ Disapproved

a) **Date of review by Council** 29-05-2019

b) **Resolution number** Oc/7.5/29/05/19

c) **Signed on behalf of Council**