



Molemole Municipality

ICT CHANGE MANAGEMENT POLICY

Contents

| | | |
|-----|--------------------------------------|----|
| 1. | Preamble | 3 |
| 2. | Acronyms and definitions..... | 3 |
| 3. | Purpose..... | 4 |
| 4. | Objective of this Policy | 4 |
| 5. | Regulatory Framework..... | 4 |
| 6. | Scope of the policy | 5 |
| 7. | Process Overview | 5 |
| 8. | Roles and Responsibilities | 9 |
| 9. | Change Lead Times..... | 10 |
| 10. | Consequences of non-compliance | 11 |
| 11. | Implementation..... | 11 |
| 12. | Policy review..... | 11 |

1. Preamble

The complexity of current business environments, and the diverse technology used in ICT infrastructure environments demands a greater control to minimize risk and potential impact on the business.

Procedures should be instituted to ensure that all changes are recorded, followed up and escalated to management when necessary. It is important that these procedures are adhered to at all times.

2. Acronyms and definitions

- 2.1 Accountability means ensuring that the actions of an entity or individual may be traced uniquely to that entity or individual, who may then be held responsible for that action;
- 2.2 Authentication means establishing the validity of a claimed entity/verification of the identity of an individual or application;
- 2.3 Availability means being accessible and useable upon demand by an authorised entity;
- 2.4 Confidentiality means that information is not made available or disclosed to unauthorised individuals, entities or processes. This principle should be maintained throughout the usage of the policy;
- 2.8 Information and communication systems mean applications and systems to support the business, utilising information technology as an enabler or tool;
- 2.9 Information technology means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information;

- 2.10 Monitoring means performance measurement to ensure the confidentiality, availability and integrity of operational systems and information;
- 2.11 VPN means Virtual Private Network;
- 2.12 SLA means Service Level Agreement;

3. Purpose

The purpose of this policy is to provide the Molemole Municipality with a procedure for the change control function that shall be established to manage record and track all changes for Molemole Municipality ICT environment.

4. Objective of this Policy

The objective of this policy is to ensure that standardized processes are followed and adhered to accordingly. This is to ensure that no changes take place as a quick change, with “after the fact” documentation, without any prior authorisation.

5. Regulatory Framework

The following regulatory frameworks govern the execution of the ICT Change Management Policy and were taken into consideration during the drafting of the guidelines and policy:

- (a) State Information Technology Act (Act no 88 of 1998);
- (b) Protection of Information Act (Act no 84 of 1982);
- (c) Minimum Information Security Standards (MISS), Second Edition March 1998;
- (d) Municipality Internet Usage Policy;
- (e) Municipality Email Policy;
- (g) Municipality ICT Security Policy;
- (h) Municipality IT Service Management Strategy.

6. Scope of the policy

This policy applies to all employees of the Molemole Municipality, including learners and interns as well as all other stakeholders who make use of and have authorized access to the Molemole Municipality ICT network and systems.

7. Process Overview

The Change Management Process seeks to manage and control the changes through processes and procedures and then ensuring that the appropriate authority levels exist for each change.

The following process steps shall be used within Molemole Municipality:

7.1 Change Initiation

7.1.1 A change is initiated when the requirements for a change has been identified. This request for change can be initiated for the following reasons:

- (a) Change to infrastructure components.
- (b) Resolving problems.
- (c) Project related activities.
- (d) Ad-hoc activities that influence service delivery.

7.2 Change Planning and Building

7.2.1 Under the responsibility of change planning and building, changes may be scheduled and planning may be provided if necessary for the optimum control of the change.

7.2.2 Change Management has a coordination role, supported by line management, to ensure that activities are both resourced and also completed according to schedule.

7.3 Change Logging and Filtering

- 7.3.1 Under the responsibility of the IT Manager, changes are logged to the IT Office.
- 7.3.2 Each Change may be categorized accordingly.
- 7.3.3 A Request for Change Form (Annexure A) needs to be completed for the following changes to the ICT environment:

| CLASS | ITEM | DEFINITION |
|-------------|-------------------|--|
| Significant | Install | New requirement introduced |
| Minor | Move | Move of any component within the Infrastructure environment |
| Significant | Addition | Additional requirements (including releases and or upgrades) within the Infrastructure environment |
| Minor | Configuration | A change to the function or the assembly to the Infrastructure environment |
| Significant | Decommission | Removal of any component from the Infrastructure environment |
| Minor | Operational state | Change from the current operation state of a component within the Infrastructure environment |

- 7.3.4 There are two change types that needs to be adhered to based on the above classes and items:

| CHANGE TYPE | DEFINITION |
|---|--|
| Major Changes | For changes that need to be channeled via the ICT Steering Committee after which approval or rejection will be provided |
| Pre-approved changes | For changes that can take place without being channeled via the ICT Steering Committee, e.g. password resets / creation of new user accounts |
| Major CHANGES | PRE-APPROVED CHANGES |
| May cause down-time on production systems | May not cause down-time on any system |
| May affect one or more SLAs | May not affect any SLA |

| | |
|--------------------------------------|------------------------------|
| May affect configuration information | May not affect any processes |
| May affect processes for services | |
| Changed with high risk involved | |

7.4 Emergency Changes

7.4.1 The emergency change management process shall provide a change control mechanism in the event of an emergency. The goal is not to bypass the Change Management Processes but rather to speed up the process and execute it quickly and efficiently when the normal process cannot be followed due to an emergency.

7.4.2 The following criteria shall be accepted as Emergency Changes

- (a) Production loss
- (b) Financial loss
- (c) Prevention of death
- (d) Legislation changes

7.5 Change Approval

7.5.1 Prior to the approval of changes, an approval indicator shall be allocated to the change to enable the correct workflow associated with the required approval. The risks of the Change will determine the required approval:

| CATEGORY | VALUES | | |
|--------------------------|--------------------|-----------------|-----------|
| | 1 | 2 | 3 |
| 1. Change Classification | Major | Significant | Minor |
| 2. Priority | High | Medium | Low |
| 3. Impact | Multiple districts | Single district | No impact |
| 4. Implementation | Exceed 4 hours | Complex | Simple |
| 5. Black out | Exceed 4 hours | Complex | Simple |

7.5.2 The sum of the value of the five risk categories may determine the approval process:

| | |
|-------------|--|
| Low risk | Greater than 10 = Minor Approval required |
| Medium risk | From 6 to 10 = Significant Approval required |

| | |
|-----------|---------------------------------------|
| High risk | Less than 6 = Major Approval required |
|-----------|---------------------------------------|

7.6 Change Implementation

- 7.6.1 IT Unit shall be responsible for implementation of all changes as scheduled.
- 7.6.2 Feedback regarding the success or failure of the change shall be provided to the ICT STEERING COMMITTEE within 5 days after the planned completion time.

7.7 Change Review and Reporting

- 7.7.1 IT Manager shall perform an evaluation of the changes implemented. The purpose of this review shall be:
 - 7.7.1.1 Establish if the change had the desired effect and met the objectives
 - 7.7.1.2 Tasks and follow-up actions assigned to correct any problems or inefficiencies arising in the change management process itself as a result of ineffective changes
 - 7.7.1.3 Where resources were used to implement the change as planned, and any problems or discrepancies fed back to ICT STEERING COMMITTEE helping to improve the future estimating process
 - 7.7.1.4 Review satisfactory and abandoned changes, and formally closes them in the ICT help desk system.

7.8 Communication

- 7.8.1 Communication will be managed according to the predefined communication structure for each project. Communication shall include:
 - (a) Change approvals
 - (b) Change notifications
 - (c) Change control escalations
 - (d) Change management processes and procedure changes
 - (e) Change management standard changes
 - (f) Change management policy changes.

8. Roles and Responsibilities

Different owners of processes and responsibilities can be identified. The Municipal Manager must delegate the responsibilities of Manager Change Management to Corporate Services Strategic Manager.

8.1 Manager: Change Management

The manager for change management shall be responsible for:

- 8.1.1 Defining of the Change Management process, procedure, division of work and the roles and responsibilities within the process
- 8.1.2 Contributing to the evaluation or establishment of the change management system, ensuring conformance to documentation standards
- 8.1.3 Maintaining the change management system in accordance with agreed procedures
- 8.1.4 Reviews on procedures and other processes checking for compliance against the quality system, and external standards where appropriate
- 8.1.5 Communicating all updates and/or changes of the Change Management Process
- 8.1.6 Promoting awareness of the importance of a structured change management process, working with other business units

8.2 ICT Steering Committee

8.2.1 The ICT Steering Committee shall:

- 8.2.1.1 Review all high impact changes to be implemented
- 8.2.1.2 Review any change that was implemented unsuccessfully or had to be cancelled
- 8.2.1.3 Monitor routine and low impact changes.

8.3 IT Unit

- 8.3.1 Implement Change requests as per above mentioned Change Management Process
- 8.3.2 Provide regular feedback on progress regarding the change request and schedule.
- 8.3.3 Screen all the changes to ensure the correct category, type and item have been selected.

9. Change Lead Times

9.1 Change lead time is the amount of time required to evaluate and adequately plan for change implementation. Lead time is measured from the time the change is submitted until the change is actually implemented. Lead time shall vary by the type of change.

9.2 All changes to be submitted shall be done within the following lead time matrix:

| SERVICE | LEAD TIME |
|---|---------------|
| APPLICATION SYSTEMS | |
| New Application Releases | 1 month |
| Incident Fixes | 12 – 24 hours |
| Emergencies | 12 hours |
| OPERATIONS | |
| Installation of hardware | 1 – 2 months |
| Consumable – tapes / cartridges | 2 weeks |
| Changes to Schedules | 48 hours |
| Hardware maintenance | 1 month |
| Changes to operation of servers | 1 week |
| NETWORK | |
| Installation of new data lines | 4 months |
| In- and outdoor transfer of data lines | 1 month |
| Installation of new equipment on existing network | 2 weeks |
| Incident fixes | 3 weeks |
| TECHNICAL SUPPORT | |
| New application release | 3 weeks |
| Environmental changes | 2 months |
| Incident fixes | 24 – 48 hours |
| Software evaluation | 2 weeks |
| The lead time for non-standard changes that require research shall be negotiated with SBU's concerned, and will depend on the nature and complexity of the change or captured in Operational Service Level Agreements | |

10. Consequences of non-compliance

Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

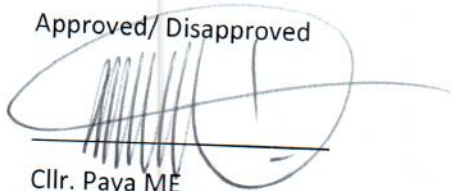
11. Implementation

This policy comes into effect from the date of approval.

12. Policy review

This policy shall be reviewed after 3 years from the date of approval or should the need arise.

Approved/ Disapproved



Cllr. Paya ME

Mayor

31/05/2022

Date

Annexure A

Change Request Form

| Requestor Information: | | | |
|----------------------------------|--|--------------|--|
| First Name | | Employee No. | |
| Last Name | | Email | |
| Date Requested | | Contact No. | |
| Signature | | Office | |
| Change request reference no | | | |
| 1. DESCRIPTION OF CHANGE | | | |
| | | | |
| 2. BUSINESS JUSTIFICATION | | | |
| | | | |

3. Risk of not implementing the update/upgrade

4. Estimated Cost of the update/upgrade

5. Roll back procedure/ Back out

6. NATURE AND PRIORITY

| CATEGORY | VALUES | | |
|--------------------------|------------------|---------------|-----------|
| | 1 | 2 | 3 |
| 6. Change Classification | Major | Significant | Minor |
| 7. Priority | High | Medium | Low |
| 8. Impact | Multiple systems | Single system | No impact |
| 9. Implementation | Exceed 4 hours | Complex | Simple |
| 10. Black out | Exceed 4 hours | Complex | Simple |

4. AUTHORISATION AND APPROVAL

| | Name | Title | Date | Signature |
|----------------|------|-------|------|-----------|
| Recommended by | | | | |
| Approved by | | | | |
| Implemented by | | | | |